SIRK

Styring – Internrevisjon – Risiko – Kontroll

Nr 2 2017

IIA Norge

REDAKTØRENS SPALTE

ELLEN BRATAAS

Oj, da var det jul igjen! Tiden går fortere for hvert år, og det er flere enn meg som føler det slik. Siden tiden er en konstant faktor, så må det være noe med samfunnet eller noen ytre faktorer som bringer frem følelsen av alt går mye fortere nå enn før. Er det den overveldende overfloden av informasjon, et samfunn i rask endring, kunnskapens halveringstid, eller er det rett og slett alderen som bringer frem #denfølelsen?

Mange av oss har våknet opp dette året med en litt guffen smak av GDPR på tungen. Sakte men sikkert går det opp for enhver at kravene i den nye personvernforordningen bringer med seg mye ekstra jobb. Vi bruker for lang tid på å bli bevisste dette merarbeidet, og vi vet med sikkerhet at tiden mot implementeringsfristen i mai kommer til å rase av sted og sannsynligvis bli i korteste laget.
Jeg har trodd at Bitcoin var noe av det hotteste på valutamarkedet nå, men i dette nummeret av SIRK kan dere lese at personopplysninger er den nye valutaen. Som med alle verdier er det derfor viktig å ha full oversikt. Det er altså slik at med all den tid og de forberedelser som gjøres for å bli compliant med kravene i GDPR, legges også grunnlaget for nye muligheter. Dette perspektivet tror jeg med fordel flere kunne hatt nytte av å fokusere på.

SIRK inneholder mye mer enn bare GDPR. Vi har satt sammen en variert portefølje av artikler på områdene virksomhetsstyring, internrevisjon, risikostyring og compliance. Den røde tråden i dette nummeret går ikke på tematikk, men heller at du som leser skal få faglig påfyll, inspirasjon og lett humor sånn på tampen av året.

«Festina lente» (skynd deg langsomt) er et uttrykk som er tillagt keiser Augustus, Romerrikets første keiser. «Skynd deg langsomt» er også mottoet til Lillestrøm videregående skole hvor jeg gikk i forrige århundre. Et gammelt uttrykk og et godt motto som står seg den dag i dag! Kanskje vil det være mulig å bremse tiden hvis vi var flinkere til å skynde oss langsomt; være mer til stede i nuet? Ikke vet jeg, men det er kanskje verdt et forsøk...hvis jeg får tid....

Sekretariatet sender en stor takk til alle som har bidratt i foreningsarbeidet gjennom året, og sammen med redaksjonen ønsker vi alle en fredelig jul og et godt nytt år!

Redaksjonen ønsker alle en en riktig så God Jul og et Godt nytt år!

STYRELEDER HAR ORDET

INGUNN VALVATNE
STYRELEDER
IIA NORGE

I perioden rundt årsskiftet kan det være vanskelig å leve i nuet, noe som ellers er en god leveregel. Vi skal planlegge 2018, samtidig som vi ser oss tilbake til det som har vært. Risikovurderinger skal gjennomføres og kontrollvurderinger skal oppsummeres og rapporteres. Det store spørsmålet i rapporteringen må være om vi har lykkes i rollen i den forstand at vi har bidratt til trygghet og innsikt hos dem vi er til for. Det være seg styrer eller, i noen organisasjoner, daglig ledelse.

En av gledene ved å være engasjert i IIA Norge er innsyn i det store mangfoldet i tilnærming, hvordan ulike internrevisjonsavdelinger velger å løse sine oppdrag. Her er det ingen fasit. Et fellestrekk er det likevel at styrer ønsker mest mulig trygghet «for penga». Da er det store spørsmålet: Hvor langt skal vi ha mot til å gå? Skal vi for sikkerhets skyld fremheve våre «gule» funn, slik at ingen kan komme tilbake etterpå dersom noe skjer? Er det for skummelt å friskmelde? Eller skal vi våge å ta et helhetsblikk og konkludere «grønt» når vi mener kontrollmiljøet er modent og robust. Internrevisorer er kjent for å være et forsiktig folkeferd med lange tradisjoner for forbehold i alle vurderinger. Men er det slik at akkurat vi, som eneste yrkesgruppe, skal slippe unna å ta risiko?

Dette henger selvsagt sammen med kvaliteten i arbeidet gjennom året og om vi har truffet spikeren på hodet med våre risikovurderinger. Vi må ha testet nok, slik at vi er godt rustet til å beskrive situasjonene, hvilket igjen er uløselig knyttet til hvorvidt vi har en god verktøykasse som vi bruker. De dager er forbi hvor internrevisjonen satt med sine store permer med bilag. Digitalisering av arbeidsprosesser og verktøy setter oss nå i stand til og analyse store mengder data med nye muligheter dersom vi er modige og villige til å henge med. Har vi noe valg?

2017 har gitt meg mange anledninger til å diskutere utfordringer og metoder med kollegaer i forskjellige organisasjoner. En kollega fortalte at hans avdeling nå består av 70% IT- kompetanse, gjerne med doktorgrad og «big data» som spesialitet. Han hevdet at ny metodikk nå medfører 100 % revisjonsdekning i kritiske prosesser.

Dette er interessante perspektiver i styrerom der helhetlige vurderinger etterspørres. Og ja, dersom vi har gode risikovurderinger i årsplanleggingen og riktig revisjonstilnærming gjennom året, må vi ha mot til å stole på vurderingene vi har gjort når vi skal oppsummere til styret.

Vårt nyttårsforsett bør være å bli enda modigere og samtidig sikre at verktøykassen vår har gode og relevante verktøyer for vår tid. Vi må alle ta sats for å sikre at internrevisjonen blir enda bedre rustet til å bidra med innsikt.

God jul til alle medlemmer!

Neste utgivelse er mai 2018

Årsabonnement: Kr. 150

Annonsepriser:
Kr. 5.000 for en helside
Kr. 3.000 for en halvside
Kr. 6.500 for baksiden
(mva. tilkommer)

Opplag: 1000
Meningen og påstander som fremkommer i artikler eller innlegg er ikke nødvendigvis sammenfallende med IIA Norges syn.

Grafisk produksjon:
Merkur Grafisk AS

Trykksak
2041 0672

Forsidebilde:
Foto: corgarashu/shutterstock.com

Deloitte.

I takt med tiden

Verden blir ikke mindre. Den blir større, mer kompleks og med raskere endringstakt enn noen gang. Det som tidligere var stabil vekst, er nå mer usikkert. Det som tidligere var et greit kostnadsnivå, må reduseres. Det som tidligere var en langsiktig lønnsom avtale, må reforhandles. Det som tidligere var effektive prosesser, må nå digitaliseres.

Når du står overfor store og krevende internrevisjoner, kan det ha verdi å lytte til rådgivere med innsikt, som våger å stille de utfordrende spørsmålene. Spørsmålene du kanskje ikke vil høre, men som du likevel bør begynne å tenke på før det er for sent. Vi kaller det ***impact that matters***.

For mer informasjon, kontakt Helene Raa Bamrud
Tlf: 974 23 678, hbamrud@deloitte.no

INNHOLD

RISIKOSTYRING

COMPLIANCE

VIRKSOMHETSSTYRING

40

59

63

16

30

INTERNREVISJON

ANNET

FASTE SPALTER

Derfor kan nye personvernregler bli et konkurransefortrinn

INTERVJU MED
HENRIK DAGESTAD
Advokat, BDO Advokater AS

Av
REIDAR DØLI
Oslo Børs VPS

Alle snakker om de nye personvernreglene, men få er opptatt av de kommersielle mulighetene som ligger i en solid implementering.

Den nye personvernforordningen (GDPR) trer i kraft i mai 2018, og det meste som har vært sagt og skrevet så langt har handlet om alle utfordringene dette medfører. Vi tok kontakt med BDO Advokater og Henrik Dagestad som er opptatt av også andre sider ved den nye forordningen.

Tror på kommersielle oppsider

Når EUs forordning for personvern blir norsk lov i 2018, betyr dette at vi får et nytt regelverk som for de fleste virksomheter vil oppleves som en betydelig skjerpelse av de pliktene som finnes i dag. Men, virksomheter som har et aktivt forhold til disse nye reglene, vil kunne oppleve betydelige konkurransefortrinn i årene som kommer, sier han. Dagestad leder BDOs ekspertgruppe på området. BDO fokuserer på de kommersielle oppsidene som ligger i de nye forordningene i en serie topplederkonferanser i Oslo, Trondheim og Stavanger i løpet av høsten.

I forkant av konkurrentene

Ifølge Dagestad tar det erfaringsmessig lang tid før alle virksomheter klarer å

Kilde: BDO. Henrik Dagestad, BDO Advokater AS

etterleve skjerpelser i et regelverk. Han viser blant annet til hvor tidkrevende det har vært å få norske bedrifter til å følge opp antikorrupsjonsreglene som ble innført i 2003.

Det tar nok likevel ikke så lang tid før innkjøpsansvarlige vil kreve at leverandører har dokumentasjon på at de etterlever de nye personvernreglene. Dette vil gi muligheter til å hevde seg konkurransemessig for de som har alt på stell, sier Dagestad, som tror at relativt få vil være i stand til å kunne gi all nødvendig dokumentasjon den første tiden etter at den nye forordningen trer i kraft.

Mange er for sent ute

Personverneksperten påpeker at det for mange virksomheter vil bli en krevende øvelse å få på plass alt de nye reglene krever.

Virksomhetene må blant annet:

- skaffe en oversikt over all behandling av personopplysninger i virksomheten, og oversikten må i tillegg inneholde det rettslige grunnlaget for behandlingen og hvor opplysningene kommer fra
- lage rutiner for å følge de nye reglene
- vurdere risiko og personvernkonsekvenser

Det haster med å komme i gang med dette arbeidet hvis man skal komme i mål innen mai 2018. Det er et stort stykke arbeid som skal legges ned for mange virksomheter, sannsynligvis mer omfattende enn enkelte er klar over. Det kommer derimot til å bli desto mer lønnsomt for de som velger å gi seg selv et forsprang, sier Dagestad.

Hvordan opplever dere nå at kjennskapen er til den nye personvernforordningen og status i implementering ute i virksomhetene?

GDPR er jo blitt et Buzzord både nasjonalt og internasjonalt og det er ikke tvil om at nær sagt alle virksomheter kjenner til at det er nye personvernregler på vei. Samtidig opplever vi at det fremdeles er mange virksomheter som ikke vet mer om selve innholdet i de nye reglene. Enkelte virksomheter er fremdeles av den oppfatning at dette regelverket ikke gjelder for de ettersom de ikke behandler personopplysninger.

Mange virksomheter har vært proaktive og igangsatt GDPR-prosjekter og er allerede på god vei med å kartlegge behandlingsaktiviteter, gjennomføre risikovurderinger og evaluere etterlevelse av gjeldende personvernregelverk og hvordan de ligger an sett opp mot GDPR.

Andre virksomheter begynner imidlertid å få litt dårlig tid. Vi sitter med inntrykk av at mange virksomheter har gått rundt og ventet på bransjestandarder, konkrete veiledninger fra Datatilsynet eller en eller annen form for ferdig løsning som gjør at de ikke trenger å legge ned så mye egeninnsats for å forberede seg til GDPR. Etterhvert som tiden har gått, og slike løsninger ikke har dukket opp, er det nok flere og flere som har innsett at de nå begynner å få litt dårlig tid.

Hva bør virksomhetene legge spesiell vekt på for å ivareta de kommersielle mulighetene som følger av nye personvernreglene?

Man kommer ingen vei i personvernarbeidet uten at man har en fullstendig oversikt over alle personopplysninger virksomheten behandler. For det første er dette et lovpålagt krav i GDPR, men også fra et kommersielt ståsted er dette svært viktig.

Det sies at personopplysninger er den nye valutaen. Som med alle verdier, er det derfor viktig å ha full oversikt. Dersom virksomheter ikke har oversikt over hvilke verdier de har i selskapet, eller hvor de befinner seg, vil de heller ikke ha forutsetninger for å beskytte verdiene eller treffe tiltak for å øke verdiene.

Avhengig av risikobildet, bør virksomheter videre legge vekt på å endre måten man tenker om personvern i virksomheten. Satt på spissen, har personvern tidligere ikke vært en del av virksomheters risikobilde og i den grad ansvaret har vært plassert, har det tilfalt Turid på HR. Er det en ting som virksomheter særskilt bør jobbe med som følge av GDPR er det å jobbe med å endre hvordan virksomheten ser på personvern. Personvern må gå fra å være en byrde til å bli sett på som en potensiell ressurs og et verdiøkende område.

I det nevnte eksempelet med innkjøpsansvarlige vil kreve dokumentasjon fra leverandører på etterlevelse av de nye personvernreglene, hva slags dokumentasjon ser dere for dere?

GDPR legger opp til en godkjennelsesordning (European Data Protection Seal), som man kan sertifisere seg etter. Det er imidlertid usikkert hvordan dette kommer til å bli i praksis. Det er Datatilsynet som er ansvarlig for denne ordningen. Imidlertid er det verdt å merke seg at typen dokumentasjon man bør etterspørre fra leverandører vil bero på om leverandøren er databehandler for virksomheten. Dersom dette er tilfellet, er det et krav om at virksomheten i databehandleravtalen med leverandøren (databehandleren) må fastsette hvilke konkrete sikkerhetstiltak databehandleren må ha på plass. Dette er et område det syndes mye mot, da virksomheter ofte nøyer seg med kun å pålegge leverandøren å ha tilfredsstillende sikkerhetstiltak.

Virksomheter må nå etterspørre og ha konkret kunnskap om leverandørens (databehandlerens) informasjonssikkerhetstiltak. Videre bør man også jevnlig etterspørre sikkerhetsrevisjoner fra eksterne parter knyttet til etterlevelse av personvernregelverket og informasjonssikkerhetstiltakene for leverandører som er databehandlere.

Avslutningsvis, hvordan kan internrevisjonen bidra til at en bedrift utnytter de kommersielle mulighetene som følger av nye personvernreglene?

Internrevisjonen kan spille en viktig rolle i arbeidet med å evaluere og bekrefte om virksomheten etterlever personvernregelverket, og være en proaktiv sparringspartner og rådgiver. I dag et det etter min erfaring ikke tilstrekkelig fokus på personvern i internrevisjonssammenheng, men dette bør endre seg fremover. Internrevisjonen bør øke sin kompetanse på personvernområdet og/eller tilknytte seg ressurser med denne fagkompetansen slik at man i større grad kan hjelpe virksomhetene med å etterleve regelverket. Min påstand er at de virksomhetene som etterlever GDPR fra mai 2018 og kan dokumentere dette, vil få et konkurransefortrinn. Nettopp fordi så mange andre ikke kan det.

Full fokus på GDPR

INTERVJU MED
CATHRINE FAYE LØDRUP
Advokat, Coop Norge SA

Av
MARIT TRODAL
IIA Norge
og
REIDAR DØLI
Oslo Børs VPS

Coop ble tildelt Fidusprisen i september i år, i konkurranse med blant annet Skatteetaten og Brønnøysundregisteret. Fidusprisen gis til en bedrift eller statlig virksomhet som har utmerket seg innen informasjonssikkerhet. Juryen består av Datatilsynet, Næringslivets Sikkerhetsråd og Norsk Senter for informasjonssikring. I begrunnelsen fra juryen vises det til at Coop er i front i sin bransje og går utover det man kan forvente innenfor bekjempelse av datakriminalitet og forebyggende informasjonssikkerhet. De har en modell for sitt sikkerhetsarbeid som i stor grad involverer Coops medlemmer.

Dette lover godt for at arbeidet med personvernlovgivning også er godt ivaretatt. Vi tok en prat med Cathrine Faye Lødrup (Advokat Coop Norge SA - juridisk avdeling) for å høre hvordan Coop jobber med å implementere personvernlovgivningen.

Hva gjør personvern så aktuelt for Coop?

Coop har ca. 1.6 millioner medlemmer og 28 000 ansatte og følgelig behandler vi store mengder persondata, både sentralt og i samvirkelagsstrukturen. De sensitive dataene vi behandler gjelder ansatte og dekker opplysninger om helse og fagorganisering. Vi innhenter ingen sensitive personopplysninger fra medlemmene.

Hvordan er Coop organisert?

Coop har en oppbygging som er ganske spesiell, hvor du som kunde kan melde deg inn i et samvirkelag og bli medeier i Coop. Hvert samvirkelag er en egen juridisk enhet. Coop har i dag 86 samvirkelag.

Vi som jobber sentralt skal bistå alle de juridiske enhetene i Coop-systemet i arbeidet med GDPR. Det er viktig at alle enheter har kunnskap om personvernlovgivningen og ivaretar ansatte og medlemmene i tråd med lovverket. I en såpass komplisert organisasjonsstruktur som både inneholder enkeltstående franchisetakere og samvirkelag, ofte med mange underliggende butikker, er det krevende å få til, men like fullt viktig er at alle etterlever krav og lovverk. Det er viktig at medlemmene har tillit til varemerket Coop.

Hvordan er det å drive personvern i denne organisasjonen?

Det er en krevende jobb å sikre at hele organisasjonen opererer i tråd med lovverk. Men samarbeidet er godt på tvers av organisasjonen og personvern har stor oppmerksomhet.

Hvordan har dere gått løs på GDPR?

Vi gjennomførte først en grov kartlegging av alle avdelinger i Coop Norge SA med datterselskaper i forhold til GDPR, og har arbeidet videre i forhold til resultatene av den opp mot personvernlovgivningen. Vi har også sett på hvorvidt de samtykkene vi har i dag i tråd med lovgivningen.

Hvordan har dere engasjert organisasjonen i dette arbeidet?

Det har vært viktig med forankring hos konsernsjefen og ledelsen i Coop. Vi har hatt møte med alle ledergruppene i forbindelse med kartleggingen av interne

> Det er viktig at alle enheter har kunnskap om personvernlovgivningen og ivaretar ansatte og medlemmene i tråd med lovverket.

prosedyrer og prosesser. Vi lagde også en spørreundersøkelse som ble sendt ut til ledelsen i fellesorganisasjonen. Formålet var å kartlegge alle systemene og prosesser hvor vi behandler personopplysninger i dag, og hvilke personopplysninger vi faktisk behandler. Vi ønsket også å vite hvordan man i praksis oppbevarer personopplysningene, hvilket formål de har, tilgangsrutiner og annen grunnleggende informasjon knyttet til personopplysningene. I tillegg har vi laget et e-læringskurs som blir obligatorisk for alle ansatte. Dette er delt inn i to nivåer; Ett for de som jobber mye med personvern til daglig og et annet for de som skal vite det som er mest grunnleggende. Vi har også vurdert og konkludert med at vi trenger et eget personvernombud siden vi monitorer en betydelig medlemsmasse og har mange ansatte.

Hvor lenge har dere jobbet med forberedelsene til GDPR?

Jeg har jobbet med dette jevnlig i 1 ½ år og fremover vil det bli full fokus for min del.

Hva er IT sin rolle i dette arbeidet?

IT ser på dataflyten av persondata i systemene når det gjelder medlemmer, ansatte, bedrifter og netthandel.

Med GDPR kommer det krav til dataportabilitet hvilket medfører at vi må legge til rette for at medlemmene kan ta med sine opplysninger til andre på en enkel måte. Dette krever også et system som enkelt kan hente ut medlemmers personlige opplysninger fra datasystemene. IT-sikkerhet er også viktig i forhold til overleveringen.

GDPR handler jo mye om informasjonssikkerhet og internkontroll...

Ja, det gjør jo det. Vi er gode på informasjonssikkerhet og det vi gjør nå er jo å sikre at vi har en systematisk tilnærming som dekker alle relevante områder. Vi har rutiner på å foreta risikovurderinger av systemene til samarbeidspartnere og vi må sørge for at alle databehandleravtaler er i tråd med ny lovgivning.

Hva er status på prosessen?

Vi har utarbeidet overordnet policy og har mange rutiner på plass allerede. I tillegg arbeider vi med å samle alle opplysningene på ett sted. Ellers følger vi med på de veiledningene som kommer for å se om dette påvirker arbeidet vårt, særlig innenfor medlemsordningen. Vi vurderer hvorvidt vi har behov for å innhente nye samtykker for å være i tråd med de nye reglene. Vi forbereder oss på flere mulig scenarioer inntil alt er klar.

Hvilke forretningsmessige muligheter ser dere når det gjelder GDPR?

Det går spesielt på tillit og godt omdømme, noe som igjen kan gi Coop et konkurransefortrinn. Vi ser at forbrukerne har tillit til at vi håndterer deres opplysninger på en skikkelig måte. Dette viser jo Fidusprisen også. For oss er det viktig å være tro mot konseptet og våre verdier.

Human Rights Due Dilligence

– Forventninger og praksis

Av
ELISABETH AASERUD
Prosjektleder Konsernrevisjonen
Avinor

Av
MARIT TRODAL
Prosjektleder IIA Norge

De internasjonale menneskerettighetene er tatt inn i en rekke standarder for ansvarlig forretningsførsel for næringslivet. Nasjonalt og internasjonalt er det avdekket flere saker hvor sårbare mennesker blir utnyttet. Dette viser at Human Rights Due Dilligence stadig er aktuelt.

Moderne slaveri er et paraplybegrep som dekker slavearbeid og praksis som ligner på slaveri, tvangsarbeid og menneskehandel. En rekke bransjer er spesielt utsatt, for eksempel bygg og anlegg. Avinor har vært involvert i flere store byggeprosjekter og har opprettet en compliancefunksjon som bl.a har et særskilt fokus på arbeidslivskriminalitet.

Om Avinor

Avinor er et statlig aksjeselskap eid av Samferdselsdepartementet. Selskapet har ansvar for drift av 45 lufthavner fordelt over hele landet, og en samlet flysikringstjeneste for sivil og militær sektor. Virksomheten skal drives på en sikker, effektiv og miljøvennlig måte. Eier har høye forventninger til Avinors arbeid med samfunnsansvar. Samfunnsansvaret er integrert i strategisk planlegging og skal sikre ansvarlig forretningsførsel.

Avinor er en betydelig innkjøper av varer og tjenester. Drift av 45 lufthavner over hele landet medfører et stort omfang av større og mindre byggeprosjekter. Det aller største er utbyggingen av terminal to på Oslo Lufthavn Gardermoen. Prosjektet har pågått i perioden 2012-2017 og har en prislapp på 14 milliarder kroner. Det har bestått av mer enn 150 kontrakter og 600-700 underentreprenører med ansatte fra flere land.

Compliance i Avinor

Mari Wiken er Complianceansvarlig i Avinor og med 15 års fartstid har hun god oversikt over utfordringer og risikoområder selskapet er eksponert for.

Hva er bakgrunnen for at Avinor opprettet en compliance enhet og hvilket mandat har den?

Med bakgrunn i den risikoeksponeringen Avinor er utsatt for, og de forventningene eier og samfunnet for øvrig har til oss ble det besluttet å opprette en compliance funksjon i selskapet i 2014.

Funksjonens formål er å promotere compliance i virksomheten. Den skal ha en forebyggende, rådgivende og kontrollerende rolle, bistå ledelsen med rådgivning i spørsmål om regeletterlevelse og bidra til virksomhetens etterlevelse av gjeldende eksterne og interne krav og forventninger. Dette innebærer bl.a å gi råd om risikobegrensende tiltak, om akseptabel adferd og praksis i forhold til tolkning av eksterne og interne regler, samt sørge for opplæring og trening. Funksjonen har et særskilt fokus på antikorrupsjon, misligheter og arbeidslivskriminalitet. Når det gjelder arbeidslivskriminalitet skal compliancefunksjonen definere innholdet i Avinors påseplikt og stille krav til virksomheten, foreslå relevante tiltak, kontrollere

Oslo Lufthavn.
Kilde: Oslo Lufthavn AS / Espen Solli

hvordan Avinor følger opp sitt ansvar og etablere sanksjoner ved manglende etterlevelse.

Hvordan har dere jobbet med å kartlegge risiko? Hvilke erfaringer har dere gjort dere?

I en stor organisasjon som Avinor vil det være en risiko for brudd på de etiske retningslinjene og andre lover og regler. Sammen med konsernrevisjonen gjennomførte vi i 2016 en risikoworkshop hvor ansatte fra flere deler av konsernet var representert. I denne workshopen kom 3. partsrisiko, samt risiko knyttet til kontraktsoppfølging, anskaffelser og utbyggingsprosjekter høyt opp.

Blant tiltakene som ble identifisert var å sikre risikovurdering av alle 3. parter og utføre Integrity Due Diligence (IDD), samt å implementere systematisk oppfølging av viktige leverandører. Konsernledelsen har nå vedtatt å inngå samarbeidsavtale med Skatt Øst om forsterket innsats mot arbeidsmarkedskriminalitet. Vi ser for oss at bygg & anleggskontrakter og -prosjekter vil bli omfattet av samarbeidsavtalen. Vi ønsker også å vurdere andre bransjer, eksempelvis renhold.

Formålet med avtalen er å etablere et løpende samarbeid som forsterker og utvikler effekten av partenes tiltak mot arbeidsmarkedskriminalitet. Målet med samarbeidet er å utveksle opplysninger som bidrar til å sikre Avinor seriøse leverandører og underleverandører som opptrer i samsvar med norsk skatte- og avgiftslovgivning. Virkeområdet for avtalen er Avinors leverandører og underleverandører, som representerer bransjer som er risikoutsatt for skatte- og avgiftskriminalitet. Samarbeidsavtalen vil gjelde for kontrakter Avinor har over hele landet.

Menneskerettigheter kan være så mangt, men hvilke er spesielt relevante for Avinor?

Når det gjelder menneskerettigheter har vi ikke satt oss ned og vurdert konkret hvilke menneskerettigheter som treffer oss spesielt. Det er jo flere som er relevante, f.eks Right to enjoy just and favorable conditions of work, Right to privacy, Right to freedom of association, Right not to be subject to slavery, servitude or forced labour, og Rights to liberty and security of the person[1].

Når det er sagt, så er antikorrupsjon og sikring av at arbeidsforhold er i tråd med de universelle menneskerettigheter og med gjeldende avtaleverk i arbeidslivet sentrale elementer i dialogen med Avinors leverandører av varer og tjenester. Avinor har også inngått en avtale med StartBANK. StartBANK har et samarbeid med Skatteetaten om tilgang på skatte- og avgiftsinformasjon som oppdateres i sanntid. StartBANK gir tilgang til kvalitetssikret informasjon om blant annet leverandørenes forsikringer, standarder for samfunnsansvar (CSR), HMS- og kvalitetsstandarder, sikkerhetserklæringer og økonomiske tall. Videre har vi en avtale om ansvarlig leverandøradferd med tilhørende prinsipper. Vi inngår avtaler pr. leverandør hvor de forplikter seg til overholdelse av blant annet menneskerettigheter. Disse avtalene er oversatt til mange språk.

Jeg vil også trekke frem at Avinor er medlem av Transparency International, at vår samfunnsansvarsrapport som er utarbeidet i henhold til Global Reporting Initiative (GRI, versjon 4), og at Avinors arbeid

[1] *Kilde: www.ungreporting.com*

med samfunnsansvar bygger på OECDs retningslinjer for ansvarlig næringsliv.

Hvordan har dere jobbet på utbyggingsprosjektet på Gardermoen? Hvordan tror du modenheten er rundt dette temaet ellers i bransjen eller i norske virksomheter generelt?

Som leder av varslingsutvalget er jeg opptatt av at varslingskanalen vår skal være tilgjengelig for både ansatte og andre. Det er en uavhengig kanal hvor de kan varsle om potensielt kritikkverdige forhold. Dette er viktig for at vi skal kunne ta tak i de sakene som kommer, lære av dem og jobbe for at det ikke skal skje igjen. Da utbyggingen på Gardermoen pågikk fikk vi laget såkalte varslingsplakater som informerte om hvordan man går frem for å varsle. Plakatene ble trykket opp på flere språk, inkludert norsk og engelsk, og hengt opp på HMS-tavler på byggeplassen.

Utbyggingen av terminal to (T2) på Gardermoen ble ledet av ÅF Advansia som var hoved-entreprenør. De laget en oversikt over hvilke lover og regler selskaper må forholde seg til, blant annet i forhold til sosial dumping. Formålet var å avdekke forhold som har vært konkurransevridende fordi tilbydere har gjort besparelser ved ikke å forholde seg til regelverk som blant annet sikrer gode arbeidsforhold for arbeidstakere. Oversikten til ÅF Advanisa ble svært omfattende og resulterte etter hvert i en sjekkliste på 260 sider!

I følge Økokrim er ca. 20 % av bedrifter bevisst kriminelle, 20 % er ikke kriminelle og 60 % er i en gråsone og vet ikke hvordan de skal være 'in compliance' med alle de lovene og reglene som de treffes av. På T2 prosjektet var det en egen LO-koordinator som gikk rundt på byggeplassen og snakket med ansatte hos den enkelte leverandør for å kartlegge om det var tilfredsstillende arbeidsforhold. I tillegg var det ukentlige møter hvor man diskuterte ulike risikoforhold og det ble gjennomført revisjoner hvor man med utgangspunkt i en hovedleverandør tok for seg hele leverandørkjeden ned til bemanningsbyråer. I disse prosessene fant man flere brudd som måtte følges opp.

Det er derfor utrolig viktig at det er full fokus på IDD - også her hjemme.

MENNESKERETTIGHETER

Menneskerettigheter er grunnleggende rettigheter som tilkommer alle uavhengig av etnisitet, kjønn, språk, farge, religion, politisk tilhørighet og andre forhold. Det finnes en rekke internasjonale konvensjoner som regulerer statens plikter, og vi forbinder gjerne menneskerettigheter med myndigheter og at dette er en plikt som faller på stater, ikke på virksomheter. Dette er i endring.

I 2011 ble FNs veiledende prinsipper for næringsliv og menneskerettigheter lansert. Dette er et rammeverk som henviser til FNs verdenserklæring fra 1948, konvensjonene fra 1966 som dekker økonomiske, sosiale, politiske og sivile rettigheter, samt ILOs (International Labour Organisation) kjernekonvensjoner knyttet til arbeidsliv. Samme år oppdaterte OECD sine retningslinjer for flernasjonale selskaper og integrerte FNs veiledende prinsipper og la til at alle OECD-land skal ha et eget kontaktpunkt for å sikre oppfølging av prinsippene. Siden da har FNs veiledende prinsipper utviklet seg til å bli en internasjonalt anerkjent standard som er integrert i FN Global Compact, ISO 26 000, Equator Principles og International Finance Corporation Performance Standards.

Hva forventes av virksomheter?

I henhold til FNs veiledende prinsipper må virksomheter vite og vise at de respekterer menneskerettigheter. Hver enkelt virksomhet må selv vurdere relevans og ressursbruk ut ifra en risikobasert tilnærming. I korte trekk forventes det at virksomheter skal:

- Etablere retningslinjer for menneskerettigheter og prosesser som står i forhold til størrelsen og risikoeksponeringen virksomheten møter i sin verdikjede.
- Ha aktsomhetsprosedyrer for å identifisere faktisk og potensiell risiko i verdikjeden, forebygge, begrense og gjøre rede for hvordan virksomheten søker å respektere menneskerettighetene.
- Sikre at prosedyrer er på plass for å håndtere eventuelle negative innvirkninger på menneskerettigheter.

I Norge har Utenriksdepartementet utarbeidet 'Næringsliv og Menneskerettigheter - Nasjonal handlingsplan for oppfølging av FNs veiledende prinsipper'. Denne skisserer forventninger til både offentlige og private virksomheter. Gitt at prinsippene er veiledende er det ikke satt en standard for hvem disse gjelder for og hvor de bør tas i bruk, men det slås fast at næringslivet har et selvstendig ansvar for å respektere menneskerettigheter, selv om dette ikke er et rettslig pålagt ansvar. Det forventes likevel at næringsliv skal operere i henhold til en global standard der lokale lover og regler ikke er tilstrekkelige for å ivareta menneskerettighetene.

Internasjonal utvikling

I takt med økt global fokus etablerer land lover og regler som skal beskytte enkeltpersoner og sårbare grupper mot brudd på menneskerettigheter i forbindelse med næringslivsaktivitet. EU har gjennom sitt Non-Financial Reporting Directive 2014/95 også pålagt medlemsstater å implementere lovverk som skal bidra til større transparens knyttet til menneskerettigheter og potensielle risiko i globale leverandørkjeder. I 2015 ble UK Modern Slavery Act innført og andre land som Sveits, Australia, Nederland, USA og Frankrike er i ferd med å innføre lignende lovverk.

International Labour Organisation (ILO) anslår i sine seneste estimater fra oktober 2017 at 40,3 millioner mennesker jobber innenfor ulike former for slaveri. Av disse er om lag 25 millioner i tvangsarbeid og 15 millioner i tvangsekteskap. Andelen som er i tvangsarbeid har økt fra 21 til 25 millioner, mens antall barnearbeidere har gått ned fra 168 til 152 millioner de senere årene.

KURS OG NETTVERKSAKTIVITETER VÅREN 2018

Aktiviteter og kurs legges ut kontinuerlig på www.iia.no, men her er en oversikt over det som allerede er på plass:

CIA EXAMINATION PREPARATION COURSE

11th and 12th January, 09.00 – 17.00

If you need a kick-off or some help in preparing for the different CIA-parts, we are happy to inform you about our CIA preparation courses lead by Carl Proctor with The Chartered IIA UK & Ireland.You have the options of signing up for one of the days only, or both days.

Day one focuses on Part 1 and 2, and day two is dedicated to Part 3. These parts are considered the core global syllabus of the CIA exam. All courses will be held in English.
During these two days we will go through various topics covered in all the parts, have group discussions, and explore an efficient and systematic method for approaching a complex test. We learn how to prepare for the CIA exam and analyse different types of questions that illustrate different ways a question can be asked in the test.

INTRODUKSJON TIL HELHETLIG RISIKOSTYRING

18. januar, 08.30 – 16.00

Kursen er egnet for både nyansatte som får et ansvar innenfor risikostyring og til de som har jobbet en stund med risikostyring og ønsker å fordype seg ytterligere i helhetlig risikostyring. Kurset forutsetter ikke forkunnskaper og vil dekke temaer fra definisjoner og rammeverk til analysemetoder og rapportering. Det legges opp til god tid til diskusjoner gjennom dagen vi bruker praktiske oppgaver (case).

Kurset dekker:
- Risiko og risikostyring
- Hva forstår vi med rammeverk, prosess og metode i risikostyring?
- Hva er hovedbudskapene til COSO-ERM rammeverket og ISO 31000 standarden?
- Organisering
- Modenhet
- Analysemetoder
- Rapportering
- Samarbeid med andre funksjoner
- Fallgruver og suksesskriterier

GDPR FOR FINANSSEKTOREN

25. januar, tretimers seminar

Nettverk finans inviterer til tre timers seminar der GDPR står på agendaen. Hva er spesielt for finanssektoren? Nærmere agenda legges ut på www.iia.no.

HVORDAN OPPDAGE KORRUPSJON, SVINDEL OG MISLIGHETER – RASKT OG TIDLIG?

31. januar, 08.30 – 16.30

På denne dagen vil du lære hvordan man oppdager røde flagg, bidrar til å spare penger og unngår dyre og komplekse granskninger. Ved bruk av praktiske eksempler, realistiske dokumenter, scenarioer, m.m. får dere en verktøykasse som kan brukes umiddelbart.
Kurset dekker:
- Teknikker og metoder for å identifisere når leverandører og kunder utnytter deg.
- Koblingen mellom agenter, mellommenn, konsulenter og til og med ansatte som får mer enn de fortjener.
- Avtaler med frontselskaper og skitne penger, falsk rapportering, regnskapssvindel, interessekonflikter og andre former for uetisk adferd.
- Måter å oppdage røde flagg ved intervjuer, observasjoner og "think like a thief"-metodikk.
- Forskningsmetode for å finne de sentrale fakta for effektiv utredning.
- Hvordan man utvikler sine egne strukturerte tester for å oppdage røde flagg.
- Pragmatiske løsninger, opprettelser og kostnadseffektive gjenvinninger ved tilfeller av mislighet og korrupsjon.
- Fordelene ved internt samarbeid mot misligheter og korrupsjon (omdømme, interne kontroller og kultur).

MEDLEMSMØTE: COMPLIANCE & KAFFE VÅREN 2018

31. januar, 4. april og 30. mai, 15.00 – 16.30

Nettverk Compliance sitt initiativ til en uformell møteplass hvor aktuelle temaer innen compliance blir tatt opp. Fokus på diskusjon og erfaringsutveksling. Ønsker for tema kan gjerne spilles inn til post@iia.no.

INTRODUKSJON TIL INTERNREVISJON

6. mars, 08.30 – 16.30

På denne dagen vil vi gi en innføring i internrevisors roller og ansvar, begrepsavklaringer og definisjoner, samt hvilke etiske regler og hvilke krav som ligger i internrevisjonens standarder. Kurset gir deltagerne de nødvendige grunnkunnskaper i internrevisjon gjennom introduksjon til internrevisjonens rammeverk, spesielt rettet mot de obligatoriske delene.

Les mer om alle kursene og meld deg på via vår nettside www.iia.no.

Hvem kjenner til de etiske retningslinjene (code of conduct)?

Kilde: Ingunn Staalberg

Av
CAROLINE D. DITLEV-SIMONSEN
Professor
Handelshøyskolen BI

Etikk og samfunnsansvar blir stadig viktigere. For de fleste bedrifter er det i dag frivillig å utvikle *code of conduct* – eller etiske retningslinjer. Samtidig er dette i økende grad forventet i næringslivet og et krav, for eksempel knyttet til anbud. Å ha etablert slike retningslinjer er også blitt en «norm» i tråd med det å ta samfunnsansvar. I viktige anbefalinger, som NUES eierstyring og selskapsledelse, vises det til tema etikk og samfunnsansvar flere steder. På side 10 står det for eksempel «Styret bør klargjøre selskapets verdigrunnlag og i samsvar med dette utforme retningslinjer for etikk og samfunnsansvar.»

Etiske regler er ikke bare knyttet til bedrifter. Organisasjoner er minst like opptatt av tema for å sette en ramme for bransjen som sådan. The Institute of Internal Auditors har Etiske regler og standarder for profesjonell utøvelse av internrevisjon (2017)[1] på 35 sider, Den Norske Revisorforeningen har sine egne regler om etikk på 55 sider som gjelder for all medlemmer[2] som igjen er basert på IFAC Code of Ethics for Professional Accountants på 114 sider[3].

I tillegg har alle store revisorselskaper som PWC, Deloitte, EY og KPMG, sine egne etiske retningslinjer, eller code of conduct. Det samme gjelder større norske bedrifter. Samtidig er innholdet i og omfanget av disse retningslinjene svært variert.

Er det at en organisasjon eller bedrifter har et omfattende dokument med etiske retningslinjer eller code of conduct en indikasjon på at disse bedriftene i sin daglig drift er i tråd med disse? Ikke nødvendigvis. Enron for eksempel hadde et velskrevet Code of Ethics på 64 sider publisert i 2000. Så, selv om det umiddelbart kan oppfattes som de bedrifter som har de mest omfattende etiske regler er de som opererer mest etisk, er ikke dette nødvendigvis tilfellet.

For at ansatte skal handle i henhold til de etiske retningslinjene er det helt sentralt at de kjenner til disse. Dette kan høres veldig opplagt ut, samtidig kan de være få i selskapet som faktisk vet av disse reglene – eller hvor de er tilgjengelige. I mange selskaper signerer man slike regler når man blir ansatt, men ser dem sjelden igjen – med mindre det avdekkes brudd på disse reglene.

Man kan spørre seg, hva er formålet med etiske retningslinjer? For mange er risiko reduksjon, altså det å unngå feiltrinn og «skandaler», ansett som en viktig motivasjon. Slike hendelser kan innebære negative konsekvenser for selskapet – ikke minst når det gjelder omdømme.

Gode retningslinjer trenger allikevel ikke bare være knyttet til risiko reduksjon. Det viser seg at etiske retningslinjer som er godt integrert kan ha positiv innvirkning på ansatte. Når ansatte vet hvordan det er forventet at man skal oppføre seg, er det større sjanse for at vi greier å ta de rette valgene. Det kan også gi en god følelse og tilhørighet blant ansatte hvis det er klare regler for hvor grensen går for akseptabel oppførsel.

Allikevel, det er ikke alltid nok å utforme etiske regler og sikre at de ansatte kjenner disse. Vi må også vite hvordan disse skal virke i praksis når man står overfor et valg, og vi trenger trening.

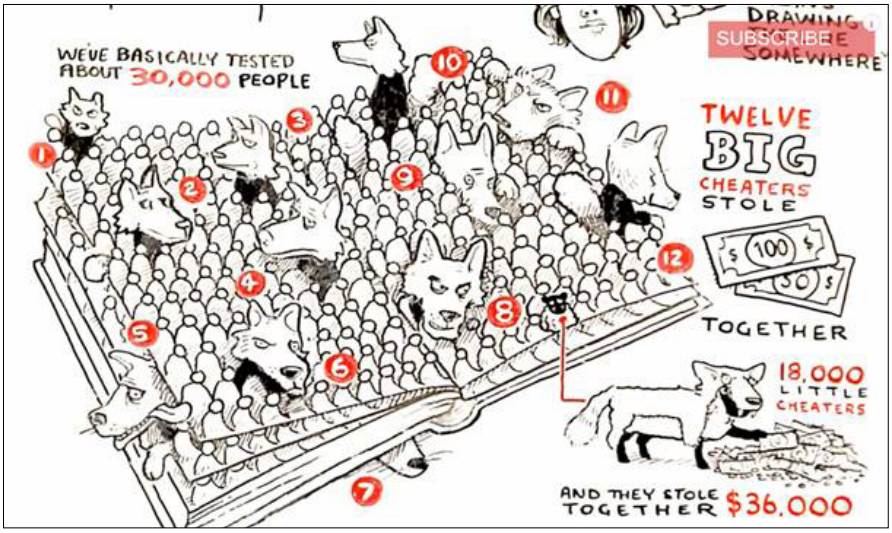
Følgende kan være en ramme for å sikre kvalitet og kunnskap knyttet til et selskaps code of conduct eller etiske retningslinjer.

1. Sikre at initiativet er forankret i ledelsen.
2. Involvere ansatte til å være med å utforme retningslinjer, gjerne i form av en gruppe som samarbeider om dette.
3. Identifiser hvilke tema som er mest relevant i selskapet, bruk et «språk» som alle forstår.
4. Gjør retningslinjene tilgjengelig for alle - og minn dem på at de eksisterer.
5. Tren opp de ansatte til å bli kjent med retningslinjene og hvordan man kan benytte seg av disse. Små «drypp» av praktiske etiske dilemma på selskapets intranett, skjermer i fellesrom og i nyhetsbrev er eksempler på effektiv formidling og trening. Be ansatte komme med forslag til aktuelle situasjoner å formidle.
6. Sjekk at opplegget når frem og dekker behovet.
7. Revider og oppdater reglene – det skjer stadig endringer innen feltet.

Er selskapet nå sikret å unngå skandaler knyttet til uetisk oppførsel? Nei, ikke nødvendigvis. Allikevel, slike retningslinjer bidrar til å redusere sjansen for uønskede situasjoner. Videre kan slike retningslinjer gjøre ansatte mer komfortable til å ta de rette avgjørelser i situasjoner der de er i tvil. Det forsterker mestringsfølelsen og er positivt for de ansatte.

Til slutt er det naturlig å komme med noen refleksjoner knyttet til hvor de største utfordringene ligger. Selv om det de fleste bedrifter frykter er store skandaler knyttet til feilgrep som man leser om i aviser, er det ikke disse som har den mest negative konsekvensen for samfunnet.

De største etiske utfordringen knyttet til samfunnet er, som forfatteren Dan Ariely sin bestseller bok *The (Honest) Truth About Dishonesty* dokumenterer, ikke de store enkelt sakene som dekkes i media om underslag og tilsvarende. Den største utfordringen er de mange små feilgrep som gjøres. I følge Ariely som testet 30 000 personer så fant han bare 12 «big cheaters» som til sammen stjal $150, mens de



18 000 «little cheaters» stjal tilsammen $ 36 000[4]. Omfanget av 'little cheaters' er langt større enn de svært få 'big cheaters.'

Det å ha gode etiske retningslinjer eller code of conduct er altså viktig og et steg i riktig retning. Samtidig er det også viktig å ta med i betraktning den menneskelige psyke, eller hvordan vi fungerer, i praksis.

[1] *http://iia.no/produkt/standarder-for-internrevisjon-2/*
[2] *https://www.revisorforeningen.no/globalassets/fag/etikk/DnRs_regler_om_etikk*
[3] *https://www.ifac.org/system/files/publications/files/ifac-code-of-ethics-for.pdf*
[4] *https://www.youtube.com/watch?v=XBmJay_qdNc*

Strategisk risiko

– Den største årsaken til verditap i større norske børsnoterte selskaper. Har din virksomhet fokus på strategisk risiko?

Av
HERMANN KRISTIANSEN
Trafikkinformatør i NSB siden 2011
Executive Master of Management ved Handelshøyskolen BI, 2008-2018.

Hva er verdien av en adekvat risikostyring?

En god og adekvat risikostyring handler om å være forberedt på de risikoene man faktisk er eksponert for. Sitter man med et risikobilde som ikke stemmer med virkeligheten når hendelser inntreffer, kan det koste dyrt både i direkte utgifter og i markedsverdi. Min prosjektoppgave ved Handelshøyskolen BI trekker samme konklusjon som lignende undersøkelser utført i USA i 2012[1] og 2015[2], nemlig at strategisk risiko er den hyppigste årsaken til verdifall i børsnoterte selskaper (se figur 1). Operasjonell risiko er noe mange selskaper har et konkret forhold til, mens strategisk risiko ikke i samme grad er fokusert på. I min oppgave undersøkte jeg blant annet hvor godt forberedt norske selskaper er på å håndtere uønskede fremtidige hendelser. Dette ved å analysere risikotyper, og hvor stor betydning adekvat risikostyring har for å begrense verditap.

Undersøkelsen

Min undersøkelse omfatter 92 av de 238 selskapene som var notert på den norske børsen i 2015, og inkluderer alle bransjer. Jeg gikk inn i aksjekurshistorikken i perioden 2010-2015 til samtlige bedrifter, og fant frem til det største fallet for hvert selskap som kunne tilskrives en enkelt hendelse. Jeg benyttet meg av årsrapporter og nyhetsartikler fra de aktuelle årene for å finne frem til risikotyper som kan beskrive hendelsene. Samtidig undersøkte jeg hvordan selskapene jobbet med risikostyring, og fant frem til hvilke risikotyper hvert selskap mente de var mest eksponert for. Utvalget omfatter selskaper med omsetning større enn ca. NOK 1 mrd. Disse ble delt opp i tre størrelseskategorier for å analysere forskjeller sett i lys av omsetning.

Begreper

For å måle adekvat risikostyring, bruker jeg begrepet *risikodekning*. Begrepet sier noe om hvor godt dekket man er mot faktisk inntruffet risiko, og består av en sammenligning mellom *risikofokus* og *årsaksrisiko*. Risikofokus er bedriftens risikostyring/-bilde, og årsaksrisiko er de risikotypene som beskriver den faktiske hendelsen som inntraff. Jeg benyttet fire risikotyper i denne undersøkelsen, etter inspirasjon av undersøkelsen gjennomført av Booz&Co[1]:

- Strategisk
- Ekstern
- Operasjonell
- (Non-)Compliance

Finansiell risiko er ofte med i slike kategoriseringer, men i denne undersøkelsen ble det sett på som en konsekvens av de andre risikotypene. Det vil si at hvis det er feil i regnskapene, ble det klassifisert som compliance-risiko i min undersøkelse. Strategisk risiko ble derimot sett på som den risikoen et selskap er eksponert for i forhold til hvordan det har posisjonert seg f. eks. i et marked, altså risiko ved den strategien man velger. Ved bruk av finansiell risiko som en risikotype, som beskriver risikoen for tapene som følger av den strategiske risikoen, vil det derfor i denne sammenheng være tilstrekkelig å klassifisere finansiell risiko under strategisk risiko. Strategisk risiko skiller seg igjen fra ekstern risiko, selv om de ofte ser like ut. Forskjellen er at man ikke kan styre ekstern risiko ved å velge en annen strategi.

Funn

Diagrammet i figur 2 oppsummerer selskapenes risikodekning.

«Ikke dekket» betyr at man ikke var forberedt på noen av de to risikotypene som inntraff, mens «delvis dekket» betyr at man har hatt fokus på en av to inn-

Funn	Booz & Co 2012[1]	HBR 2015[2]	Denne undersøkelsen
Andel av verditaphendelser forårsaket av strategisk risiko	81%	86%	63%

Figur 1, Strategisk risiko som årsak til verdifall

trufne risikotypene. «Dekket» betyr at risikotypene for årsak og fokus matcher. Hendelsene som inntraff var likevel så ulike fra det virkelighetsbildet bedriften satt med, at de ble delt opp i «dekket» og «match». «Match» er de tilfellene hvor det som inntraff var det samme som forventet.

Funnene viser at «dekket» og «match» kategoriene bør ses i sammenheng. Undersøkelsen indikerer videre at få norske bedrifter er dårlig dekket. Det er tydelig at det kun er de minste selskapene som var «udekket,» og at det kun er de største selskapene som er representert i de to beste kategoriene.

Om man ser «dekket» og «match» under ett, finner vi de fleste selskapene der. Dette lover godt for norske selskaper. Det har en signifikant betydning for verdifall når en uønsket hendelse inntreffer, slik synliggjort i diagram i figur 3:

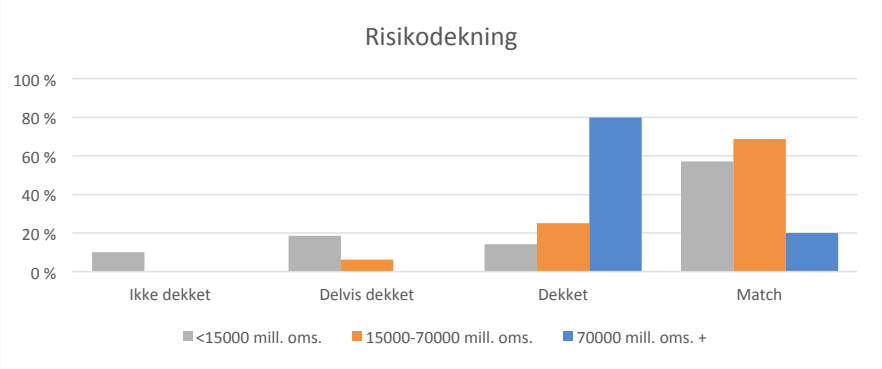
De gjennomsnittlige tapene ved «ikke dekket» og «delvis dekket» er hhv. 52,2% og 51,5%. Det å være «dekket» begrenser snittapet til 37,6%, og «match» til 33%. Når de to dårligste kategoriene ses under ett og sammenlignes med de to beste, gir dette gjennomsnittlig en differanse på 16,6 prosentpoeng i tapsbegrensning.

Undersøkelsen fokuserte også på verditap per risikotype uavhengig av risikodekning (se figur 4). Funnet viser at tapene er størst for de risikoene som inntreffer sjeldent, nemlig ekstern og compliance risikoene. Strategisk og operasjonell risiko koster eierne omtrent like mye. Legg også merke til at ingen av de største selskapene (blå søyle) er med i kategorien «Strategisk».

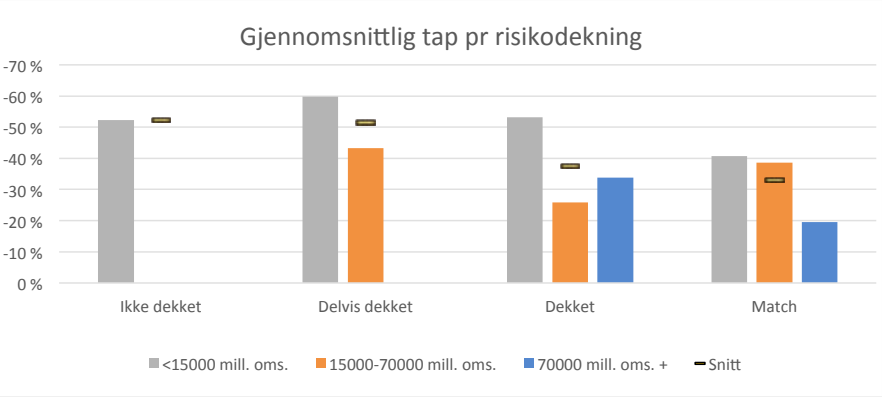
Konklusjon

Strategisk risiko hadde inntruffet i 58 av de 92 tilfellene som ble undersøkt, noe som gjør det til den mest sannsynlige risikotypen. Når slike hendelser i snitt koster eierne 40% av verdiene, er det signifikant at en god risikostyring kan begrense det tapet med i snitt 16-17 prosentpoeng. For de fleste eiere med innflytelse representerer dette meget reelle verdier.

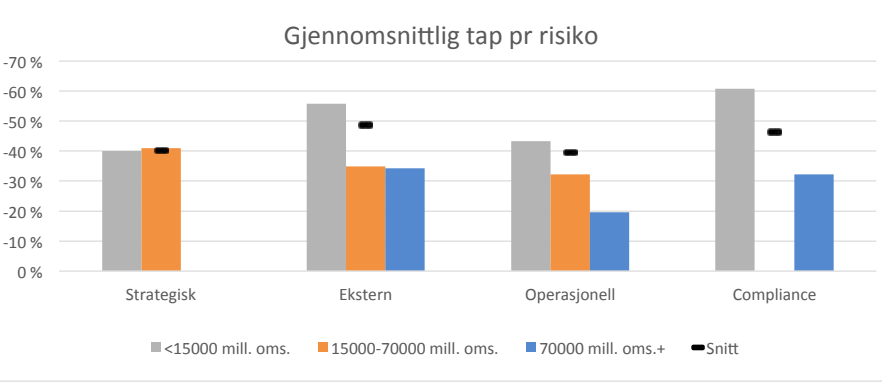
Strategisk risiko har ikke bare høy sannsynlighet for å inntreffe, men også store potensielle konsekvenser. Dette tilsier at strategisk risiko er av grunnleggende betydning for et hvert selskap.



Figur 2. Risikodekning



Figur 3. Tap pr risikodekning



Figur 4. Tap pr risiko

ERM (Enterprise Risk Management) dvs. helhetlig risikostyring vil i det tilfelle være et sentralt styringsverktøy. Samtidig er strategisk risiko en direkte konsekvens av beslutninger tatt øverst i organisasjonen. Dette medfører at organisatorisk plassering av risikostyringen har stor betydning, og at legitimitet og forståelse av risikostyringen hos toppledelse og styre er kritisk for virksomhetens suksess.

[1] *Booz Co., The Root Causes of Value Destruction - How Strategic Resiliency Can Help, 2012*

[2] *Harvard Business Review, How to live with Risks. You can't get rid of them – but you can get ahead of them., juli-august 2015*

Fra internrevisjon til risikostyring

Etter mange år innen internrevisjon i virksomheter som Norske Skog, Telenor og Yara, og som konsulent i EYs Risk avdeling, gikk Øyvind Hestnes tidligere i år inn i en ny rolle i Yara; VP Enterprise Risk Management.

Av
MARIT TRODAL
Prosjektleder IIA Norge

> Kunnskap og bevissthet må ligge i bunnen. Jeg mener at noe av det viktigste i risikostyring er å samle de riktige menneskene rundt et bord for å ha en meningsfull diskusjon om risiko knyttet til forretningen og dens mål.

Kan du fortelle om din rolle i Yara?

I min stilling som VP Enterprise Risk Management rapporterer jeg til CFO i Yara. Jeg er alene i denne avdelingen, men samarbeider tett med de ulike segmentene og ekspertfunksjonene. I tillegg støttes ERM funksjonen av risikofasilitatorer som er etablert i den globale organisasjonen. Disse har som rolle å bistå meg i implementeringen av ERM rammeverket, samt støtte lokal ledelse i utøvelsen av risikostyringsprosessene.

Hvordan utarter dette arbeidet seg rent praktisk?

Jeg har mye fokus på opplæring og å skape økt bevissthet ute i organisasjonen. Vi må være tydelige på at risikostyring skal være verdiskapende for virksomheten, samt at den skal knyttes opp mot måloppnåelse. Jeg har møtt mange som har sagt at dette er så komplisert og vanskelig. Det kan fort bli mye fokus på verktøy og rapportering som en mekanisk øvelse, men det er forskjell på risikorapportering og risikostyring; sistnevnte handler om å bistå organisasjonen i å integrere risikostyring i strategi og businessprosessene. Det er dette som er min tilnærming. Jeg bistår organisasjonen ved blant annet å drive opplæring, fasilitere risikoworkshops, samt etablere prosesser for effektiv integrering av risikostyring i strategi- og forretningsprosessene. Jeg har fokus på å gjøre dette enkelt og praktisk, slik at det gir verdi for organisasjonen.

Hvordan er du involvert i strategiprosessen?

Vi hadde nylig en workshop med ledelsen hvor vi sammen kartla og diskuterte strategiske risikoområder. Disse var blant

annet knyttet til det grønne skiftet, klimaendringer og potensielle regulatoriske endringer fremover. Risikodiskusjonen er en integrert del av strategiprosessen i Yara.

Hvordan kommer din erfaring fra Yaras internrevisjon til nytte i din nye rolle?

Jeg har gjennom mer enn 4 år i Yaras internrevisjon blitt kjent med store deler av organisasjonen og prosessene. I tillegg lærte jeg viktigheten av å være forretningsorientert for å kunne være relevant for organisasjonen. Rollen som internrevisor ga meg også kunnskap om organisasjonens modenhet knyttet til risikostyring. En læring er at Det nytter ikke å gi folk verktøy hvis folk ikke vet hvordan de skal bruke det. Kunnskap og bevissthet må ligge i bunnen. Jeg mener at noe av det viktigste i risikostyring er å samle de riktige menneskene rundt et bord for å ha en meningsfull diskusjon om risiko knyttet til forretningen og dens mål. Vurdering av risiko er ikke en øvelse man skal gjøre alene.

Hvordan måle organisasjonskultur?

Av
MAZHAR B. AHMAD
Leder risikostyring konsern,
Gjensidige Forsikring ASA

I am able to control only that which I am aware of. That which I am unaware of controls me. Awareness empowers me. No two human minds or bodies are the same. How can I tell you how to use yours? Only you can discover how, with awareness.

– Sir John Withmore

Bakgrunn og kontekst

Med utgangspunkt i standarder som ISO/FDIS 31000 og «COSO Enterprise Risk Management—Integrating with Strategy and Performance» (2017) – forkortet heretter til COSO, vil jeg belyse viktigheten av organisasjonskultur i virksomhetens søken etter kontinuerlig forbedring av dens risikostyringssystemer.

I forslaget til ny ISO 31000 standard heter det at «Human behaviour and culture significantly influence all aspects of risk management at each level and stage». I praksis ser vi som jobber med risikostyring i det daglige at kultur er og forblir noe av det viktigste en virksomhet etablerer og videreutvikler. Den kan til dels erstatte både harde regler og softe prinsipper da dette blir det nærmeste man kommer «risk management by design and by default», men samtidig er dette vanskelige temaer å takle.

ISO standarden sier videre at det er viktig at risikostyring er tilpasset organisasjonens kultur samt at organisasjonens kultur er en viktig komponent i den interne konteksten av virksomheten, og som vi vet vil vi til en viss grad kunne påvirke, endre og styre interne forhold i virksomheten; «the dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process».

Fra «COSO 1 (internkontroll)» både i 1992 og 2013 utgaven er «kontrollmiljø» grunnsteinen og det bærende elementet som all internkontroll bygger på. «COSO 2 (ERM)» viderefører begrepet internt miljø i 2004, og i den oppdaterte utgaven fra 2017 er «kultur» inntatt som et prinsipp i flere av komponentene i rammeverket. I begrepet «internt miljø» ble følgende lagt til grunn:

«Internal Environment – The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate. »

I den oppdaterte utgaven legger COSO høy vekt på betydningen av kultur:

«Boards can also ask senior management to talk not only about risk processes but also about culture. How does the culture enable or inhibit responsible risk taking? What lens does management use to monitor the risk culture, and how has that changed? As things change—and things will change whether or not they're on the entity's radar—how can the board be confident of an appropriate and timely response from management?»

Videre adresserer den eksplisitt prinsippene «Defines Desired Culture» og «Reports on Risk, Culture, and Performance» (se prinsipper som er markert i gult i figur 1 på neste side).

Selv om ISO 31000 og COSO legger opp til at organisasjonskultur er viktig, er det få praktiske verktøy tilgjengelig. . Dette skyldes kanskje at organisasjonskultur anses å være noe abstrakt og lite målbart, og krevende å evaluere?

Fortvil ikke. Det finnes faktisk gode verktøy og metoder der ute, men disse må hentes fra andre fagområder enn tradisjonelle standarder innenfor risikostyring og internkontroll. Det betyr også en investe-

Governance & Culture	Strategy and Objective-Setting	Performance	Review & Revision	Information, Communication and Reporting
Exercises board risk oversight	Analyzes business context	Identifies risk	Assesses substantial change	Leverages information and technology
Establishes operating structures	Defines risk appetite	Assesses severity of risk	Reviews risks and performance	Communicates risk information
Defines desired culture	Evaluates alternative strategies	Prioritizes risk	Pursues improvement in Enterprise Risk Management	Reports on risk, culture and performance
Demonstrates commitment to core values	Formulates business objectives	Implements risk responses		
Attracts, develops and retains capable individuals		Develops portfolio view		

Figur 1 Risk Management Principles - Enterprise Risk Management Integrating with Strategy and Performance (2017).

ring i ny kunnskap og bruk av andre ikke-tradisjonelle metoder i ens eget arbeid.

Verktøyet jeg har tenkt å belyse er kalt «Organizational Cultural Assessment Instrument» (OCAI) og baserer seg på «Competing values framework».

Organizational cultural assessment instrument(OCAI)

OCAI ble utviklet av Kim Cameron (PhD, University of Michigan) og Robert E. Quinn (Professor Emeritus, Ross School of Business) i 1999. Formålet med OCAI er å vurdere seks viktige dimensjoner av organisasjonskultur. Ved å fullføre «diagnostiseringen» vil man tegne et bilde av hvordan organisasjonen fungerer og verdiene som kjennetegner den.

Cameron og Quinn utviklet et rammeverk (se figur 2) basert på det de definerte som motstridende krefter eller konkurrerende verdier. Deres utgangspunkt var at organisasjonskultur kan måles og at den endrer seg over tid.

Rammeverket antar at det er fire forskjellige arketyper av organisasjonskultur som defineres i de respektive modellene «Clan», «Adhocracy», «Hierarchy» og «Market».

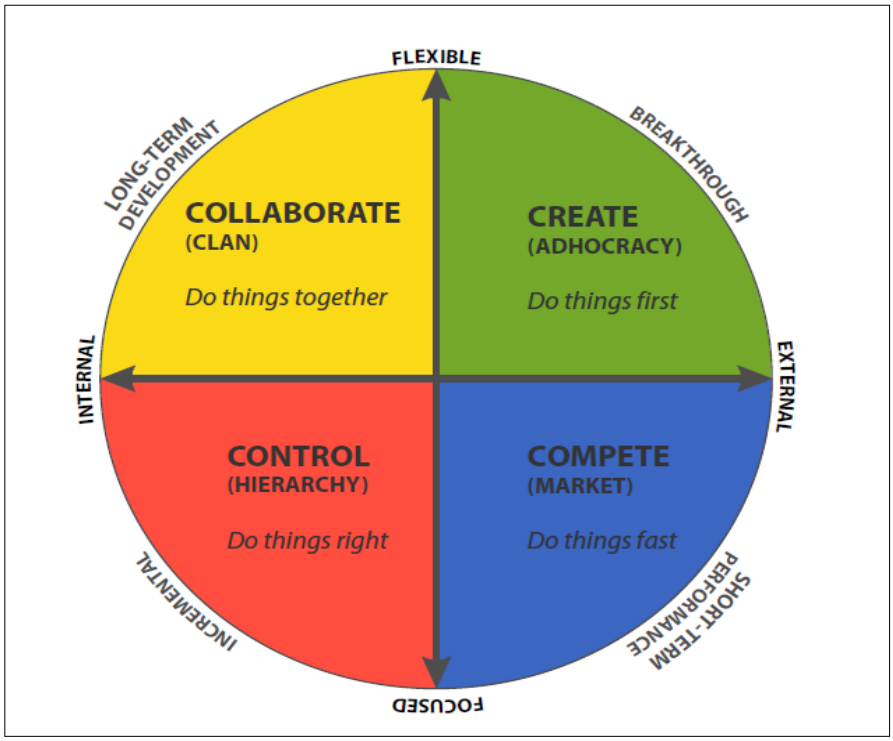
I tillegg er det seks viktige dimensjoner som defineres med forskjellige foretrukne tilnærminger. Etter min mening kan disse modellene også benyttes for å styrke arbeidet med å utvikle risikostyring og risikostyringsprosesser, for i neste omgang å understøtte og utvikle en organisasjonskultur som går i takt med organisasjonen, både «as is» og «to be».

De 4 organisasjonsmodellene

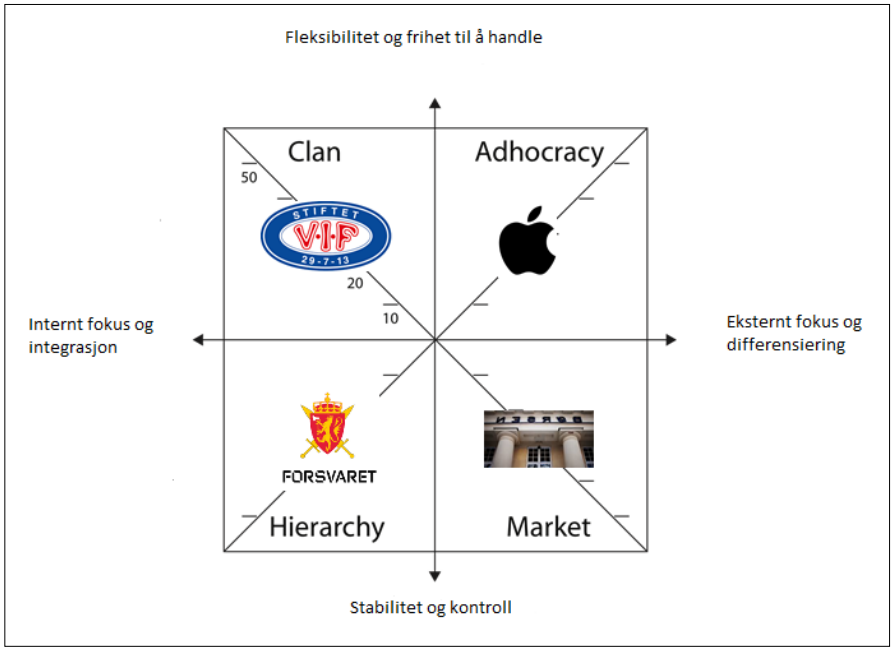
«Kontroll» (hierarki)-kulturen er basert på Webers teori om byråkrati og hvor verdier som tradisjon, konsistens, samarbeid og samsvar råder. Hierarkimodellen fokuserer mer på interne enn eksterne problemer og verdier som stabilitet og kontroll råder over fleksibilitet og skjønn. Dette er den tradisjonelle «kommando og kontroll»-verdikjeden, som fungerer bra hvis målet er effektivitet og organisasjonsmiljøet er stabilt og enkelt – dvs. hvis det er svært få endringer i kunder, kundepreferanser, konkurranse, teknologi mv.

«Konkuranse»(markeds)-kulturen verdsetter også stabilitet og kontroll, men fokuserer mer på eksterne forhold (markedet) snarere enn interne problemer. Denne kulturen har en tendens til å se det ytre miljø som truende, og søker å identifisere trusler og muligheter ettersom det søker konkurransefortrinn og fortjeneste i dette verdensbildet.

«Samarbeid»(klan)-kulturen fokuserer på interne problemer og verdier som fleksibilitet og skjønn verdsettes, i stedet for å søke stabilitet og kontroll. Målet er å



Figur 2 Ulike typer organisasjonskultur[1]



Figur 3: Eksempel på virksomheter plassert i de ulike kulturdimensjonene

styre miljøet gjennom samarbeid, deltakelse og konsensus.

«Adhoc»-(krati)-kulturen fokuserer på eksterne problemer og verdier som fleksibilitet og skjønn verdsettes, i stedet for å søke stabilitet og kontroll; dens nøkkelverdier er kreativitet og risikotaking. Organisasjonskart er midlertidige eller ikke-eksisterende; roller og fysisk arbeidssted er også midlertidig. Adhockrati er en type organisasjon som er antonym med byråkrati.

For å illustrere modellen har jeg forsøkt å sette inn 4 typer av organisasjoner i de nevnte organisasjonsformene (se figur 3 over). Det må bemerkes at det alltid vil være noen type organisasjoner som flyter mellom disse «konkurrerende kreftene».

Eksempelvis kan Forsvaret innad i organisasjonen ha funksjoner med en annen form for organisering enn den klassisk hierarkiske. Det kan også være forskjellige sub-kulturer, avhengig av funksjon og virkeområde. Vålerenga Fotball har en «hard kjerne» som identifiserer seg med klanen, mens andre vil være i periferien av denne klanen.

Dimensjoner av organisasjonskultur

De seks dimensjoner av organisasjonskultur er ifølge Cameron og Quinn:

- dominerende egenskaper i organisasjonen;
- organisatorisk lederskap i organisasjonen;
- ledelse av ansatte i organisasjonen;
- limet i organisasjonen;
- strategisk fokus i organisasjonen;
- sist, men ikke minst kriterier for suksess i organisasjonen.

OCAI består av en rekke «statements» som det skal tas stilling til, og scoringen [fra 0 til 100 per statement per dimensjon] vektes i forhold til det man anser som den ideelle situasjonsbeskrivelsen. Rammeverket kan både benyttes for «as is» og «to be» vurderinger, og sammen med supplerende dybdeintervjuer og understøttende analyser vil arbeidet kunne gi et meget nyttig bidrag til forståelsen av organisasjonens kultur.

Konklusjon

Organisasjonskultur er et viktig fundament i risikostyring og internkontroll. Internasjonalt ser vi en utvikling der tilsynsmyndigheter vektlegger «conduct risks» [2] i sine tilsynsgjennomganger, spesielt innen bank og finans. Organisasjonskultur vektlegges i økende grad, men det gjenstår å se om det utvikler seg god praksis, slik at vi får en systematisk og god evaluering av organisasjonskultur.

Ved å bruke OCAI har man et nyttig verktøy for å bestemme i hvilken grad organisasjonens kultur støtter dens målbilde, samt til å identifisere underliggende elementer som kan virke mot oppnåelse av målbildet. Det kan være nyttig for enhver organisasjon å bevisst definere sin egenart og organisasjonskultur og søke å identifisere kulturelle elementer som både støtter - og hindrer – endringsarbeid.

[1] *Cameron, K. S., & Quinn, R. E. (1999). Diagnosing and changing organizational culture: Based on the competing values framework. Reading, MA: Addison-Wesley.*

[2] *Det er mange definisjoner på conduct risk. Jeg har benyttet følgende: «the risk that firm behaviour will result in poor outcomes for customers»*

Visualisering av risikobildet

Grunnlag for best mulig beslutningsstøtte


Av
ANNELIN THORKILDSEN
– Senior Rådgiver Risikostyring – Bouvet AS


Av
LINN EIKELAND
– Senior Rådgiver HMS og Risikostyring
– Watchcom AS


Av
INGRID JACOBSEN
– Senior Rådgiver Risikostyring – Bouvet AS

Bedrifters risikostyring handler om å sikre riktig balanse mellom på den ene siden å utvikle og skape verdier for å nå virksomhetens mål, og på den andre siden å unngå ulykker, skader og tap.

Næringslivet står overfor hyppige endringer i eksterne forhold, noe som fordrer rask omstilling for å være i front av utviklingen og ivareta konkurransekraften. Bedrifter skal forholde seg til både risiko og muligheter, og risikoanalyser er et verktøy for beslutningstøtte i denne prosessen. Forhold som teknologiutvikling, utkontraktering, fusjoner, nye regelverk og digitalisering er bare noen av endringene som er gjeldende for mange virksomheter. Komplekse problemstillinger med tilhørende usikkerhetsmomenter hvor mange faktorer, mye data og ulike ekspertvurderinger skal tas hensyn til, sees i sammenheng og analyseres, krever egnede og inkluderende metoder og verktøy for å oppnå en helhetlig tilnærming, noe som vil gi et best mulig grunnlag for å kunne ta solide og velfunderte beslutninger.

Gitt dagens utfordringer og behov er det relevant å spørre seg om hvorvidt verktøy som tradisjonelle risikomatriser gir det beste grunnlaget for å kunne ta beslutninger stilt overfor komplekse problemstillinger.

Sannsynlighetsbegrepet

Ved tradisjonelle risikoanalyser avdekkes aktuelle risikoer, og det samlede risikobildet presenteres ofte i en tradisjonell risikomatrise. Identifiserte uønskede hendelser plasseres i risikomatrisen i henhold til vurdering av sannsynlighet og konsekvens, og utfra en rangering av disse kan man ta stilling til hvilke risikoer virksomheten er villig til å akseptere og hvilke som krever tiltak i henhold til virksomhetens vedtatte akseptkriterier for risiko.

Tradisjonelt er risiko og risikoforståelse basert på objektiv sannsynlighet og historiske data. Dersom vi kan anta at fremtiden er en gjentakelse av fortiden, er det lite problematisk å forholde seg til en slik objektiv sannsynlighet, ofte representert ved et tall som baseres på hvor hyppig en hendelse forekommer, som et mål på risikoen for at en gitt hendelse vil inntreffe.

Dersom man for eksempel får presentert en analyse som viser at den objektive sannsynligheten for at et dataangrep inntreffer er 10-5, P(dataangrep)=10-5, gir den beregnede sannsynligheten ikke mye informasjon i seg selv annet enn at sannsynligheten er veldig lav. Men, hva betyr det i praksis for virksomheten? Som beslutningstaker ønsker man å få innblikk i hva som ligger bak dette tallet, for eksempel hvorfor sannsynligheten er lav og om den kommer til å fortsette å være lav også i fremtiden. Gitt den teknologiske utviklingen vi står overfor, er det fornuftig å basere våre vurderinger utelukkende på historisk data, når vi vet at virksomheter utvikler seg, lærer av tidligere hendelser enten det gjelder egne eller andres, og iverksetter tiltak, samtidig som eksterne og interne forhold endrer seg uopphørlig? Det å kun beregne sannsynligheten basert på tidligere registrerte hendelser vil ikke alltid være hensiktsmessig; -fremtiden kan ikke antas å være en direkte gjentakelse av historien.

«Som beslutningstaker ønsker man å få innblikk i hva som ligger bak dette tallet, for eksempel hvorfor sannsynligheten er lav og om den kommer til å fortsette å være lav også i fremtiden.»

Tradisjonelle risikostyrings-metoder - utfordringer

For problemstillinger knyttet til operasjonell risiko, som omhandler mennesker og organisasjoner i sitt daglige virke, vil det ikke være mulig å anta at historien gjentar seg, og det er dermed ikke hensiktsmessig å beregne en objektiv «sann» sannsynlighet kun basert på historiske data. I denne sammenhengen oppstår det et tydelig behov for å dreie fokus mot kunnskapsbasert sannsynlighet som bygger på all tilgjengelig informasjon, innbefattet observasjoner og data, relevant kunnskap og erfaringer. Resultatet bør presenteres som en argumentasjon knyttet til virksomhetens risikonivå.

Å forholde seg til et punkt i en tradisjonell risikomatrise kan være uhåndgripelig og gir liten reell beslutningsverdi med mindre man i tillegg får informasjon om hva som ligger i sannsynlighetsbegrepet og samtidig oppnår en forståelse for hvilke årsaker og risikopåvirkende forhold som faktisk påvirker hvorvidt hendelsen inntreffer og hvilke årsaker som er særlig risikodrivende for den vurderte hendelsen. Vi ønsker at risikobildet skal gi en oversikt og forståelse av risikoen ved å belyse årsakssammenhenger, samt hvorvidt det finnes aktuelle tiltak og effekten av disse. Det bør også fremkomme hvilke forutsetninger, antakelser og kunnskap som ligger til grunn for analysen og dermed også resultatene. Usikkerheten i vurderingene bør altså kommuniseres.

Fra risikomatriser og fokus på historikk, til visualiserte risikobilder basert på all tilgjengelig kunnskap

For å styrke underlaget for beslutninger bør en risikovurdering gi svar på følgende spørsmål:

- Er risikoen høy/lav?
- Er risikoen akseptabel?
- Hvilke påvirkende faktorer er mest kritiske?
- Hva er konsekvensene hvis det går galt?
- Hvilke tiltak har størst risikoreduserende effekt?

For å gi reell beslutningsstøtte vedrørende ulike aktiviteter og mulige tiltak, bør risikoanalysen gi oversikt over fenomenet og skape forståelse hos beslutningstaker. Risiko er ikke statisk, men utvikler seg over tid, og for å kunne ta best mulige beslutninger bør man, i tillegg til å ha kjennskap til om risikoen er høy eller lav, også ha forståelse for sammenhenger mellom ulike risikopåvirkende faktorer og det at uønskede hendelser oppstår. En slik helhetlig tilnærming vil gi nyttig informasjon om hvilke risikopåvirkende faktorer som er gjeldende og hvilke avhengigheter som eksisterer mellom dem. Dette gir informasjon som bidrar til å kunne ta velbegrunnede valg vedrørende effektive tiltak.

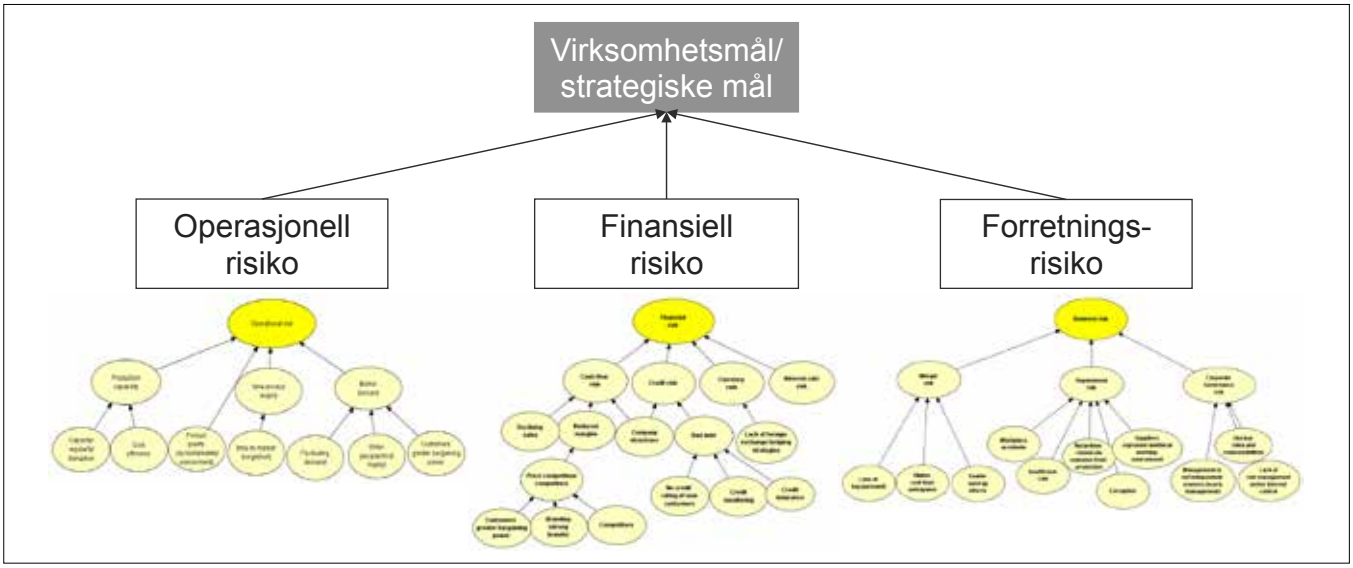
I eksempelet gitt ovenfor for risikoanalyse av et dataangrep, kan man spørre seg: Er sannsynligheten for et angrep vurdert som lav fordi det ikke har rammet tidligere (beregning basert utelukkende på historiske data)? Eller er den vurdert som lav fordi virksomheten nettopp har gjennomført en penetrasjonstest som viste robusthet, i tillegg til at de ansatte har vært på kurs for å lære å oppdage phishing-angrep? Den beregnede sannsynligheten er den samme, men de oppgitte begrunnelsene vitner om ulik grad av modenhet hva gjelder risikobevissthet og kontroll, og dermed ulik grad av risikoeksponering for den gitte organisasjonen.

Tradisjonelle risikomatriser er ikke et verktøy som gjør bruker i stand til selv å helhetlig vurdere risiko, den visualiserer kun resultatet av noens vurdering. Begrunnelsen for vurderingene er like viktige som sluttresultatet for å gi reell beslutningsstøtte. Det handler om å skape forståelse for-, og eierskap og tillit til de vurderingene som er gjort gjennom en synliggjøring av analysens styrker og begrensninger.

«Tradisjonelle risikomatriser er ikke et verktøy som gjør bruker i stand til selv å helhetlig vurdere risiko, den visualiserer kun resultatet av noens vurdering.»

Uavhengig av om analysen er av kvalitativ eller kvantitativ karakter vil det alltid gjøres antagelser før en begynner å vurdere eller beregne risiko. Denne viktige informasjonen fremkommer ofte ikke i tradisjonelle risikomatriser. Matrisen kan derfor i beste fall være lite informativ, og i verste fall være direkte misvisende. Utover hvilke forutsetninger analysen baseres på, er kunnskap og usikkerhet viktig å inkludere i den helhetlige vurderingen. I noen analyser er vurderingene som er gjort lite kontroversielle, det er for eksempel benyttet relevante eksperter på områder eller det finnes store mengder relevante statistiske data å basere resultatene på. Analysen er med andre ord gjort med høy grad av kunnskap, det vil si at det er lite usikkerhet omkring vurderingene. I andre tilfeller kan vurderinger være gjort med liten grad av kunnskap. Beslutningstaker vil være svært avhengig av å vite hvor grundig og med hvilken grad av kunnskapsstyrke risikovurderingen er utført. Avgjørelsene vil i stor grad påvirkes av graden av usikkerhet/sikkerhet knyttet til beslutningsgrunnlaget. Et eksempel hentet fra Petroleumstilsynets (Ptil) notat «Risikobegrepet i petroleumsvirksomheten», som beskriver hvordan ulik grad av kunnskap kan påvirke opplevelsen og håndteringen av risiko, lyder som følgende: «Tenk deg at du kjører på en vei som er bred og rett, du har god oversikt (kunnskap) og liten usikkerhet omkring hvilke konsekvenser som vil møte deg. Du kan holde en relativt høy hastighet og allikevel føle deg trygg. Kontra at du kjører på en smal og svingete vei med liten oversikt og dermed stor usikkerhet omkring hva som møte deg rundt neste sving. På grunn av den store usikkerheten, vil din beslutning angående fart med stor sannsynlighet være annerledes enn i det første alternativet»

For å tilgjengeliggjøre mer av informasjonen relatert til vurderinger og resultater på en enkel og intuitiv måte, kan problemstillinger struktureres og visualiseres i grafiske risikobilder. Et visualisert risikobilde beskriver sammenhengen mellom uønskede hendelser, årsaker og risikodrivere; en grafisk presentasjon av hendelsesforløpet. Vurderinger og resultater forklares og begrunnes logisk slik at det er mulig å involvere de relevante rollene og funksjonene i organisasjonen som det er nødvendig å inkludere for å oppnå en sunn risikostyring. Visuelle risikobilder kan benyttes til å kartlegge hendelser som kan påvirke virksomhetens måloppnåelse, både på et overordnet nivå og et mer detaljert nivå.



Figur 1: Helhetlig tilnærming til virksomhetsrisiko.

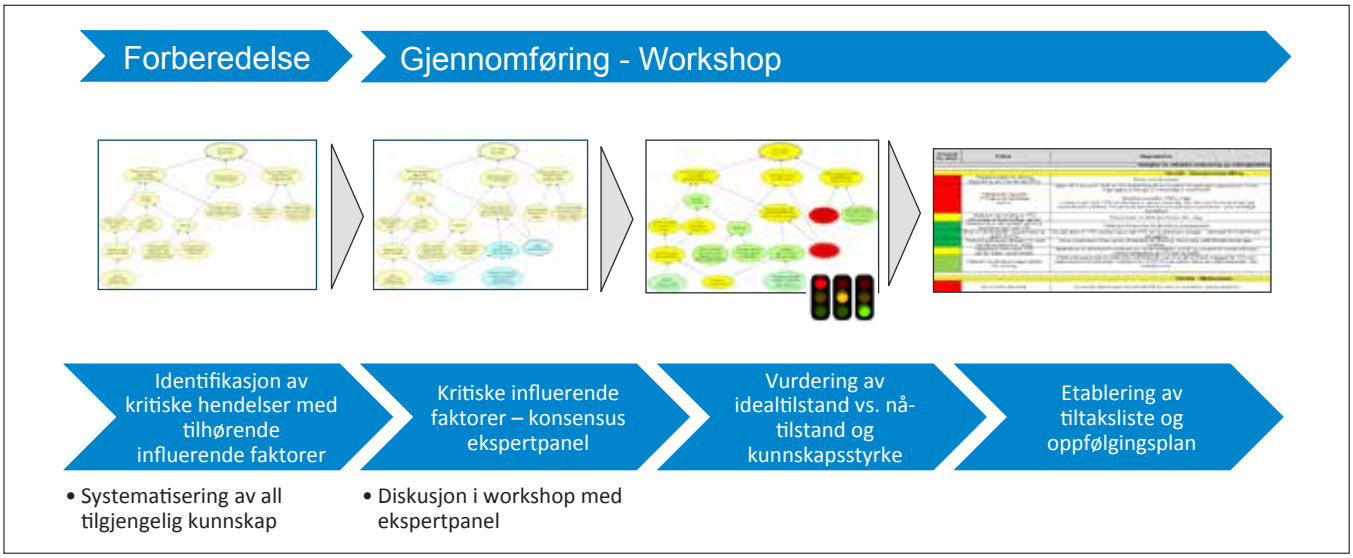
Prosess for risikovurdering med visualiserte risikobilder

Selve prosessen for gjennomføring av risikoanalyser ved bruk av metoder som inkorporerer all tilgjengelig kunnskap og benytter visualisering som verktøy, skiller seg ikke i særlig grad fra bruk av tradisjonelle risikomatriser. Planleggingsfasen tillegges mer vekt ved bruk av visuelle nettverk, da man i forkant av analysemøter forbereder et grafisk utgangspunkt for diskusjon.

Teknologien som kan brukes for å systematisere, dokumentere og kommunisere risikobildet, heter Bayesiansk nettverk (også kjent som «Bayesian Belief Networks», kausale sannsynlighetsmodeller, Bayes nets, etc.). Bayesiansk nettverk er grafiske diagrammer som strukturerer kunnskap om et emne ved å beskrive influensforhold mellom nøkkelvariabler. Det består av en kvalitativ og en kvantitativ del og bygger på sannsynligheten for at noe skjer gitt den kunnskapen vi har. Et Bayesiansk nettverk visualiserer risikobildet (kausale sammenhenger og influerende faktorer), noe som bidrar til å lette arbeidet med å etablere en felles forståelse av risikobildet og relevante årsaksmekanismer. Resultatet er en oversiktlig redegjørelse for et etablert risikobilde; et scenario, en prosess eller et system med tilhørende risikoer, inklusive tydelig fremheving av forbedringsområder som utgangspunkt for vurdering og prioritering av tiltak.

Identifikasjon av kritiske hendelser med tilhørende influerende faktorer

Arbeidet starter ved innsamling av all tilgjengelig informasjon, det vil si tidligere analyser, historiske data og annen litteratur, for eksempel vitenskapelige teorier som vedrører og er relevant for analyseobjektet. Informasjonen brukes til å kartlegge og strukturere potensielle uønskede hendelser, trusler, årsaker, risikodrivere og eksisterende kontroller



Figur 2: Risikoanalyseprosess med grafiske nettverk som utgangspunkt for diskusjon (Visualiseringsverktøy levert av Combitech AS).

inn i et nettverk. Nettverket danner grunnlaget for det videre analysearbeidet.

Figur 3 nedenfor illustrerer et eksempel på hendelsen «Utlevering av sensitiv informasjon». Denne hendelsen kan inntreffe på tre ulike måter; enten ved at en ansatt misbruker sin tilgang, ved en utilsiktet lekkasje eller ved at en ekstern uautorisert person får tilgang. De tre årsakene er hovedrisikodrivere for denne hendelsen.

Kritiske influerende faktorer-konsensus ekspertpanel

Når utgangspunktet for nettverket foreligger, gjennomføres en workshop med et ekspertpanel. Her inkluderes alle personer som har kunnskap om analyseobjektet, i tillegg til andre interessenter, det være seg alt fra teknikere til helsepersonell. Etablert nettverket i steg 1 vil danne utgangspunktet for diskusjonen og utgjøre grunnlaget for en systematisk gjennomgang. Risikoanalyseobjektet og konteksten er definert i det grafiske utgangspunktet og alle involverte vil fra første øyeblikk få en intuitiv forståelse for- og oversikt over problemstillingen. Erfaringer fra denne type verktøy viser at det gir mye engasjement blant deltakerne i kartlegging av risiko. Underveis i gjennomgangen vil nettverket oppdateres med nye tilkomster eller endringer hva gjelder årsaker, konsekvenser og kontroller/barrierer basert på utfallet av diskusjonen i workshopen. Et visuelt nettverk med en hierarkisk struktur gir støtte i arbeidet med å klargjøre hva som er årsaksfaktorer, hendelser og konsekvenser. Risikodrivere og uønskede hendelser blir på denne måten presist definert og vil være mulig å sammenstille og prioritere. Resultatet for deltakerne er en bedre oversikt over og innsikt i mekanismene som potensielt kan lede til uønskede hendelser.

Vurdering av idealtilstand vs. nå-tilstand og kunnskapsstyrke

Når et omforent risikobilde er etablert, starter arbeidet med å vurdere sannsynligheten for at risikoene kan inntreffe. I workshopen vil en starte på nederste nivå i nettverket, det vil si med rotårsakene (kalt input noder i Bayesiansk nettverk), som for eksempel kan være trusler, tilstand til organisasjonskultur eller eksisterende kontroller.

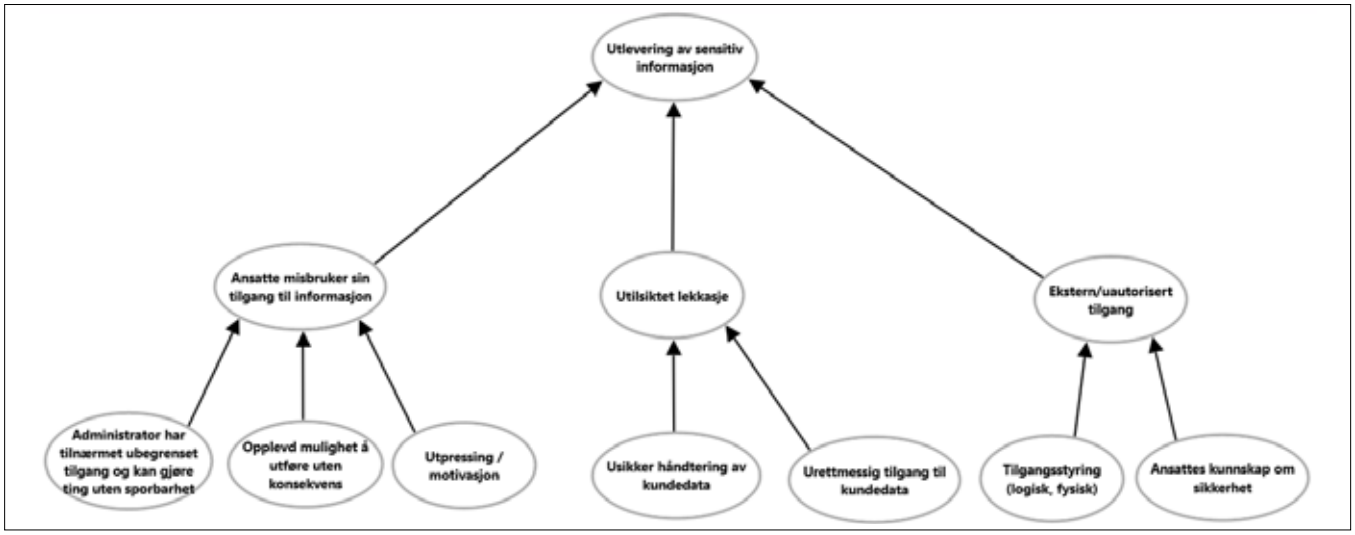
Å fastsette sannsynlighet og konsekvens i en kvalitativ analyse kan være vanskelig, men å fastsette kritikalitet i forhold til en referanseverdi, det vil si å fastsette hvor langt organisasjonen befinner seg i fra ønsket eller ideell tilstand for en faktor/årsak på et lavere nivå i årsakssammenhengene, vil oppleves svært konkret, og kan gjøres med større grad av kunnskap.

«Å fastsette sannsynlighet og konsekvens i en kvalitativ analyse kan være vanskelig, men, å fastsette kritikalitet i forhold til en referanseverdi vil oppleves svært konkret, og kan gjøres med større grad av kunnskap. »

Figur 4: Fastsettelse av kritikalitet i forhold til referanseverdi (idealtilstand).

Figur 5: Begrunnelse av kritikalitet i forhold til idealtilstand/ønsket tilstand.

Angivelse av tilstand vurderes altså ved å kartlegge gapet mellom ønsket optimal tilstand, det man kan kalle en idealtilstand for rotårsaken, og faktisk tilstand per i dag. Ønsket tilstand defineres ved hjelp av organisasjonens egne prosedyrer og retningslinjer, eventuelt beste praksis, standarder eller myndighetskrav. Nå-tilstanden blir vurdert i henhold til en kvalitativ skala med fargeangivelse. Dersom avstanden til ønsket tilstand er stor, vil tilstanden til faktoren vurderes til rød. Er faktisk tilstand i motsetning lik ønsket tilstand, vurderes tilstanden til grønn. Vurderingen av tilstand til intern-



Figur 3: Risikobilde (scenario) som utgangspunkt for diskusjon.

kontroller kan for eksempel gjøres med utgangspunkt i resultatene av intern- evt. eksternrevisjon.

Faktorer vektes i forhold til hverandre, og basert på de ulike faktorenes tillagte betydning, vil tilstander aggregeres oppover i nettverket ved hjelp av kunnskapsbasert sannsynlighetsvurdering. Det vil si at man gjør en vurdering av hvorvidt en gitt risikodriver vil inntreffe basert på den informasjonen som er gitt lenger ned i nettverket. Slik aggregeres tilstander helt til topphendelsen i nettverket, og på denne måten baseres den aggregerte sannsynligheten for at en uønsket hendelse skal inntreffe på årsakssammenhengene og tilstanden til influerende faktorer samt tilstanden til eksisterende kontroller/barrierer. I figur 6 er det illustrert hvordan et ferdigstilt visualisert risikobilde kan se ut.

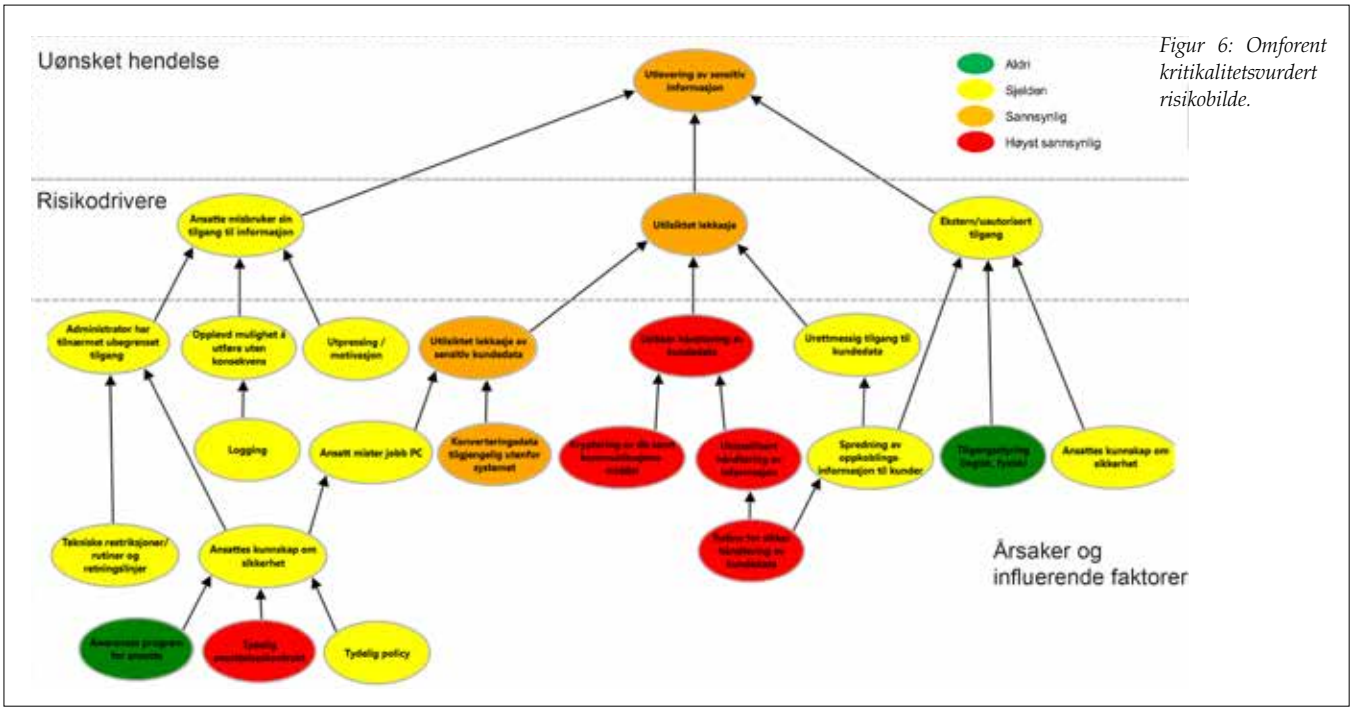
Usikkerhet i vurderingene i form av mangel på informasjon, manglende forståelse eller kunnskap, visualiseres ved å benytte trafikklys knyttet til faktorene. Kunnskapsstyrke benyttes som begrep for å beskrive usikkerhet omkring tilstanden til en faktor. Som et eksempel kan det gjøres en vurdering av en faktor uten at relevant ekspertise har fått bidratt med sin erfaring, eller til tross for at det eksisterer svært lite informasjon eller tilgjengelig kunnskap på området. Slike vurderinger vil gi analysen enkelte begrensninger som bør fremkomme eksplisitt som bakgrunn for tolkning av resultatene. «Å håndtere usikkerhet innebærer å skape en forståelse for begrensningene av vår kunnskap og ta konsekvensene av det» (Ptil).

Figur 7: Trafikklys for informasjon vedrørende grad av kunnskap tilstandsvurderingen er basert på.

Etablering av tiltaksliste og oppfølgingsplan

Analysen vil gi en velfundert basis for å kartlegge tiltak og diskutere effekten av disse for videre prioritering. Nettverkene vil bidra til å belyse avhengigheter der felles årsaker og influerende faktorer vil ha betydning for valg av tiltak. Tiltak kan også innebære å fremskaffe ytterligere informasjon om faktorer som hvor graden av kunnskap ikke har vært tilstrekkelig. Resultatet av en visualisering av risikobildet vil dermed være et omforent risikobilde med informasjon om årsakssammenhenger og hvordan ulike årsaker og hendelser påvirker hverandre, samt en synliggjøring av effekten av implementerte og foreslåtte risikoreduserende tiltak. Visualiseringen som verktøy er svært godt egnet til å skape eierskap til risikoene blant de ansatte, og ikke minst til å kommunisere det samlede risikobildet til ledelsen og slik bidra til å forankre risikoer hvor beslutninger tas. Muligheten til å aggregere og detaljere risikobildet gjør det også velegnet til kommunikasjon av risikoeksponeringen på ulike nivåer.

«Visualiseringen som verktøy er svært godt egnet til å skape eierskap til risikoene blant de ansatte, og ikke minst til å kommunisere det samlede risikobildet til ledelsen og slik bidra til å forankre risikoer hvor beslutninger tas.»



Figur 6: Omforent kritikalitetsvurdert risikobilde.

Allerede kartlagte og dokumenterte hendelser kan i stor grad gjenbrukes som utgangspunkt ved tilsvarende analyser da mekanismene som kan lede til en uønsket hendelse ofte kan ha likheter selv om fenomenet som studeres har rot i ulike avdelinger, systemer eller prosesser. Nettverkene baseres så ofte som mulig på forskning og vitenskapelige teorier omkring et fenomen (for eksempel svindelteori), hvordan det kan oppstå og hvordan det utarter seg. Dette kan bidra til å løfte kvaliteten til risikoanalysene i organisasjonen. I tillegg til at kvaliteten på analysene over tid vil bedres på grunn av oppdateringer og eventuelle tilføyinger, kan det å sitte på grundig utarbeidede modeller som utgangspunkt for videre analyser av relevante hendelser, lette risikostyringsarbeidet på lang sikt. Metoden er over tid tidsbesparende og kostnadseffektiv.

Konklusjon

Tradisjonelle metoder for risikoanalyser presenterer ofte risikoer enkeltvis og uavhengig av hverandre. I praksis vet vi at risikoer ikke oppstår isolert eller opptrer i et vakuum. Mange risikoer har gjerne flere sammenfallende årsaker, og noen risikoer med sammenfallende årsaker kan gjerne reduseres ved ett og samme tiltak. I et komplekst og sammensatt risikobilde er det vesentlig å kunne se sammenhenger på tvers og oppnå en bedre forståelse av hva som skjer dersom flere influerende faktorer inntreffer samtidig. Dette kan gjøres på en enkel og intuitiv måte ved å visualisere risikobildet i et nettverk.

Visualiseringen legger også til rette for konstruktive diskusjoner omkring risiko, og er i tillegg et utmerket verktøy for å kommunisere risikobildet til alle involverte parter.

Erfaring med denne type verktøy viser at det skaper mye engasjement. De involverte kjenner seg igjen i «sine» kartlagte prosesser, systemer og problemstillinger, og får oversikt over hvilke farer/trusler og årsaker som kan lede til uønskede hendelser, hvilke barrierer/kontroller som eksisterer og hvor det evt. mangler sannsynlighets- eller konsekvensreduserende tiltak. Dette gir ofte opphav til fruktbare diskusjoner rundt trusler og sårbarheter, hvordan risiko kan oppstå og hendelser inntreffe. I en risikoidentifikasjonsprosess ønsker man slik kreativitet for å avdekke all mulig relevant risiko. Bruk av matrise-metodens sjekklister eller ustrukturerte diskusjoner identifiserer gjerne kjente trusler og risikoer, men stimulerer i liten grad deltagerne til å avdekke nye sammenhenger. Visuelle nettverk legger til rette for en strukturert gjennomgang som også stimulerer til kreativitet, slik at hittil ukjente risikoer, og ukjente effekter av kjente årsaksforhold og mulige samspill dem imellom, avdekkes.

Som beslutningsgrunnlag gir det visuelle risikobildet en intuitiv forståelse og oversikt. Metoden evner å inngi tillit til gitte vurderinger da det tydelig fremkommer hvilke forutsetninger vurderingene baseres på, og resultatenes validitet styrkes ved synliggjøringen av kunnskapsstyrke.

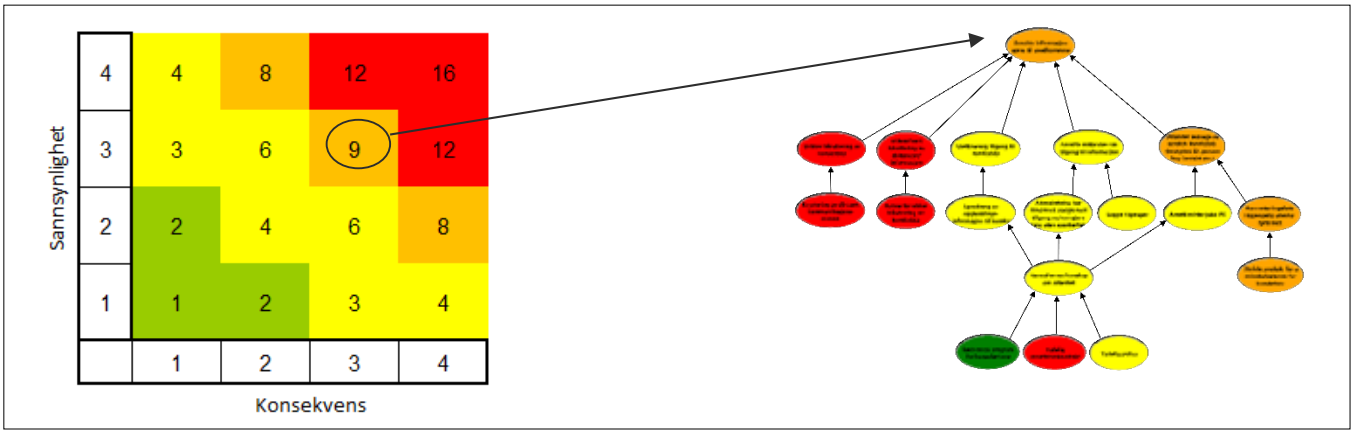
Metoden gir, til forskjell fra tradisjonell metode, følgende fordeler:

- Øker forståelse, eierskap og engasjement på tvers av organisasjonen
- Viser sammenhenger og påvirkning mellom forskjellige årsaksfaktorer og risikoer
- Illustrerer risiko både på detalj- og på aggregert nivå
- Øker Management buy-in

Generelt kan man si at metodene som skal gi best mulig beslutningsstøtte i risikostyringssammenheng, bør ta høyde for senere års utvikling innen risikostyringsfaget, med økt fokus på kunnskapsdimensjon og usikkerhet. Man ser generelt en trend og en utvikling som beveger seg fra tradisjonelle risikomatriser og bruk av såkalt objektiv sannsynlighet basert på historiske data, mot en vektlegging av økt risikoforståelse og en erkjennelse av at man i stor grad opererer med subjektive sannsynligheter basert på (mye eller lite) kunnskap og erfaring. Visualisert risikoanalyse med utgangspunkt i Bayesiansk nettverk, er en metode som vil være i samsvar med dette ønsket om økt fokus på helhetlig risikoforståelse.

Referanser

- *Andersen, L.B, Häger, D. (2014). Contributions to Bayesian network model design for operational risk in financial industry.*
- *Andersen, L.B., Häger, D. (2014). Objectivity and the measurement of operational risk, reconsidered.*
- *Aven, T. (2015) Risikostyring. 2. Utgave, Universitetsforlaget.*
- *Aven, T., Røed, W., Wiencke, H.S. (2008). Risikoanalyse. 1. Utgave, Universitetsforlaget.*
- *Aven, T., Artikkel – Tradisjonell risikomatrise. Store norske leksikon*
- *Ptil (Petroleumstilsynet) (2016), Notat – Risikobegrepet i petroleumsvirksomheten. Petroleumstilsynet*



Figur 8: Sammenligning mellom tradisjonell matrise og visuelt nettverk. Risikoen er «9», hvorfor er den relativt høy og hva betyr det for oss? Det visuelle nettverket gir en forklaring til risikonivået og synliggjør sårbarheter.

COSOs nye rammeverk for risikostyring: «Enterprise Risk Management – Integrating with Strategy and Performance»

Av
TOR SOLBJØRG
Revisjonssjef i Helse Nord RHF og leder av IIA Norges fag- og metodekomité

BAKGRUNN

COSOs rammeverk for helhetlig risikostyring, COSO ERM, ble publisert i 2004. Norges Interne Revisorers Forening (NIRF), nå IIA Norge, ga den ut i norsk språkdrakt året etter. Rammeverket har oppnådd en sterk posisjon her til lands, og ligger bl.a. til grunn for metodedokumentet «Risikostyring i staten» (utgitt i 2005 av Senter for statlig økonomistyring SSØ, nå Direktoratet for økonomistyring – DFØ). «Veileder for risikostyringsfunksjonen», publisert av IIA Norge i februar 2017, bygger også på COSO-rammeverket. (Et annet anerkjent og mye anvendt rammeverk, er som kjent ISO 31000.)

Mye har endret seg siden 2004, også rundt temaene risiko og risikostyring. I juni 2016 sendte dermed COSO utkast til et sterkt omarbeidet rammeverk på høring, nå med betegnelsen «Enterprise Risk Management – Integrating with Strategy and Performance». Både IIA Global og IIA Norge ga innspill innen høringsfristen (september 2016), og vi var langt fra alene. COSO mottok et stort antall uttalelser, til dels med forslag til betydelige endringer. Det videre arbeidet tok lang tid, men 6. september i år la de ut følgende melding på hjemmesiden sin: «COSO Issues Important Update to ERM Framework».

Det nye rammeverket foreligger per i dag bare i engelskspråklig versjon, så de norske begrepene i denne artikkelen står helt og fullt for min regning.

HVA BESTÅR DET NYE RAMMEVERKET AV?

Den nye versjonen av COSO ERM består av selve rammeverket, et dokument på 110 sider, samt Executive Summary («Sammendrag») og Appendices («Vedlegg»).

Jeg vil også nevne dokumentet «Frequently asked Questions» («FAQ») som ligger på COSOs hjemmeside.

Appendices består av fire kapitler: A) Project Background and Approach for Revising the Framework – B) Summary of Public Comments – C) Roles and Responsibilities for Enterprise Risk Management – D) Risk Profile Illustrations.

Noen ord om to av disse kapitlene:
I pkt C går man først relativt grundig inn på «typical board oversight practices of ERM». Deretter ser man på oppgavene til hhv Chief Executive Officer og Chief Risk Officer, før man tar en gjennomgang av oppgavene til øvrige ledere, fordelt på hhv første, andre og tredje linje slik vi kjenner dem fra Three Lines of Defence-modellen. Også eksternrevisors rolle omtales.

Illustrasjonene i Appendices pkt D, som er nye i COSO ERM-sammenheng, blir i FAQ beskrevet slik: «The risk profiles demonstrate how the type and severity of risk can change in response to changes in the level of performance for a given strategy or business objective.» Og videre: «By incorporating the concepts of risk appetite, performance and risk into a single graphic, the risk profiles offer a dynamic and comprehensive view of risk and enable more risk-aware decision-making.»

HVA ER NYTT?

Alle som kjenner 2004-versjonen vil umiddelbart se at det nå er gjort vesentlige endringer på sentrale punkter. Jeg har særlig merket meg følgende:

Ny definisjon
Definisjonen av risikostyring lyder nå: The culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving and realizing value.

Ikke bare er dette en helt ny formulering, selve vinklingen er en annen enn i den gamle definisjonen, som beskrev prosessen helhetlig risikostyring.

Fokus på strategi
I det nye rammeverket blir risikostyringens rolle knyttet til organisasjonens strategier sterkere vektlagt, noe som går fram allerede av navnet (undertittelen) og av definisjonen. Videre kommer det til uttrykk i form av fokus på:

- muligheten for at strategiske målsettinger ikke underbygger eller samsvarer med organisasjonens formål, visjoner og etiske verdier
- konsekvensene av organisasjonens valg av strategi, og
- risiko knyttet til gjennomføring av strategien.

Klarere kobling mot prestasjoner/ resultater

Hensikten med risikostyring har alltid vært å bidra til måloppnåelse, herunder innfrielse av prestasjons- og resultatmål. At COSO nå tar ordet «performance» inn i navnet på rammeverket, signaliserer en enda sterkere vektlegging av at risikostyringen skal bidra til bedre prestasjoner og resultater.

Kuben er borte

Kuben som illustrerte forholdet mellom komponenter, målsettingskategorier og enheter, inngår ikke i det nye rammeverket. Den er erstattet av andre grafiske fremstillinger.

Komponenter og prinsipper

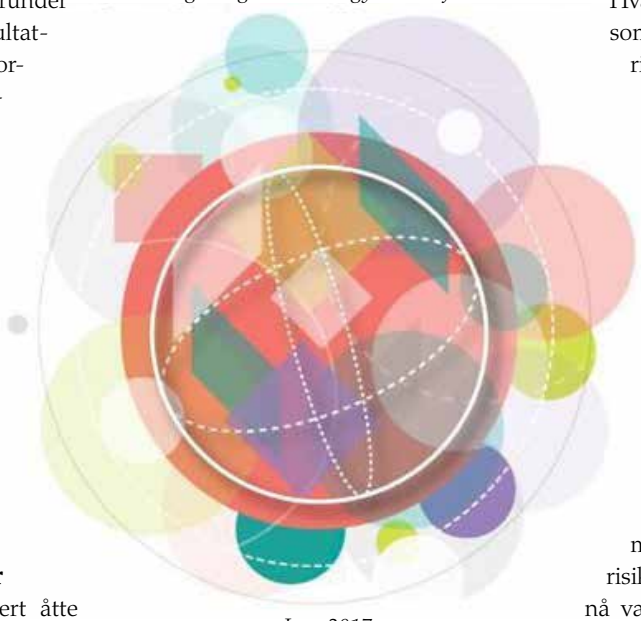
I 2004-versjonen var det definert åtte komponenter som står sentralt i risikostyringen. Også det nye rammeverket benytter komponenter, nå redusert til fem. Disse har andre navn enn tidligere, men oppbygging og innhold er lett gjenkjennelig. Komponentene er nå supplert med underliggende prinsipper, 20 til sammen, et mønsteret vi kjenner igjen fra COSOs internkontrollrammeverk.

Definisjonen av risiko er endret

COSO definerer nå risiko slik: The possibility that events will occur and effect the achievement of strategy and business objectives.

I det gamle rammeverket ble risiko definert som «det at en hendelse kan inntreffe og påvirke måloppnåelsen negativt». Slik defineres det også i COSOs gjeldende rammeverk for internkontroll, men i det nye risikostyringsrammeverket er det altså endret, slik at «risiko» omfatter både positive og negative effekter. Endringen reflekterer det selvsagte poenget at man i risikostyringen ikke bare skal være opptatt av farene for manglende måloppnåelse, men også av mulighetene for forbedringer. Det er et viktig budskap, men jeg må vedgå at jeg personlig ikke er begeistret for at muligheter nå defineres som risiko!

Enterprise Risk Management
Integrating with Strategy and Performance



June 2017

En ny kategori risikohåndtering – to pursue

Det opprinnelige rammeverket beskrev fire alternativer for håndtering av risiko: Å unngå den, redusere den, dele den eller akseptere den. De fire er beholdt, men nå har man lagt til en femte kategori: to pursue. Altså å «forfølge», «etterstrebe» e.l., og det utdypes slik: Action is taken that accepts increased risk to achieve improved performance. Et godt eksempel på de endringene som er gjort i rammeverket for å understreke at risikostyring også dreier seg om å utnytte muligheter!

Andre endringer.

I «Frequently Asked Questions» lister COSO opp en rekke «Key Changes». Flere av dem er omtalt ovenfor, men det vises også til at det nye rammeverket:

- styrker fokus på å integrere risikostyring
- utdyper kulturens betydning
- knytter risikostyringen klarere opp mot beslutningene som tas i organisasjonen
- gjør en klarere avgrensning mellom risikostyring og intern styring og kontroll, og
- utdyper skillet mellom risikoappetitt og toleranse.

HVA NÅ?

Hva vil det så bety for organisasjoner som per i dag gjennomfører risikostyring etter mønster fra «gamle COSO ERM», at det har kommet et helt nytt rammeverk? COSO understreker selv, bl.a. i FAQ, at det er fullt akseptabelt fortsatt å anvende 2004-rammeverket. Basert på min første gjennomlesing kan jeg heller ikke se at det er grunnleggende endringer i 2017-utgaven som gjør at man kommer helt feil ut ved å beholde et opplegg basert på det gamle rammeverket, eller på DFØ-varianten av dette, men selvfølgelig: I virksomheter hvor man ikke er fornøyd med hvordan risikostyringen håndteres i dag, kan det nå være fornuftig å «starte forfra» med utgangspunkt i «Enterprise Risk Management – Integrating with Strategy and Performance». Jeg vil imidlertid tro den beste løsningen for mange er å legge dette til grunn for gjennomgang, evaluering og oppdatering/forbedring av det risikostyringsopplegget organisasjonen allerede benytter.

Executive Summary og Frequently Asked Questions (FAQ) ligger fritt tilgjengelig på COSOs hjemmeside. Hele dokumentsamlingen kan kjøpes fra IIA Norge for kr 990,-(medlemspris) eller man kan kjøpe det fra IIA eller AICPA.

IIA Norge vil publisere en norsk versjon av Sammendraget (Executive Summary) etter nyttår, og vil da invitere til medlemsmøte om det nye rammeverket.

Det diffuse omdømmet

Hva er det som gjør at virksomheter går på et omdømmetap? Hva er egentlig omdømme og omdømmekapital?

Av
MARIT TRODAL
Prosjektleder IIA Norge

Nils M. Apeland beskriver omdømme som «summen av oppfatninger som ulike interessentgrupper har av virksomheten» (Apeland, 2010:18). Det handler om relasjoner mellom en virksomhet og ulike interessenter. Professor ved Institutt for kommunikasjon og kultur på BI Peggy S. Brønn og professor Øyvind Ihlen understreker også at omdømme ikke er et øyeblikksbilde, men noe som formes over tid. ('Åpen eller innadvendt', 2009).

Et godt omdømme

I tre år på rad har Finn.no blitt kåret til den bedriften som har det beste omdømmet blant de 50 mest synlige virksomhetene i Norge, mens REMA faller mest. Det viser tall fra omdømmemålingen RepTrak Norge, som årlig gjennomføres av Apeland og Reputation Institute.

RepTrak baserer en virksomhets omdømmescore på fire spørsmål: Tillit, beundring, respekt og følelse for virksomheten. Dette gir en score på mellom 0 og 100. I tillegg gis det score på 23 attributter innen følgende syv dimensjoner: Produkter og tjenester, samfunnsansvar, arbeidsmiljø, innovasjon, ledelse, etikk og økonomi.

Finn.no får en omdømmescore på 86,4 poeng av 100 mulige og slår internasjonale giganter som IKEA, Apple og Microsoft. «Finn.no leverer en god tjeneste, som er det viktigste for folk. I tillegg oppfattes de som gode på etikk og innovasjon», sier administrerende direktør Ole Christian Apeland i kommunikasjonsbyrået Apeland. REMA har falt fra 74,3 poeng i 2016 til 66,9 poeng i 2017. Dette forklarer Apeland med at det har vært mye støy rundt REMA de seneste månedene. Deres data viste blant annet at folk var kritiske til bestevennstrategien og at appen Æ ikke ga kjeden det ønskede løftet. Omdømmet til REMA har fått seg et solid trøkk, i følge Apeland. En kombinasjon av uheldige strategiske valg og hendelser som trolig kunne vært håndtert bedre har tæret på omdømmekapitalen til REMA.

Kilde: Shutterstock.com

Hva er omdømmekapital?

Omdømmekapital er en verdi som virksomheter bygger opp over tid og som kan fungere som en buffer i tøffe tider. Det kan sammenlignes med god helse. Har du dårlig helse derimot…

Diffust? Her kan teori fra merkevarebygging være interessant å skjele til. Sjekk Keller's Brand Equity Model for ytterligere inspirasjon. Selv om denne modellen har fokus på produkt branding kan den også være relevant for å vurdere omdømme på virksomhetsnivå.

I en mye sitert artikkel innenfor kommunikasjon og markedsføring; «Opportunity platforms and safety nets» (2000), basert på forskning av Charles Fombrun og kolleger, hevdes det at virksomheter ved systematisk å bygge opp omdømmekapital kan høste to viktige gevinster. Rådgiver i Bedre Kommunikasjon Nils M. Apeland beskriver i sin artikkel 'Springbrett eller sikkerhetsnett?' (august 2017) disse gevinstene som følger:

1. Virksomheter med stor omdømmekapital får et springbrett som gjør at den kan komme høyere enn den ville gjort uten. I næringslivet handler det om tilgang på kunder og kapital, på samarbeidspartnere, nye talenter og på goodwill fra media og myndigheter. Omdømmevinnerne oppnår altså enklere gode resultater, fordi det gode omdømmet gir dem fart og høyde når de tar sats fra springbrettet.

2. Den andre gevinsten er et sikkerhetsnett, som illustrert på sirkus. Nettet redder livet til akrobatene om de skulle

falle ned. Tilsvarende gjelder for en virksomhet med høy grad av tillit og anerkjennelse. Den vil ha et mer solid sikkerhetsnett og derfor være bedre rustet til å tåle kritikk og motgang.

I følge Apeland ser man dette også i praksis når en velrennomert virksomhet kommer i en krise. Krisen går raskere over og fører til mindre varig skade, om den håndteres godt og i tide.

Forutsetninger som må være på plass

Brønn og Ihlen (2009) beskriver hvilke forutsetninger som må være tilstede for å bygge et godt omdømme: Vi må starte med å se nærmere på organisasjonens identitet. Denne kan deles inn i tre faktorer:

1. Visuell identitet
2. Organisasjonsidentitet
3. Virksomhetsidentitet

Hva er virksomhetens visjon? Mål, normer og verdier? Hva er det som kjennetegner oss? Hva gjør oss unike? Det må være samsvar mellom visuell identitet og de andre faktorene. Identiteten må ha substans og forankring. Her støter offentlige virksomheter gjerne på hindringer, siden de fyller en gitt oppgave og gjerne ikke kan velge sin identitet. Mulighetene for å være unik, synlig og åpen er derfor svært ulik mellom offentlig og privat sektor.

Det viktige er likevel å vite hvilken atferd som er akseptert på veien mot målet og demonstrere dette i praksis. Brønn og Ihlen beskriver det som følger: «Å kommunisere hva vi gjør, er ikke på langt nær så viktig som å vise i praksis at vi gjør som vi sier. Omdømme bygges over lang tid gjennom konsekvent atferd, og atferden må stemme overens med interessentenes forventninger». Her kan både verdier og etiske retningslinjer bidra til å tydeliggjøre hvilken adferd som er akseptert.

«Den største risikoen for omdømmetap oppstår når det blir et gap mellom hva virksomheten gjør og hva det forventes at den skal gjøre.»

Forventninger endrer seg over tid og er i så måte et bevegelig mål å orientere seg etter. Det er derfor viktig å være lydhør for hvilke forventninger ulike interessenter har. Et godt omdømme er et resultat av gode relasjoner mellom organisasjonen og sentrale interessenter – kunder, leverandører, ansatte, myndigheter etc. Dersom virksomheter legger vekt på relasjoner, vil de også få et godt omdømme, er anbefalingen fra BI-forskerne.

Omdømmerisiko og muligheter

I Basel II, som omhandler risikostyring i finansinstitusjoner er omdømmerisiko definert som følger: «Reputational risk can be defined as the risk arising from negative perception on the part of customers, counterparties, shareholders, investors or regulators that can adversely affect a bank's ability to maintain existing, or establish new, business relationships and continued access to sources of funding (eg through the interbank or securitisation markets.»

Negative oppfatninger kan være så mangt. Å vurdere omdømmerisiko og negative konsekvenser kan være diffust og krevende. Hvordan måler vi den? Er det en egen risikotype eller en konsekvens knyttet til andre typer risikoer? Forenklet sett handler det om ikke å møte forventningene til interessentene, og det kan skje på ulikt vis. Går vi tilbake til Apeland og Finn.no så handler mye om å levere et godt produkt eller tjeneste til sine kunder og at kundene har tillit til virksomheten. Det må være samsvar mellom hva virksomheten sier den leverer og det den faktisk leverer – over tid. I tillegg kommer andre faktorer som etikk, samfunnsansvar, økonomi og evne til innovasjon. Driver virksomheten uetisk? Har den underleverandører som driver uetisk eller på annen måte kritikkverdig? Går man noen år tilbake så måtte lederen i Adecco Helse gå av, etter brudd på Arbeidsmiljøloven på sykehjem i Oslo hvor Adecco Helse hadde kontrakt med kommunen. Orden i eget hus og leverandørkjede er også sentralt å ha kontroll over.

Omdømmerisiko kan også knyttes opp mot en virksomhets evne til innovasjon eller mangel på sådan. Leverer virksomheten på forventningene til de ulike interessentene? Evner de å overgå forventningene? Dette fordrer igjen at virksomheter har relasjoner til de ulike interessenter og forstår hva som beveger seg. Finn.no hadde ikke vært der de er i dag uten at Schibsted i sin tid hadde tatt det strategiske veivalget de gjorde. Deres evne til innovasjon har også bidratt til å styrke omdømmet og gi Finn.no en troverdighet blant interessenter – et godt springbrett for fremtiden.

Kilder:

https://www.apeland.no/wp-content/uploads/2017/04/RepTrakNorge2017.pdf
http://kvisvikconsulting.no/omdomme-viktigste-aktivum-og-storste-risiko/
http://forskning.no/ledelse-og-organisasjon-kommunikasjon-abc-i-naeringsliv-sosiale-relasjoner/2009/11/nokkelen-til-gull
https://www.magma.no/omdoemmesikring
http://www.jstor.org/stable/1252054

HVORDAN REVIDERE OMDØMMET?

Omdømmerisiko er uløselig knyttet sammen med en virksomhets strategiske utvikling. I så fall må man forvente å kunne se omdømmerisiko være del av internrevisjonens vurdering av vesentlige risikoer og eventuelle konsekvenser knyttet til disse.

Hvis man velger å utføre en revisjon knyttet til omdømmebygging kan følgende områder være aktuelle å vurdere:

- Hvilken tilnærming har virksomheten til omdømmebygging?
- Hvilken strategi og hvilke virkemidler har virksomheten anvendt for å bygge omdømme?
- Er det gjennomført en interessentanalyse?
- Hvordan er ansvaret for å følge opp relasjoner med viktige interessenter fordelt i organisasjonen?
- Hvordan har man kvalitetssikret og evaluert omdømmearbeidet?
- Hvilke beredskapsplaner har virksomheten på plass for håndtering av hendelser?

Julegavetips – i siste liten

Vi krysser fingrene for en rask postgang, for i så fall kan du glede et helt revisjonsutvalg eller styre med nye kaffekopper til jul.

Er dere flere på avdelingen som trenger musematter? Denne vil glede enhver internrevisor og kanskje en og annen leder.

Sjekk ut flere gaver som disse på https://www.zazzle.co.uk/s/internal+audit

Noen ganger er null-toleranse for gaver kjipt…. For denne tror vi mange ledere av internrevisjoner rundt omkring ville likt å få! (Et tips kan være å kjøpe den til seg selv?)

Hvem er nissen?

Det er mange av våre medlemmer som lever spennende liv ved siden av å jobbe i internrevisjonen, deriblant denne personen.

Vedkommende hjelper til i julestria og dekker store deler av den nordlige halvkule for Julenissen. Personen er i likhet med Julenissen jovial av natur og glad i å finne ut hvem som har vært snill eller slem.

Kjenner du igjen nissen?
Send svar til post@iia.no, merket «Julenisse». Premieres

Her er en annen vinner under treet - tror vi!

Om ikke denne hette-genseren egner seg på kontoret hele året, så er budskapet viktig å få frem nå i desember....

Sjekk
https://www.sunfrog.com
for flere gavetips

Learning from the enemy

Internal Auditors and Fraud

By
JORGE NUNES
Internal Audit Director, The University of Porto, Portugal. Jorge is a frequent speaker in Portugal and abroad on internal audit, especially in relation to fraud. He has also authored a number of articles on the same subjects.

Introduction

In this article, I look at the role of internal auditors in the area of fraud prevention. I first examine fraud and the specific role of internal audit in that context before presenting data in respect of fraud cases leading to a conclusion as to the important role internal audit should play in reporting on and reinforcing sound internal controls in the organisation.

What is fraud?

Almost every time a new big fraud scheme is known to the public, we hear the question: where were the auditors?

The answer can be so simple, since we really know every detail of the fraud!

But first of all, let us be clear on the definition of fraud.

According to the ACFE – Association of Certified Fraud Examiners, occupational fraud and abuse is the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.

Anyone could easily say it takes two stages: the intention (or «motivation») of the employee and a lack of control on the organization.

Figure 1 The Fraud Triangle

Some criminologists have tried to explain why people commit fraud. One of them, Donald Cressey, developed a theory – known as the Fraud Triangle (see figure1) – that explains the factors that lead to fraud – pressure, opportunity and rationalization.

Cressey's hypothesis states that trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations

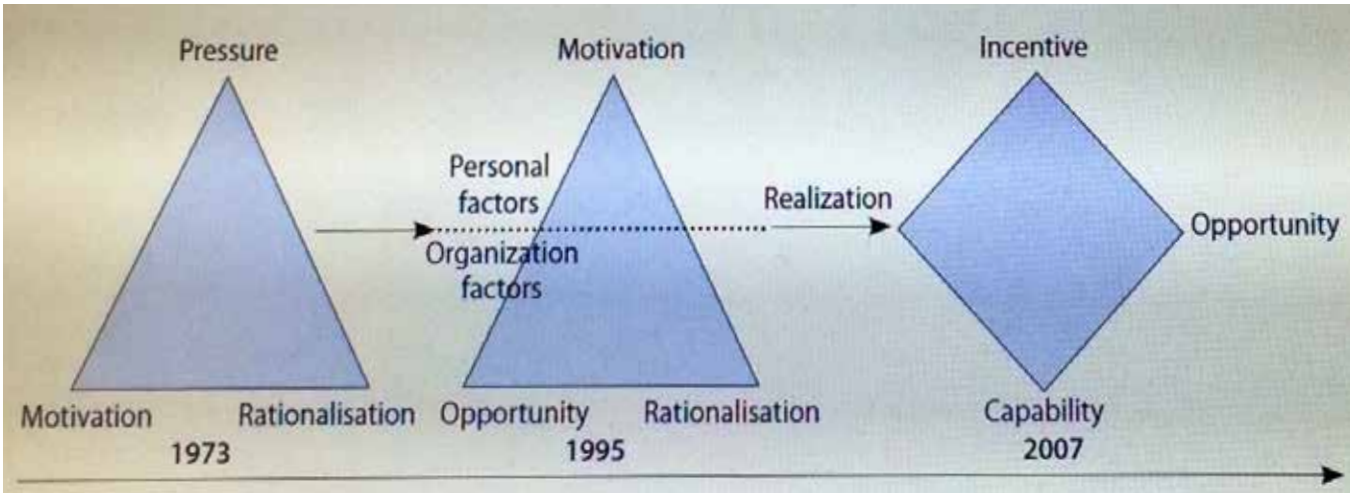


Figure 2 The fraud diamond

which enable them to adjust their conceptions of themselves as trusted persons with their conception of themselves as users of the entrusted funds or property.

Also trying to explain white-collar crime, Wolf and Hamerson created the Fraud Diamond (see figure 2), adding to Cressey's triangle the Capability, that provides the individual with the capacity to execute the fraud.

What is the role of internal audit in relation to the fraud area?

Assuming that most larger organizations have an internal audit function, the question is what can/should/must internal auditors do in the fraud area.

The IIA – Institute of Internal Auditors, in the 2016 IPPF, introduced the mission of internal audit: to enhance and protect organizational value by providing risk-based and objective assurance, advice and insight.

According to the IPPF glossary, fraud is any illegal act characterized by deceit, concealment, or violation of trust. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

In the attribute standards, more specifically related to proficiency, we have the following mention of fraud:

«1210.A2: Internal Auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud»

So, internal auditors must be able to identify the existence of the risk of fraud, while doing their job in the organization, and then evaluate how the organization is reacting to the existing fraud risk.

We have a further mention of fraud in the performance standard related to risk management, which is essential for a risk based auditing process:

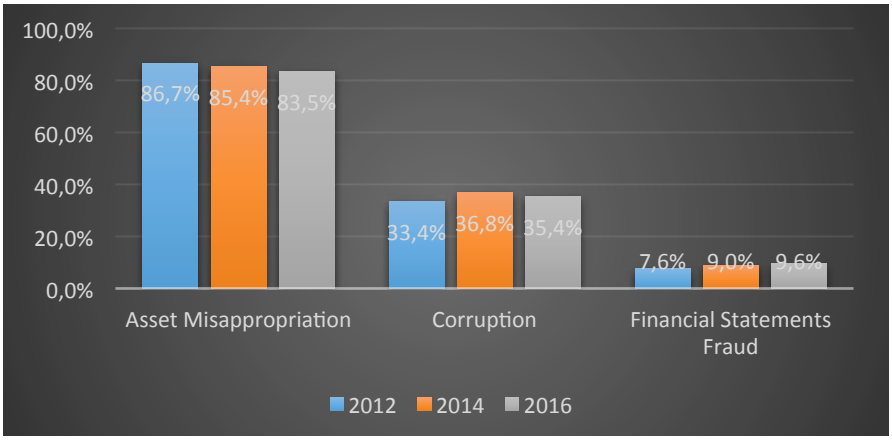


Figure 3 Analysis of fraud cases - ACFE

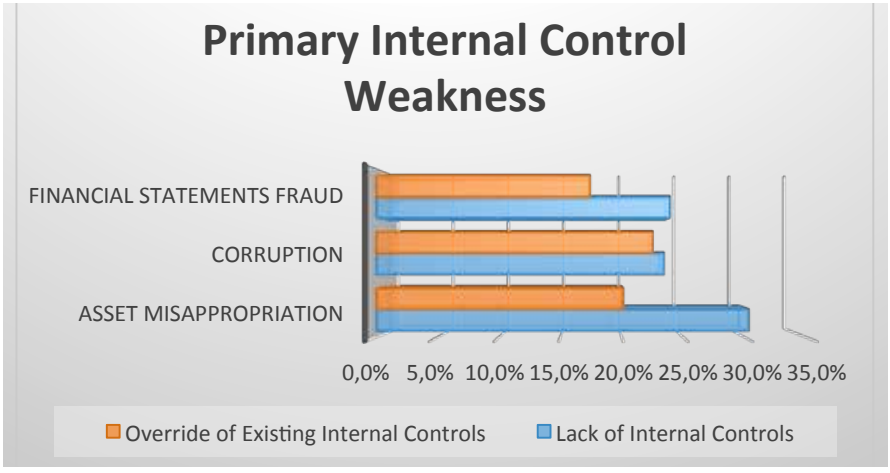


Figure 4 Primary internal control weakness - ACFE

«2120.A2: The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.»

After reading these definitions, we can easily think that the focus of internal auditors should be how to help protect the organization´s assets and resources and taking on an important role in fraud prevention.

Analysis of fraud cases

According to a report of the Association of Certified Fraud Examiners (ACFE´s Report to the Nations of 2016 - 2.410 cases of fraud in 114 different countries), the total losses caused exceeded 6.3 billion USD, with a median loss of 150.000 USD per case.

The Certified Fraud Examiners who participated in that survey also estimated that the typical organization loses 5% of revenues in a given year as a result of fraud.

To examine better the possible contribution by internal auditors, we can observe an analysis of fraud cases according to the primary categories of occupational fraud (see figure 3).

Asset Misappropriation is by far the most common type of fraud, representing 83,5% of the cases, but with a lower median loss of 125.000 USD. Then comes corruption, which represents 35% of the fraud cases in Western Europe.

At the other end of the scale is financial statement fraud with 9,6% of cases, but with a higher median loss, near the million USD, however, in most organizations, the financial statements are examined by external auditors and other entities so that we may assume this type of fraud will already be subject to audit.

Based on this analysis it is more likely that internal auditors will put their effort into the area of greatest risk of loss and that is asset misappropriation.

Another important conclusion of the ACFE Report is the significance of internal controls to fraud. It was shown that in almost 50% of fraud cases the problem was related to internal controls, namely:
- lack of internal controls 29,3%
- override of existing internal controls 20,3%

And weakness in internal controls applies to each primary category of occupational fraud, as below.

Asset misappropriation is a major area with thousands of activities and corresponding control requirements and it is also identified as having a high lack of internal controls.

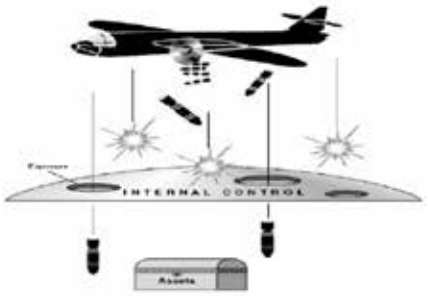
The lack of internal controls is also significant in respect of financial statement fraud, but here the problem is more likely to be specifically related to the accounting and financial areas.

Corruption may of course be found in all areas of the organization.

Conclusion

With a background from this analysis, and according to the three lines of defence model, internal audit should report to senior management, and the governing body as to whether the effectiveness of the internal control environment has been impaired and whether the organization´s risk management framework needs to be reinforced.

Although in my opinion internal auditors should not be involved in fraud investigation, they may still play an important role in helping in both the investigation and legal area. Internal audit should contribute to fraud prevention programs and the politics and culture of the organization, bringing their knowledge and



experience in evaluating internal controls with proficiency and due professional care.

Internal audit credibility and value are enhanced when auditors are proactive and their evaluations offer new insights and consider future impact.

Fraudsters will always try to be one step ahead, and we as internal auditors must always try to learn from the enemy.

Går leder av internrevisjonen ut på dato?

«Når lederen av internrevisjonen har vært mer enn sju år i stillingen bør revisjonskomitéen behandle komiteformannens vurdering av uavhengigheten og objektiviteten til revisjonslederen, og deretter bør denne saken tas opp til behandling årlig.» Slik lyder det i den nylig oppdaterte (etter fire år) «Financial Services Code» i UK. Dette er en veiledning i tråd med god praksis for internrevisorer i finansielle virksomheter utarbeidet av en arbeidskomité der internrevisorer er i minoritet. Det har etter hvert kommet krav til begrenset engasjement for eksterne revisorer i børsnoterte selskaper, men dette er første gang det uttrykkes noe lignende i forhold til internrevisjonsleder. Bakgrunnen for kravet er ønske om at leder av internrevisjonen opprettholder det nødvendige kritiske blikket. Kan denne praksisen utvikle seg til en ny norm for internrevisjonsledere?

Av andre oppdateringer kan det nevnes følgende:

1. Et krav til at revisjonskomiteen spesifikt vurderer om de aksepterer det som fremkommer i internrevisjonens årsplan om revisjonssyklus for områder som ikke revideres for hvert år.
2. Et krav til at internrevisjonen skal vurdere kvaliteten av arbeidet i første og andre linjen, og ikke bare vurdere om prosessene følges. Her nevnes for eksempel at dette vil kunne gjelde for vurdering av risikomodeller.
3. Et krav til årlig rapportering til revisjonskomiteen med en vurdering av om risikostyringsrammeverket etterleves i praksis.
4. Når det gjelder risikokultur skal internrevisjonen ikke bare vurdere «tone at the top», men også vurdere adferd gjennom hele organisasjonen.
5. Når det skjer intern gransking og årsaksanalyse av en sak skal internrevisjonen gi en vurdering av saken til styret, revisjons- og/eller risikokomité, herunder en vurdering av den faktiske rollen til 1., 2. og 3. forsvarslinje.
6. Leder av internrevisjonen skal sikre tilstrekkelig erfaring og kunnskap i internrevisjonsavdeling, i tillegg til tilstrekkelig teknisk kunnskap. Som kommentar til dette punktet nevnes viktigheten av at lederen får tilgang til tilstrekkelig fagkunnskap gjennom f.eks å leie inn ressurser som mangler in-house.

Den oppdaterte veilederen er, etter min mening, relevant og god praksis for alle internrevisjonsavdelinger, uavhengig av bransje. Veilederen er et levende dokument som nå er revidert fire år etter sin introduksjon. Neste revisjon er planlagt om ytterligere fem år.

«Financial Services Code» kan lastes ned fra https://www.iia.org.uk/resources/sector-specific-standards-guidance/financial-services/financial-services-code/

Martin Stevens

www.pwc.no/karriere

Er du analytisk, engasjert og kreativ?

pwc

Ta gjerne kontakt for en uformell samtale

Eli Moe-Helgesen
Tlf: 952 60 113
eli.moe-helgesen@pwc.com

Jonas Gaudernack
Tlf: 952 60 769
jonas.gaudernack@pwc.com

Petra Liset
Tlf: 952 60 152
petra.liset@pwc.com

PwC har en voksende RISK- og internrevisjonspraksis med mange erfarne spesialister. Vi er nå på jakt etter nye kollegaer. Ideelt sett har du 3-6 års erfaring innen rådgivning, revisjon, eller internrevisjon, og du er i ferd med å spesialisere deg på utvalgte bransjer og problemstillinger.

Hos PwC vil du inngå i et erfarent spesialistteam der det forventes at du kan analysere komplekse problemstillinger, komme opp med kreative løsninger og formidle disse på en engasjerende måte.

Internrevisjonens interne kvalitetssikring

– En spørrerunde blant fem internrevisjonsavdelinger

Av
MARTIN STEVENS
Konsernrevisjonen, Gjensidige

Vi som jobber med internrevisjon bruker mye av vår arbeidsdag til å forespørre ledere i våre virksomheter om de har oversikt over de vesentligste risikoene og nøkkelkontrollene i virksomheten og om kontrollarbeid er dokumentert. Derfor blir kvalitetssikring av internrevisjonsarbeid et sannhetens øyeblikk hvor vi kan vise at vi selv lever opp til de samme forventningene som vi har til ledelse i organisasjonen for øvrig.

I Norge er det til dels stor variasjon i størrelsen på internrevisjonsavdelingene. Selv om vi ikke har noen internrevisjonsavdelinger som kan konkurrere med Citibank med sine mer enn 1.800 ansatte på verdens basis, har vi noen få avdelinger med ca. 40-50 ansatte og mange som ligger i størrelsesorden 3-10 ansatte. Vi har forespurt 5 revisjonsavdelinger av ulike størrelser (se figur 1) om hvordan de gjennomfører sitt kvalitetssikringsarbeid.

Internrevisjonsstandardene stiller klare krav til kvalitetssikring (se figur 2). Jeg sitter imidlertid igjen med følelsen av at kvalitetssikring (QA) ikke bare utføres

fordi man må, men også fordi det gir en egen verdi til internrevisorer og ikke minst til våre interessenter (dvs. primært toppledelsen og styret). Dette er uttrykt slik av en av de virksomhetene «gjennom kvalitetssikring danner vi oss et mer helhetlig bilde av kvalitet og forbedringsområder på tvers av internrevisjonen. Det gir også verdi med et QA team med deltagere fra ulike revisjonsgrupper som kan sparre og komme med forbedringsforslag for å sikre en god og mer enhetlig etterlevelse av metodikkravene og kommunikasjon av resultater fra revisjoner.» En annen sier at «verdien kommer også frem i forbindelse med kommunikasjon til interessenter (styret, og ledelsen)».

Våre spørsmål var rettet mot to forskjellige aspekter av kvalitetssikringsarbeid:
1. Ved utførelse av revisjonsprosjekter
2. Ved periodiske gjennomganger

Disse omhandles i nærmere detalj nedenfor:

1. Ved utførelse av revisjonsprosjekter

Det er en generell enighet om at de mest kritiske faser der kvalitetssikring finner

Virksomhetens navn	Ansatte i internrevisjon	Ansatte i virksomheten	Type virksomhet
Universitetet i Oslo	5	7.000	Offentlig
BKK AS	2	1.100	Privat næringsliv
Statoil ASA	41 (derav 50% internrevisorer, 50% granskere)	20.500	Børsnotert
DNB Bank ASA	43	9.500	Børsnotert
NAV	16	14.000	Offentlig

Figur 1 Nøkkeltall for internrevisjonsavdelinger i denne undersøkelsen

sted i et revisjonsoppdrag er ved utferdigelse av oppdragsbeskrivelse og ved rapportering (både utkast og endelig rapport). En forteller at formålet med kvalitetssikring er todelt. Først å påse at metodikken følges og dernest at det er tilstrekkelig faglig nivå i revisjonen. Når det gjelder det siste punktet påpekes det at en viktig del av kvalitetssikringen er at avdelingen har kompetente revisorer og at det settes sammen team med revisorer og eksperter som passer til oppdraget.

Den som utfører den formelle kvalitetssikringen blir for de mindre organisasjoner gjerne revisjonsleder mens de større avdelingene har egne QA-ansvarlige, eventuelt kombinert med en som hare en rolle som fagansvarlig. Noen legger i tillegg vekt på at kvalitetssikring skal skje ved revisjonsgjennomføringen og ved oppfølging av revisjonsanbefalinger i etterkant. En mindre avdeling forteller at det benyttes innleide fageksperter til å sikre kvaliteten i prosjektet og sluttproduktet.

Det er flere som påpeker at det er viktig med egenevaluering av oppdraget også i revisjonsteamet. En av de mindre avdelingene forteller at det i ukentlige avdelingsmøter diskuteres åpent om utfordringer i revisjonsoppdragene og om det er fanget opp risikoer i det siste som kan ha betydning for pågående revisjonsarbeid.

Resultat av kvalitetssikringshandlinger kan også være integrert i internrevisjonavdelingens målbilde og KPI-oppfølging og således en integrert del av avdelingens forbedringsarbeid. Følgende 3 eksempler på slike KPI'er fikk vi fra en av avdelingene:

- leveringstid på rapporter
- andel oppfylt revisjonsplan
- tilbakemeldinger fra revidert enhet.

2. Ved periodiske gjennomganger

De fleste avdelinger forteller om at det foretas en årlig intern egenevaluering som består dels av egne erfaringer i oppdragene og dels av tilbakemeldinger fra de reviderte enheter. Sistnevnte er innhentet gjennom evalueringsskjemaer etter hvert fullførte oppdrag. I tillegg vil det også kunne gjennomføres en runde med samtaler med interessenter der temaet er måloppnåelse og forventninger. En av avdelingene bruker ressurser utenom avdelingen til å fasilitere en slik gjennomgang. En liten avdeling forteller at på grunn av avdelingens størrelse benyttes en ekstern konsulent til å intervjue interessenter og at resultatet av denne gjennomgangen blir lagt frem og diskutert med revisjonsutvalgets leder og konsernsjef.

Når det gjelder årlige faglige gjennomganger er det én større avdeling som forteller at det utføres av Kvalitetsansvarlig (egen rolle i internrevisjonen) som setter sammen et team på 3-4 seniormedarbeidere fra ulike revisjonsgrupper. I en av de andre avdelingene er det revisjonssjefen som gjennomfører kvalitetssikringen. I dette arbeidet er det fokus på at det er sammenheng gjennom hele revisjonsprosessen, dvs. «en rød tråd» gjennom oppdraget fra planlegging til endelig rapport.

Resultatet av kvalitetssikringsarbeidet blir som regel kommunisert tilbake til revisjonsavdelingen løpende slik at forbedringer kan iverksettes umiddelbart.

Det fortelles at utover det som har vært nevnt om tilbakemelding fra interessentene og faglige gjennomganger er en viktig del av kvalitetssikringen å sørge for den faglige utviklingen av medarbeiderne. Noen forteller i tillegg om at for hver medarbeider utarbeides et kompetanseprogram som følges opp regelmessig.

To av de som ble intervjuet peker i tillegg på at det hvert 5. år gjennomføres en ekstern evaluering av enheten med gjennomgang av utøvelsesstandardene. Ekstern evaluering var ikke et undersøkt tema i denne spørregjennomgangen men er et tydelig krav i standardene.

Konklusjon

Intern kvalitetssikring oppfattes som viktig i alle de forespurte revisjonsavdelinger. I de mindre organisasjoner er revisjonsleder direkte involvert mens de store har gjerne egne fagstillinger som bistår i dette arbeidet. Internrevisjonsavdelinger bruker også egne og eksterne evalueringer aktivt i sine forbedringsprosesser. Med bakgrunn i denne undersøkelsen tegnes det et bilde av at internrevisorer er flinkere enn skomakerens barn i å overføre sine kunnskaper til eget arbeid.

HVA SIER IPPF (IIAS INTERNREVISJONS-STANDARDER) OM KVALITETSSIKRING?

IPPF er tydelig på at kvalitetssikring er en grunnleggende og ufravikelig komponent i å drive en profesjonell internrevisjonsavdeling. Kravene er spesifisert i 1300-serien. Viktige momenter er:

- Det skal foreligge et ajourført program for kvalitetssikring og forbedringer som omfatter både interne og eksterne evalueringer (1300, 1310).
- Interne kvalitetssikring skal omfatte løpende oppfølging av arbeidet som presteres samt periodiske egenevalueringer (av andre enn de som er direkte ansvarlig for det revisjonsarbeidet som gjennomgås) (1311).
- Ekstern evalueringer må utføres minst en gang hvert femte år av en kvalifisert, uavhengig person eller et evalueringsteam utenfor organisasjonen (1312).
- Krav til rapportering til toppledelsen og styret om resultatet av den interne og eksterne kvalitetssikringen med avtalte handlingsplaner for å forbedre prosessen og i tilfeller der svakhetene i forhold til standardene er konstatert må disse rapporteres sammen med en redegjørelse for konsekvensene av disse mangler (1320, 1322).

Figur 2 Krav til kvalitetssikring

Nyopprettet internrevisjon i Politidirektoratet (POD)

INTERVJU MED
SIGMUND NORDHUS
Internrevisjonssjefen i den nyopprettede internrevisjonen i POD

Av
OLA OTTERDAL
Seniorrådgiver
Forsvarsdepartementet

> Vi har brukt mye tid, både internt i direktoratet og i etaten for øvrig, på å informere om internrevisjonens rolle og oppgaver.

I 2016 var Politi- og lensmannsetaten en av 23 statlige virksomheter som konkluderte ja på spørsmålet om å ta i bruk internrevisjon. Vi har intervjuet Sigmund Nordhus, internrevisjonssjefen i en av de største etatene som nylig har etablert internrevisjon.

Hvorfor ønsket du å bli internrevisjonssjef i POD?

Å lede internrevisjonen i politiet framsto for meg som en svært viktig og spennende jobb. Jeg har alltid hatt interesse for justissektoren. Under studietiden jobbet jeg på Ila Landsfengsel som fengselsbetjent og i tiden som seksjonsleder i Riksrevisjonen hadde jeg i en periode ansvaret for forvaltningsrevisjoner på Justis- og beredskapsdepartementets område, blant annet av Politiet. Politiet har et svært viktig samfunnsoppdrag knyttet til kriminalitetsbekjempelse, til forebygging og håndtering av anslag mot samfunnet, kriser og ulykker, samt opprettholdelse av den alminnelige ro og orden. Det er en kompleks organisasjon med et stort ansvarsområde og oppgaver som i stor grad skjer i samvirke med andre statlige aktører, kommunale etater, det sivile samfunn og internasjonale samarbeidsmyndigheter. Jobben som internrevisor i Politiet gir gode muligheter for faglig utvikling og til å bidra til forbedringsarbeidet i etaten.

Hvordan er internrevisjonen organisert og hvordan foregår rapporteringen?

Internrevisjonen er plassert i stab direkte under politidirektøren. Vi rapporterer også direkte til politidirektøren og det er direktøren som fastsetter budsjettet vårt. Ansvarsområdet vårt dekker hele politi- og lensmannsetaten, det vil si direktoratet, de 12 politidistriktene, Nasjonalt ID-senter og særorganene (Kripos, Økokrim, Politiets utlendingsenhet, UP, Politihøgskolen og Grensekommissariatet). Internrevisjonen har for tiden 6 medarbeidere.

Kan du si litt om hvordan dere har gått fram for å etablere internrevisjonsenheten?

I den første fasen av oppbyggingen av enheten har vi fått på plass en instruks for internrevisjonsfunksjonen og laget et rammeverk for alle de faglige og administrative prosessene i enheten. Vi har også rekruttert opp med medarbeidere med bred og variert erfaring fra revisjon og utredningsarbeid, slik at vi nå både har medarbeidere med politifaglig- og revisjonsfaglig bakgrunn. Og så har vi brukt mye tid, både internt i direktoratet og i etaten for øvrig, på å informere om internrevisjonens rolle og oppgaver. Dette har vært viktig for å skape forståelse for den jobben vi skal gjøre, samtidig som det har vært lærerikt for oss å bli bedre kjent med de forskjellige delene av etaten.

Senere har vi også gjennomført risikomøter i ulike deler av virksomheten og brukt dette som grunnlag for utforming av årets revisjonsplan. En mer systematisk metode for risikovurderinger er et av de områdene vi skal jobbe mer med fram mot neste års plan.

Hva slags strategi har du for internrevisjonsenheten i POD?

Vi skal være et kompetent fagmiljø som gir reell merverdi for etaten, utover ren

rapportering av funn og observasjoner. Vi ønsker å framstå som en proaktiv og serviceorientert enhet med fokus på kritiske risikoer og problemstillinger. Og vi skal bidra til å fremme kvalitetsforbedringer og nytenkning, både gjennom revisjon og rådgivning.

Det er viktig at vi besitter revisjonsfaglig kjernekompetanse og utvikler denne, men like viktig er det at vi forstår organisasjonen, interessentene og deres behov. Vi må være tett på ledelsen og på sentrale prosesser for å forstå risikoene organisasjonen står ovenfor. Som del av risikovurderingsprosessen og planarbeidet vårt, må vi ha bred dialog med de ulike delene av etaten for å sikre relevans og forankring. Videre må vi være i stand til å utnytte hele internrevisjonens mandat, som jo dekker både virksomhetsstyring, risikostyring og kontroll. Vi må tenke bredt når det gjelder å identifisere mulige revisjoner og vi må kunne bruke alle tilgjengelige metoder i revisors verktøykasse.

Internrevisjoner må også følges opp for at anbefalingene i rapportene skal gi effekt. Vi skal derfor ha et robust oppfølgingsregime hvor de anbefalingene politidirektøren slutter seg til «følges til døra», dvs. at revisjonen følges opp helt til anbefalingene er implementert.

Sist, men ikke minst: Politiets internrevisjon skal være en god, inkluderende og lærende arbeidsplass hvor medarbeiderne gleder seg til å komme på jobb hver dag!

Hva slags metoder vil dere benytte i revisjonsoppdragene?

Ambisjonen vår er at vi til enhver tid skal kunne benytte de metodene som er best egnet til å besvare problemstillingen i revisjonen – det er viktig at eventuell manglende kjennskap til metoder og verktøy ikke blir førende for den framgangsmåten som benyttes. Til sammen har vi også mye kompetanse og erfaring med bruk av ulike kvalitative og kvantitative metoder.

I praksis vil nok ulike kvalitative framgangsmåter, som intervjuer, spørrebrev, observasjon og dokumentanalyser benyttes i alle revisjonene våre. I tillegg vil nok analyser av statistikk, i form av uttrekk fra ulike fagsystemer osv., være en gjenganger. Men det er viktig at vi tilpasser

Kilde: Politidirektoratet

Følgende personer ses på fotografiet av de ansatte: Sittende: Sigmund Nordhus. Fra venstre (stående): Inger-Johanne Weidel, Anita Kleppe Sivertsen, Christian Winger Solvang, Knut Kværner og Eirin Fremstad.

> Generelt mener jeg det er viktig å benytte flere metoder for å belyse en og samme problemstilling, såkalt triangulering.

metodebruken til de temaene vi til enhver tid ser på; metodene for å sjekke etterlevelsen på et område vil kunne være veldig forskjellige fra metodene som er egnet til å studere produktivitet, årsaksforhold, eller effekter på organisasjons- eller brukernivå. Utviklingen av nye analyseverktøy og den teknologiske utviklingen gir oss også muligheter vi må kunne utnytte i revisjonssammenheng.

Generelt mener jeg det er viktig å benytte flere metoder for å belyse en og samme problemstilling, såkalt triangulering. Eksempelvis vil ensidig bruk av intervjudata i revisjoner ofte framstå som subjektive meningsytringer og revisjonsfunnene derved som anekdotiske. Revisjonsfunn som understøttes av statistiske analyser, dokumentanalyser, observasjon etc., styrker revisjonenes utsagnskraft.

Metode handler også om valg av fokus og omfang (scope) i revisjonene. Vi vil etterstrebe å gjennomføre revisjoner som omfatter hele etaten eller benytte metoder som gjør oss i stand til å generalisere funnene til hele etaten.

Hvordan blir fordelingen mellom bekreftelses- og rådgivningsoppdrag?

Ifølge instruksen vår skal rådgivningsoppdrag være planlagt og framgå av årsplanen. I årets plan har vi kun bekreftelsesoppdrag på programmet. Til neste år vil vi planlegge med noen rådgivningsoppdrag, i dialog med ulike deler av organisasjonen. På sikt vil nok rådgivningsoppdragene utgjøre en større del av porteføljen.

Hva slags forskjell kan en internrevisjon utgjøre i denne etaten?

Jeg tror internrevisjonen kan yte et viktig bidrag til forbedringsarbeidet i politi- og lensmannsetaten på mange områder.

Dette fordrer at vi er relevante og har oppmerksomhet på de viktigste risikoområdene innenfor sentrale deler av virksomhetens mål og strategier. Vi må levere rapporter som dekker hele etaten, som peker på årsakene til avvik og som gir realistiske anbefalinger. Indikasjoner på at vi skaper merverdi, vil vi få når oppfølgingen av revisjonene viser at anbefalingene følges, at interessentene våre er på linje med oss når det gjelder vurdering av risiko og at rådgivningen vår er etterspurt.

Hvordan ser dere for dere å samarbeide, koordinere og samordne arbeidet med andre miljøer for styring og kontroll intern og eksternt?

Riksrevisjonen jobber i mange tilfeller innenfor det samme området som internrevisjonen. Det er derfor viktig å holde seg orientert om deres arbeid. Jeg deltar på møtene Riksrevisjonen har med POD og vi holder Riksrevisjonen løpende orientert om våre aktiviteter.

Det er også mye å lære av andre fagmiljøer som jobber med tilsyn og kontroll, eksempelvis NSM som har utviklet mye god metode for sikkerhetsrevisjoner. Vi vil også delta aktivt i IIA- sammenheng og knytte oss til relevante faggrupper der. I tillegg har vi etablert kontakt med noen av politidirektoratene i de nordiske landene som i lengre tid har hatt egen internrevisjon.

Har dere noen tips til andre som skal etablere internrevisjon?

Å etablere en internrevisjonsinstruks som gir et tilstrekkelig mandat for internrevisjonsfunksjonen, er viktig. Likeså å sikre forankring og løpende kontakt med virksomhetsleder/direktør/styre. Det er etter min oppfatning også nødvendig å rekruttere medarbeidere med revisjonsbakgrunn, IIA-sertifiseringer etc. I tillegg kan medarbeidere som allerede jobber i virksomheten være verdt sin vekt i gull - de kjenner virksomheten og dens utfordringer. Jeg tror også det er viktig å bruke tid på gjøre seg godt kjent med virksomheten og å etablere et robust faglig rammeverk før man kaster seg inn i revisjonsoppgavene. Og, som tidligere nevnt: Etabler et solid oppfølgingsregime!

> Vi vil delta aktivt i IIA-sammenheng og knytte oss til relevante faggrupper der.

Kilde: Politidirektoratet

Klar for å gå av med pensjon!

INTERVJU MED
FRIDTHJOF RØER
Avtroppende internrevisjonsleder i Orkla ASA

Av
MARIT TRODAL
Projektleder IIA Norge

Vi tok en prat med avtroppende internrevisjonsleder Fridthjof Røer i Orkla ASA, for å få et tilbakeblikk på internrevisjonens utvikling.

Hvor lenge har du jobbet i Orkla?
Jeg overlater ansvaret til min etterfølger 1. november og er tilgjengelig for Orkla ut året. Jeg har ledet internrevisjonen i Orkla i 24 år. Før det var jeg 15 år som eksternrevisor i Arthur Andersen og et par år i AS Revision (i dag BDO). Jeg hadde forøvrig ingen planer om å bli internrevisor, men da jeg ble forespurt om å ta stillingen i Orkla ble fristelsen for stor. På den tiden hadde Orkla fusjonert først med Borregaard og så med Nora og Ringnes og var et av Norges mest spennende konsern.

Hvilke rapporteringslinjer hadde du som leder for internrevisjonen da?
Dette var før Corporate Governance ble en realitet, så jeg rapporterte til økonomidirektør, som rapporterte til stabssjef som satt i ledergruppen til daværende konsernsjef Jens P. Heyerdahl. På den tiden hadde jeg ingen rapporteringslinje til styret. Det stoppet hos konsernsjefen som var svært opptatt av bedriftskultur og som bad meg om at alle uregelmessigheter ble rapportert direkte til ham.

Kilde: Nikolai Polikanov

Hvordan har dere utviklet internrevisjonen over tid?
Da jeg overtok, drev internrevisjonen for det meste med finansiell revisjon for ekstern revisor da dette ga besparelser i revisjonshonorar. Da jeg begynte var vi 10 ansatte i avdelingen med varierende alder og bakgrunn. I årene som fulgte ble andelen finansiell revisjon bygget ned i takt med endringer i avdelingens personalmessige sammensetning og konsernets økende behov for prosjektstøtte. Samtidig økte kravene til ekstern revisors uavhengighet. Dette kulminerte med kritikk fra Finanstilsynet mot samarbeidsmodellen mellom ekstern og intern revisor i Orkla for året 2000. Ekstern revisor ble pålagt å gjøre mer arbeid uavhengig av internrevisjonens arbeid.

Hva har vært drivkreftene i Orkla for forandringer?
Da jeg ble ansatt var det et ønske om å få inn høy kompetanse i stillingen, og det var ikke så vanlig i internrevisjoner på den tiden. Hele revisjonsopplegget ble jo endret over tid, og det ble en klar endring da Corporate Governance ble et begrep. I 2002 fant administrasjonen og styret ut at min rolle burde gjøres mer uavhengig, så da endret man rapporteringslinjen fra økonomidirektør til stabssjef. Samtidig fikk jeg rett til å rapportere enkeltsaker direkte til styret etter eget skjønn.

Det var Finn Jebsen som var administrerende på denne tiden. Han var opptatt

av intern kontroll og etablerte et eget kontrollutvalg som bestod av nøkkelpersoner fra administrasjonen. Dette utvalget var forløperen til dagens revisjonsutvalg som styret besluttet å etablere i 2004. Jeg var sekretær for både kontrollutvalget og for revisjonsutvalget.

Hva har fungert bra og mindre bra?

Synet på og anseelsen til internrevisjon har egentlig bare blitt bedre og bedre. Jeg har lagt vekt på å ansette folk med høy kompetanse i avdelingen. Orkla er et internasjonalt konsern, så det er også viktig å få inn folk med ulik kulturbakgrunn og språkkunnskaper. Da Orkla i perioder fikk mer virksomhet i Polen, Kina og Russland, fikk jeg ansatt flinke folk med polsk, kinesisk og russisk bakgrunn. Vår avdeling ble i så måte nylig trukket frem som et godt eksempel i Orklas internmagasin, og det er jo hyggelig at det blir lagt merke til.

Er det noe du er spesielt stolt av å ha oppnådd her i Orkla?

Jeg er mest stolt av at internrevisjonen har fått et godt rykte internt i Orkla og at det er god forståelse for betydningen av intern kontroll. Vi blir stadig forespurt om å gi bistand og råd til organisasjonen.

Det sies jo i Orkla at du er intet mindre enn et levende oppslagsverk…

Internrevisjonen sitter sentralt plassert og har i sitt mandat tilgang til all intern informasjon. Så ja, jeg har kunnskap om mye historikk og mange transaksjoner. Det er i dag ca 250 legale enheter i Orkla, men jeg tipper at det i min periode til sammen har vært over 700 selskaper innom selskapslisten til Orkla. Det har vært utfordrende og spennende å skulle holde oversikten over et konsern i en slik utvikling.

Hva har du opplevd som mest frustrerende?

Orkla har i mange år vært basert på lokalt selvstyre, og da er det krevende å skulle etablere felles rammeverk for prosesser. Men vi har forsøkt å tilpasse vårt kontrollarbeid til den verdenen vi opererer i. Dette er i endring nå, ettersom Orkla har endret strategi under mottoet «One Orkla» som innebærer større samhandling på tvers av forretningsområder. Denne endringen er krevende, men fører mye godt med seg. Jeg opplever at Orkla er kjennetegnet av kvalitet i saksbehandlingen før endringer iverksettes, et godt eksempel er de ansattes involvering i utformingen av Orklas nye hovedkvarter som blir ferdig i 2019.

Kilde: Privat

Hvordan har du opplevd det å skulle være uavhengig i en virksomhet hvor du har vært så lenge og kjenner så mange?

Vi har et tydelig mandat for internrevisjonen med klare rapporteringslinjer og jeg føler trygg støtte hos revisjonsutvalg og styret. Vi har en ryddig konsernsjef med «åpen dør». Jeg føler ikke at uavhengighet har vært noe problem. Det er heller ingen ulempe å ha lang erfaring når man skal ivareta sin uavhengighet. Jeg har arbeidet under 6 ulike konsernsjefer i min tid, men kulturen i veggene er den samme. Jeg tror de som kommer inn i Orkla opplever at vi tar våre etiske retningslinjer alvorlig.

Hva skal du gjøre nå fremover?

Nå har jeg jobbet lenge, så nå skal jeg gjøre andre ting. Bruke tid på hobbyer og å holde meg i form. Så har jeg jo fått et barnebarn i sommer…

Kommer vi til å se deg i IIA-sammenheng?

Har ikke tenkt så mye på det. Men hvis noen ønsker å diskutere noe med meg er det bare å slå på tråden.

Artificial Intelligence – A New Disruptive Power for Early Adopters?

Av
ESA LEPORANTA
Systems Audit Manager,
Nets Branch Norway

Not too long ago, AI seemed a distant dream for especially interested researchers. Today it is all around us. We carry it in our pockets on a smartphone, it›s in our cars and in many of the web services we use throughout the day. The technology has now matured to a level where it, regardless of future progress in the field, is set to disrupt almost any technology based industry[1].

Where computer systems once had to be programmed to execute rigidly defined tasks, they can now be given a generalized strategy for learning, enabling them to adapt to new data inputs without being explicitly reprogrammed.

There is a focus on AI now because three elements have come together and created an inflexion point: computing power, sophisticated algorithms and vast amounts of data, says Matthew Davey, managing director, global head of business solutions, Société Générale Securities Services. As daunting as AI may seem for many banks, industry analyst Celent[2] believes that most institutions should be exploring at least the basic forms of AI, as it will have an impact on front, middle and back offices at banks[3]. According to Computer Sweden, banks have taken the lead in implementing virtual assistants. Increased competition between banks, customer benefits[4] and reduced costs[5] are mentioned as three main reasons for this development.

At JPMorgan Chase & Co., a learning machine is parsing financial deals that once kept legal teams busy for thousands of hours. The program, called COIN, for Contract Intelligence, does the mind-numbing job of interpreting commercial-loan agreements that, until the project went online in June, consumed 360,000 hours of work each year by lawyers and loan officers. The software reviews documents in seconds, is less error-prone and never asks for vacation. The internal systems at this NewYork-based bank, a hybrid from decades of mergers, had too many redundant software programs that didn't work together seamlessly. After visiting companies including Apple Inc. and Facebook Inc. three years ago to understand how their developers worked, the bank set out to create its own computing cloud called Gaia that went online last year[6].

> Most institutions should explore the basic forms of AI.

According to Casper von Koskull, President and Group CEO of Nordea, Nordea is working to create an efficient and scalable bank for the future by building capabilities and automating processes with support from close to 200 robots in production and having the first live chatbot with AI in Norway[7].

All this AI development came to the fore last year, when a program called AlphaGo beat the reigning human world champion at «go», an ancient Chinese board game considered to be one of the most complex pastimes man has ever devised. The game has remained as one of the hardest challenges for artificial intelligence because of the vast number of possible moves — more than the number of atoms in the universe — and the need to employ creativity to win. To crush 18-times

world champion Lee Sedol, AlphaGo trained the game for the equivalent of 3000 years[8]. Now, an even more superior competitor is in town. AlphaGo Zero has beaten AlphaGo 100-0 after training for just a fraction of the time needed by AlphaGo by playing against itself[9].

According to Microsoft's Bill Gates, humans should be worried about the threat posed by Artificial intelligence. His view has been backed up by the likes of Mr Musk and Professor Stephen Hawking, who have both warned about the possibility that AI could evolve to the point that it was beyond human control[10].

Artificial intelligence and other technologies will cause people «more pain than happiness» over the next three decades, according to Jack Ma, the chairman and founder of Alibaba. «Machines should only do what humans cannot,» he said. «Only in this way can we have the opportunities to keep machines as working partners with humans, rather than as replacements.» Even so, Ma acknowledged that in the future companies will likely be run by robots[11].

CTO of Fujitsu, Dr. Joseph Reger compares the future of artificial intelligence to the threat of nuclear weapons. In order to avoid nuclear weapons, there are international agreements, agreed policies and global control. «There are no such rules when looking at the machine learning and artificial intelligence.» «We need to discuss what this means for humanity, and agree on the rules of the game.»

The development of artificial intelligence is considered to be progressing exponentially in three stages. Now we are in the first phase, that is, in the narrow artificial intelligence phase. The computer can perform very simple tasks from large data streams faster and more accurately than a person. The second stage, which can go on for several decades, is about the level of general artificial intelligence.

> Machines should only do what humans cannot.

«Then the computer is performing better than any human being from almost any reasoning.» This stage of development is surely coming, but it is not sure whether it will last 20 or 30 years or longer. In the future, a third step is super AI. «At this point, the artificial intelligence performs better than humans in all computation and reasoning.» Dr. Reger says that the third stage means that artificial intelligence can itself create a new artificial intelligence. «Here, the computer begins to consider whether it needs more help from people.»

To avoid this, Dr. Reger says that everyone has to understand this topic as it will revolutionize all aspects of life. «This is how we have decided to work in Fujitsu.» We start training machine training and artificial intelligence in different forms at all levels of our organization, not just information management and managing director, as the phenomenon is connected to all digital developments[12].

Many industry experts are also concerned about the possibility of discriminatory practices that could come from using AI systems. For instance, Facebook's advertising mechanism allowed advertisers to exclude certain groups based on race, gender and other factors that are prohibited when advertising employment or housing; Facebook has since updated its system to prevent those advertisers from using those traits to target their advertising[13].

Artificial intelligence is revolutionizing the world as an industrial revolution, but it has a multiple impact, according to a Finnish start-up entrepreneur, economist Maria Ritola. «The exponential development of artificial intelligence changes the world just like electricity,» Ritola said in his speech at the European Commission Spring Seminar in 2017. «Everything is changing as a result of this development. It´s a cold fact.»

Ritola is a founding member of Iris AI, a small business organization, and belongs to a few Finnish AI operators. Founded in 2015, Iris AI has been selected as one of the ten most innovative companies in the world.

Established in Norway this London-based start-up has a big target: its founders want to promote the exploitation of science and solve the world´s major problems by means of artificial intelligence. Iris AI, which has accessed up to 30 million open source research papers, helps companies, start-ups, and researchers find research into new innovations. AI also offers incredible opportunities in addition to

1 The New Wave of Artificial Intelligence, Whitepaper, EVRY
2 https://www.celent.com/insights/940768915
3 http://www.bankingtech.com/1019722/artificial-intelligence-the-shape-of-things-to-come/
4 https://computersweden.idg.se/2.2683/1.676415/banker-leder-ai-bottar
5 http://www.bankingtech.com/1019722/artificial-intelligence-the-shape-of-things-to-come/
6 https://www.bloomberg.com/news/articles/2017-02-28/jpmorgan-marshals-an-army-of-developers-to-automate-high-finance
7 https://www.nordea.com/Images/33-230367/Nordea%20Transformation%202017-10-27.pdf
8 Talouselämä, 38/2017, Nokian Risto Siilasmaa opiskelee tekoälyä. Sinunkin pitäisi.
9 https://www.theregister.co.uk/2017/10/18/deepminds_latest_alphago_software_doesnt_need_human_data_to_win
10 www.bbc.com/news/31047780
11 https://www.theguardian.com/technology/2017/apr/24/alibaba-jack-ma-artificial-intelligence-more-pain-than-happiness
12 http://www.tekniikkatalous.fi/tekniikka/ict/fujitsu-johta-ja-varoittaa-tekoalyn-vaarosta-voi-olla-ihmiskunnan-kauhistuttavin-ase-6644724
13 https://www.paymentssource.com/news/simility-combines-3-d-secure-with-ai-in-new-version-of-is-e-commerce-fraud-platform

the threats, Ritola remarks. According to her, 3,000 research articles, over 60,000 books and 200,000 news articles are published every day. The amount of existing data is huge and no one can read and internalize more than a fraction of it.

«The positive news is that computing power is growing even faster than data, followed by an exponential curve, doubling its power every two years as shown by Moore´s law.» This computing power together with data creates the potential that we have not previously seen», she says[14].

A survey commissioned by the US authorities showed that 83 percent of low-paid workers could be replaced by machines. This applies primarily to jobs performing repetitive tasks, such as in fast food chains or warehouses. The occupations that will not be touched by AI, are the ones where people work with people, such as kindergarten teachers, psychologists and personal trainers[15].

Michael Chui, James Manyika and Mehdi Miremadi from McKinsey claim that automation will eliminate very few professions altogether, but will affect almost all jobs. In some cases, increased use of machines will not cause the number of tasks carried out by people to be reduced as a result of a rise in total demand[16].

Dagens Næringsliv, the Norwegian business publication, wrote this summer about a robot in the AF Group that will control every slate stone to the new National Museum. The robot is managed from an app and records inventories, orders and makes changes to such orders. According to Morten Grongstad, Group CEO of AF Gruppen, this innovation has given very clear benefits and he believes such measures are important for strengthening the competitiveness of Norwegian industry[17].

> Everyone has to understand this topic.

One of the world´s largest active investment funds[18], Man Group, has used AI since 2014. In 2015, artificial intelligence contributed to about half of the returns in one of Man Group›s largest funds, although AI only had control of a small proportion of the total assets. According to Nick Granger, who launched the testing of AI in Man Group, the structure and management of such systems are labour-intensive requiring the need for employees with new types of expertise for a long time to come[19].

Norwegian business leaders should read up on AI, because here´s money to earn, says Associate Professor Morten Goodwin in Norwegian School of Economics. According to Mr. Goodwin, AI is used much more often abroad. Companies like Facebook and Google use the technology to sort data. In Norway, data sets are smaller and it becomes more difficult to see the advantages of using AI[20].

For workers of the future, the ability to adapt their skills to the changing needs of the workplace will be critical. Lifelong learning must become the norm – and for the moment, the reality falls far short of the necessity[21]. IIA's paper, Artificial Intelligence – Considerations for the Profession of IA, strongly supports this view by stating that also internal auditors must understand IA basics by growing their competencies in several areas[22].

According to McKinsey[23], early evidence suggests that AI can deliver real value to serious adopters and can be a powerful force for disruption. AI's dependence on a digital foundation and the fact that it often must be trained on unique data mean that there are no shortcuts for firms. Early adopters are creating competitive advantages, and the gap to the laggards looks set to grow.

AI poses also some challenges, described among others by Edlich and Sohoni[24] and

> What information do you need to train your AI?

in a paper of Finextra[25], but the advantages look bigger. The chair of Nokia, Risto Siilasmaa, started to study artificial intelligence in the University of Stanford this summer. He suggests that we have a way to go until AI operates at the same intelligence levels as cats or human beings, but all companies should think what information it needs in the future to train its AI better than its competitors[26].

14 http://www.talouselama.fi/uutiset/suomalaisyrittaja-varoittaa-tekoaly-pyyhkaisee-suuremmalla-voimalla-kuin-teollinen-vallankumous-vaikutuksiltaan-3-000-kertainen-ilmio-6650301?_ga=2.77254805.1013179845.1495435805-1704214623.1485511675

15 Artificial Intelligence – er norske bedriftsledere klare?, NHH symposiet 22-23 mars. 2017

16 McKinsey Quarterly, Where machines could replace humans – and where they can't (yet), July 2016

17 DN, Stokk dum robot har stålkontroll på hver stein til Nasjonalmuseet, 9. juni 2017

18 http://nordic.businessinsider.com/here-are-the-11-top-dogss-of-the-hedge-fund-industry-2017-6?r=US&IR=T

19 Artificial Intelligence – er norske bedriftsledere klare?, NHH symposiet 22-23 mars. 2017

20 https://www.bloomberg.com/news/features/2017-09-27/the-massive-hedge-fund-betting-on-ai

21 Getting ready for the future of the work, McKinsey Quarterly, September 2017

22 The Institute of Internal Auditors, Artificial Intelligence – Considerations for the Profession of Internal Auditing, 2017.

23 McKinsey Global Institute, Discussion Paper, Artificial Intelligence The Next Digital Frontier?, June 2017

24 Burned by the bots: Why robotic automation is stumbling, Digital McKinsey, 24. May 2017

25 A research Paper from Finextra – The Next Big Wave: How financial institutions can stay ahead of the AI revolution, May 2017

26 Talouselämä, 38/2017, Nokian Risto Siilasmaa opiskelee tekoälyä. Sinunkin pitäisi.

Empowerment and challenges for the Internal Audit Function

The new Dutch Corporate Governance Code

BY
DRS. LASZLO NAGY,
EMIA RO

Laszlo is chief editor of Audit Magazine (IIA Netherlands). Laszlo is also a management consultant and boardroom advisor regarding internal audit, risk management, process management and business control. Laszlo is responsible for the business risk services team of Improven, a consulting firm.

One year ago, in December 2016, the Dutch Corporate Governance Code Monitoring Committee, chaired by Prof.dr. Jaap van Manen, published the revised Dutch Corporate Governance Code. This Code has been revised at the request of several Dutch institutions. Amongst them the trade unions CNV and FNV, representative of institutional investors Eumedion, stock exchange organization Euronext, association of stockholders VEB, association of securities-issuing companies VEUO and the representative for Dutch industries and employers VNO-NCW.

From a broad perspective, in the 'look and feel', the most important changes in the new Code are the central role of long-term value creation and the company culture as important components of effective corporate governance. The revised Code is not only a next step for good corporate governance, but is also changing the relevance and role of the Internal Audit Function (IAF).

History of the Code

The Dutch Corporate Governance Code ('the Code') was introduced in 2003 by the Committee, chaired by former Unilever CEO Morris Tabaksblat. The Code, formerly also known as 'the Tabaksblat Code', focused on the governance of listed companies. The Code contains both principles and best practice provisions for the relation between the management board, the supervisory board and the shareholders of the listed company. The principles achieved broad acceptance and helped develop attitudes and minimum standards for good corporate governance.

Compliance with the Code is in accordance with the 'apply or explain' principle. Companies should in essence apply the principles and best practice provisions of the Code, however companies may deviate from these. In such case, they are expected to provide sound explanation for any non-compliance or non-application of a provision. According to Dutch law information on compliance with the Code should form part of the annual report of the company. This gives current and future shareholders the opportunity to have insight into the company´s functioning and actions.

The original Code was adopted in 2003 by the Tabaksblat Committee, and later, in December 2008, amended by the Frijns Committee. In 2016 the Code was revised by the Van Manen Committee. According to Dutch law listed companies are required to report on compliance with the revised Code as of the 2017 financial year.

The Van Manen Committee found several reasons to make necessary revisions to the Code. An important reason was that even though most listed companies had complied with the Code, since the start of the original Code in 2003 there had been many adverse incidents in these companies, such as financial fraud and bankruptcies. The chairman Van Manen stated his view that many of these incidents were based on the pursuit of short-term profits resulting in long-term problems and weak business models. Additionally, the Van Manen Committee concluded that the Code had become more a topic for legal experts instead of for boards and shareholders. That was also the reason that the Van Manen Committee held a broad consultation with existing and new stakeholders; not only with the original advising partners, but for instance with all involved listed companies

and several professional organizations such as the institutes for chartered accountants and internal auditors. The goal was to gain broad insight into existing problems, challenges and possible solutions and best practices.

The revised Code and the Internal Audit Function

Since the start of the Code in 2003, the Internal Audit Function has a role in the Code. In the original Code principle V.3 stated: «The internal accountant has an important role in assessing the companies' risk and control system.» The corresponding best practice was that the external (statutory) auditor and the Audit Committee are involved in both the planning and the outcomes of the internal audits. In that period, the Code's focus for the Internal Audit Function was more on financial reporting and control.

In the revised 2008-Code, the Internal Audit Function was more empowered due to the latest best practices and it was stated that:

- The Internal Audit Function has direct access to the chairman of the Audit Committee and the external (statutory) auditor; and

- If the company does not have an Internal Audit Function, the Audit Committee is required to evaluate annually whether there is still no necessity to have an Internal Audit Function. This evaluation should be part of the Supervisory Board's report to shareholders (annual report).

However changes were made to the Code, Internal Audit did not have the formal role and importance it would become with the revised 2016-Code. The focus was still more on financial reporting risks and absence of an Internal Audit Function within a company could still be substantiated with economic reasons, such as the limited size of the company.

In the revised 2016-Code, Internal Audit Function's role has been revised as well. Instead of a more reactive and more financial reporting and control oriented internal audit function, it has shifted into a more active and a strategy and operations oriented assurance and consulting function. As stated in principle 1.3 (Internal Audit Function) of the revised Code: «The duty of the internal audit function is to assess the design and the operation of the internal risk management and control systems. The management board is responsible for the internal audit function. The supervisory board oversees the internal audit function and maintains regular contact with the person fulfilling this function.»

Within this principle, several important statements are made:

- Companies are expected to have an internal risk management and control system;

- These systems need to be assessed;

- Internal audit has the role of assessing these risk management and control systems;

- Internal audit is in direct contact with both the management board and the supervisory board.

Regarding the risk management and control system, the revised Code follows the Committee's focus on long-term value creation and the company culture as important components of effective corporate governance. These elements are also addressed in the principles regarding risk management:

- Principle 1.2 Risk Management: «The company should have adequate internal risk management and control systems in place. The management board is responsible for identifying and managing the risks associated with the company's strategy and activities.»

- Principle 1.2.1 Risk Assessment: «The management board should identify and analyse the risks associated with the strategy and activities of the company and its affiliated enterprise. It is responsible for establishing the risk appetite, and also the measures that are put in place in order to counter the risks being taken.»

- Principle 1.2.2 Implementation: «Based on the risk assessment, the management board should design, implement and maintain adequate internal risk management and control systems. To the extent relevant, these systems should be integrated into the work processes within the company and its affiliated enterprises, and should be familiar to those whose work they are relevant to.»

- Principle 1.2.3 Monitoring of effectiveness: «The management board should monitor the operation of the internal risk management and control systems and should carry out a systematic assessment of their design and effectiveness at least once a year. This monitoring should cover all material control measures relating to strategic, operational, compliance and reporting risks. Attention should be given to observed weaknesses, instances of misconduct and irregularities, indications from whistleblowers, lessons learned and findings from the internal audit function and the external auditor. Where necessary, improvements should be made to internal risk management and control systems.»

As mentioned before, the Internal Audit Function has an important and mandatory role in the risk management process of the company. Regarding the functioning of the Internal Audit Function, the Code also includes the following principles:

- Principle 1.3.1 Appointment and dismissal: «The management board both appoints and dismisses the senior internal auditor. Both the appointment and the dismissal of the senior internal auditor should be submitted to the supervisory board for approval, along with the recommendation issued by the audit committee.»

- Principles 1.3.2 Assessment of the internal audit function: «The management board should assess the way in which the internal audit function fulfils its responsibility annually, taking into account the audit committee's opinion.»

- Principle 1.3.3 Internal audit plan: «The internal audit function should draw up an audit plan, involving the management board, the audit committee and the external auditor in this process. The audit plan should be submitted to the management board, and then to the supervisory board, for approval. In this internal audit plan, attention should be paid to the interaction with the external auditor.»

- Principle 1.3.4 Performance of work: «The internal audit function should have sufficient resources to execute the internal audit plan and have access to information that is important for the performance of its work. The internal audit function should have direct access to the

audit committee and the external auditor. Records should be kept of how the audit committee is informed by the internal audit function.»

- Principle 1.3.5 Reports of findings: «The internal audit function should report its audit results to the management board and the essence of its audit results to the audit committee and should inform the external auditor. The research findings of the internal audit function should, at least, include the following:

- i. any flaws in the effectiveness of the internal risk management and control systems;
- ii. any findings and observations with a material impact on the risk profile of the company and its affiliated enterprise; and
- iii. any failings in the follow-up of recommendations made by the internal audit function.»

- Principle 1.3.6 Absence of an internal audit department: «If there is no separate department for the internal audit function, the supervisory board will assess annually whether adequate alternative measures have been taken, partly on the basis of a recommendation issued by the audit committee, and will consider whether it is necessary to establish an internal audit department. The supervisory board should include the conclusions, along with any resulting recommendations and alternative measures, in the report of the supervisory board.»

The Internal Audit Function: empowerment and challenges

The revised Code includes both empowerment and challenges for the Internal Audit Function. On the one side, due to the formal inclusion of Internal Audit's role in the Code, companies need to comply with the principles. As Committee chairman Van Manen stated: «If with the revised Code companies do not have a well-functioning Internal Audit Function, they really have something to explain to their shareholders». Empowerment is not only because of the inclusion of Internal Audit in the Code, but more because of:

- Internal Audit's role in the organization-wide risk management. From strategy to operation;
- Internal Audit's link with both the management board and the supervisory board;
- Internal Audit's interaction with the external auditor, in which each party has its own special role.

These empowerment factors are not only helping, but also challenging the Internal Audit Function. The function must be well-staffed, innovative, communicative and able to meet the companies' needs and long-term requirements to provide both assurance and advice to the Board regarding the long-term value creation and strengthening of the company culture. Instead of focusing on short term financial control, Internal Audit should focus on the company's strategic risks, risk appetite and corresponding level of control in line with company's risk appetite. It must focus also on the culture of the company, for instance in the use of soft controls.

These changes will challenge not only the company, buts also the Internal Audit Function and its auditors. This is also what the message is conveyed by the Dutch IIA chapter (IIA Netherland). Many years ago, IIA Netherland's Board started an 'Advocacy' process in which IIA started to actively inform relevant stakeholders about the role of the Internal Audit Function and current best practices and developments. IIA Board members had meetings with stakeholders such as the Dutch Corporate Governance Code Monitoring Committee, management and supervisory board members of listed companies and representatives of relevant Dutch institutions, such as the advising parties to the Monitoring Committee. In these meetings stakeholders not only affirmed the past achievements of the Internal Audit Function, but also emphasized the necessity for a continuous improvement.

In the end it resulted in the inclusion of the Internal Audit Function in the revised Code, as described above. As Committee Chairman Jaap van Manen stated: «Our Committee spoke to many representatives of many organizations, amongst them also IIA Netherland. Many representatives emphasized the great importance of their organization and profession. But I have a simple rule: I believe an organization or profession is really that important if not they themselves, but relevant stakeholders, like supervisory board members, say they are important. That's why the Internal Audit Function has the formal role as described in the revised Code». On the other hand, Van Manen had a warning too: «The Internal Auditors managed to convince relevant stakeholders of the importance and quality they have and the added value they can bring into the strategic development of the companies they work for. But 'noblesse oblige': you will have to meet continuously the expectations you made and provide the expected added value.»

The conclusion is that the revised Code empowers the Internal Audit Function and allows it to make a big next step towards adding more value to companies, their boards and stakeholders. But internal auditors cannot sit and wait, they meet new challenges. They and their professional organization, the IIA, need to be constantly taking further steps in meeting the expectations and challenges by continuously strengthening the knowledge and skills of internal auditors.

You can find the Dutch Corporate Governance Code and other documents (partly in English) on the website of the Monitoring Committee (www.mccg.nl) and IIA Netherlands (www.iia.nl).

Contact information: https://www.linkedin.com/in/laszlo-nagy-44735a4/

GRC - hva rører seg?

Risiko- og compliancenettverkene i IIA Norge arrangerte i oktober et seminar med fokus på Governance, Risk og Compliance (GRC). Hvordan jobber virksomheter med disse prosessene? Hvilke trender ser vi?

Av
MARIT TRODAL
Projektleder IIA Norge

Stian Sviggum fra PWC innledet dagen med å definere begrepene innenfor GRC. Det er viktig at alle fagmiljøene som jobber innenfor de ulike områdene har en felles forståelse av begrepene. Stian hevder at Enterprise Risk Management bør være 'hub' for de som jobber med virksomhetsstyring, risiko og compliance. **God risikostyring er en forutsetning som må legges til grunn for alt arbeid med virksomhetsstyring. En utfordring mange står ovenfor er å skape en helhetlig tilnærming hvor man unngår interne siloer.** Slike siloer kjennetegnes av at de som jobber mer eller mindre isolert med sitt og rapporterer hver for seg og regelmessig opp til ledelse og styret. Det kan være krevende for ledelsen og styret og skulle håndtere informasjon fra både risikostyring, compliance og andre stabsenheter som berører de ulike temaene. Det ender ofte opp med at ledelsen noe forenklet sagt må sammenligne pærer, bananer og hvitevarer. Globalt ser man nå en gryende trend i retning av at man samler GRC-relaterte stabsfunksjoner i en «virksomhetsstyringsstab» direkte under CEO. En slik organisering skal bidra til en helhetlig tilnærming til GRC – både på strategisk nivå og på tvers av organisasjonen. Man ser også eksempler på at noen styrer ønsker å etablere en stilling av typen Chief Risk Officer som en motvekt til CEO og på samme nivå i organisasjonen.

Seminaret bestod også av flere eksempler på hvordan Aker Solutions, Yara og Multiconsult utøver sitt arbeid med compliance og hvilke typer compliance risiko de ulike virksomhetene har fokus på. I Aker har man fokus på risikoer knyttet til internasjonale sanksjoner, anti-korrupsjon, leverandørkjede og menneskerettigheter. Fokuset er å sikre at compliance risiko blir vurdert i prosjektets tidligfase, samtidig som beslutninger knyttet til hvorvidt virksomheten skal gå inn i risikoområder vektlegges av førstelinjen. Dette arbeidet må balanseres ved

Kilde: www.classic-castle.com

at compliance ikke kan si 'nei' til alt, spesielt når markedet er dårlig. Compliancefunksjonen i Aker Solutions jobber derfor mye med risikoreduserende tiltak for å finne et riktig balansepunkt mellom compliance risiko og kommersielle muligheter.

I Yara har compliance-arbeidet fått ny giv med ny CEO og styre. Da selskapet lanserte sin nye Etikkhåndbok for alle ansatte i Yara, hadde CEO egenhendig signert alle 15000 eksemplarer. Yara har i likhet med mange andre etablert en varslingsportal og opplever en økning i antall henvendelser og varsler som blir registrert. Dette vitner om sterkere bevissthet internt rundt korrupsjonsutfordringer. Yara har også hatt et økt fokus på å redusere risiko knyttet til logistikk og transaksjoner i leverandørkjeden. De har blant annet i samarbeid med andre aktører i 'The Maritime Anti-Corruption Network' kartlagt problemområder i en rekke havner, og jobbet systematisk med å få bukt med krav om tilretteleggingsbetalinger.

Multiconsult er i stor grad en norskbasert virksomhet, som med økte internasjonale ambisjoner vil få et endret risikobilde. Complianceavdelingen har fokus på å bygge bevissthet i førstelinjen om hvilke premisser som skal legges til grunn for selskapets kommersielle og strategiske vurderinger. Multiconsult jobber målrettet for å sikre at lokal ledelse og nøkkelroller i organisasjonen vurderer alle mulige risikoer når beslutninger fattes. Oppdragsgivere som Verdensbanken og andre internasjonale aktører forventer transparens og etterrettelighet fra sine leverandører.

Ingrid Årstad fra Statens Petroleumstilsyn har forsket på forebygging av storulykker og hvilke mekanismer som ligger til grunn. En storulykke består av en rekke ulike risikobidrag. Tradisjonelt har petroleumsbransjen en tendens til å se for snevert på de bakenforliggende årsakssammenhengene. Ingrid påpeker at man innen olje- og gassnæringen har en tendens til å koble risiko opp mot KPIer, men man må også vurdere hva disse KPIene ikke sier noe om. Hva faller mellom stoler? Hvordan sikrer man at man får frem alle perspektiver på risiko og at ekspertisen ute i organisasjonen blir inkludert? Årstad benyttet en modell av en ku for å illustrere at vår tilnærming til risiko aldri blir så levende som en ordentlig ku.

«Vi kan forsøke å lage en kompleks modell av noe som er tilnærmet likt en ku, men den er til syvende og sist bare en modell.»

Risikopersepsjon sier noe om at folk opplever risiko forskjellig. Det som er akseptabel risiko for en leder kan være totalt uakseptabelt for et styremedlem. Dette er også et element som må inn i risikostyringen. Ayse Nordal fra Undervisningsbygg beskrev hvordan ulike tilnærminger til risikobegrepet kan påvirke virksomheters arbeid med risikostyring, og poengterte blant annet hvor viktig det er å integrere risikotenkningen i planleggingsfasen og i beslutningene. Vi må følge med på hva førstelinjen gjør, slik at de som jobber i 2. linjen kan bidra med relevante råd i et stadig mer komplekst verdensbilde. Her kan man også spørre seg om hvordan 2. linjen best skal organisere seg og om uavhengighet fra 1. linjen er veien å gå fremover. Etter over 20 år innen compliance i bank og finans er ikke Frede Rognlien i SEB overbevist om at den uavhengigheten som 'three lines of defence'-modellen foreskriver er løsningen. Kanskje er ikke 'defence' den beste betegnelsen i en tid hvor virksomheter må være mer proaktive og se muligheter.

Pål Fure, CEO i Dentsu Aegis Network Norden og anerkjent trendforsker og analytiker – satte til slutt skapet på plass: Er du en virksomhet i dag så er den enten en start-up eller en turnaround. Styret må forstå digitaliseringen som nå foregår og hvilke sentrale trender vi ser. Det trengs mer fokus på innovasjon, og denne må sitte tett på førstelinjen. «Jeg vil bli grenseløst urolig om det havner i stab», uttrykte Fure. Det som er viktig for funksjoner som compliance, risiko og -virksomhetsstyring er å bli mer agile. Han har tro på en 'compliance bonanza' i fremtiden, men ikke nødvendigvis slik vi kjenner den per i dag. Informasjon må tilflyte beslutningstakere mye raskere. Skap noe nytt! Reset organisasjonen. Et eksempel kan være General Data Protection Act, som alle nå skal forholde seg til og jobber med å være klare til å implementere innen 25. mai 2018. Hvor mange har fokus på det som skjer rundt neste sving? Hva med alle mulighetene denne lovgivningen også åpner opp for?

Noe å tenke på inn i 2018…

Det var en gang

SIRK har, som profesjonen internrevisjon, endret seg over tid, og da kan det være interessant og artig å ta en titt i bakspeilet for å se hvor vi har vært.

FOR 20 ÅR SIDEN

IT-revisjon

«Internrevisor må inn i IT-verdenen for fullt» lyder oppmuntring fra Unni Leivestad, revisjonssjef i Toll- og avgiftsdirektoratet. «Vi må skaffe oss kompetanse på dette området som er blitt svært sentralt i hverdagen.» Hun sier videre at «i dagens samfunn inngår IT som en integrert del av den ordinære virksomhet.» Hun forteller om erfaring fra å ha gjennomført en revisjon av et stort IT-Prosjekt i direktoratet.

Jeg tenker at det er ikke mindre aktuelt at alle som jobber i internrevisjon i dag også må besitte IT-revisjonskompetanse, eller?

Personvern

Under overskriften «Verdt å vite» opplyses det om lovforslag (NOU 1997:19) om «et bedre personvern». Behovet for en lov som skal erstatte Personregisterloven forklares å stamme «fra teknologisk utvikling som stadig åpner for nye muligheter til å innsamle, bearbeide og bruke personopplysninger, og dels Norges forpliktelser til å gjennomføre et EF- direktiv».

Den gamle personvernloven var banebrytende og førte til fremveksten av et Datatilsyn med tenner. I dag står vi ovenfor innføring i 2018 av en EU-forordningen GDPR (General Data Protection Regulation) som stiller forsterkede ansvar for et godt internkontrollregime internt hos bedrifter og fastsetter muligheter for myndigheter til å gi bøter som svir.

FOR 40 ÅR SIDEN

Automatisk regnskapsføring

Bankrevisoren trykker i sin helhet rundskriv nr. 13/76 fra Bankinspeksjonen (nå Finanstilsynet). Rundskrivets overskrift er «Forskrifter om løsblad og film». Det tillates for første gang at man kan benytte løsblad, definert som «løse kort, blad eller lister» i sin regnskapsføring og videre at «den maskinelle behandling kan være mer eller mindre automatisk (programstyrt) med bruk av mekanisk, elektromekanisk eller elektronisk utstyr».

Det er nå utenkelig at det finnes annen måte å føre en banks regnskap på enn elektronisk, men den gang var dette et gjennombrudd. Det stilles forutsetninger for å kunne bruke automatisk bokføring som f.eks «beskrivelse av behandlingsreglene, illustrert ved systemkart, programbeskrivelse, kjøreinstrukser, brukerhåndbøker og posteringsinstrukser». Men for langt skulle man ikke gå i bruk av automatisering. Det ble fortsatt stilt krav til at «det skal føres en innbundet hovedbok og en innbundet årsregnskapsbok». Det tar tid å endre vaner…..

Martin Stevens

Find the truth early and reconcile ourselves with it

A Realistic Alternative to Zero Tolerance

BY
NIGEL KRISHNA IYER

Nigel has over 20 years' experience investigating and detecting fraud and corruption. A computer scientist and qualified chartered accountant Nigel soon found that his true passion lay in rooting out corruption and fraud. Nigel is also today a qualified dramatist and has written a number of films and plays based on his experiences, many of which are used in teaching worldwide. He has written several books and papers, and teaches widely how to defend organisations against the «commercial dark arts». He is also a fellow of the University of Leicester School of Business.

Zero tolerance or truth and reconciliation

Seven years ago I made a short film called «Fraud and Corruption – Forgiveness and Compassion,» (see https://www.youtube.com/watch?v=UYEfReo7Y6c) which was based on a true story and demonstrated how we often treat the symptoms of corruption and fraud. We tend to «throw the book at» the few people that we catch, but because it is hard to investigate complex cases, the big cheaters often get away and the root causes remain unresolved.

Three years ago, in Johannesburg, South Africa I held a short session for around 2,500 people on how pro-active investigation, coupled with a liberal dose of understanding and forgiveness, motivates people to speak up, thereby tackling the epidemic problem of fraud and waste in social-upliftment programs. Just before I spoke, the Minister of Trade, Mr Bob Davies, read a short speech where he reiterated the policy of «zero tolerance» saying that his government would show «no mercy» when it came to cases of suspected corruption and fraud. I met Bob briefly afterwards and he seemed like a very pleasant chap, but I was left shocked and wondering whether Mr. Davies's speechwriter was even born in time to witness the success of Nelson Mandela's Truth and Reconciliation committee and one of the most famous examples ever of restorative justice in our times. (And imagine the reaction of Bob's children if he came home one day and announced that from now on he would show no mercy and absolutely zero tolerance to any misdemeanours and wrongdoings in his own family)?

> Our policy is «zero tolerance» - the government would show «no mercy»
>
> *- Bob Davies, Minister of Trade, South Africa (2014)*

A blame culture

Let's face it: fraud and corruption is all around us. Surely if we are so heavy handed with the few «sinners» that we catch, won't the large majority who did not get caught breath a huge sigh of relief and just try even harder to stay hidden? And what does our no mercy, intolerant stance say to the people who are caught? Won't they feel hard done by, unlucky or in most cases bitter?

Whether it's a new scapegoat the media has in its sights, or some more fallout from the «Panama Papers,» I feel that we are becoming an intolerant, dispassionate society where there is less and less room for people to stand up and admit they are wrong. Even though we know that there are hundreds of examples out there, we carry on pointing the finger at scapegoats…. because it is safe to do that.

Knowledge of Dirty Money

Take the example of this real «post Panama-Papers» dilemma which came to my attention: A CEO is under pressure because it is discovered that his company has been dealing with customers who have accounts and shell companies in one or more of the Dirty Money Centres (my name for tax havens when they are misused).

With the help of his PR and legal advisors he manages to defend himself admirably in the media both accepting full responsibility for not having done more and for not being more aware, but at the same time raising the understandable issue: «How could I possibly know everything that goes on in a company as large as this?» Had this same CEO forgotten that many years ago– albeit in a former life and in a much more junior position – he was rather involved and instrumental

> «An eye for an eye will make the whole world blind"
>
> *– Mahatma Gandhi*

in sending money to so-called Dirty Money Centres? The purpose of the money was defined as «finder's fees», «commissions» and facilitation payments which he now knows have been the subject of media investigations into bribery and corruption involving a number of countries. Of course, he was only carrying out the orders of his superiors…and he never took any money for himself, but with hindsight he feels that he behaved rather naively at that time.

But the question remains: What should he do now?

If he genuinely wants to lie flat and «bare all» he feels he must talk openly about his past experiences. But on the other hand, today's intolerant society would crucify him and a scandal-hungry media would have a field day. So, he does as many of us do and hopes that the past stays hidden. In an ideal world, our CEO would be able «come clean» and admit his mistakes even more fully, earning respect for this action, and encouraging other executives who feel trapped by similar circumstances to also step forward and talk about their past experiences and what we can all learn from them. But to get closer to this ideal world we all need to invoke those human traits in us called forgiveness and compassion, and turn the zero-tolerance down (for a while at least). Owning up to our mistakes

As Gandhi once said, «An eye for an eye will make the whole world blind.» When it comes to how much corruption and fraud is costing the world today, I believe that we are blind already. The word «truth» (or veritas) is used much in the legal world and «reconciliation» also describes an accounting tool used to show that money is in agreement.

Surely, we want societies where people are allowed to tell the truth, societies where people are encouraged to own up to their mistakes, so that we can reconcile the money to where it should really have gone? For this to happen we need to think afresh. We need new ways to deal with fraud and corruption. Ways that actually work.

Where do we go from here?

Fresh ideas need fertile soil in which to germinate and this implies a new mindset. The starting point should in my view be based on:

- A recognition that fraud and corruption amounts to an unnecessary cost which, if we thought collectively (rather than individually) we would all prefer to avoid. - In other words, finding fraud early needs to be seen as «good news» rather than a shock. But this also means that we need to all work together and avoid playing the «blame game».
- Wanting less whistleblowers rather than more because we have a reinvigorated belief that, by working together, people can detect fraud and corruption early and deal with it calmly, efficiently and (unfortunately for the media) in a rather unspectacular way

> «You will achieve more in this world through acts of mercy than you will through acts of retribution.»
>
> *– Nelson Mandela*

A final realisation is that we have to stop relying on others like police, the media, regulators, external auditors (or the whistleblower who incidentally may never turn up) to find fraud. - Even if we don't know it as yet, the tools and techniques to find fraud before it finds you are available to us all. As we enter a new and more democratic age - everyone can today find fraud and corruption, remembering that it at the same time pays to show as much forgiveness and compassion as we can.

KURS

Hvor?: Aker Solutions, Fornebu - Møterom Engineerium
Når?: 31.01.2018, kl. 09:00 - 17:00
Tittel: Hvordan oppdage korrupsjon, svindel og misligheter – raskt og tidlig? På denne dagen vil du lære hvordan man oppdager røde flagg, bidrar til å spare penger og unngår dyre og komplekse granskninger. Ved bruk av praktiske case eksempler, realistiske dokumenter, scenarioer, m.m. får dere en verktøykasse som kan brukes umiddelbart.

Kurset dekker:

- Teknikker og metoder for å identifisere når leverandører og kunder utnytter deg.
- Hvordan avsløre agenter, mellommenn, konsulenter og til og med ansatte som tar mer betalt enn de har rett til.
- Avtaler med frontselskaper og skitne penger, falsk rapportering, regnskapssvindel, interessekonflikter og andre former for uetisk adferd.
- Hvordan oppdage røde flagg ved intervjuer og «think like a thief»-metodikk.
- Gjennomgåelse av en metode for å raskt identifisere nøkkelinformasjon for effektiv gransking.
- Hvordan utvikle egne strukturerte tester for å oppdage røde flagg.
- Praktiske løsninger for å håndtere skader og gjenoppbygge tillit kostnadseffektivt, etter mislighet og korrupsjon.
- Hvilke fordeler det gir å samarbeide internt for å motvirke misligheter og korrupsjon (omdømme, interne kontroller og kultur).

Foredragsholdere:
Kurset holdes av Veronica Morino og Nigel Iyer som begge har lang erfaring fra utredning av både misligheter og korrupsjon. De har utviklet 'B4' over flere år: en fem-stegs metode der målet er «Find Fraud B4 it Finds You».

Kursavgift:
- Ordinært: kr. 3 700,-
- Medlemmer: kr. 3 200,-

Påmelding: IIA Norge, www.iia.no/aktiviteter

Begeistring gjennom tjeneste-design i Lånekassen

Av
OLA OTTERDAL
Seniorrådgiver,
Forsvarsdepartementet

Tjenestedesign er et tankesett eller en metode som handler om å få organisasjoner til å sette kunden eller brukeren i sentrum og å levere helhetlige og meningsfylte tjenester til brukerne. Tankesettet er ikke nytt, men det har fått et oppsving de siste par årene. Metoden har et stort potensiale i å bidra til innovasjon, effektivisering, forenkling av interne prosesser, og, ikke minst, i å skape gode brukeropplevelser. Når en virksomhet anvender tjenestedesign på en god måte, får kundene bedre og enklere tjenester og organisasjonen sparer penger. To fluer i en smekk!

Metoden har stor relevans i offentlig sektor. Skattebetalernes penger skal brukes effektivt og etterspørselen etter tjenester av god kvalitet øker. Behov for samordning og fokuset på digitalisering gjør også metoden mer aktuell enn før. Metoden kan gi viktige bidrag til å oppnå effekter for brukere og samfunn på en kostnadseffektiv måte. Det finnes mange gode eksempler på vellykkede tjenestedesignprosjekter – på sykehus og sykehjem, på legevakter, i kommuner, i Skatteetaten, i privat sektor. You name it! Difi fikk i 2015 i oppgave å øke statlige virksomheters innovasjonsevne, blant annet ved hjelp av denne metoden. Kommunenes Sentralforbund kom omtrent samtidig med en praktisk guide for hvordan kommuner og fylkeskommuner kan jobbe med denne metoden for å gi bedre tjenester. Denne artikkelen løfter frem Lånekassen som suksesshistorie på å bruke og dra nytte av tjenestedesign.

Tjenestedesign er midt i blinken for Lånekassen

Tjenestedesign har et bredt nedslagsfelt og kan være fornuftig å bruke for mange typer virksomheter. Men Lånekassen er en nærmest perfekt virksomhet å anvende metoden på. Virksomheten har jobbet over mange år med å videreutvikle digitale tjenester og er per i dag i praksis en heldigital virksomhet. 99 % av de over en million kundene har digital dialog med Lånekassen. Lånekassen mottar 830 000 søknader hvert år og de aller fleste sendes elektronisk. Lanekassen.no har omtrent 7,2 millioner besøk hvert år. Kundene har også et langt livsløp eller kundeforhold til Lånekassen. Med slike volum kan virksomheten forsvare å bruke noen kroner på tjenestedesign og å lage gode kundereiser for sine mange kunder.

«Kundene er opptatte av at ting er lette å finne, lette å forstå og lette å få til. Da må vi tenke tjenester og tjenestekjeder fra kundens ståsted. Vi ønsket å bruke en enhetlig metodikk i prosessene som hele virksomheten kjenner til, og som setter forventninger og krav til helhetlig tenkning i planlegging og utforming av systemer og tjenester», sier kommunikasjonsdirektør i Lånekassen Anne-Berit Herstad.

Lånekassens «tjenestereise-reise»

Lånekassen er blant de mest modne virksomhetene på tjenestedesign i det offentlige og har gjort tjenestedesign til en strategisk satsning. Virksomheten kjøpte konsulenthjelp for å få fart på dette for 2-3 år siden, men besluttet da å bygge opp kompetansen internt. 5 medarbeidere – 2 fra kommunikasjonsseksjonen, 2 fra utviklingsavdelingen og 1 fra IT-avdelingen fikk opplæring og har jobbet med dette siden. Siden man jobbet ganske bredt med dette, så man også behov for å få til en forankring i toppledelsen. I januar 2016 vedtok ledelsen et Metodedirektiv for tjenestereise og det er også utarbeidet et eget målbilde for systemene ut mot kundene. I tillegg er det utarbeidet en egen sjekkliste for de som skal benytte metoden. Som i annet utviklingsarbeid i Lånekassen, ble det stilt krav om å estimere gevinster gjennom en egen gevinstplan. Bedre kundeopplevelse, færre henvendelser og bedre økonomi for Lånekassen er eksempler på gevinster som ble identifisert.

Kundeinnsikt

Når man skal brukerrette tjenestene, er innsikt i kundens behov helt essensielt. Lånekassen har jobbet systematisk med å skaffe seg slik innsikt fra ulike kilder. Difis innbyggerundersøkelse er en generell kilde til hvordan kundene opplever Lånekassen og her kommer Lånekassen høyt opp på listen.

I tillegg overvåker og analyserer Lånekassen trafikken på nettsidene og i sosiale medier, og gjennomfører spørreundersøkelser, kundeintervjuer og brukertesting. Lånekassen analyserer også svarene fra en spørreboks som ligger på artiklene på lanekassen.no. Innsikten som kundesenteret sitter på angående kundenes spørsmål, prosessforståelse og begrepsbruk blir også daglig formidlet gjennom tett dialog og samarbeid mellom kundesenteret og kommunikasjonsseksjonen. Også andre medarbeidere internt i tillegg til kundebehandlerne blir involvert gjennom workshops. Disse kildene gir hjelp til å identifisere de mest sentrale punktene i kundereisen som igjen gir innspill til justeringer i oppsettet på nettsidene.

Tjenestedesign gir bedre måloppnåelse

Hvordan påvirker tjenestedesign styring og muligheter for måloppnåelse? Det er vanlig å organisere en virksomhet rundt de viktigste leveransene og prosessene knyttet til disse leveransene. Men det er ofte en stor utfordring å levere tjenestene på en helhetlig, sammenhengende, intuitiv og brukervennlig måte. Dersom man skaffer seg systematisk innsikt i hvordan kundene opplever tjenesteleveransene, vil man ofte identifisere et behov for gjøre tilpasninger i interne prosesser og arbeidsmåter. I Lånekassen har tjenestedesign skjedd i samspill med andre utviklingsprosesser. Dette har også endret kundens adferd. Metoden har gitt innspill til tekniske og språklige forbedringer og bidratt til å gjøre tjenestene mer intuitive. Dette har igjen ført til bedre interaksjonsdesign og bidratt til reduksjon i henvendelser. Man har vurdert behovet for å ta i bruk ny teknologi i lys av den innsikten som er opparbeidet, men dette må vurderes kritisk. Som ledd i dette har man også invitert til forslag til endringer og innført kreativ destruksjon. Det vil si at man tar bort arbeidsmåter som ikke fungerer og vurderer kritisk om nye arbeidsmåter bør innføres.

Mye av det som kom ut av kundereisene er ennå ikke utviklet. Det er blitt gjennomført konseptutredninger og revideringer av målbildet for kundeopplevelser, som vil danne grunnlag for framtidig

Fra en stor kundereise som ble gjort i forbindelse med en behovsanalyse som ble gjennomført med Making Waves.
Fra venstre: Ingunn Egedius (Lånekassen), Espen Grimnes (Lånekassen), Cecilie Liset (Making Waves) og Jenny Shi (NoA).

Espen Grimnes og Ingunn Egedius, publisert i fagbladet Kommunikasjon (1/2017).

utvikling. Noe av det som hittil er blitt utviklet, kom på lufta i sommer og det er for tidlig å si noe om den fulle effekten av tiltaket. Lånekassen ønsker også å se sine tjenester inn i en større tjenestekjede. Det vil si inn mot andre/ samarbeidspartnere. Det vil kreve en del, da Lånekassen kommer til å se tjenesten fra kundens side, framfor hvem som eier tjenesten og hvilket reglement de har å forholde seg til. Det er en stor mengde datafangst fra andre inn mot Lånekassen, da er det ønskelig at kunden skal finne mest mulig offentlig data om seg selv.

Lånekassens lærdommer så langt

Lånekassens erfaringer så langt med tjenestedesign, har gitt god innsikt i kundegruppene og har avdekket nye kundebehov. Øvelsen med å tegne opp kundenes kontaktpunkt og se disse i sammenheng med Lånekassens prosesser i ulike faser har vært svært nyttig.

Basert på erfaringer så langt er dette de beste tipsene Lånekassen vil gi til andre:

- Sørg for en god forankring i toppledelsen
- Bygg opp kompetanse internt
- Brukerinvolvering/brukerinnsikt bør være en naturlig del i utviklingsprosesser
- Beslutningstakere bør være med i kundereiseprosjekter
- Ikke glem å involvere tverrfaglig, der det er naturlig
- Ha tydelige mål og avgrensning for kundereisen og sett av nok tid til innsiktsfasen
- Vis fram internt hvilke funn man har gjort i innsiktsfasen
- Det å koble funn i kundereisen med kvantitative data som nettrafikk eller funn i større undersøkelser er ofte nyttig og nødvendig

Veien videre

Lånekassen har fått til mye på kort tid med metoden, men da med utgangspunkt i Lånekassens eget regelverk og eget ansvarsområde. Men for kunden er ikke dette nødvendigvis en logisk avgrensning. Som også Stortingsmeldingen Digital agenda påpeker, er det nå viktig å se på hvilke tjenester som bør ses i sammenheng med andre virksomheters tjenester.

Gull og grønne Apple

Når Apple lanserer nye produkter venter elektronikkentusiaster verden over i spenning. Men hvem fikk med seg lanseringen av roboten Liam i 2016?

Av
MARIT TRODAL
Prosjektleder IIA Norge

Mobiltelefonen og computeren vi bruker er i dag ikke designet med tanke på reparasjon eller effektiv resirkulering. Samsung måtte høsten 2016 tilbakekalle omkring 4,3 millioner Galaxy Note 7 telefoner, som følge av eksplosjonsfare ved oppheting av batteriet. Men hvordan skulle Samsung håndtere dette betydelige antallet med telefoner? Synd for Samsung at de ikke hadde Liam til å hjelpe seg.

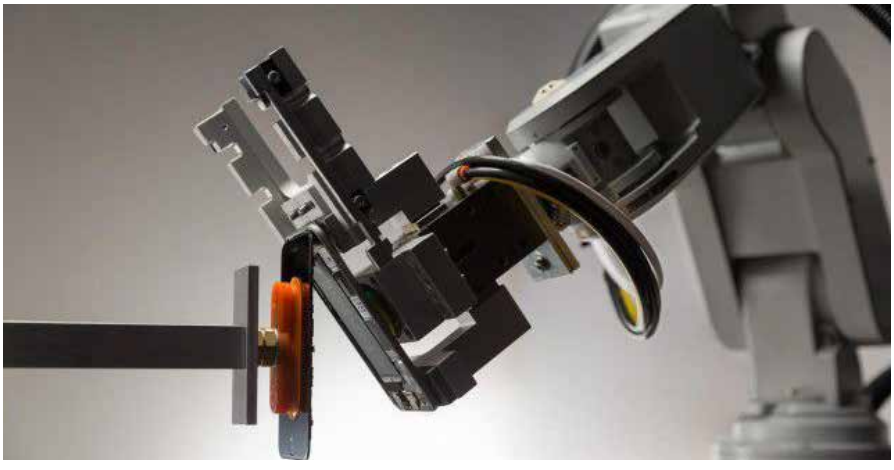
Hvem er Liam?

Apple har utviklet et robotsystem som kan automatisere prosessen med å plukke fra hverandre en iPhone6 og bidra til at viktige metaller kan bli gjenvunnet. Robotsystemet har fått navnet Liam og per i dag opererer han i California og Nederland. I løpet av 11 sekunder kan Liam demontere og ta ut 8 ulike komponenter, deriblant batteriet, høyttaler og alarm modulen i en iphone6. Det er et steg i en grønnere retning, men det er langt igjen. Med dagens kapasitet estimerer Apple at Liam kan demontere 1,2 millioner iPhone6 årlig. Hva utgjør dette i den store sammenhengen?

En typisk mobiltelefon i dag inneholder ulike konsentrasjoner av gull, sølv, kobber, kvikksølv, litium, kobolt, tantalum og en rekke andre mineraler som bidrar til at elektronisk utstyr som mobiler og nettbrett blir mindre, lettere og at batteriet får lengre levetid. Men dette innebærer også at avfallshåndteringen blir langt mer krevende. Det er til dels små komponenter som består av ørsmå konsentrasjoner av mineraler. Hvordan demontere komponentene effektivt? Hvordan skille ut mineraler for gjenbruk?

Liam er fortsatt et pilotsystem, spesialisert på en iPhone-modell med kapasitet til å ta ut kun noen enkelte komponenter. Det krever presisjon å skille ut små konsentrasjoner av mineraler og fokuset er derfor på noen utvalgte, deriblant gull. I en enkelt mobiltelefon er det ca. 3o mg gull og i følge Apple klarte selskapet i 2015 å gjenvinne i overkant av ett tonn gull med anslått verdi omtrent 40 millioner USD. Dette høres ut som en dråpe i havet, gitt at Apple i 2016 solgte 215,4 millioner iPhones på verdensbasis. Men

> Det krever presisjon å skille ut små konsentrasjoner av mineraler og fokuset er derfor på noen utvalgte, deriblant gull.



Kilde: Apple

det viser også at potensialet for å hente ut og gjenbruke mineraler er enormt.

Hva skjer med din mobiltelefon ved retur?

I Norge har vi et retursystem og vårt elektroniske avfall sendes til gjenvinning. Det er likevel kun omkring 20% av mobiltelefonene i Norge som gjenvinnes. Tallet for Europa er 10% (2013, www.renas.no). Så hva skjer med resten som kommer i retur? Realiteten er at veldig lite elektronikk blir gjenbrukt. På global basis er elektronisk

> Et smutthull ved eksport er å deklarere elektronikk som 'second hand' og ikke avfall når man shipper det ut av landet.

avfall et samfunnsproblem som øker i omfang, og ifølge estimater i rapporten «Waste Crimes» fra UN Environmental Program (UNEP), blir 50 millioner tonn elektronisk avfall produsert i løpet av 2017. Dette er opp 20% fra 2015, og handler i stor grad om computerer og smarttelefoner. UNEP anslår også at rundt 80% av elektronisk utstyr ender opp på søppeldynga eller i forbrenningsanlegg. Til tross for at det er ulovlig å eksportere avfall, så kan man følge strømmen av elektronisk avfall til land som Kina, India, Ghana, Nigeria, Pakistan eller Bangladesh. Et smutthull ved eksport er å deklarere elektronikk som 'second hand' og ikke avfall når man shipper det ut av landet, i stedet for å ta kostnaden ved å håndtere farlig avfall forskriftsmessig. I mottakerlandene er det ingen Liam som demonterer, men mennesker som med enkle verktøy som hammer og bruk av flammer demonterer telefoner for å hente ut mineraler som enkelt kan hentes ut, deriblant kobber. Designet til mange smarttelefoner er gjerne sånn at det krever en robots presisjon for å hente ut ørsmå komponenter (2). Samsung møtte også denne utfordringen med Galaxy Note 7. Det var ikke en enkel sak å bytte batteri på alle telefonene, i og med at telefonen ikke var designet for at man kunne erstatte enkeltkomponenter.

Verden trenger mineraler

Veien fra gruve til ferdig produkt kan være både kompleks og lite transparent. Batterier i smarttelefoner og annen elektronikk består for eksempel av litium og kobolt. Den Demokratiske Republikken Kongo er rik på mineralressurser og dekker i dag 65% av den globale etterspørselen etter kobolt. Utfordringer knyttet til mineralutvinning i Kongo og en rekke andre sentralafrikanske land har ført til at amerikanske myndigheter, OECD og etter hvert EU har satt fokus på mineraler som utvinnes i områder hvor risikoen er høy for barne- og slavearbeid og at krigsherrer finansierer krigføring gjennom salg av gull, tantalum, tungsten og tinn – kjent som 'Conflict minerals' i amerikansk lovgivning. Men det er ikke bare disse mineralene det kan knyttes risiko til. Kobolt i Kongo er preget av risiko for barnearbeid, men kanskje ikke i like stor grad finansiering av våpen til krigføring mellom krigsherrer? Hva med tinnindustrien i Malaysia? Litium i Argentina? Kina? Afghanistan? I takt med økt etterspørsel fra elektronikkbransjen, batteri- og bilprodusenter, utforskes mulige forekomster i en rekke land. Litium betegnes gjerne som 'det hvite gullet.' Volkswagen gikk i september 2017 ut med et anbud for å sikre leveranser av kobolt for ti år fremover fra 2019. Dette blir av VW omtalt som et av de største innkjøpsprosjektene i bilindustriens historie, med en totalramme på 50 milliarder euro.

Verden trenger bærekraftig utvinning og bruk av mineraler, og i stedet for å havne på søppeldynga eller forbrenningsanlegg må de inn i et lukket kretsløp og gjenbrukes på nytt og på nytt. Høres dette usannsynlig ut? Vel, i april 2017 lanserte Apple sin miljøstatusrapport 'Progress Report 2017', hvor de inkluderte følgende målsetning:

«Can we one day stop mining the earth altogether? It sounds crazy, but we're working on it. We're moving toward a closed-loop supply chain. One day we'd like to be able to build new products with just recycled materials, including your old products.»

Apple har fått en del oppmerksomhet rundt denne målsetningen. Det er uvanlig at Apple går ut og setter seg mål uten å sette en tidsramme, og de har samtidig lagt listen veldig høyt for hele bransjen.

Et lukket kretsløp innebærer at man tenker sirkulært. En sirkulær økonomi er basert på gjenbruk, reparasjon, oppussing, forbedring og materialgjenvinning, i motsetning til en lineær modell, der man utvinner ressurser, produserer, bruker og kaster via deponi eller forbrenning. Målet er at færrest mulig ressurser går tapt, men gjenbrukes i en annen form.

Det ser ut som Liam er en investering for fremtiden som konkurrenter snarest bør kopiere og videreutvikle.

> «Can we one day stop mining the earth altogether? It sounds crazy, but we're working on it. We're moving toward a closed-loop supply chain. One day we'd like to be able to build new products with just recycled materials, including your old products.»

Kilder:

1 http://nordic.businessinsider.com/apple-liam-iphone-recycling-robot-photos-video-2017-4?r=US&IR=T
http://renas.no/designet-for-gjenvinning/
http://uk.businessinsider.com/apple-recovered-40m-in-gold-from-recycled-products-2016-4?r=US&IR=T
https://www.reuters.com/article/us-volkswagen-cobalt-evs-exclusive/exclusive-vw-moves-to-secure-cobalt-supplies-in-shift-to-electric-cars-idUSKCN1BX1RE
https://www.theatlantic.com/technology/archive/2016/09/the-global-cost-of-electronic-waste/502019/
http://www.abc.net.au/news/2017-03-10/australian-e-waste-ending-up-in-toxic-african-dump/8339760

Kontakt mellom internrevisjons-miljøet i Norge og utlandet

Av
MARTIN STEVENS
Konsernrevisjon i Gjensidige

Det å titte utover vårt eget rekkverk kan ofte gi innsikt og merverdi til vårt daglige arbeid. I dette innlegget har vi intervjuet to internrevisorer som har gjort nettopp dette. Avslutningsvis vil jeg gjerne fortelle om hvordan våre veiledere for Compliance- og Risikostyringsfunksjoner har blitt mottatt internasjonalt.

DELTAGELSE PÅ BALTIC AND SCANDINAVIAN ROUNDTABLE 11-12.05.17 I PÄRNU I ESTLAND

Nils Hjelle, internrevisjonsdirektør i Barne-, ungdoms- og familiedirektoratet (Bufdir)

Hva slags format var det lagt opp til for konferansen?
Vi var ca. 40 deltakere fra syv forskjellige land. Konferansen var veldig interaktiv, noe jeg personlig likte godt og som skilte denne konferansen fra de fleste andre jeg har deltatt på. Kun korte innlegg og dermed mye tid til erfaringsdeling og diskusjon - både i mindre grupper og plenum. Årets konferanse hadde to parallelle spor. Jeg oppfatter at arrangøren IIA Estonia ved sin meget dyktige konferanseledelse ønsker å bevare dette interaktive grunnpreget, så hvis antall deltakere øker videre (doblet fra 2016 til 2017!), håper og tror jeg det blir flere parallelle spor i samme format.

Hva har du tatt tilbake med deg som du kan bruke i ditt daglige arbeid?
Ikke enkelt å peke på konkrete forhold, men i spontan-evalueringen framhevet jeg temaene «Key performance indicators of IA», «Human resources audit» og «Overall opinion». Denne nyttevurderingen står seg absolutt også et halvt år etter. I nevnte evaluering satt vi forøvrig i en sirkel og ga uhøytidelige tilbakemeldinger, også med humor og latter - noe som understreker det uformelle preget og den positive energien som preget hele konferansen.

Noen ville kanskje tenke på at de må lære av de store land som USA og England men du bekrefter at dere lærte mye av hverandre, helt uavhengig av nasjonalitet. Tenker du å delta igjen til neste år?
Veldig gjerne, hvis kalenderen tillater det. Kort reisetid, meget lav deltakeravgift (ca. 50 euro for deltakelse, kost & losji i to døgn) og ikke minst det interaktive formatet gjør denne konferansen til et skikkelig «Kinderegg».

Du har vært på andre internasjonale konferanser – er det noen som har gjort særlig inntrykk?
Har deltatt en del ganger på ECIIA sin årskonferanse (og også den store internasjonale når den har vært i Europa), og har fått både faglig påfyll og utvidet nettverk. Disse konferansene er store «på godt og vondt». På den ene side kan jeg velge akkurat de temaer der jeg mest trenger påfyll. På den annen side er fokus innenfor temaet noen ganger mer prisgitt hva

«speaker» (oftest utmerket!) har å by på enn akkurat det vi deltakere kanskje trenger eller egentlig har spørsmål om, men dette «enveis-grunnpreget» er jo nærmest gitt på så store konferanser.

«Nordic Light», som jeg også har deltatt på, er også verdt å anbefale - i praksis en hybrid mellom den interaktive og uformelle «Roundtable» og de større sistnevnte. Etter det jeg kjenner til har IIA Iceland tatt på seg arrangøransvar i 2018.

Til slutt; de færreste av SIRKs lesere har hørt om Pärnu, hva slags sted var det?
Pärnu er Estlands «sommer-hovedstad» med både sjarmerende arkitektur og lang strand med promenade. En av landets større byer (nr. 4), men den har kun ca. 40.000 innbyggere.

DELTAGELSE I INTERNASJONALT KOMITÉARBEID

Teis Stokka, revisjonsdirektør i Skatteetaten

Hvilke internasjonale fora innenfor IIA har du deltatt på de siste årene?
Jeg har sittet i følgende komitéer og bl.a. jobbet med understående temaer:
- Professional Issues Committee

- Risk Management
- Coordination of Assurance Providers
- Assurance Mapping

- Professional Responsibility and Ethics Committee

- Jevnlig gjennomgang og oppdatering av IIAs etiske retningslinjer
- Vi har laget manuskript til videoer som tar for seg ulike etiske dilemmaer. Disse ligger på Audit Channel på IIAs hjemmeside
- Vi har bidratt til å utvikle en rekke Practice Advisories og Practice Guides
- Vi blir orientert om aktuelle mislighetssaker og mislighetstrender hvor medlemmer av IIA eller administrative ansatte i IIA er involvert
- Jobbet med oppdatering av «Competency Framework»

- Public Sector Committee

- Jobbet med «Auditing of third party providers» (framework?)
- Revisjon av tverrdepartementale og tverretatlige prosesser og prosjekt

I forbindelse med komitéarbeidet har jeg også deltatt på enkelte internasjonale IIA konferanser.

Hva har du tatt tilbake med deg som du kan bruke i ditt daglige arbeid?

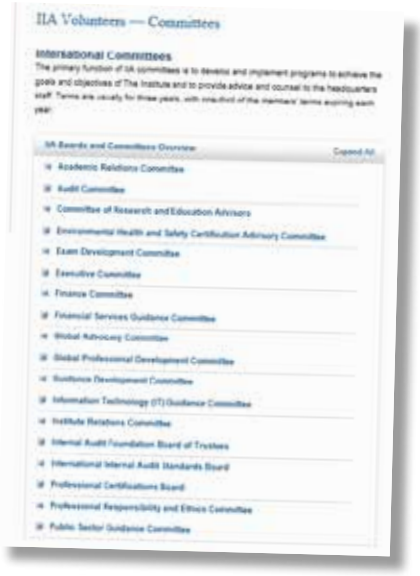
Jeg har blitt tidlig oppdatert på endringer i standarder, trender og beste praksis. Dette er et godt utgangspunkt for videreutvikling av vår egen internrevisjon i Skatteetaten.

I komitéene diskuteres aktuelle faglige problemstillinger sammen med svært kompetente fagpersoner, med sikte på å utvikle veiledninger som alle IIAs medlemmer kan nyte godt av. Dette er også temaer på enkelte avdelingsmøter i internrevisjonsenheten jeg leder.

Hvilke fordeler ser du med nettverksbygging?

Jeg bruker mitt internasjonale nettverk aktivt for å diskutere aktuelle saker jeg er involvert i. Jeg mottar også henvendelser fra andre i nettverket.. Dette er faglig utviklende, og kan bidra til høyere kvalitet på internrevisjonens produkter. Som eksempel kan nevnes at det i forkant av den internasjonale konferansen i London ble arrangert et todagers seminar i IIA Norges regi i Skatteetatens lokaler. Innledere ble for en stor del hentet fra mitt nettverk av internasjonale internrevisjonskapasiteter. Seminaret hadde høy deltakelse, og vi mottok svært positive tilbakemeldinger på det faglige utbyttet.

Vi har også etablert et eget nettverk for revisjonssjefer fra skatteetatene i Norge, Sverige, Finland, Storbritannia, USA, Canada, Australia, New Zealand og Nederland. Dette er et godt forum for diskusjon av revisjonsutfordringer som er spesifikke for skatteetater. I tillegg har vi en løpende utveksling av informasjon og problemstillinger gjennom året.



IIA NORGES INTERNASJONALE BIDRAG

Personlig har jeg aldri tidligere opplevd at fagdokumenter blir revet vekk av publikum med en gang de presenteres. Min erfaring er at disse veilederne fyller et behov for definisjon av 2. linjefunksjons ansvarsområder og virkemåte som det ikke finnes tilsvarende av noe annet sted i verden.

Veilederne ble utarbeidet for å fylle et behov vi har i Norge, men har også blitt oversatt til engelsk. Den engelske utgaven har blitt tatt godt imot av fagfolk i Bulgaria, Slovenia, London, Litauen og Stockholm.

Den gjengse tilbakemelding jeg får er at veilederne treffer blink. De definerer en god praksis som de fleste fagfolk mener bør være på plass.

Takket være styret og administrasjonen i IIA Norge er disse veilederne (på både norsk og engelsk) gjort tilgjengelig for alle faginteresserte. De finnes som PDF på IIA Norges websider. Vær med og spre disse veilederne blant dine kolleger og ansatte i compliance og risikostyring!

Martin Stevens

Kronprinsesse Ellen av (IIA) Norge

IIA Norge kunne den 1. september 2017 markere at det var 10 år siden Ellen Brataas, vår høyt skattede generalsekretær, steg over dørterskelen til foreningens kontor for første gang.

Dette var anledningen til at redaksjonen inviterte seg til en fredagsprat på Ellens kontor.

INTERVJU MED
ELLEN BRATAAS
Generalsekretær IIA

Av
REIDAR DØLI

Ellen Brataas
Kilde: Moment Studio

Ellen, husker du noe av hva som skjedde på jobb den første dagen?

Nei, men jeg husker veldig godt dag to: boksalg for studentene på BI. Heisen i Munkedamsveien 3 B sto og jeg måtte slite meg ned trappene fra 4. etasje med 12 kasser bøker og slepe disse videre frem til BI. Hadde aldri gjettet på at jobben kunne bli så til de grader fysisk.

På dette tidspunktet kjente Ellen godt til ISACA men hun visste ikke så mye om NIRF, som det het frem til ikke altfor lenge siden. Det hele startet med at hun ble kontaktet av en headhunter som jobbet på oppdrag fra styret. Interessen ble vekket jo mer informasjon hun fikk og hun kom på jobbintervju med Solbjørg Lie, som var styreleder den gang. Deretter gikk det ikke lenge før hun var ansatt som generalsekretær i NIRF. Det var etablert en administrasjon et par år i forveien hvor Frank Alvern hadde vært inne på engasjement som generalsekretær i en periode på halvannet år. Ellen ble sådan den første fast ansatte generalsekretæren. Hun brakte inn mye relevant IT-revisjonserfaring og hadde bakgrunn fra Skattefogden i Oslo og Akershus, EY, Evry og Oslo Kommunerevisjon. Hun sier at det som fikk henne til å begynne i jobben var en kombinasjon av at hun er nysgjerrig og liker utfordringer, og generelt sett er kjent for å si ja til det meste.

Ellen reflekterer over utviklingen i foreningen gjennom disse 10 årene. Det første som kan sies er at foreningen har blitt mye mer profesjonalisert gjennom denne perioden. Styret var veldig operativt helt frem til 2005 da sekretariatet ble etablert. Det arbeidet som styret hadde måttet utføre ble gradvis overført til administrasjonen. Etter hvert har administrasjonen fått en mye mer aktiv rolle, både for utførelse og koordineringen av aktiviteter i alle nettverkene og komiteene. Sekretariatet har økt med ytterligere en fagressurs slik at de nå er tre. Det er stor aktivitet i risikostyringsnettverket og compliancenettverket som også har kommet til i løpet av denne perioden. Det er etablert et nettverk for ansatte internrevisjonsledere som fungerer veldig bra. Et stort fremskritt har det vært i utviklingen og befestningen av kvalitetskontrollen. Det kan nevnes at det i løpet av 2017 er gjennomført ikke mindre enn 8

slike evalueringer i regi av IIA Norge! Enkelte ting tar lenger tid enn andre, som eksempelvis daværende styreleder, Solbjørg Lie, sin henvendelse til Finansdepartementet i 2008 om «Behov for utredning av internrevisjon i statlig sektor» som kan sies å være initiativet som resulterte i R-117 «Vurdering av etablering av internrevisjon» i 2016.

Et annet område som vi jobber mer strukturert og målrettet mot nå, er relasjonsbygging, forteller Ellen engasjert. Styret har definert interessenter og fagmiljøer vi ønsker å påvirke og samarbeide med. Eksempelvis har vi dialog med flere høyskoler og universiteter rundt viktigheten av at fremtidens ledere har tilstrekkelig innsikt i risikostyring og internkontroll som en integrert del av ledelsesfaget, herunder internrevisjonens rolle som støttespiller for styrer og ledelse. Dette arbeidet bærer nå frukter. Internrevisjon er kommet inn som valgfag på revisorstudiet på BI og vi er i oppstartsfasen av å bygge moduler for compliance og risikostyring ved andre institusjoner. Kanskje kommer det en sertifiseringsordning på Risikostyring og Compliance på sikt? Med god hjelp fra styret er vi i gang med dette arbeidet. Stort var det også å jobbe frem mot og få gjennomslag for etablering av internrevisjon i statlig sektor. Dessuten har NUES nå åpnet døren. Vi har også jevnlig dialog med DFØ og Riksrevisjonen.

Mette-Marit parodi. Kilde: Privat

Norske deltakere på ECIIA konferanse i Basel 2017. Kilde: Privat

Ellen spretter opp av kontorstolen og sier at vi må få med at hun er veldig imponert over alle de som deltar aktivt i foreningen og er fulle av engasjement. Hun må ofte spørre noen om å utføre en oppgave som medfører mye jobb – og det uten betaling. Likevel svarer de ja til oppgaven, fordi de synes det er spennende og de ønsker å bidra. Hvis det i det hele tatt er noen begrensninger på denne innsatsen så er det at tiden ikke alltid strekker til. Uten alle de tillitsvalgte og all den frivillige innsatsen, hadde ikke IIA Norge vært noe særlig til forening.

Etter 10 år er det fortsatt kjempespennende å gå på jobb. Ellen synes hun lærer noe nytt og møter nye mennesker hver dag. Hun kommer deretter inn på et nytt tema, nemlig at foreningen nok i mange sammenhenger fremstår som vel seriøs. Hun forsøker selv å leve etter mottoet om at ingen har vondt av å by litt på seg selv. Intervjueren oppfatter det som Ellen sier som et velment råd til alle oss andre. Er man åpen fortsetter hun, da blir andre også mer åpen tilbake. Dette er relasjonsbyggende. By på deg selv! Vis deg fra en annen side. Dette har generalsekretæren praktisert i ulike sammenhenger. Spesielt minneverdig for medlemmer i foreningen var da hun på en årskonferanse for noen år tilbake dukket opp som Mette-Marit på scenen. Dette stuntet var til ære for Svein og hans runde bursdag som sammenfalt med årskonferansen. Den dag i dag opplever Ellen at folk husker henne som kronprinsesse og gir henne positive tilbakemeldinger. En skikkelig ice breaker.

> *Ellen om medlemmene:*
> «IIA Norges medlemmer er engasjerte, kunnskapsrike og mangfoldige.»

Jeg tør mye mer nå enn for 10 år siden, fortsetter hun. Nå er det til stadighet pre-

sentasjoner i store og små forsamlinger, i innland og i utland. Det er hyggelig å få gode tilbakemeldinger slik som fra BI eller fra revisjonsutvalg etter presentasjon av en QA rapport. Hun føler at hun har opparbeidet en faglig troverdighet uten å være for seriøs, og da blir det morsomt! Denne veksten har vært nyttig også i privat sammenheng tilføyer hun.

Hva er høydepunktet gjennom et år i foreningen?

Det er årskonferansen. Dette er hovedarrangementet gjennom et år og dessuten det eneste som er statisk. Alt annet er i endring. Konferansen har tatt en veldig bra retning etter hvert. Andre høydepunkt kan være mer på det personlige plan. For eksempel hvis jeg har sagt ja til noe som i utgangspunktet virker ganske krevende, så gjør jeg det, og det går bra, da er det et skikkelig løft.

Et godt eksempel er da Ellen var key note speaker på den østerrikske konferansen for tre år siden og skulle «hoppe etter» Deanna Sullivan, en svært anerkjent foredragsholder bl.a. på internasjonale konferanser i regi av IIA, og det gikk skikkelig bra. I fjor satt Ellen i panelet i NY på IIAs Global Council sammen med to andre og skulle snakke om å håndtere media. Grunnlaget for å uttale seg om dette mente Ellen at var noe tynt siden hun hadde vært i en slik situasjon kun en gang, men det ble vellykket.

Hvordan er det internasjonale samarbeidet i IIA?

Det er viktig at de små institutter er representert, for i hovedsak er de aller fleste små institutter av de i overkant 100 landene som IIA globalt består av. Samarbeidet globalt er i hovedsak bra synes Ellen, men en amerikansk moderforening medfører mye byråkrati og et skjemavelde og rapporteringskrav hvor hensikten noen ganger er vanskelig å forstå. Et slikt samarbeid av frivillige krefter medfører også «long time to market» når det gjelder veiledninger til dagsaktuelle temaer. Det europeiske samarbeidet fremstår som mer relevant. Det er godt samarbeid, læringsdeling og man kommer tidligere ut med løsninger. Flere institutter samarbeider nå om en veileder GDPR, som et eksempel, og det er de europeiske instituttene som laget Hot topics for internal audit 2018. Ellen setter også veldig pris på den europeiske CEO gruppen. Der blir det gjort gode og konkrete tiltak for å få fremdrift.

tror det vil skje store endringer i måten medlemmene jobber på. Digitalisering er et stikkord. Da må også foreningen endre seg. Det kan også være at de små avdelingene, som det er mange av i Norge, må se på om det finnes andre arbeids- og samarbeidsformer for å dekke det stadig utvidede kompetansebehovet. Der kan IIA Norge ha en rolle. Vi må kanskje også finne andre plattformer for raskere og mer effektiv informasjonsdeling. Andre institutter prøver ut apper som inngangsport i stedet for nettsider, mens andre etablerer work-spaces.

Ellen om kvalitetskontrollen:
«Fascinerende er det at selv om vi følger de samme retningslinjene så er virksomhetenes individuelle løsninger svært forskjellige.»

Hva så med IIA Norge fremover blir siste spørsmål

Til dette svarer generalsekretæren med en refleksjon tilbake til kvalitetsgjennomgangene som oppsto fordi det var en plikt, men som senere ble til ett behov. Slik kan det kanskje bli på flere områder fremover. Ellen har erfart at det beste er å komme i dialog med interessentene, slik som styrer og revisjonsutvalg og la internrevisjonen komme i fokus. Interessentene må tenke på hva internrevisjonen er og hvorfor den er til. Hva som ellers vil skje fremover er avhengig av medlemmenes behov. Ellen

Vi avslutter samtalen med å si til Ellen at vi er mange som setter pris på hennes innsats som generalsekretær, vi takker for de 10 årene og ser frem til fortsettelsen.

ECIIA konferanse 2017. Kilde: Privat

Turbulente tider - også for internrevisor

Av
ELI MOE-HELGESEN
Risk Advisory Services, PWC

De siste 13 årene har PwC årlig gjennomført en global undersøkelse av trender innenfor internrevisjonsprofesjonen. Et tydelig trekk gjennom de siste årene har vært at internrevisjonens viktigste interessenter – styret og ledelsen i virksomheten - forventer mer, og at internrevisjonen kontinuerlig har evnet å levere stadig høyere verdi. Men i 2017-undersøkelsen faller interessentenes tilfredshet for første gang på flere år. Hva kan dette skyldes?

Andelen selskaper som opplever at internrevisjonen er klart verdifull for virksomheten, falt fra 54% i 2016 til 44% i år - den laveste andelen på fem år. Den gode nyheten er at omtrent like mange av de samme selskapene ønsker at internrevisor skal påta seg en viktigere rolle, slik at virksomheten blir bedre i stand til å håndtere interne og eksterne hendelser som verken lar seg planlegge eller forutse.

Mer komplekse trusler og muligheter. Henger internrevisjonen med?

Næringslivet i både privat og offentlig sektor står overfor betydelige endringer. Både interne og kunderettede prosesser digitaliseres, et grønt skifte er på vei, mange bransjer står overfor nye aktører og gamle forretningsmodeller utfordres. Og i dette bildet søker interessenter og brukere av internrevisjonen støtte og bidrag til verdiskaping fra sine internrevisjonsfunksjoner. Styret og ledelsen sier det er særlig viktig at internrevisjonen utviser evne til fleksibilitet og tilpasning i tider som disse.

Vi spurte hvilke krefter styre og ledelse er mest bekymret for, og utfordringer som endret regulering, endringer i forretningsmodeller, cyber-trusler, finansiell stress og teknologi scorer høyt.

Dette stemmer godt overens med hva vi observerer i Norge. Norske virksomheter forteller at de står overfor mer komplekse trusler og muligheter enn før. Risikoen kommer fra nye kilder og påvirker selskapene raskere.

Styret og ledelsen ønsker internrevisjonens bidrag

Internrevisors gylne mulighet - og store utfordring - er å spille en enda større rolle i møte med disse populært kalt disruptive kreftene. Evner vi ikke å bidra på disse viktige områdene risikerer vi som jobber med internrevisjon å utspille vår rolle. Den gode nyheten er at internrevisjonens støtte og innsikt er ønsket. Undersøkelsen viser at interessentene ønsker at internrevisjon skal spille en stadig viktigere rolle. Mens få (7%) vurderer at internrevisjonen i dag spiller en strategisk viktig rolle, ønsker nesten halvparten (48%) at internrevisjonen skal ta en slik rolle i virksomheten i løpet av de neste fem årene.

Figur 1 - Hvor mange av internrevisjonens interessenter mener internrevisjonen bidrar til vesentlig verdi for virksomheten

Hva gjør de beste?

I undersøkelsen er det en gruppe på ca. 18% av internrevisjonsfunksjonene som får vesentlig bedre tilbakemeldinger fra styret og ledelsen enn resten av virksomhetene. Vi har kalt disse «agile» internrevisjoner, og har forsøkte å identifisere hva disse gjøre annerledes enn resten av populasjonen. Og det er noen forhold som ser ut til å peke seg ut.

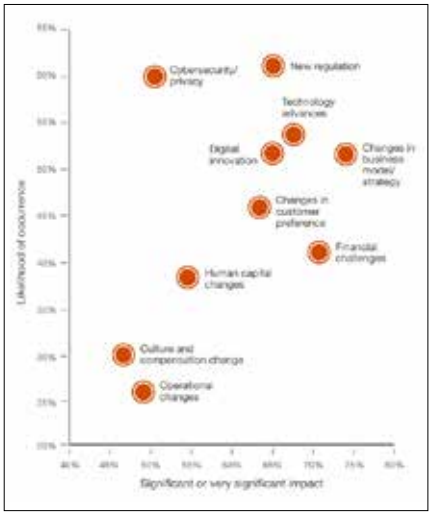
De internrevisjonsfunksjonene som oppfattes som mest verdiskapende...

- ser ut til å være mer fokusert på endringer og disrupsjon, og inkluderer dette inn i sine internrevisjonsplaner

OM UNDERSØKELSEN:

Undersøkelse er basert på en spørreundersøkelse med svar fra 1.892 personer fra hele verden. Av disse er 58% ledere av internrevisjon og 42% er internrevisjonens hovedinteressenter; styremedlemmer, medlemmer i revisjonsutvalg eller ledere internrevisjonen rapporterer til. I tillegg er det gjennomført 70 dybdeintervjuer.

Figur 2 - Hva er de viktigste kreftene som antas å ville påvirke virksomhetene fremover?



Figur 3 - Hvilke endringer er mest sannsynlige, og hvilke påvirkning kan disse gi?

Figur 4 - Hva gjør de beste?

- har forbedret prosessen for risikokartlegging og -vurdering, og tar større hensyn til strategisk risiko i sitt arbeid
- jobber i større grad enn resten av populasjonen tett med andre risiko-/ compliancefunksjoner, og bidrar til en mer enhetlig risikoprosess på tvers av ulike interne funksjoner
- har endret fokus og sammensetning av porteføljen av revisjonsprosjekter, og jobber mer med risikoer som er av strategisk betydning for virksomheten
- omstiller og «fremtidsretter» sine avdelinger oftere, og investerer i teknologi og analysekapasitet
- bruker i større grad prosjektledere og teammedlemmer med kompletterende typer kunnskap som kommer utenfra egen organisasjon.

Veien videre - Alltid beredt!

Vår klare holdning er at mange virksomheter - både offentlige og private - kan hente betydelig verdi fra sin internrevisjon. Evne til å forstå risiko og justere fokus ut fra endring ser ut til å være fellesnevnerne for de virksomhetene hvor internrevisjonen oppleves som mest verdifulle for sine interessenter. I likhet med speiderbevegelsen må internrevisor rett og slett alltid være beredt. Det forutsetter at hun eller han løfter blikket og ser konturene av gryende endringer før de oppstår. I tillegg til å skimte endringene, må internrevisor også vite hva det betyr for selskapet og hvordan de skal reagere. Derfor må internrevisor samarbeide tett med andre deler av organisasjonen, samt investere i ny og relevant teknologi for å styrke sin analysekapasitet.

Vil du lese mer om undersøkelsen, se https://www.pwc.com/us/2017internal-auditstudy

Generalsekretæren informerer

AV ELLEN BRATAAS

RAPPORTERING AV VEDLIKEHOLDSPOENG

Det nærmer seg årsslutt og vi minner alle innehavere av IIA-sertifiseringer om at fristen for innrapportering av CPE-poeng for inneværende år må gjøres innen 31. desember 2017. Dette gjøres via portalen Certification Candidate Management System (CCMS) på www.globaliia.org. Her bekrefter du kun om du har tilstrekkelig poeng eller ei. Oversikt over og dokumentasjon på hvilke aktiviteter du har deltatt på skal ikke sendes inn før en eventuell kontroll fra IIA globalt.

Antall vedlikeholdspoeng for Diplomert internrevisor rapporteres til post@iia.no innen 31. desember 2017. Heller ikke her skal du sende med dokumentasjon før en eventuell stikkprøvekontroll. Det kan være smart å oppbevare dokumentasjon for tre år tilbake.

OPPDATERT KVALITETSMANUAL

Foreningen har merket stor etterspørsel etter eksterne evalueringer i 2017. Dette skyldes at det nå er gått fem år siden de første internrevisjonsfunksjonene hadde en gjennomgang, samt at flere internrevisjoner gjennomfører en ekstern evaluering for første gang. Til informasjon til dere som går med planer om en ekstern evaluering, har IIA nå lansert en oppdatert versjon av kvalitetsmetodikken, en god støtte til å forberede den eksterne evalueringen.

NY STRUKTURERING AV INNHOLDET PÅ CIA-EKSAMEN FRA 2019

IIA globalt jobber for tiden med å gjøre om på innholdet i de tre delene av CIA eksamen. Det totale innholdet vil ikke forandre seg mye, men endringen omfatter inndelingen av innholdet i de forskjellige delene. Den nye strukturen skal etter planen lanseres fra begynnelsen av 2019. For mer informasjon, se CIA Exam Syllabi Revision.

VI GRATULERER FØLGENDE MEDLEMMER

Diplomert internrevisor
Runar Røstbø, DNB Bank ASA

Certified Internal Auditor (CIA)
Hanne Lønnemo, Oslo kommune, Kommunerevisjonen
Saira Nisar, DNB Bank ASA

AT THE JUNCTION OF CORPORATE GOVERNANCE AND CYBERSECURITY

The joint guidance from ECIIA and FERMA enables companies to make consistent and understandable decisions about their security measures, risk management and overall cyber security posture. The document contains recommendations for a cyber governance model that will benefit European organisations – public and private – in managing their exposures to cyber risks.

The timing is particularly relevant since we are in the final year before the effective implementation of two major EU laws: the Network and Information Security (NIS) Directive and the General Data Protection Regulation (GDPR).

HOT TOPICS FOR THE INTERNAL AUDIT PLAN 2018

A wider group of European Institutes of Internal Auditors have been interviewing Chief Audit Executives (CAEs) from major organisations in six European countries – France, Italy, the Netherlands, Spain, Switzerland and the UK. The Hot Topics included in this report reflect risk areas that are being prioritised by CAEs as they prepare their audit plans for 2018 and make longer-term risk assessments.

For some readers, these themes will already be fully reflected in their audit plans for the coming year. They may want to use our research to highlight to their audit committees that they are indeed on the right track. For others, this report may serve as a timely reminder as they finalise their plans for 2018 and beyond of issues that merit serious reflection. And for all, we hope that our publication will provide a fresh and relevant talking point, both for internal audit professionals and for audit committees and other stakeholders.

KONFERANSER VERDT Å MERKE SEG

IIAs International Conference, 6. – 9. mai 2018, Dubai, De forente arabiske emirater
IIAs årlige konferanse, 28. og 29. mai 2018, Bergen

ECIIA Conference, 3. – 5. oktober 2018, Madrid, Spania

The Institute of Internal Auditors | Global

Følg oss for øvrig på Nyhetsbloggen, Twitter, LinkedIn og Facebook.

PRACTIC GUIDE - ENGAGEMENT PLANNING: ASSESSING FRAUD RISK

This guide is a practical tool to help internal auditors plan an audit engagement in conformance with Standards 2210.A1 and 2210.A2. The practice guide describes the characteristics of fraud and the process of identifying and assessing fraud risks when planning individual audit engagements. It outlines the process of incorporating a fraud risk assessment into engagement planning, including how to:

- Gather information.
- Brainstorm fraud scenarios.
- Identify fraud risks and rate their significance.
- Determine which fraud risks should be evaluated further during the engagement.

PRACTICE GUIDE - ENGAGEMENT PLANNING: ESTABLISHING OBJECTIVES AND SCOPE

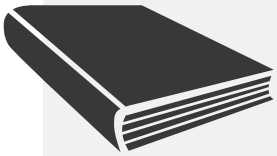
This practice guide contains the engagement planning steps necessary to fulfill Standard 2200 – Engagement Planning through Standard 2220 – Engagement Scope. The guide also offers guidance on how internal auditors can use a risk and control matrix and heat map to prioritize the risks, then use the results to form the engagement objectives and scope, in conformance with the Standards. Established engagement objectives and scope enable internal auditors to focus efforts on the significant risks in the area or process under review, develop the engagement work program, and communicate clearly with management and the board.

Engagement planning generally includes the following steps:

- Understand the context and purpose of the engagement.
- Gather information to understand the area or process under review.
- Conduct a preliminary risk assessment of the area or process under review.
- Form engagement objectives.
- Establish engagement scope.
- Allocate resources.
- Document the plan.

NYTT KRAV FRA 2018 – TO ETIKKRELATERTE CPE-POENG

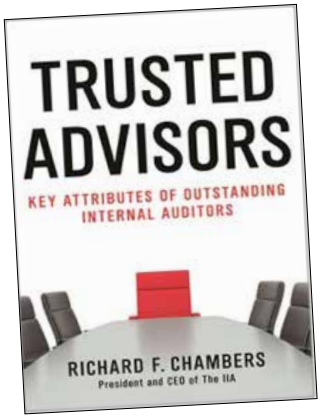
IIA globalt har besluttet at fra og med 2018 må alle innehavere av IIA-sertifiseringer kunne rapportere at 2 CPE-poeng er relatert til etikk. Mange har allerede etikktrening på jobben, men også enkelte aktiviteter i IIA Norges regi vil relateres til etikktrening, eksempelvis gjennom foredrag på årskonferansen.



Av
ESA LEPORANTA
Systems Audit Manager,
Nets Norway Branch

Trusted Advisors – Key Attributes of Outstanding Internal Auditors

By Richard F. Chambers



In his latest book, IIAs President and CEO Richard F. Chambers, shares the traits and characteristics of trusted advisors as identified by the world's leading chief audit executives (CAEs).

Chambers introduces his book by defining the word trust and challenges all of us who are audit practitioners on the very first page of his book by asking, do those we audit mistrust whether we as auditors understand the business and whether we will not simply waste their time over the course of the audit?

Chambers describes the concept of Being trusted as a metalesson, a lesson about lessons, by believing in what we internal auditors do is not as important as how we do it. Internal auditors who rise above challenges have achieved a balance between technical and soft skills by building a broad portfolio of complementary attributes.

After a survey of nearly 300 top CAEs as well as one-on-one interviews with top audit practitioners, Chambers presents nine attributes in three categories to become a trusted advisor.

Chambers believes that successful internal auditors must possess the attributes in the personal category and apply them in every transaction with others. This category focuses on who internal auditors are at the very core of their being and includes attributes such as being 1) Ethically resilient, 2) Results focused, 3) Intellectually curious and 4) Open-minded.

Attributes in the relational category look at how internal auditors deal with others and include attributes as 5) being Dynamic communicators, 6) forming Insightful Relationships and being 7) Inspirational Leaders. Success in these areas depends on building, fostering and maintaining good relationships. At the same time, Chambers again challenges us by stating that he doesn't suggest that internal auditors should always strive to be liked; «sometimes internal auditors can be right or they can be liked, but not both».

In the last category, describing professional attributes, Chambers looks at the knowledge and skills of the outstanding auditors, including attributes such as 8) Critical thinking and 9) Technical expertise.

Each attribute is examined in detail with separate chapters to help internal auditors to strengthen their skills in the respective areas.

As the book clearly shows, it is important that we as auditors not only focus extensively on developing our technical skills, but also work to balance the scales between what we know and how we get things done, not forgetting the impact of passion. As expressed by Richard Chambers himself, outstanding auditors really believe in the contribution internal audit makes and take great pride in being part of that good work.

I warmly recommend this book for all internal audit practitioners, who target becoming true masters of this fascinating field of work.

IIA Norge avliver myter!

Internrevisjonen blir noen ganger misforstått. Bidraget til verdiskapning i virksomhetene vi jobber i er betydelig, og hvem vet hvor verden hadde vært i dag hvis det ikke fantes internrevisjoner?

Det aner oss at det er en del myter om internrevisjonen der ute, og vi i IIA Norge tok en runde på Karl Johan for å spørre folk hva de tenker om internrevisjonen. Vi opptrådde helt objektivt og uavhengig, i henhold til IIA standardene.

Lite ante vel vi at bevisstheten rundt internrevisjonen er så høy…

Først treffer vi to kvinner som viste seg å være ledere innen statlig sektor.

Hvordan opplever dere internrevisjonen? Gjør de noe nytte for seg?

«Jeg opplever at arbeidet internrevisjonen gjør er nyttig og at dette er et gode for å jobbe med forbedring. Vi må tåle å få kritikk og at feil blir påpekt. Det ligger mye læring i rapportene fra internrevisjonen.» Den andre føyer til:

«Jeg synes det er artig når jeg får mailer fra Internrevisjonen, for da vet jeg at jeg lærer noe nytt. Revisjon lukter jo støv, men er kvalitetssikring.»

Artig, men lukter støv? Vi velger å overse kommentaren om støv og følger opp kvalitetssikring og læring;

«Det er viktig at vi får tatt ut læringseffekt. Det er et ønske fra både styret og administrasjonen at vi skal få til endring. Vi kan ikke bare se på endrede rutiner og prosedyrer, men hvordan sikre at de etterleves?»

En mann stopper og ber om å få komme med en kommentar:

«Suksessen til internrevisjonen ligger i å være en strategisk ressurs som man kan brukes til å komme fremover, forenkle og forbedre. Svaret på alt kan ikke være enda mer kontroll, flere rutiner og prosedyrer. Det kan bli uhåndterlig for linjen og organisasjonen. Noen problemstillinger kan falle mellom to stoler og her tror jeg internrevisjonen kan ha en viktig rolle og spille.»

Plutselig står vi der med tre engasjerte intervjuobjekter, som alle har klare meninger om internrevisjonen. Her er det bare å lytte og notere. Mannen sitter i en lederstilling innen helsesektoren og han forteller:

«Vi fikk raskt på plass en internrevisjon og har brukt denne som et strategisk verktøy for å få et objektivt syn på områder hvor vi har hatt forskjellige syn.»

Hvor objektiv er internrevisjonen da?

Den ene kvinnelige lederen tar ordet; «I forhold til linjen er de objektive og upartiske. Kanskje til tider litt for objektive. De kan oppleves som steile når de først har gjort seg opp en mening.»

«De har skråblikket, står utenfor og skuer inn. Så nært et objektivt blikk som mulig. Det gir en viss tyngde hvis en oppfatning kan underbygges med en bekreftelse fra internrevisjonen. De er et godt lederverktøy. Det er ingen hos oss som tuller med internrevisjonen…» legger den andre kvinnen til og alle nikker samtykkende.

Vi takker for praten og går videre til Spikersuppa hvor vi henvender oss til en kvinne og en mann som sitter sammen på en benk. Hun viser seg å være styreleder med lang erfaring fra offentlige virksomheter:

«Det er et stort ansvar å være styreleder og da er det godt å ha konsernrevisjonen som trygghet. De gjør mye med begrensede ressurser. Omfanget av arbeidet de gjør er imponerende,» sier hun.

Mannen ved siden av henne sitter som representant i et styre og føyer til;

«Jeg registrerer at mange internrevisjonsrapporter havner under orientering og til slutt. Det burde vært flere beslutningspunkter og de burde stått høyere på agendaen. De blir stemoderlig behandlet.»

Makan, tenker vi! Hva er oddsen for at vi skal møte så mange som vet så mye om internrevisjonen og skjønner hvor viktig funksjonen er for å skape merverdi i en virksomhet?

Vi går videre til Kaffebrenneriet, hvor vi treffer på en mann i svart dress som venter utålmodig på sin americano. Han er på vei til et møte, men har tid til ett spørsmål:

Kan du si noe om kvaliteten på arbeidet til internrevisjonen?

«De reviderer jo ikke strategiprosessen. Det skal bli interessant når en fra McKinsey går til internrevisjonen. Det har ikke skjedd så langt….» sier han og skynder seg av sted.

Stemmer det da? Vi er ikke helt sikre, men det var en interessant betraktning. En dame som sitter og leser avisen ved vinduet snur seg:

«En av forutsetningene for at de skal lykkes er at de klarer å ha et forbedringsperspektiv. Det er lettere å lykkes om man får frem forbedringsperspektivet fremfor kontrollperspektivet.»

Jepp! Godt lederverktøy, forbedring og læring, strategisk ressurs. Det er noe som opptar folk nå for tiden når det gjelder internrevisjonen. Vi noterer flittig og når vi titter opp blir vi oppmerksomme på en smilende mann som står tett ved:

«Jeg er veldig glad i internrevisjonen!»

Kilder: Eksterne evalueringer gjennomført av IIA Norge, utsagn hentet fra intervjuer med interessenter i ulike private og offentlige virksomheter.

Returadresse
IIA Norge
Postboks 1417 Vika
0115 Oslo

Er personvern et konkurransefortrinn hos deg?

Mai 2018: EUs nye personvernforordning
Er du forberedt og klar for nytt regelverk?

Virksomheter med et aktivt forhold til de nye personvernreglene vil kunne oppleve betydelige konkurransefortrinn i årene som kommer. Et godt stykke arbeid skal legges ned for mange virksomheter, sannsynligvis mer omfattende enn enkelte er klar over.

Våre spesialister innen personvern og internrevisjon er klare til å være proaktive sparringspartnere og rådgivere for deg. Slik kan du etterleve reglene og utnytte muligheten du har til å være i forkant av konkurrentene.

KONTAKT OSS

Henrik Dagestad
Direktør/Advokat - BDO Advokater
+47 901 77 117, henrik.dagestad@bdo.no

Dorothee Sauer
Senior Manager - Rådgivning
+47 942 96 198, dorothee.sauer@bdo.no

Kristian Thaysen
Partner - Rådgivning
+47 940 15 007, kristian.thaysen@bdo.no