SIRK

Styring – Internrevisjon – Risiko – Kontroll

Nr 2 2016

IIA NORGE

Hvem skal granske? s. 6

Med etikk som hjertesak s. 18

Blokkjede-teknologien s. 48

REDAKTØRENS SPALTE

ELLEN BRATAAS

Denne høsten har konseptet «den fjerde industrielle revolusjon» fanget min oppmerksomhet. Digitalisering og innovasjon er to av de mest velbrukte ordene gjennom hele 2016, men hva betyr det egentlig for oss personlig og i arbeidslivet? Med den fjerde industrielle revolusjon følger omstilling, automatisering, robotisering og derav også helt sikkert nye forretningsmodeller. En verden i endring har vi alltid hatt. Uten endring, ingen progresjon! Men aldri tidligere har endringene skjedd i et raskere tempo enn nå. Er det hurtigheten på endringene som gjør at det er vanskelig å se sammenhenger og å forstå relasjoner? Eller er det fordi vi lever store deler av våre liv gjennom sosiale medier der informasjonen siles gjennom algoritmer tilpasset den enkelte? Hvorfor blir vi lammet av sjokk ved å våkne opp til Brexit eller til at Donald Trump blir USAs neste president, når vi egentlig burde sett muligheten for at dette kunne skje...om vi bare hadde fulgt med på totaliteten av alle signalene som pekte i de retningene?

Jeg gleder meg til en spennende og mer digital fremtid, men med tanke på hvor fort utviklingen går, frykter jeg å ikke henge med i svingene. Det som var riktig før er plutselig ikke lenger et alternativ. Endringer skaper nye risikoer og med nye risikoer i rask endring må kontrollfunksjoner også tenke nytt. Hva blir de nye områdene kontrollfunksjoner må ha fokus på og hvordan gjennomføre bekreftelser på mer hensiktsmessige måter, er spørsmål som må stå på enhver agenda i tiden fremover. Hvor lang tid (eller kanskje heller hvor raskt) vil det gå før ansvarsområder som tidligere lå inn under internrevisjon eller compliance, bli automatisert eller overtatt av kontrollroboten «Control 1.0»?

Noen risikoer kommer til, andre blir mindre viktige. På de neste sidene kan du lese mer om hva vi kan forvente av blokkjede-teknologien på kort sikt og hvordan revidere i en stadig mer digitalisert verden. Velkjente mislighetssaker, arbeid med compliance og verdibasert vs. regelstyrt ledelse er også temaer som blir omhandlet i denne utgaven.

Ønsker alle medlemmer og samarbeidspartnere en riktig god jul og ønske om et innovativt, digitalisert godt nytt år og avslutter med et sitat fra boken til Asbjørn Nygård som tar revisorhumor på alvor: «Definisjon av revisor: Revisor er en som løser et problem du ikke visste du hadde, på en måte du ikke forstår.»

PRESIDENTEN HAR ORDET

INGUNN VALVATNE
PRESIDENT
IIA NORGE

Desember er en travel måned. Ikke bare skal året avsluttes med julearrangementer for familie, venner og kollegaer, det skal også tenkes fremover. Mange er vi vel som legger siste hånd på revisjonsplanen for neste år. Årets siste styremøte i IIA Norge vil også ta for seg nettopp strategi og handlingsplan for 2017.

Strategien vår er vel gjennomtenkt, og innholdet står seg godt også for neste år. Vi skal fortsette arbeidet med å befeste og videreutvikle internrevisjonens rolle som styre- og lederstøtte. Det er kanskje det mest krevende målet, som kun kan oppnås gjennom iherdig videreutvikling av vår rolle som profesjon. Panamaavsløringene må sies å være nærmest utdebattert. Vi må likevel ta innover oss at saken også avslørte at det hersker uklare oppfatninger om rollen vår der ute, og at vi ikke har klart å formidle dette klart nok. Dette blir en viktig oppgave for IIA Norge i årene framover.

Det er ingen liten oppgave, og den gjøres ikke en gang for alle. På 90 tallet var utvikling av rammeverk for risikostyring og egenvurderinger en stor ny oppgave for internrevisjon. Etter finansskandalene på starten av 2000 tallet ble vi tildelt en helt ny rolle i å bekrefte internkontrollen i finansiell rapportering som følge av Sarbanes-Oxley regler. Finanskrisen i 2008 ga igjen næring til diskusjon av rollen. Det reiste spørsmål om hvilken rolle vi hadde, og ikke minst hvilken rolle vi burde ha tatt, i å avdekke sårbarheter som ledet til krisen.

Våre viktigste brukere er styrer, revisjonsutvalg og toppledere. Forventingene til deres oversikt over styring og kontroll er stadig økende ettersom kompleksiteten øker. En omfattende brukerundersøkelse nylig gjennomført av IIA, avslører en økt misnøye med den tradisjonelle måten å utøve internrevisjon på. Satt på spissen opplever mange styrer at fokuset er for snevert, og at internrevisjonen ikke er det verktøyet den skulle være som støtte for styrer i å ivareta sitt kontrollansvar.

Siden 1990 tallet har mange virksomheter etablert egne risikoavdelinger og etterlevelsesfunksjoner for å støtte ledelsen i utøvelse av sitt ansvar. Det betyr at vi må ruste oss for å gi styret en vurdering av eierstyring og selskapsledelse i bredere forstand. For å sitere Richard Chamber's kommentar til undersøkelsen; «time to move out of the comfort zone". Dette blir viktig for foreningen fremover. Her spiller kurs og opplæring en nøkkelrolle, sammen med alle initiativer som tas i alle foreningens komiteer og nettverk. Jeg vil benytte anledningen til å sende en særlig julehilsen til alle dere som deltar i foreningens nettverk og komiteer. Også til sekretariatet som yter god service til oss alle. Til sammen utgjør dere selve drivhjulet i foreningen. God jul også til alle medlemmer!

MEDIEKOMITEEN

Ellen Brataas
Generalsekretær
IIA Norge

Reidar Døli
Internrevisor,
Oslo Børs VPS

Martin Stevens
Internrevisor,
Gjensidige Forsikring

Esa Leporanta
Systems Audit Manager,
Nets Norway Branch

Magnus Digernes
Head of Enterprise Risk Management
Yara

Neste utgivelse er juni 2017

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
Meninger og påstander som fremkommer i artikler eller innlegg er ikke nødvendigvis sammenfallende med IIA Norges syn.

Grafisk produksjon:
Merkur Grafisk AS

Forsidebilde:
Foto: corgarashu/shutterstock.com

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

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.

© 2016 PwC. Med enerett. I denne sammenheng refererer "PwC" seg til PricewaterhouseCoopers AS, Advokatfirmaet PricewaterhouseCoopers AS, PricewaterhouseCoopers Accounting AS, PricewaterhouseCoopers Skatterådgivere AS og PricewaterhouseCoopers Services AS som alle er separate juridiske enheter og uavhengige medlemsfirmaer i PricewaterhouseCoopers International Limited.

INNHOLD

INTERNREVISJON

8 Endrede IIA standarder fra 1. januar 2017

14 Ekstern evaluering – krav, valg og erfaringer

44 Revisjon i en digital verden

47 Ny fellesavtale på internrevisjon for statlige virksomheter

59 Humor i særklasse

RISIKOSTYRING

9 Vill vest i Wells Fargo

10 Effektiv implementering av COSOs nye anti-mislighetshåndbok

13 Hva skjer med Risikostyringsforskriften?

30 Risikomatriser- forutsetninger og fallgruver

39 Hvorfor bør styret stille tydeligere krav til risikostyringen?

COMPLIANCE

6 Hvem skal granske?

17 Despite mature compliance programs we all need guidance on «adequate procedures»

50 Intervju med Frede Aas Rognlien om korrupsjon

52 Ny personvernforordning - Gjensidiges forberedelser

54 Hvitvaskingsloven og eiendomsmeglere

22

39

44

9

18

VIRKSOMHETSSTYRING

18 Lasse Birkeland – med etikk som hjertesak

22 «Banking is people» – men regelstyrt eller verdistyrt?

26 Erfaringer med programvare for internrevisjon, risikostyring og compliance

32 Introducing a fresh approach and new medicine to tackle the constant headache of fraud and corruption (Part 1)

35 Styringssystem for sikkerhet

48 Hva kan vi forvente av blokkjedeteknologien på kort sikt?

FASTE SPALTER

2 Redaktørens spalte

3 Presidenten har ordet

58 Kursaktiviteter 2016

57 Det var en gang

60 Generalsekretæren informerer

63 På tampen

INTERNREVISJONEN VS. COMPLIANCE-ENHETEN:

Hvem skal granske?

Av
PARTNER OG ADVOKAT NICOLAI SKRIDSHOL OG SPECIAL ADVISOR LENE EIA BOLLESTAD
Granskingsavdelingen i Steenstrup Stordrange

Med respekt overfor de selskaper og personer som muligens vil være av en annen mening, tillater vi oss likevel å dele noen tanker om hva vi tror er den mest hensiktsmessige plasseringen av ansvar for gjennomføring av private granskinger.

Vi er av den oppfatning at selskaper, organisasjoner og offentlige institusjoner kan gjennomføre granskinger. Vi tenker da både på situasjoner der granskingen gjennomføres med eller uten mistanke om at korrupsjon, annen økonomisk kriminalitet eller brudd på interne eller eksterne retningslinjer har funnet sted. Dersom et selskap skal gjennomføre granskingen, er det avhengig av om undersøkelsen kan gjennomføres på en forsvarlig måte; hvor de(n) som gjennomfører granskingen innehar rett kompetanse og hvor det er fornuftig at selskapet gjennomfører slik korrupsjonsgransking.

Dersom selskapet innehar korrekt kompetanse og det både er fornuftig og forsvarlig at selskapet gransker, blir neste spørsmål om eksterne spesialister skal delta i hele eller deler av granskingen; blant annet av hensyn til å få muliggjort erfaringsutveksling i arbeidet med å finne frem til relevant faktum.

Forutsatt at det private selskapet innehar kompetanse til å gjennomføre granskingen alene eller sammen med ekstern kompetanse, blir spørsmålet om hvilken del av organisasjonen som skal ha ansvaret for å gjennomføre granskingen. Denne avgjørelsen bør selskapet ha vurdert så tidlig som mulig og helst i god tid før det eventuelt skulle bli nødvendig å gjennomføre gransking.

Ved gjennomføring av granskinger er det viktig at den delen av selskapet som skal gjennomføre granskingen innehar uavhengighet, kompetanse og tilstrekkelig med ressurser til å finne frem til relevant faktum. I tillegg er det viktig at enheten kan rapportere direkte til styret eller øverstbesluttende organ. Erfaringsmessig omfatter en Compliance-enhets rolle å fungere som rådgivere overfor selskapet for øvrig, typisk ved å bistå i transaksjoner, med bakgrunnsundersøkelser og ved å gi råd om selskapets investeringer i eksisterende og nye selskaper, markeder og land. Dette er arbeidsoppgaver som kan innebære at det er risiko for at det kan reises kritikk fra blant annet omverdenen ved en senere gransking der ansvaret for slike undersøkelser også tilligger Compliance-enheten.

Ovennevnte standpunkt begrunnes i at løpende deltakelse i selskapets forretningsprosesser vil kunne innebære at det kan stilles spørsmål ved om alt av relevant faktum er funnet frem til og presentert i den senere granskingen. Blant annet kan det oppstå usikkerhet om Compliance-enheten har ubevisst eller bevisst latt være å finne frem til alt relevant faktum, fordi de mener de kjenner tilstrekkelig sider av virksomhetens prosesser og faktum allerede. En slik situasjon kan innebære at enheten ikke ser det objektive behovet for ytterligere undersøkelser eller ikke ser nødvendigheten av å utfordre faktum som er kjent, men ikke undergitt kritisk analyse. Dette vil kunne ha sin bakgrunn i at kulturen (tone at the top) ikke aksepterer at «etablerte sannheter» utfordres. Andre ganger kan det være fordi Compliance-enheten selv har gitt råd og innspill til selskapets virksomhet og at den ikke ønsker å vise eventuelle svakheter ved de råd som er gitt eller så enkelt som at de ikke kan eller skal granske seg selv.

Med blant annet fokus på det grunnleggende behovet for tillit til at granskingen er gjennomført med nødvendig uavhengighet og på en forventet forsvarlig måte, er det etter vår mening ofte mest hensiktsmessig at internrevisjonen (Internal Corporate Audit) innehar ansvaret for granskinger. Denne enheten skal være uav-

hengig og har som oftest lang erfaring med å gjennomføre krevende revisjoner av ulike deler av selskapets virksomhet. Dersom denne enheten innehar den nødvendige faglige kompetansen til å gjennomføre granskingen, vil en slik enhet kunne finne frem til relevant faktum på en forsvarlig måte, gjennomføre krevende prosesser internt og samtidig inneha den objektive tilliten til at prosessen er gjennomført på en profesjonell og forsvarlig måte. I tillegg vil den enheten normalt ha en direkte rapporteringslinje til styret. Dersom det ikke er tilrettelagt for eller ønskelig at internrevisjonen skal ha ansvaret for granskinger, kan et alternativ være at det etableres en egen enhet som trer sammen når det er behov for granskinger. En slik enhet bør underlegges de samme krav til blant annet uavhengighet, kompetanse og rapporteringslinje til styret som gjelder for internrevisjonens forsvarlige arbeid med granskinger. Avslutningsvis kan det også nevnes at ansatte vil kunne finne det krevende å kontakte Compliance-enheten når man har spørsmål, da de ikke vet hvilken rolle Compliance velger å inneha ved mottak av informasjonen; er enheten rådgiver eller gransker? Dette kan skape distanse og manglende informasjonsflyt til viktige funksjoner som eksempelvis Compliance-enheten. Dette er også forhold som tilsier at varslingsmottak bør være hos andre avdelinger enn Compliance-enheten; eksempelvis hos internrevisjonen.

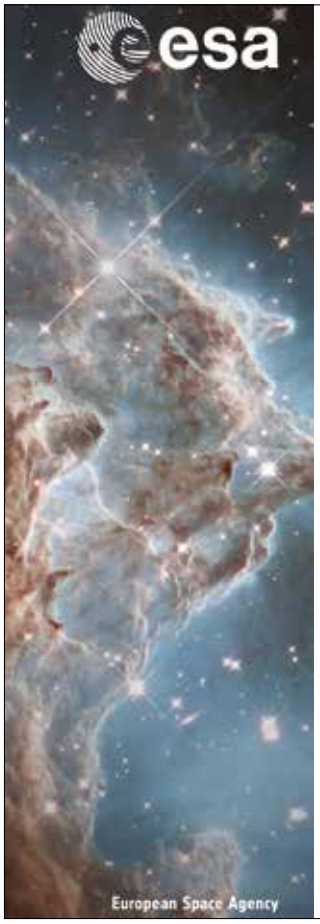
Uansett hvilken avdeling i selskapet som innehar ansvaret for gransking, er det forventet at prosessen gjennomføres forsvarlig og med den nødvendige uavhengighet til virksomheten. Dette skaper troverdighet til prosessen, både internt og eksternt.

Lykke til med plassering av granskingsansvar og eventuell(e) fremtidig(e) gransking(er). Det blir interessant og spennende å følge dere.

Bon Voyage!

PRAKTISKE TIPS FOR Å SIKRE EN VELLYKKET OG FORSVARLIG GRANSKNINGSPROSESS:

- Godt gjennomtenkt mandat bør utarbeides før granskingen påstartes; fordrer nært samarbeid mellom oppdragsgiver og granskere
- Teamet må inneha granskekompetanse og tilstrekkelig uavhengighet
- Løpende involvering fra oppdragsgiver for å sikre forankring, forståelse og tillit i organisasjonen
- God kommunikasjon og informasjon til involverte parter
- Grunnleggende rettsprinsipper må etterleves i prosessen, for eksempel kontradiksjonsprinsippet og vern mot selvinkriminering
- Fremgangsmåte ved innsamling av dokumentasjon og data, intervjuer og analyse av funn må følge god praksis
- Rapporten skal svare ut mandatet og gi en objektiv beskrivelse av de faktiske omstendighetene



The European Space Agency (ESA) is seeking an

Internal Auditor (m/f)

in the Internal Audit and Evaluation Service, Director General's Services
to be based at the ESA Headquarters in Paris, France or ESTEC, Noordwijk, Netherlands

The European Space Agency (ESA) is an intergovernmental organisation whose mission is to shape the development of Europe's space capability and ensure that investment in space continues to deliver benefits to the citizens of Europe. ESA employs about 2200 staff members across Europe and has a budget of 5.2 billion euros.

Within the Internal Audit and Evaluation Service, the postholder will conduct audits of the Agency's activities and carry out management consultancy assignments to ensure the effectiveness of ESA's organisation and the adequacy of controls and risk management to achieve the Agency's strategic objective

Applicants for this post should have a Master's degree in auditing, engineering, business administration, or other relevant discipline, with a minimum of three years' experience of internal auditing in an international environment. Candidates should be Certified Internal Auditors or the equivalent. Certified competence in auditing Management Information Systems will be considered a strong asset.

Excellent analytical, organisational and coordination skills and the ability to provide quality summary output against tight deadlines are prerequisites for this post as well as good communication and interpersonal skills.

The working languages of the Agency are English and French. A good knowledge of one of these is required together with a working knowledge of the other.

For a complete job description visit the **http://www.esa.int/About_Us/Careers_at_ESA/Vacancies** or visit the **«Careers at ESA»** webpage. If you wish to apply, please complete the online application form which can be found by clicking on the link within the vacancy notice, reference ESA/VN-HO(2016)019

Closing date: 4 th January 2017

ESA is an equal opportunities employer that offers challenging career opportunities and excellent employment conditions.

Please note that applications are only considered from nationals of one of the following States: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the United Kingdom and Canada.

Aktor

Endrede IIA standarder fra 1. januar 2017

Av
TRYGVE SØRLIE
Trygve Sørlie Services
EPF og medlem av IIASB
frem til juni 2016

International Internal Audit Standards Board (IIASB) har vedtatt endringer i de internasjonale standardene for profesjonell utøvelse av internrevisjon med virkning fra 1. januar 2017. Vedtaket kom etter en 90 dagers høring og gjennomgang av 1 144 svar fra organisasjoner og enkeltindivider fra hele verden samt vurdering og godkjenning fra «International Practice Framework Oversight Council». IIASB har arbeidet med endringene siden standardene sist ble endret 1. januar 2013.

Endringene introduserer to nye standarder:

1112 – Som omhandler sikringstiltak i situasjoner når revisjonssjefen blir bedt om å påta seg roller ut over internrevisjon.

1130.A3 – Som omhandler forutsetninger som må være til stede for at internrevisjonen kan utføre bekreftelsestjenester på områder den tidligere har gitt rådgivning på, for ikke å svekke objektiviteten til internrevisjonsfunksjonen.

Endringene bedrer sammenhengen mellom standardene, kjerneprinsippene og internrevisjonens formål.

Det er foretatt en rekke endringer i standardene for å få en bedre sammenheng mellom standardene, kjerneprinsippene og internrevisjonens formål. Det er særlig de to kjerneprinsippene «Tilpasser seg organisasjonens strategier, mål og risikoer» og «Er innsiktsfull, proaktiv og fremtidsfokusert» som tidligere var lite omtalt i standardene og som derfor har medført et behov for tilpasning av standardene.

Endringene oppdaterer eksisterende standarder:

En rekke standarder er oppdatert for å gjøre innholdet tydeligere og lettere å forstå samt for å presisere det som kreves for å være i overensstemmelse med standardene.

En nyhet er at det i **1300-serien** presiseres at styret bør oppfordres til å ha tilsyn med internrevisjonens program for kvalitetssikring og forbedring samt den eksterne evalueringen, for å redusere faren for interessekonflikter. Videre er kravet til revisjonssjefens årlige rapportering til toppledelsen og styret om kvalitets- og forbedringsprogrammet samt nåværende situasjon i forhold til hvorvidt internrevisjonsfunksjonen er i overensstemmelse med standardene, skjerpet.

Standard 2050 omhandler nå i tillegg til samhandling, også situasjonen når internrevisjonen benytter arbeidet til andre bekreftelses og tjeneste leverandører og en fortolkning av hva dette innebærer.

Standard 2060 presiserer nå at internrevisjonen i sin periodiske rapportering til toppledelsen og styret skal inkludere en omtale av internrevisjonens overensstemmelse med de etiske reglene og standardene. I tolkingen av standard 2060 er det også tatt inn en samlet opplisting av de kravene standardene setter til internrevisjonens rapportering til toppledelsen og styret.

I **standard 2210.A3** er det kommet en ny tolkning som lister opp tre typer kriterier for evaluere governance, risikostyring og kontroller og eksempler på hva disse kan være.

I tolkingen av **standard 2450** Om overordnede uttalelser er det nå kommet et krav om at rapporteringen skal inkludere en oppsummering av informasjonen som støtter opp under uttalelsen.

Til slutt kan det nevnes at definisjonen av «Styret» er endret slik at den på en bedre måte enn tidligere passer inn i offentlig sektor og andre steder som ikke har et tradisjonelt styre.

De endrede IIA standardene som trer i kraft fra 1. januar 2017 er publisert på norsk på www.iia.no.

Vill vest i Wells Fargo

Foto: Joseph Sohm/Shutterstock

Wells Fargo har røtter tilbake til 1852 og ble drevet i de første 50 år som en kombinert bank og diligenceselskap. Jeg må tilstå at det er fra reklame på hestevogner i gamle westernfilmer jeg kjenner best navnet. Faktisk vokste Wells Fargo fra denne spede begynnelsen til å bli utnevnt i 2014 til å være verdens mest verdifulle bankmerkevare og ble den 2. største bank i verden etter markedsverdi. Man var med andre ord helt på toppen av bankpyramiden.

Det fatale skjedde for banken 8. september 2016 da det amerikanske forbrukerrådet for finans offentliggjorde at Wells Fargo hadde gått med på å betale en bot på USD 185 millioner. Banken hadde opprettet ca. 2 millioner kontoer uten kundenes samtykke men som kundene ble belastet gebyr for. I tillegg hadde man utstedt kredittkort med falske pinkoder. Bakgrunnen for dette var et enormt salgspress på de ansatte. Kryssalg var målet. En ansatt har senere fortalt at han måtte vise til at han hadde solgt minst fire lån og fire kredittkort i uken– og han måtte nå dette målet for å beholde jobben. Det var ikke snakk en gang om at han skulle få bonus for å ha nådd salgsmålet. I alt 5.300 ansatte måtte ta sin hatt og gå på grunn av disse fiktive salgene. Man kan trygt si at det hadde vokst frem en ukultur og hvem var ansvarlig for det?

I en offentlig høring i senatet to uker senere kom det tydelig frem at ansvaret skulle plasseres på skuldrene til bankens CEO John Stumpf og han ble åpent oppfordret til å gå av. Først ga Stumpf avkall på en tildeling av aksjer (regulert av lønns- og bonusavtalen) på USD 42 millioner. Når ikke det var nok til å stille motbøren fra media, og etter enda en senathøring valgte han å si opp sin stilling 12. oktober 2016. Det hører med til historien at etter at nyheten om hans avgang ble kjent steg aksjeverdien med 1,8 % etter et fall på 17% i året hittil.

Som en sjeldenhet blant skandaler av denne typen var det toppsjefen Stumpf som tok sin hatt og gikk. Dette henger nok sammen med at han personifiserte den ukulturen som hadde vokst frem. Han sto frem med slagordet «Eight is Great» som skulle henvise til at de ansatte skulle få solgt åtte forskjellige bankprodukter til hver kunde.

Dette er nok et eksempel på at fisken råtner fra hodet. Gammel lærdom er like relevant. Tone at the top er viktig. Salgsmål skal ikke kunne overkjøre etisk behandling av kunden. Urealistiske mål kan føre til at noen bestemmer seg for å fikse det slik at målene oppnås. Det spesielle med saken er kanskje det at banken ikke tjente penger en gang på å opprette disse falske kontoene men de tapte enormt på skadet renommé blant kunder og investorer.

Martin Stevens
Medieutvalget

Effektiv implementering av COSOs nye anti-mislighetshåndbok

I september 2016 lanserte COSO sammen med ACFE (Association of Certified Fraud Examiners) en ny håndbok for risikostyring av misligheter (Fraud Risk Management Guide), for å hjelpe organisasjoner å beskytte seg selv og sine interessenter fra interne og eksterne misligheter.

Av
KJETIL HELVIG,
CFE OG STYREMEDLEM ACFE NORGE
Leder av Integrity & Compliance,
EYs granskingsavdeling

Håndboken beskriver viktigheten av å håndtere mislighetsrisiko på følgende måte: *«Store mislighetssaker har ført til kollaps av organisasjoner, betydelige tap av eiendeler og investeringer, høye saksomkostninger, fengsling av nøkkelpersoner, og tap av tillit i kapitalmarkedet og i offentlig sektor.»*

I denne artikkelen vil jeg gi en oppsummering av anti-mislighetshåndboken og dens forhold til COSOs rammeverk for internkontroll. Videre vil jeg beskrive COSOs definisjon av misligheter, prinsippene for mislighetsrisikovurdering og –risikostyring, og avslutningsvis gi en praktisk veiledning for implementeringen av anti-mislighetshåndboken.

COSOs rammeverk for internkontroll

Helt fra lanseringen av det opprinnelige rammeverket for interkontroll i 1992 har COSO gitt veiledning i eierstyring og internkontroll, som har vært omfattende brukt som ledende praksis ved en rekke organisasjoner. Håndboken i mislighetsrisikostyring bygger på COSOs 2013-oppdatering av rammeverket for internkontroll hvor mislighetsrisikovurderinger ble introdusert som et eget prinsipp. COSO anser nå mislighetsrisikostyring som «en integrert del av bedriftens styring og internkontrollmiljø», og understreker at både styret og toppledelsen har et sentralt ansvar for mislighetsrisikostyring.

Anti-mislighetshåndboken anbefaler en helhetlig vurdering av risikoer for misligheter, separat fra risikoen for internkontrollfeil. Håndboken anbefaler også at hver organisasjon etablerer et mislighetsrisikoprogram. Som støtte til denne anbefalingen inkluderer COSO ulike verktøy og ressurser for å gjennomføre en mislighetsrisikovurdering, skrive en anti-mislighetsretningslinje og etablere et gjennomgående anti-mislighetsprogram.

Organisasjoner bør gjennomgå anti-mislighetshåndboken for å vurdere deres eksponering mot misligheter, benchmarke sine elementer opp mot COSOs prinsipper for mislighetsrisikostyring og vurdere hvordan virksomheten kan tilpasse innhold i håndboken til deres spesifikke behov. Hver organisasjon bør ta valg basert på en forståelse av mislighetsrisikoen og risikotoleransen i organisasjonen, sammen med kost-nytte betraktninger ved spesifikke anti-mislighetskontroller.

Uredelig regnskapsrapportering	▸ Enhver tilsiktet feilinformasjon av et regnskap representerer en uredelig regnskapsrapportering.
Uredelig ikke-finansiell rapportering	▸ Uredelig ikke-finansiell rapportering av risiko og ordninger som kan føre til uriktig rapportering av miljø, sikkerhet, kvalitetssikring eller operasjonelle beregninger.
Underslag av eiendeler	▸ Foretatt av ansatte, kunder eller leverandører, inkludert kriminelle organisasjoner, påvirker faste og immaterielle eiendeler og forretningsmuligheter. ▸ Eksempler på dette er tyveri, fiktive leverandørfakturaer, falske kundekrav og eksterne cyberangrep
Andre ulovlige handlinger og korrupsjon	▸ Ulovlige handlinger kan være brudd på lover eller reguleringer som kan ha en materiell direkte eller indirekte påvirkning på den eksterne finansielle revisjonen. ▸ Eksempler er brudd på lover og reguleringer som bestikkelser, ulovlig bruk av personopplysninger, handelshemmeligheter eller nasjonal sikkerhetsinformasjon, og brudd på arbeidsmiljø-, konkurranse- eller forbrukerlovgivning. ▸ Korrupsjon er ifølge håndboken definert som «misbruk av makt i betrodde stillinger for privat vinning.»

COSOs definisjon på misligheter

COSO definerer misligheter på følgende måte: *«Misligheter er enhver forsettlig handling eller unnlatelse formet for å bedra andre, som resulterer i at offeret lider et tap og/eller at gjerningsmannen oppnår en gevinst.»* Omfanget av mislighetsområdet er økende og håndboken deler misligheter i følgende kategorier:

Anti-mislighetshåndboken fastsetter en tilnærming for å identifisere, vurdere og håndtere dette brede spekteret med risikoer.

Styrking av 2013-rammeverkets prinsipp for mislighetsrisikovurdering

Ved revisjonen av COSOs rammeverk for internkontroll i 2013 definerte COSO 17 prinsipper som styrer design og implementering av systemer for internkontroll. For at et internkontrollsystem skal være effektivt må alle prinsippene være til stede, fungere og operere sammen på en helhetlig måte. Prinsipp 8 av 2013-rammeverket fokuserte spesielt på misligheter ved å kreve at organisasjonen vurderer «potensialet for misligheter i vurderingen av risiko for måloppnåelse».

COSO går nå utover denne mislighetsrisikovurderingen ved å fremsette fem prinsipper for mislighetsrisikostyring.

De fem mislighetsprinsippene for risikostyring er ikke obligatoriske for etterlevelse av 2013-rammeverket. Anti-mislighetshåndboken er ment å være en støtte til, og tilpasset, rammeverket. En organisasjon kan gjennomføre en mislighetsrisikovurdering etter 2013 COSO-rammeverkets prinsipp 8, eller velge å

Kontrollmiljø	Principle 1: The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.	Adresserer mislighetsrisikostyring ved å gi et grunnlag for etisk atferd og et eierstyringsprogram knyttet spesifikt til mislighetsrisiko. Håndboken sier at det er «kritisk for å lykkes med et program for mislighetsrisikostyring at et medlem av ledelsen blir tildelt et overordnet ansvar for mislighetsrisikostyring og må rapportere jevnlig til styret.»
Risikovurdering	Principle 2: The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.	Adresserer mislighetsrisikovurdering ved å identifisere konkrete risikoelementer, vurdere deres sannsynlighet og potensielle konsekvenser samt vurdere effekten av organisasjonens kontroller. Som anti-mislighetshåndboken erkjenner, er risikotoleranse en viktig faktor. En virksomhet bør investere i styringen av sine mest kritiske risikoer.
Kontrollaktiviteter	Principle 3: The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.	Adresserer mislighetskontrollaktiviteter. Kontrollene er spesifikke for hver mislighetsrisiko og er utformet for å forebygge hendelser eller avdekke dem tidlig. En organisasjon bør bruke en sammensetning av kontroller på forskjellige punkter i en forretningsprosess. Forebyggende kontroller er bredt kommunisert; avdekkende kontroller fungerer mer i bakgrunnen. Håndboken beskriver også hvordan dataanalyse kan være både en kostnadseffektiv avdekkende kontroll, men også en særegen innsikt over uregelmessigheter, trender og risikoindikatorer.
Informasjon og kommunikasjon	Principle 4: The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.	Adresserer behandlingen av rapporter om misligheter gjennom «et system for rask, kompetent, og konfidensiell vurdering, gransking, og løsning på tilfeller av brudd og påstander som involverer misligheter og annen uredelighet.» En organisasjon bør ha protokoller for mislighetsgransking og respons, og utgangspunktet bør være en «si-noe-hvis-du-ser-noe»-kultur. Videre bør organisasjonen ha klare retningslinjer for hasterapportering, saksbehandling, sikring av bevis, innhenting av juridisk og forensic regnskapsmessig bistand, vurdering av hovedårsaken og forbedring av kontroller.
Monitorering	Principle 5: The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors	Adresserer overvåking og monitorering av programaktiviteter for å sikre at hver av de fem prinsippene er tilstede og fungerer som de skal, samt påpeke svakheter. Organisasjoner bør etablere beregninger av programvirksomheten og utfall, for eksempel, år-over-år trender av mislighetshendelser. Organisasjoner bør også «vurdere kjente mislighetsordninger og nye misligheter avdekket og rapportert i andre bransjer og i andre organisasjoner i samme bransje.»

implementere håndboken som en parallell og mer omfattende mislighetsrisikostyringsprosess.

COSO gir i anti-mislighetshåndboken en detaljert veiledning til implementering av hver av de fem prinsippene for mislighetsrisikostyring:

Økt fokus på dataanalyse

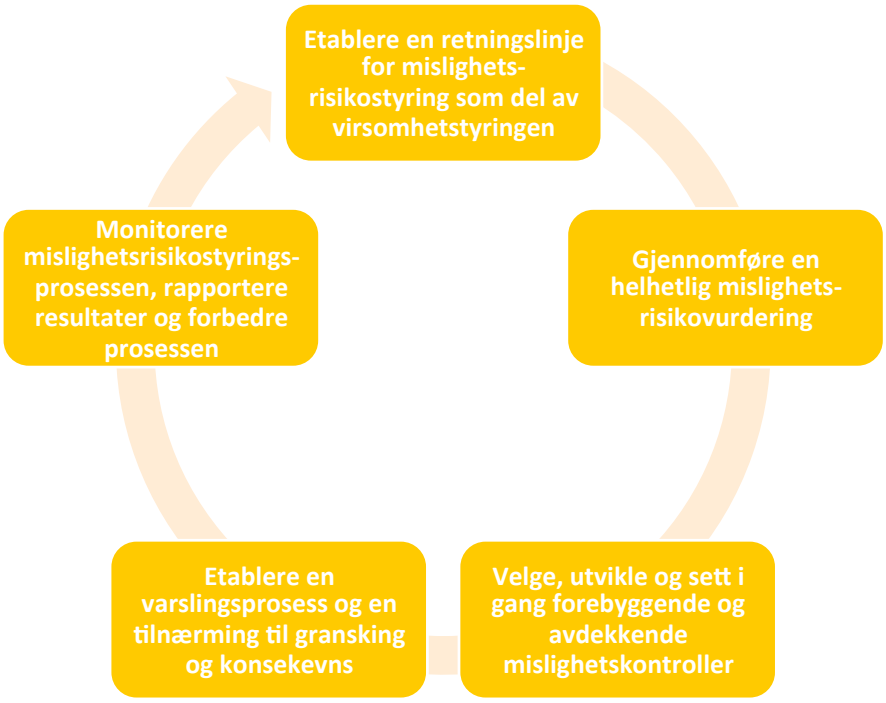
Den største endringen ved COSOs lansering av anti-mislighetshåndboken er det økte fokuset på dataanalyser. Håndboken anbefaler at hver organisasjon har «en strategi for proaktivt, ved hjelp av dataanalyseaktiviteter, å vurdere områder med høy mislighetsrisiko og overvåke forbedringstiltak og kontroller.»

EY anser dataanalyse som et viktig element for mislighetsrisikostyring. Myndigheter bruker stadig mer dataanalyse for å avdekke misligheter og faglige veiledninger oppfordrer revisorer til å bruke dataanalyse i mislighetsrisikovurderinger. Volumet av data som organisasjoner genererer har eksplodert, og mange nye analyseverktøy har kommet på markedet. COSO beskriver i håndboken hvordan dataanalyseteknikker blant annet kan hjelpe til med å identifisere transaksjoner eller trender som representerer potensielle misligheter, samt hvordan dataanalyse kan være til støtte i granskinger og videreutviklingen av internkontroll.

Anti-mislighetshåndboken gir praktiske eksempler for anvendelse av ledende dataanalyseteknikker som spenner fra enkel kategorisering til prediktiv og normative modeller, som for eksempel:

- Data stratifisering som viser transaksjoner i ulike forretningsenheter eller regioner
- Risikoscoring
- Trendanalyse
- Datavisualisering
- Statistisk og prediktiv modellering
- Big data og eksterne informasjonskilder, inkludert både strukturerte og ustrukturerte datakilder

Vedlegg E i Anti-mislighetshåndboken beskriver hvordan virksomheter kan implementere et dataanalyseprogram i sammenheng med et mislighetsrisikoprogram.



Figur: Pågående helhetlig prosess for mislighetsrisikostyring.

Hva bør organisasjoner gjøre nå?

Anti-mislighetshåndboken fastsetter en prosess for kontinuerlig og systematisk mislighetsstyring

EY anbefaler at hver organisasjon vurderer denne prosessen, og ser på publikasjonen av anti-mislighetshåndboken som en mulighet til å gjennomgå sitt mislighetsrisikosystem. Som et første skritt anbefaler vi at organisasjonen danner et team bestående av representanter fra ulike avdelinger og forretningsområder, som har ulike perspektiver på organisasjonens virksomhet, mislighetsrisiko og anti-mislighetskontroller.

EY foreslår at teamet blant annet bør vurdere følgende elementer:

- Gjennomgå anti-mislighetshåndboken som en benchmarking mot dagens situasjon
- Gjennomgå virksomhetens siste mislighetsrisikovurdering for å avgjøre om den gir et klart bilde av selskapets risiko og et solid grunnlag for beslutninger
- Vurdere hvor godt forberedt virksomheten er innenfor å forebygge, avdekke og reagere på misligheter
- Gjennomgå programmer og avdelinger som har en rolle i styringen av mislighetsrisikoer, eksempelvis organisasjonens finansielle controllerstruktur, anti-korrupsjonsprogram og cybersecurity-program.
- Gjennomgå organisasjonens mislighetsrisikostyring for å fastslå om roller og ansvar er klart definert, inkludert eventuelle forsvarslinjer, som for eksempel ledelse, mislighetsrisikoeiere og internrevisorer.
- Gjennomgå etikk og complianceprogrammet, inkludert organisasjonens etiske retningslinjer, - varslingskanal og granskingsprotokoller.
- Vurdere om styret har den informasjonen den trenger for å ha oversikt over anti-mislighetsrisikoen organisasjonen er utsatt for.
- Vurdere om ledelsen har en klar etisk «tone fra toppen», og om det er en kultur for integritet i alle organisasjonens avdelinger og evt. regionale virksomhet.
- Vurdere om ledelsen har den informasjonen som er nødvendig for å ta avgjørelser om mislighetsrisikostyring og fordeling av ressurser.
- Utarbeide anbefalinger for implementering.

Hva skjer med Risikostyrings-forskriften?

For oss som har arbeidet med risikostyring, internkontroll og internrevisjon i finans over noen år så har Finanstilsynets Forskrift om risikostyring og internkontroll vært å betrakte som selve bibelen. Den kom for første gang i kjølvannet av finanskrisen tidlig på 90-tallet og har senere vært endret flere ganger blant annet ved utvidelse av virkeområdene. I 2003 kom det en annen vesentlig endring ved at internrevisjonen ble regulert inn i forskriften. Nå står en ny endring av forskriften for døren, og mange av oss har interesse av å finne ut hva som blir nytt.

Ledernettverket for finans avholdt sin årlige høstkonferanse 20. oktober. Ett av temaene var «Nytt fra det regulatoriske området», der Are Jansrud fra Finans Norge stilte med et interessant foredrag.

Hans foredrag dekket svært mange områder, men hvis vi konsentrerer oss om Risikostyringsforskriften så er status som følger.

Finansforetaksloven trådte i kraft fra 1. januar 2016. Finanstilsynet har sendt Forslag til forskrifter til finansforetaksloven på høring med frist 1. april 2016. I dette forslaget foreslås det å rydde opp og samle en rekke av dagens forskrifter til én samleforskrift til finansforetaksloven, «finansforetaksforskriften».

Enkelte større forskrifter videreføres imidlertid parallelt med utkastet til en ny samleforskrift. For forsikringsselskap er det gitt utfyllende regler til finansforetaksloven gjennom Solvens II-forskriften som følger opp EU-regler på området. Tilsvarende vil CRD IV-regelverket for banker mv. følge av CRR/CRD IV-forskriften. Sistnevnte forskrift får regler om internrevisjon og compliancefunksjon.

Enkelte andre viktige forskrifter, særlig på bankområdet, videreføres også. Dette gjelder forskrifter om godtgjørelse, kapitalkrav, ansvarlig kapital, likviditetsstyring, mv.

Forskriftsforslagene er fortsatt ikke fastsatt, men fra tidspunktet for ikrafttredelsen av disse endrede og nye forskriftene vil finansforetakene ikke lenger være underlagt Risikostyringsforskriften.

Siden Risikostyringsforskriften ikke lenger skal gjelde for Finansinstitusjoner, blir det en endring i forskriftens § 1, som hittil har regulert 12 virkeområder. Dessuten oppheves § 6 tredje ledd: «Foretak som gjennomfører risikostyring og vurdering av risiko og kapitalbehov i samsvar med lov 10. juni 1988 nr. 40 om finansieringsvirksomhet og finansinstitusjoner (finansieringsvirksomhetsloven) § 2-9 til og med § 2-9d og forskrift 14. desember 2006 nr. 1506 (kapitalkravsforskriften) anses for å ha oppfylt kravene i første og annet ledd.»

Risikostyringsforskriften vil imidlertid fortsatt gjelde for de øvrige 11 virkeområdene.

Reidar Døli
Internrevisor
Oslo Børs VPS

Foto: Standret/Shutterstock

Ekstern evaluering – krav, valg og erfaringer

AV INTERNREVISORER LIV TVEITEN LÜDEMANN OG ANDERS LEDSAAK NORDLUND I HELSE SØR-ØST

Liv og Anders har arbeidet i Helse Sør-Øst´s konsernrevisjon siden våren 2013. Liv er utdannet sykepleier og siviløkonom fra NHH med master i økonomisk analyse, og har tidligere arbeidet i akuttmottaket på Sørlandet Sykehus og kirurgisk avdeling på Haukeland Universitetssykehus.

Anders er utdannet fysioterapeut og har mastergrad i Helsefagvitenskap. Etter turnustjeneste jobbet han som fysioterapeut på St. Olavs Hospital og ved Friskvernklinikken. Før han begynte i konsernrevisjonen HSØ arbeidet han med prosjektledelse og forvaltning i Helsedirektoratet. Begge har søknader inne om diplomering som internrevisorer.

Innledning

Fokuset på god styring og kontroll har aldri vært større enn nå. Både myndigheter, media og opinionen gransker virksomhetene for å avdekke avvik fra god praksis. Med sin særegne plassering i organisasjonen kan internrevisjonsfunksjonen bidra til bekrefte at tilstrekkelig og hensiktsmessig styring og kontroll er etablert. Med det bakteppet er kravene fra styre og ledelse til kvaliteten på internrevisjonsenhetenes arbeid økende, og det er avgjørende at revisjonsutvalgene har tillit til internrevisjonens evne til å levere. Ledere for internrevisjonsenheter er under økende press for å bevise at de bidrar med merverdi og forbedring i styring og kontroll i organisasjonen. En forutsetning for at internrevisjonsenheter gir merverdi er at de konsentrerer seg om de rette områdene, er effektive og kommuniserer klart og tydelig resultatet av sitt arbeid. Det er imidlertid indikasjoner på at evalueringsmekanismene knyttet til internrevisjonens arbeid ikke har utviklet seg i takt med det økte fokuset på internrevisjon. Dette kan medføre at det er vanskelig å vurdere om internrevisjonen faktisk leverer i tråd med interessentenes forventinger. En ekstern evaluering av internrevisjonsenheten kan bidra til å validere kvaliteten på enheten og sikre samsvar mellom forventningene til leder av internrevisjonen og styre og ledelse i virksomheten.

I forbindelsen med gjennomføringen av Master of Management - modulen «Internrevisjon; Governance -Risikostyring - Intern styring og kontroll» på BI skrev forfatterne prosjektoppgave om temaet ekstern evaluering av internrevisjonsenheten. Formålet med arbeidet var å skaffe en oversikt over de formelle krav og rammer som gjelder for ekstern evaluering, hvilke valgmuligheter som finnes for gjennomføringen gitt disse ytre rammene og hvilke erfaringer andre internrevisjonsenheter har gjort seg angående temaet. Basert på dette var det ønskelig å gi en anbefaling til hvordan konsernrevisjonen Helse Sør-Øst bør møte kravet til ekstern evaluering. I denne artikkelen presenteres et utdrag av resultatene som fremkom i arbeidet.

Metode

For å belyse kravene til og rammene for ekstern evaluering, hvilke valgmuligheter en internrevisjonsenhet har for gjennomføringen og om det har vært publisert forskning eller erfaringsbaserte artikler om emnet ble det gjennomført en dokumentundersøkelse.

For å innhente erfaringer fra andre internrevisjonsenheter ble det gjennomført en elektronisk spørreundersøkelse. Undersøkelsen ble distribuert til medlemmene i ledernettverket til IIA Norge, og utvalget ble da 39 potensielle respondenter. Det var 22 som responderte, noe som ga en svarprosent på 56, 4 %. Hovedsakelig ble det stilt spørsmål om tre hovedtemaer; beskrivelse av internrevisjonsenheten, tilnærming til kravet om ekstern evaluering og erfaringer med eventuell gjennomføring av ekstern evaluering. Data fra spørreundersøkelsen ble analysert i SPSS (versjon 21).

Krav til ekstern evaluering

Standarder for profesjonell utøvelse av internrevisjon er utgitt av The Institute of Internal Auditors (IIA) og målbæres i Norge av IIA Norge. I standardene presiseres det at selv om ulike rammebetingelser kan påvirke hvordan internrevisjon blir praktisert i forskjellige miljøer, er overensstemmelse med IIAs internasjonale standarder for profesjonell utøvelse av internrevisjon avgjørende for å sikre at internrevisorer og internrevisjonen ivaretar sitt ansvar. Standard 1300 beskriver at revisjonssjefen må utarbeide og vedlikeholde et program for kvalitetssikring og forbedring som dekker alle aspekter ved internrevisjonen. Formålet med et slikt program er å gjøre det mulig å gjennomføre vurderinger av hvorvidt internrevisjonen er i overenstemmelse med definisjonen av internrevisjon, standardene og de etiske

reglene. Programmet skal også sikre at effektiviteten og hensiktsmessigheten av internrevisjonen vurderes, og at det identifiseres muligheter til forbedring. Standard 1310 beskriver at programmet skal omfatte både interne og eksterne evalueringer. Standard 1312 beskriver at eksterne evalueringer må gjennomføres minst hvert femte år og kan være i form av fullstendige eksterne evalueringer eller egenevalueringer med uavhengig ekstern validering.

Planlegging, gjennomføring og oppfølging av ekstern evaluering

Målet med en ekstern evaluering er å kartlegge og vurdere om internrevisjonsenhetens arbeid følger IIAs definisjon av internrevisjon, de etiske reglene og standardene for utøvelse av internrevisjon. I IIAs kvalitetssikringsmanual legges det opp til at alle standardene skal vurderes i forhold til skalaen:

– Tilfredsstiller standarden
– Tilfredsstiller delvis standarden
– Tilfredsstiller ikke standarden.

En ekstern evaluering kan også identifisere forbedringsområder knyttet til effektiviteten i internrevisjonsenheten og fremme forslag til forbedringer for å styrke enhetens omdømme og kredibilitet.

Det er ofte et revisjonsutvalg under styret som har hovedansvaret for å påse at internrevisjonen utfører oppgavene sine hensiktsmessig og effektivt. Et godt fungerende styre og revisjonsutvalg bør stille spørsmål om hvorvidt internrevisjonen gir merverdi, om dens plassering i organisasjonen er hensiktsmessig og om dens oppgaver er klart definert sammenlignet med andrelinjefunksjoner som risikostyring og compliance. En sentral kilde til kunnskap om dette kan være en ekstern evaluering av internrevisjonsfunksjonen. I tillegg til å vurdere samsvar med standardene kan en godt utført ekstern evaluering gi styre og revisjonsutvalg bekreftelse på internrevisjonens prestasjoner og gi innsikt i hvordan man kan sikre optimale internrevisjonstjenester. Den eksterne evalueringen kan dermed gi styret og revisjonsutvalg grunnlag for å vurdere justeringer av internrevisjonens prioriteringer og forventninger, identifisere muligheter for å forbedre internrevisjonsfunksjonen, og optimalisere nivået av samsvar med arbeidet til andre risikofunksjoner i organisasjonen.

Eksterne evalueringer må utføres av en kvalifisert, uavhengig kontrollør eller gruppe kontrollører utenfor organisasjonen. Den eksterne parten er vanligvis et team som blir innleid til formålet. Dersom de økonomiske rammene er trange kan en mulighet også være at minimum tre uavhengige organisasjoner går sammen og gjør en «peer assessment» av hverandres internrevisjon. En uavhengig kontrollør eller gruppe av kontrollører skal ikke inneha interessemotsetninger, og de skal ikke være en del av eller underlagt samme organisasjonen som internrevisjonen tilhører. Revisjonssjefen må bruke sitt profesjonelle skjønn ved vurderingen av hvorvidt en kontrollør eller gruppe av kontrollører har tilstrekkelig kompetanse til å kvalifisere seg for det gjeldende oppdraget. En global undersøkelse blant internrevisjonsenheter utført av IIA viste at 41 % valgte et av de store konsulentfirmaene som ekstern leverandør av ekstern evaluering, 26 % valgte et IIA – institutt (IIA Norge) og de resterende valgte «peer review» eller annet. De som gjennomførte full ekstern evaluering valgte oftest et konsulentselskap (54 %), mens valg av leverandør til intern evaluering med ekstern validering fordelte seg ganske likt mellom alternativene.

Ekstern evaluering kan variere fra et smalt fokus på IIA – standardene til en mer omfattende evaluering av enheten i konteksten av interessentenes forventinger og opp mot praksis hos ledende internrevisjonsenheter i andre organisasjoner. I en global studie uført av IIA fremkommer de tre vanligste grunnene som ble oppgitt for å gjennomføre en ekstern evaluering var muligheten for å «benchmarke» praksisen i internrevisjonen, å bekrefte at arbeidet ble utført i tråd med IIA standardene og å øke den opplevde verdien av internrevisjonsenheten i organisasjonen. Det var omtrent like vanlig å gjennomføre full ekstern evaluering som intern evaluering med ekstern validering. Mange internrevisjonsledere velger å gjennomføre en egenevaluering med ekstern validering i etterkant av etablering av et program for kvalitetssikring og forbedring, for å bekrefte at kvalitet er blitt bygd inn i aktivitetene på en god måte. Internrevisjonsenheter som har eksistert i mindre enn fem år velger i større grad å gjennomføre intern evaluering med ekstern validering. Intern evaluering med ekstern validering fokuserer i mindre grad på benchmarking og identifisering av ledende praksis. En fordel med en full ekstern evaluering kan være potensialet for et bredere fokus i gjennomgangen, noe som kan bidra til nyttige diskusjoner i organisasjonen om internrevisjonens plassering og oppgaver. Evalueringsprosessen kan også bli mer robust.

Revisjonssjefen må underrette toppledelsen og styret om resultatene fra kvalitets- og forbedringsgjennomganger (Standard 1320). Gjennomføringen og oppfølgingen av resultatet skal være et bidrag til felles forståelse og enighet om internrevisjonens oppgaver og ansvar på tvers i organisasjonen. Revisjonssjefen kan kun uttale at internrevisjonen er i overensstemmelse med de internasjonale standardene for profesjonell utøvelse av internrevisjon dersom resultatene fra kvalitets- og forbedringsprogrammer støtter utsagnet (Standard 1321).

Erfaringer med ekstern evaluering i norske internrevisjonsenheter

Det var 22 som responderte på spørreundersøkelsen og alle leverte fullstendig utfylte spørreskjemaer.

Beskrivelse av respondentene

- 81,8 % (n=18) av internrevisjonsenhetene hadde 15 ansatte eller færre
- 59,1 % (n=13) av internrevisjonsenhetene hadde eksistert i mer enn ti år, 23 % (n=5) hadde eksistert i fra fem til ti år mens 18,2 % (n=4), hadde eksistert i mindre enn fem år.
- 63,6 % (n=14) av respondentene hadde styret/revisjonsutvalget som sin oppdragsgiver, mens de øvrige hadde daglig leder i virksomheten.
- 68,2 % (n=15) hadde gjennomført ekstern evaluering av internrevisjonsenheten. Blant de som hadde eksistert i fra mer enn fem år hadde 83,3 % gjennomført ekstern evaluering. Blant de som svarte nei ble det

oppgitt ulike grunner til at det ikke hadde vært gjennomført en ekstern evaluering, som at de var en nyetablert funksjon eller at ekstern evaluering ikke var blitt prioritert. De fleste av de som ikke hadde gjennomført en ekstern evaluering, planla gjennomføring i 2017-2018.

Beskrivelse av gjennomføring av ekstern evaluering

- 86,7 % (n=13) oppga at det var leder av internrevisjonsenheten som var initiativtaker til at evalueringen skulle gjennomføres. Hos de øvrige var det styret/revisjonsutvalget som hadde tatt initiativ til gjennomføringen.
- 60 % (n=9) hadde gjennomført full ekstern evaluering, og 40 % (n=6) hadde gjennomført en intern evaluering med uavhengig ekstern validering.
- 46, 7 % (n=7) benyttet IIA Norge som leverandør, mens 53,3 % (n=8) hadde benyttet et konsulentfirma.
- 46,7 % (n=7) av respondentene oppga å ha betalt 199 000 kr eller mindre i honorar til den eksterne leverandøren. Én oppga å ha betalt mer enn 600 000 kr. Tre av respondentene ønsket ikke å svare på dette spørsmålet
- 73,3 % (n=11) oppga å ha benyttet under 200 timer på gjennomføringen av den eksterne evalueringen, mens én respondent oppga å ha benyttet så mye som 400 timer. Gjennomsnittlig tidsbruk var 130, 3 timer. Median var 100 timer.

Beskrivelse av erfaringer med gjennomføringen av ekstern evaluering

- 93,3 % (n=14) av respondentene opplevde at den eksterne leverandøren oppfylte standard 1312s krav til kvalifikasjoner og uavhengighet.
- 80 % (n=12) av respondentene opplevde at hovedfokuset i evalueringen hadde favnet både det interne arbeidet i enheten og enhetens rolle/samspillet med resten av virksomheten. 13,3 % (n=2) oppga hovedfokus som det interne arbeidet i internrevisjonsenheten, mens 6,7 % (n=1) oppga enhetens rolle og samspillet med resten av organisasjonen som hovedfokus.
- 46,7 % (n=7) oppga at konklusjonen på den eksterne evalueringen var at internrevisjonen var i overensstemmelse med de internasjonale standardene for profesjonell utøvelse av internrevisjon. De øvrige oppga at konklusjonen var at internrevisjonen hovedsakelig var i overensstemmelse med de internasjonale standardene for profesjonell utøvelse av internrevisjon, men at enkelte forbedringstiltak ble anbefalt.
- 73,3 % (n=11) rapporterte resultatene av den eksterne evalueringen til oppdragsgiver for internrevisjonen i egen rapport/notat eller likende, mens 20 % (n=3) inkluderte resultatet i annen fast rapportering som årsrapportering eller liknende. 6,7 % (n=1) hadde ikke rapportert resultatet av den eksterne evalueringen til oppdragsgiver.
- 33,3 % (n=5) av respondentene oppga at den eksterne evalueringen ga stor grad av ny innsikt angående kvaliteten på internrevisjonsenheten ut over det de hadde før evalueringen, men de øvrige oppga i noen grad å ha fått økt innsikt. Ingen oppga at de ikke fikk økt innsikt angående kvaliteten på enheten gjennom den eksterne evalueringen.
- 13, 6 % (n=3) opplevde at gjennomføringen av den eksterne evalueringen i stor grad hadde bidratt til forbedring av internrevisjonsenhetens arbeid, men de resterende opplevede at gjennomføringen i noen grad hadde bidratt til forbedring. Ingen oppga at gjennomføringen ikke bidro til forbedring.
- 60 % (n=9) oppga at gjennomføringen av den eksterne evalueringen etter deres mening har påvirket internrevisjonsenhetens renommé positivt. De øvrige mente at renommeét er uforandret. Ingen mente at renommeét var negativt påvirket av gjennomføringen.

I hvilken grad hadde valg av tilnærming og leverandør påvirkning på erfaringene som ble rapportert?

Analyse av data fra spørreundersøkelsen viste ingen sammenheng mellom hvilken type ekstern evaluering som ble gjennomført og i hvor stor grad respondentene opplevde bidrag til ny innsikt eller forbedring.

Når det gjelder valg av leverandør kunne det se ut til at det var en tendens til at de som hadde benyttet IIA Norge var mest fornøyd med bidraget til ny innsikt og forbedring (tabell 1).

Forskjellene var imidlertid ikke statistisk signifikante.

Det så også ut til å være en tendens til at det var noe mindre tidkrevende å gjennomføre evalueringen med IIA Norge som leverandør (tabell 2).

Forskjellene var heller ikke her statistisk signifikante.

Oppsummering

IIAs standarder for internrevisjon stiller tydelige krav til gjennomføring av ekstern evaluering av internrevisjonsenheter minimum hvert femte år. Internrevisjonsenheter som står foran en gjennomføring av slik evaluering må gjøre valg knyttet til type ekstern evaluering og ekstern leverandør av evalueringen. Analyse av data fra spørreundersøkelse der 22 ledere av norske internrevisjonsenheter ble spurt om sine erfaringer med ekstern evaluering ga ikke grunnlag for å gi noe entydig svar på hvilken type ekstern evaluering, eller hvilken leverandør, som bør velges.

Tabell 1 Grad av ny innsikt og bidrag til forbedring fordelt på leverandør

Leverandør	Andel opplevd stor grad av ny innsikt	Andel opplevd stor grad av bidrag til forbedring
IIA Norge	42,9 % (3 av 7)	28,6 % (2 av 7)
Konsulentfirma	25 % (2 av 8)	12,5 % (1 av 8)

Tabell 2 Tidsbruk fordelt på leverandør

Leverandør	Gjennomsnitt tid brukt intern evaluering med ekstern validering	Gjennomsnitt tid brukt full ekstern evaluering
IIA Norge	123 timer	75 timer
Konsulentfirma	228,3 timer	120 timer

Despite mature compliance programs we all need guidance on «adequate procedures»

Av
EZEKIEL WARD
Yara's Chief Compliance Officer

Yara is one of Norway's oldest and largest companies. With over 110 years of history, we sell to more than 150 countries. Our revenues in 2015 reached 108 BNOK. Whilst news articles in recent years may have focused on corruption and court cases, we have quietly worked hard building up our compliance program to what it is today – world class. But in spite of reaching such a level of maturity on compliance, we operate in an environment that lacks clear, formalised expectations.

In 2009 Yara formed its first Ethics & Compliance Department («E&C»). An ethics handbook was put in place, and the first steps were taken towards greater compliance involvement in key processes. When I came on board in 2012 we formalised the scope of the program to spend our energy on three key risks – corruption, fraud and business partners. Of course we deal with many other topics, but these three are where our attention falls first and foremost. We are now becoming 16 people, all reporting with so-called 'strong lines' within Ethics & Compliance. For me, reporting to the CEO has been essential to get the weight and authority needed to undertake our challenging work. The board has been hugely supportive and proactive.

Compliance is a team game, and a great deal of people are involved in a good program. The business owns the risks and activities, but needs support from E&C, internal audit, enterprise risk management, human resources, legal, I.T., security, HESQ and others. Collaboration between departments is vital. To work together, a clear structure is needed.

1. Culture and Tone at the Top	2. Risk Management	3. Compliance Organization	4. Policies and Procedures	5. Internal Controls
6. Training and Communication	7. Consultation and Guidance	8. Whistleblowing/ Internal Reporting	9. Investigation	10. Incentives and Discipline
11. Business Partner Due Diligence	12. M&A Due Diligence	13. Post-Acquisition Implementation	14. Contract Management	15. Monitoring

At Yara we have developed 15 elements of our Compliance Program:

These 15 elements are based upon the guidance from regulators and authorities. The US Department of Justice's FCPA guidance[1] has been of particular inspiration, as has the UK Ministry of Justice's UK Bribery Act guidance.[2] Tailored, of course, to meet Yara's operations and needs.

We work actively with our 15 elements. They have been formally defined, and roles agreed amongst executive management. They form the basis for our reporting – when I visit the board of directors to provide the annual ethics and compliance update, each of the elements gets discussed.

To take an example, culture and tone at the top is measurable through our ethics survey, which last took place in 2015. Employees are able to indicate their views on how comfortable they feel speaking up – to their line manager or others. They can say whether their organisations have a good tone at the top, robust organisational justice, and whether they felt an atmosphere of trust between colleagues. Further, they were able to give feedback on whether Yara's expectations on ethics and compliance were clear (they were!) and whether there was openness of communication in their areas. Learnings from our surveys lead to concrete actions where needed, and give employees an opportunity to have their say on ethics and compliance.

Another example of how the 15 elements have been put into practice relates to internal controls. For anti-corruption and anti-fraud controls, the first step is to define them unambiguously. Pitching this at the right level is important – you need to be detailed enough that local units know what you mean, yet overarching enough that you can report meaningfully to management and to the board. At Yara we have run a multi-year process to better understand and mitigate fraud risks and implement related controls, starting with a corporate definition of fraud, high level risk assessments and aligning our approach between teams - Finance in particular. Throughout 2016 we have run fraud risk management workshops across the world, raising further awareness. Any new risks are discussed with local management and are registered on their enterprise risk management (ERM) reporting tool. This is of course part of a wider effort to combat fraud through the control environment, risk assessments and various information and monitoring activities.

The US and UK guidance gives comfort that Yara has moved in the right directions. This sort of public guidance also supports compliance professionals by giving them solid reasons for recommending a program structure to the board, CEO and management. Collaborators internally (the business, internal audit, ERM and others) get clarity on what Ethics & Compliance is working on. Stakeholder communication becomes clear and consistent.

Perhaps in Norway a formal definition and guidance on compliance programs and «adequate procedures» will be published one day … the sooner the better!

[1] *US FCPA GUIDANCE LINK https://www.justice.gov/criminal-fraud/fcpa-guidance*
[2] *UK MOJ GUIDANCE LINK https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf*

Lasse Birkeland – med etikk som hjertesak

INTERVJU MED
LASSE BIRKELAND

Birkeland er statsautorisert revisor og siviløkonom. Han har lang erfaring som ansvarlig revisor og rådgiver mot frivillige organisasjoner / stiftelser med ideelle formål og offentlig sektor. Hans spesialfelt er innenfor evaluering og utvikling av intern kontroll, tilskuddsforvaltning og ulike typer tilsyn. Han var i fire år partner i Arthur Andersen & Co's revisjonsavdeling, og var ett år engasjert i et forskningsprosjekt ved hovedkontoret i Chicago, og har ledet dette selskapets EDB-revisjon.

Videre har han en særskilt kompetanse knyttet til å evaluere og redusere mislighets- og korrupsjonsrisiko. Han har hatt en rekke oppdrag og holdt mange foredrag knyttet til revisjon, IT-revisjon, intern kontroll, attestasjon av offentlige tilskuddsmidler, Skattefunn & EUs rammeprogrammer, Stiftelsesloven, forebygging av mislighets- og korrupsjonsrisiko, herunder også etiske dilemmaer for revisorer, foretak og organisasjoner.

Han har omfattende erfaring fra mange typer virksomhet og han har bekledd en lang rekke verv. Blant annet har han vært President of The Institute of Internal Auditors, Norway Chapter i 1980/81 og han har vært medlem av IIA fra 21.10.1976!

IIA Norge har vært heldige og få et møte med Lasse Birkeland for å snakke om hans mangeårige engasjement relatert til etikk, kontroll, misligheter og korrupsjon.

Av
REIDAR DØLI
Oslo Børs VPS

Hva er det med oss mennesker som gjør at det aldri slutter å dukke opp nye mislighets- og korrupsjonssaker?

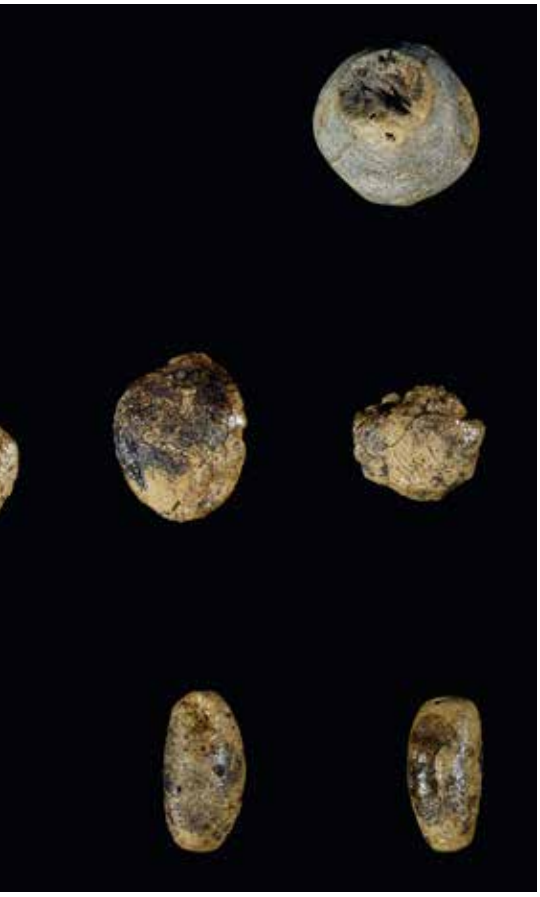
Lasse er klar på at det er mennesket og ikke teknologien som er utfordringen. Hvis en person har satt seg fore å tilegne seg en uberettiget fordel så klarer denne personen å gjøre det. Det sitter i ryggmargen på vedkommende.

Lasse henviser til utsagnet «Det bor en juksemaker i oss alle». Utsagnet er hentet fra Øystein Kock Johansens bok «Verdien av tillit» som er skrevet på oppdrag for Deloitte. De færreste mennesker har en så sterk moral at de aldri vil finne på å jukse. Dette er nærmest et urbehov og det kan dokumenteres mer enn fem tusen år til-

Verdens første «bokføringssymboler» i leire, ca. 5200 år gamle, fra Susa. Leirkulen til venstre var en form for «konvolutt» som opprinnelig inneholdt små symboler. Foto: Bridgeman Images

bake i tid. Fascinerende er det å lese når forfatteren henviser bakover i historien til de tidligste sivilisasjoner i Mesopotamia, Egypt og Kina der det var utviklet kontroller for å sikre rikenes finanser. Leirfigurer av forskjellig form ble benyttet til å angi mengder korn, kuer, sauer osv. Deretter ble de lagt i hule leirkuler som så ble brent/forseglet.

Dette skulle sikre at selger og kjøper var enige om hva den totale forsendelsen faktiske inneholdt, eller som det heter på dagens kontrollørers /revisorers stammespråk: «får betalt for det som er levert eller at det kun betales for det som er mottatt». Korrupsjonssaker vil fortsette å dukke opp, igjen og igjen. Når fristelsen blir for stor, er det ifølge Kock Johansen tilsynelatende helt tilfeldig hvem som går over grensen. De er altså ikke moralske avvikere, men helt vanlige mennesker med ganske alminnelige moralske og etiske styrker og svakheter. Historiens mange svindelsaker bekrefter ifølge Øystein Kock Johansen at revisjon og kontroll er nødvendig. Uten den hadde trolig enda



flere latt seg friste. Når det er sagt har også enkelte saker avslørt at til og med revisjonen kan være en del av svindelen. Spørsmålet eller dilemmaet om hvem som skal kontrollere kontrolløren har vært knyttet til revisjonen siden Platons tid (428 -348 f.Kr.). Øystein Kock Johansen mener også at dagens «kontrollører» har mye å lære av historien – den har en tendens til å gjenta seg.

Mye tyder på at utfordringen for det fremtidige samfunnets kontrollordninger er å finne den riktige balansen mellom kontroll og tillit. Lasses kommentar er at som punkt én så må ledelsen ikke være redd for å snakke om risikoen og praktisere en åpenhet rundt spørsmålene. Uten dette så får ukulturen lov til å utvikle seg. Et annet vesentlig poeng som ikke kan gjentas for ofte overfor de som er satt til å kontrollere er å rette oppmerksomheten også mot å gjøre de riktige tingene i stedet for bare å gjøre tingene riktig.

Lasse har lenge vært involvert i arbeidet til Innsamlingskontrollen. Denne komiteen er etablert for å kompensere for at det ikke finnes lovbestemmelser i Norge som direkte regulerer hvordan en pengeinnsamling skal foregå. Innsamlingskontrollen skal gi trygghet for at innsamlingsvirksomhet drives forsvarlig og at pengene går til det formålet som er oppgitt. Han har bl.a. sittet som representant i det utvalget som arbeidet frem nye etiske retningslinjer. Han har foretatt en overordnet vurdering av dagens kontroll som gjennomføres for nye og nåværende organisasjoner, samt sett på mulighetene for å gjøre denne kontrollen mer helhetlig og tydeligere rettet mot de aktuelle utfordringer. En stor konferanse, Confidence & Trust, gikk av stabelen i Oslo 27. mai i år. Der deltok Lasse som foredragsholder over temaene *Ethical Guidelines* og *More effective monitoring.* Målet med konferansen var å identifisere utfordringer i frivillig virksomhet hvor omdømmerisikoen kommer inn som et sentralt element, og hvilke krav som bør stilles til etikk og forvaltningskontroll.

Til spørsmålet om det er grunn til å ha høy tillit på den hjemlige arena og om det er lite juks i Norge, er Lasses kommentar at vi nok ikke er bedre her hjemme enn i andre land. Det tillitstap og den manglende åpenhet om saker som vi opplever i Norge gir ikke grunnlag til ubetinget optimisme.

Vi går videre til USA og mange husker sikkert ENRON skandalen som ble avdekket der i 2001. Denne saken involverte energiselskapet Enron og revisjonsfirmaet Arthur Andersen. Lasse var selv lokal partner i Arthur Andersen i tidsrommet 1984 – 1989, med et oppstartsår ved hovedkontoret i Chicago. Energiselskapet gikk konkurs og skandalen førte i løpet av

> Når fristelsen blir for stor, er det tilsynelatende helt tilfeldig hvem som går over grensen.

få måneder til oppløsningen av Arthur Andersen world wide. Selskapet var på den tiden et av verdens fem største revisjonsselskaper og nøt stor tillit og hadde et godt omdømme over hele verden. Denne saken utløste krav om Codes of Conduct og Compliance. Spørsmålet er om vi nå er der vi bør være.

Det er viktig å få på plass etiske retningslinjer. Dette er en grunnleggende dimensjon som tar for seg den menneskelige faktor og gir føringer og felles forståelse for hva som er akseptabelt og hva som ikke er akseptabelt i virksomheten.

Når det kommer til spørsmålet om innføringen av Compliance som et eget område i styringsstrukturen har vært vellykket, så er ikke erfaringene like entydige. Risikoen er at mindre virksomheter kveles av byråkrati og skjemavelde, dokumentasjonen tar helt overhånd. Kontrollørene er først og fremst opptatt av om alle skjema er på plass og at de er riktig utfylt og fokuserer kanskje ikke nok på om det produktet som er levert tilfredsstiller kravene. Dette gjelder ikke bare på økonomiområdet, men også innen mange andre bransjer som bygg, anlegg, helse, …

Det er stadig flere som stiller spørsmål ved om innføringen av virksomhetsstyringsmodeller som COSO ERM og tre linjes forsvarsmodellen har bidratt til det nødvendige løftet. Det er flere eksempler på at modellene ikke fullt ut stemmer overens med observert praksis. Virksomheter som har en liten sentral styringsstab og hvor funksjoner som i teorien skal ligge i 2. linjen er allokert ut i linjen, har vist seg vellykkede. Det samme gjelder prosjekter der kontrollfunksjoner er etablert i prosjektet med direkte mulighet for påvirkning i stedet for å sitte i en funksjon som kommer inn fra sidelinjen og ofte i ettertid. Andre eksempler er kjøp av tjenester fra ekstern revisor til å utvikle risikovurderinger. Grunnen til at slike modeller finner dårlig feste kan være mange, og det har også vært reist kritikk mot at de er utarbeidet og anbefalt av revisorer og rådgivere. Det er ikke gitt at målsetningene oppnås ved å arbeide i tråd med modellene som så ensidig fokuserer på et regelverk og ikke i samme grad på holdninger. Tre forsvarslinje modellen bidrar til å lage tette skott mellom funksjoner som jobber mot det samme målet. Det er et stort spørsmål om dette er den beste og mest fremtidsrettede måten å jobbe på.

Etter min vurdering har det over tid, jf. urbehovet som er omtalt av Øystein Kock Johansen ovenfor, vært reduserende drahjelp fra kontrollører i det forebyggende arbeidet mot misligheter og korrupsjon. Hvis vi ser historisk på det så hadde kontrollører frem til det forrige århundreskiftet som sitt viktigste mandat å arbeide med og avdekke misligheter. Dette er svært naturlig siden revisor har hatt de beste forutsetninger for å kunne ivareta et slikt mandat ved at hun/han har sin kompetanse innen intern kontroll. Bekreftelsen av regnskapet har siden kommet til å overskygge det som var det opprinnelige mandatet. Funksjonen har beveget seg fra å være en bloodhound til å bli en watchdog i løpet av de siste 100 år. Det er et spørsmål om kontrollørene over tid har redusert sitt ansvar og fokus på forebyggende arbeid og vedrørende intern kontroll og avdekking av «fraud». Er det et forventningsgap her eller er behovet borte?

Det store paradokset i det hele er at virksomheter som fremstår som forbilder ved å ha brukt mye ressurser på å etablere alle de anbefalte løsninger kan oppleve å bli rammet av underslag og korrupsjon, mens andre foretak med mye lavere grad av formalisme kan ha vært forskånet for dette.

En billedallegori på kontroll av kirkens regnskaper. Løven på gulvet symboliserer kontrollørens «farlighet». Foto: Bridgeman Images

Om etterforskning og granskning

Mange av oss har fått med seg «Granatmannen»-saken gjennom dokumentaren på NRK nå i oktober. Den har også vært fulgt opp i media over de siste to-tre årene, både i radio og i avisene. Saken dreier seg om en rekke eksplosjoner som i løpet av to måneder i 1965 satte sitt preg på Oslo, forårsaket av at noen hadde plassert håndgranater og granatfeller rundt om i byen. Den første eksplosjonen skjedde i Thunes vei på Skøyen 4. februar 1965. Lasse Birkeland som den gang var

19 år, utløste snubletråden til granatfellen som var festet i støtfangeren på en parkert bil. Han kom i likhet med alle ofrene for granatmannen fra det med livet i behold. Sakene ble gjenstand for omfattende medieomtale og offentlig interesse.

Fra Wikipedia og søkeord «Granatmannen» kan vi lese at det ble funnet en intakt granat fra hendelsen på Vinderen, og granaten ble sporet til et ran fra et våpendepot på Sessvollmoen. Politiet i Oslo klarte ikke å finne en mistenkt som ble tiltalt for saken, og den ble etterhvert henlagt med ukjent gjerningsmann. En politimann ble mistenkt for å stå bak hendelsene. Han begikk selvmord i 1966 og ved ransaking av hjemmet ble det funnet både granater og liner. I en rapport til politisjefen året etter ble det imidlertid ikke nevnt og saken er fortsatt uoppklart.

Lasse forteller at han har gjort seg mange tanker om denne måten å behandle saker på. Hensynet til de etterlatte er ofte grunnen til at slike saker ikke blir endelig etterforsket. Dette kan umiddelbart høres ut som en plausibel begrunnelse. Det er imidlertid et viktig forhold ved de saker som blir lagt til side uten å bli etterforsket og som er av vesentlig betydning, og det er at andre som kan ha fått mistanken kastet på seg heller aldri blir renvasket. Det er grunn til å stille et stort spørsmålstegn ved om dette hensynet veies opp mot hensynet til gjerningsmannen og dens etterlatte fra politi, påtalemyndighet og presse. For oss som opplevde terroren fra granatmannen i 1965 er det det minste vi kunne kreve at denne saken var blitt bedre etterforsket, oppklart og avsluttet den gang. Det må etterforskes - det må gjøres såpass! Lasse trekker parallellen til andre historier som ligger nærmere oss i tid som heller ikke er blitt tilstrekkelig etterforsket og oppklart.

En annen refleksjon er den tilsynelatende store forskjellen det er på etterforskninger og granskninger. I etterforskninger er forventningen at man på uavhengig grunnlag går bredt ut og søker ned i detaljer og forfølger alle relevante spor for å innhente svar. I de såkalte granskninger som vi nylig har sett eksempler på, er det gitt et avgrenset mandat fra oppdragsgiver og dette mandatet blir ofte ikke offentliggjort. Slike granskninger kan nærmest bli å betrakte som verdiløse for å oppklare saker.

Hva kan vi gjøre for å bli bedre når det gjelder å håndtere risikoen knyttet til misligheter og korrupsjon?

Jeg vil starte på toppen og si at vi må ha et lederskap som fokuserer mer på å få frem det beste hos sine medarbeidere. Vær raus med medarbeiderne og la disse få sjansen til å delta på spennende aktiviteter og utvikle seg. Tenk ikke bare på deg selv som leder som skal nyte godt av berikelsen ved å omgås likesinnede, ikke minst på tvers av landegrensene.

Akkurat nå holder jeg på å lese en bok av Ingar Skaug om Levende lederskap. Han har tung ledererfaring fra bl.a. SAS og Wilh. Wilhelmsen. Han beskriver lederskap og omstilling av ledere. Særlig er hans beskrivelser for å få det beste ut av kollegene sine interessante. Han sier blant annet følgende:

«Mange ledere er dessverre altfor opptatt av personlige posisjoner og ender opp i funksjoner de ikke er egnet for. En leder som ikke selv er på høyden med det ansvaret og de oppgavene han eller hun har, vil sjelden føle seg trygg nok til å gjøre medarbeiderne sine gode eller bedre enn dem selv. De vil ofte betrakte de beste medarbeiderne som konkurrenter, og enten ta æren for deres prestasjoner eller hindre dem i å prestere det de er gode for. Et annet symptom er lav takhøyde for uenighet. De betrakter ethvert forslag som går på tvers av deres egne ideer som en trussel – helt til de skjønner at det kan være en god idé. Da stjeler de den og utgir den litt senere som sin egen, uten å kreditere opphavsmannen. Slikt blir det ikke mye motivasjon av.»

Deretter er jeg opptatt av å legge vekk alt som har med smartness, taktikkeri og gjentjenester. Ledelsen er mektig og sitter med en asymmetrisk forhandlingsmakt. Vær derfor en rettferdig leder, legg deg flat der situasjonen krever det. Ved brudd på regler og forventninger, og i utmålingen av sanksjoner, ikke bare ta i betraktning den myndighet en har til å reagere ut ifra hva som er «riktig» eller «galt», men len deg i tillegg litt tilbake og spør deg selv om reaksjonsformen er «klok».

Virksomhetene må øve på hva som er greit og hva som ikke er greit. En god regel når du tar fatt på arbeidet med å etablere ett etikkprogram, gjerne i forbindelse med risikovurderinger knyttet til omdømme, kan være å ta som utgangspunkt at her er det «grums» (og så får organisasjonen prise seg lykkelig hvis antagelsen i ettertid skulle vise seg å være feil). Deretter bør du sette inn tiltak for å beskytte deg mot risikoen. Har du for eksempel da etablert en 10 punkts tiltaksplan så har du kanskje for de fleste formål svart opp til forventningene om det likevel skulle gå galt. Da blir det kanskje noe mer troverdig når det hevdes i media at «vi har nulltoleranse» for dette hos oss. For videre innføring i dette emnet viser Lasse til en bok av Petter Gottschalk som heter Økonomisk kriminalitet- Ledelse og samfunnsansvar. Der beskrives økonomisk kriminalitet generelt og hvitsnippkriminalitet spesielt. Det er forbrytere med økonomisk motiv, organisatorisk mulighet og avvikende atferd som begår slik kriminalitet. Dessuten er alle kjente norske hvitsnippsaker fra 2009 til 2015 blitt beskrevet i boken.

Lasse sier til slutt at han har stor respekt for de som sier at det er menneskelig å feile og at alle kan gjøre feil, alternativet vil være utvikling av et umenneskelig samfunn. Det er etablert et vell av regler og det er mange snubletråder så det er lett å gjøre feil. Det som er viktig er at vi blir mer åpne om feil, forteller om de, forsøker å lære av feilene og fokuserer på hvordan det kan gjøres bedre neste gang. Og, det er kanskje ikke alltid den beste løsningen å bytte ut de som har feilet, men heller la de få en ny sjanse til å gjøre det bedre hvis mulig.

Bilde 1 og 2:
Fra Øystein Kock Johansen for Deloitte
VERDIEN AV TILLIT, gjengitt med tillatelse fra Bridgeman

«Banking is people» – men regelstyrt eller verdistyrt?

Av
JANNE BRITT SALTKJEL
Siviløkonom fra NHH, CIA og Dipl. Internrevisor, med erfaring fra linjen og internrevisjonen i DNB, som konsulent i PwC og Deloitte og Group Compliance officer i Multiconsult. Hun er nå Senior Operational Risk Expert Nordea.

Innen ledelse og organisasjonsutvikling er det populært å karakterisere bedriftskultur som enten regelstyrt eller verdibasert. Mens verdibasert ledelse har høyt fokus på «myke» kontroller (som kompetanse, kultur, holdninger), er regelstyrt ledelse basert på «harde» kontroller (detaljerte prosedyrer og kontrollmekanismer innearbeidet i prosesser og systemer, herunder avstemming, automatiserte fullmakter og terskelverdier, attesteringsrutiner, sjekklister og to par øyne-kontroller mv.). Ingen virksomheter styres kun ved hjelp av ansattes holdninger og verdier. For eksempel vil ideelle organisasjoner ofte ha stort innslag av verdibasert ledelse, men også ha «harde» kontroller integrert i sine prosesser. Men hvordan er det andre veien; har virksomheter som i hovedsak er regelstyrt også innslag av verdibasert ledelse?

I min fartstid som ansatt i finans, industri og konsulentnæringen har jeg sett flere bransjer og foretak fra innsiden. Noe av det som slår meg, er at flere og flere i utgangspunktet regelstyrte virksomheter har supplert med verdibasert ledelse i noen år, mens finansbransjen fortsatt er nesten rendyrket regelstyrt, men så vidt har begynt å se på verdibasert ledelse.

Nytter det å jobbe med «myke» kontroller?

«En voksen persons holdninger og etiske bevissthet, er noe man har med seg hjemmefra», vil noen hevde. «Det nytter ikke å oppdra voksne folk.» Hvis det er riktig, bør man i alle fall ha gode kontroller og bakgrunnssjekker av hvem man ansetter. Det bør man

Foto: Rawpixel.com/Shutterstock

kanskje ha uansett, men er det slik at det ikke har noe for seg å jobbe med de «myke» kontrollene?

Det er ikke vanskelig å forestille seg at menneskers holdninger kan påvirkes negativt og at en ansatt med et greit moralsk kompass, likevel kan bli en ansatt som plukker fra lageret, fakturerer noen timer ekstra, aksepterer miljøkriminalitet, lukker øynene for at en kunde har kriminelle intensjoner osv. Gjentatt eksponering for uetisk atferd og holdninger, gruppepress, belønningssystemer, muligheten til å berike seg selv, rasjonalisering og rettferdiggjøring («slik gjør alle det», «vi hadde ikke overlevd om vi skulle gjort det etter boken», «det er ikke mitt problem hva kunden skal med dette») – er eksempler på krefter som kan bidra til at sunne holdninger slites ned litt for hver dag. Men er man enig i at dette kan skje, har man samtidig konstatert at holdninger kan påvirkes – det positive er at da må det være rimelig å anta at ansattes holdninger og bevissthet også kan påvirkes i positiv retning.

Foto: Pressmaster/Shutterstock

Bransjeforskjeller

Noe av forklaringen på regelfokuset i finansbransjen, ligger i at sektoren er gjennomregulert og tett overvåket av tilsynsmyndighetene. Det er krav om en rekke «harde» kontroller på detaljnivå og at kontrollene er dokumentert. Også forretningsetikk er delvis lovregulert, for eksempel gjennom Mifid (investorbeskyttelse) og AML (anti-hvitvaskingsregler) og krav til opplæring (autorisasjon for finansielle rådgivere). Det er likevel mange eksempler på at dette ikke har vært nok; flere tilfeller er omtalt i media og enkelte også behandlet i rettssystemet, som «råsalg» av spareprodukter, passiv fondsforvaltning solgt som aktiv, manglende rutiner eller innsats for å fange opp hvitvasking, en slags passiv bistand til skatteunndragelser, uansvarlige tilbud av lån til svakt stilte kundegrupper mv. Kan slike saker forebygges og hvordan? Hvor mange kontrolltiltak skal til? Kan risikoen for brudd på lover og regler, og i blant en alminnelig oppfatning av hva som er etisk akseptabelt overfor kunder og samfunn, reduseres ved at regelstyringen suppleres med økt fokus på verdibasert ledelse?

Også oljebransjen, energibransjen og telekombransjen må forholde seg til strenge krav (inkludert rapporteringskrav) fra myndighetene. Selskapene må derfor ha stor grad av regelstyring, men mange har like fullt integrert verdibasert ledelse i sine styringsmodeller. Dette kan forklares med at eksponering for miljørisiko, HMS-risiko, korrupsjonsrisiko, risiko for å krenke menneskerettigheter eller arbeidstakerrettigheter, blir drivere til å sette forretningsetikk og integritet på agendaen. Noen av selskapene har gjort seg dyrekjøpte erfaringer og har måttet ta grep pga. stygge korrupsjonssaker, bl.a. bevisstgjøre og lære ansatte opp i å identifisere og håndtere disse risikoene og integrere verdifokus i lederutviklingen.

Etiske retningslinjer som en indikator

I situasjoner der de «harde» kontrollene kommer til kort og utfallet avgjøres av den enkelte medarbeideres dømmekraft, vil det være i arbeidsgivers interesse å påvirke medarbeiderens bevissthet, holdninger, kunnskap og dømmekraft, samt å legge til rette for at ansatte kan ta opp forretningsetiske dilemmaer internt. En virksomhet som har fokus på etisk forretningsatferd vil integrere forretningsetikk i opplæringen og i belønningssystemer og ta tak i problemstillinger som oppstår – og i de aller fleste tilfeller ha etablert etiske retningslinjer[1] (eller «Code of Conduct») som et fundament for dette arbeidet. De vil i tillegg legge til rette for varsling slik at virksomheten øker mulighetene for å fange opp uetiske atferd. En overordnet sammenligning av de etiske retningslinjene i noen av de største selskapene i Norge mot anerkjent praksis[2] gir interessante observasjoner.

[1] *For banker har European Banking Authority's (EBA) «Guidelines for internal governance» fra 27.09.2011 (GL 44., punkt 9.2) en anbefaling om at ledelsen etablerer og promoterer etiske retningslinjer.*

[2] *Basert på bl.a. UN Global Compact, ISO 26000 om Samfunnsansvar, Transparency International, korrupsjonslovgivning, konkurranselovgivning, sektorspesifikke forretningsetiske risikoer*

Uønsket atferd hos ansatte kan skade omdømmet – også for banker.
Foto: Gustavo Frazao/Shutterstock

Børsnoterte selskaper

En gjennomgang av de ti største børsnoterte selskapene i Norge målt etter børsverdi (29.09.2016), viser at alle har etablert etiske retningslinjer, men at omfang, kvalitet og forankring av de etiske retningslinjene varierer. Hele åtte av de ti børsnoterte selskapene har retningslinjer av god kvalitet (syv karakterisert som nær eller på nivå med ledende praksis). To av de ti har retningslinjer av enklere kvalitet. Halvparten av de ti selskaper har etiske retningslinjer frontet av CEO. De to som har etiske retningslinjer av enklere kvalitet, er ikke frontet av CEO. Ut fra disse kriteriene kommer det eneste finansforetaket ut blant de to svakeste.

Syv av ti virksomheter har tilrettelagt for at varsling også kan komme fra eksterne, og samtlige av børstoppene utenom finansforetaket, omtaler på sine hjemmesider muligheten for å varsle anonymt.

Banker

Ser vi på de ti største bankene i Norge målt etter markedsandel, får vi et litt svakere bilde enn for de børsnoterte foretakene. Åtte av bankene har etiske retningslinjer tilgjengelig og halvparten kan karakteriseres som av god kvalitet. Tre banker har enkle versjoner på plass, en bank oppgir å ha etiske retningslinjer på plass uten at disse er offentliggjort (og kan derfor ikke vurderes), mens det for den siste bank ikke finnes noen henvisning til etiske retningslinjer. Den mest åpenbare forskjellen er at ingen av bankene har sine etiske retningslinjer frontet av CEO, dette til tross for anbefalingene fra EBA om at ledelsen bør etablere og promotere etiske retningslinjer.

Nivået henger ikke sammen med bankenes størrelse. Det er to mindre banker som kommer best ut; disse har begge gjennomgått og oppdatert sine versjoner i 2016 og kan skilte med etiske retningslinjer i tråd med anerkjent praksis. Dessuten har flere av bankene etablert etiske retningslinjer de siste to årene. Dette underbygger hypotesen om at fokus på etiske retningslinjer, og dermed mer verdibasert ledelse og «myke» kontroller, er nyere i banksektoren enn for en rekke andre sektorer, i alle fall her til lands, men at en utvikling er på gang.

Børsselskap#	Sektor	Kvalitet	Frontet av CEO	Varslingskanal
1	Olje	Gode	Ja	Intern, ekstern, anonymt
2	Telekom	Gode	Ja	Intern, ekstern, anonymt
3	Finans	Enkle	Nei	Intern
4	Næringsmiddel	Ok	Nei	Intern, anonymt
5	Forsikring	Gode	Nei	Intern, ekstern, anonymt
6	Industri	Gode	Ja	Intern, ekstern, anonymt
7	Industri	Gode	Ja	Intern, ekstern, anonymt
8	Sjømat	Gode	Nei	Intern, anonymt
9	Offshore	Enkle	Nei	Intern, ekstern, anonymt
10	Offshore	Gode	Ja	Intern, ekstern, anonymt

Bank	Kvalitet	Frontet av CEO	Varslingskanal
Bank 1	Enkle	Nei	Intern
Bank 2	Enkle	Nei	Intern, anonym
Bank 3	Gode	Nei	Intern, anonym
Bank 4	Gode	Nei	Intern, anonym
Bank 5	Enkle	Nei	Intern
Bank 6	Ukjent	?	Ikke oppgitt
Bank 7	Gode	Nei	Intern, ekstern, anonymt
Bank 8	-	-	Ikke oppgitt
Bank 9	Gode	Nei	Internt
Bank 10	Gode	Nei	Internt

Den største forskjellen observert er at det ikke er noen trend i banknæringen i Norge å åpne for ekstern varsling. Det er dessuten kun bankene med utenlandske morselskaper som eksplisitt på sine hjemmesider nevner muligheten for å varsle anonymt.

En slik overordnet vurdering vil aldri gi det fulle bildet og det kan være forhold som ikke har kommet med i gjennomgangen over, som kan endre bildet for enkelte av aktørene; eksempelvis kan det være topledere som er mer engasjert i dette arbeidet enn det som fremgår av de etiske retningslinjene. Men en virksomhet og en topleder som fokuserer på forretningsetikk vil som regel vise omverdenen hva man ønsker å stå for, samt

forsterke budskapet overfor egne ansatte. Resultatet fra gjennomgangen gir derfor en indikasjon på at banknæringen ikke kan sies å være ledende når det gjelder fokus på forretningsetikk.

Den evige «tonen på toppen»

Verdibasert ledelse med fokus på etiske retningslinjer og varslingskanaler er ingen trylleformel som rydder opp i forretningsetiske dilemmaer eller ukultur, og som garanterer for godt omdømme. En forutsetning for at etiske retningslinjer skal ha noe for seg, er tonen på toppen - ledelsen må stå helhjertet bak budskapet om forretningsetisk atferd. Det er derfor litt underlig at ikke bankene velger å ha CEO som «avsender» på sine etiske retningslinjer.

Å være avsender vil imidlertid heller ikke være nok. Det er flere eksempler på at virksomheter med omfattende etiske retningslinjer likevel er «pill råtne» - energiselskapet ENRON er kanskje det mest lysende eksempelet, mens Wells Fargo – det amerikanske finanskonsernet – har hatt etiske retningslinjer som viser seg ikke å ha vært reelt forankret i toppen. Disse eksemplene fjerner imidlertid ikke den allmenne oppfatningen både i virksomheter og til dels hos myndigheter[3], om at det hjelper å bygge bevissthet og kultur rundt etisk atferd. Men for at etiske retningslinjer skal være mer enn bare festtaler, må ledere – mellomledere inkludert – vise vilje til selv å følge de etiske retningslinjene og aktivt støtte oppunder og belønne den atferden de ønsker, samt sanksjonere mot uønsket atferd. Dersom ledelsen ønsker at ansatte skal oppføre med god margin innenfor loven og det som anses som etisk forsvarlig, så er det slik atferd som må belønnes. Hvis det ikke er ønskelig at ansatte opptrer i gråsoner, må det ikke lønne seg for den ansatte å gjøre nettopp det. Ledelsen kan ikke si at selskapet forventer høy integritet hos de ansatte, men samtidig dele ut de største bonusene eller forfremmelser til personale som kutter flest hjørner. I tillegg til incentivmodell kan ledelsen vise at de mener alvor ved å legge til rette for anonym varsling og ekstern varsling, og et system for å følge opp varslene på en grundig måte som gir resultater. Dette er forhold som bankene må ta inn over seg hvis de ønsker å benytte verdibasert ledelse for å redusere operasjonell risiko og omdømmetap.

Foto: 1000 Words/Shutterstock

Veien videre i finansbransjen

Det er mye i dagens bilde som taler for økt regelstyring og flere «harde» kontroller i finansnæringen, blant annet gjennom ytterligere styrking av kontrollene i 1., 2. og 3. linje, økt kontroll av tredjeparter, forsterket fokus på IT- og cybersikkerhet mv. Imidlertid kan det også ha noe for seg i større grad å supplere regelstyrt ledelse med verdibasert ledelse om man skal skotte til andre sektorer. Jeg mener det er vanskelig å komme utenom økt satsing også på «myke» kontroller, i tillegg til «harde» kontroller som har vist seg gang på gang ikke å være nok. «Banking is people», er et gammelt bankuttrykk. Tross automatisering og globalisering – «it still is».

[3] *Dette kan man bl.a. se i rettsvesenet der virksomheter som har jobbet mye med kompetansebygging, kultur og holdningsskapende arbeid i mindre grad holdes ansvarlig dersom en ansatt begår misligheter, enn dersom virksomheten ikke har gjort noe aktivt for å forebygge dette. Eksempelvis Morgan Stanley og Garth Peterson-saken i Shanghai, Norconsult-saken der selskapets arbeid med antikorrupsjon i etterkant av forholdet som tiltalen gjaldt, ble vektlagt da Høyesteretts valgte å ikke ilegge selskapet foretaksstraff.*

Erfaringer med programvare for internrevisjon, risikostyring og compliance

Programvare for internrevisjon, risikostyring og/eller compliance (eller GRC; Governance, Risk and Compliance[1]) har vært på markedet i flere tiår. Som med all annen teknologi skjer det raskt endringer, og i løpet av de siste årene har denne type programvare spesielt bedret seg innen; analyse, visualisering og integrering mot eksisterende systemer. Virksomheter som har tatt en beslutning om å ikke investere i verktøy bør derfor gjøre nye vurderinger med jevne mellomrom.

Av
MAGNUS DIGERNES
Head of Enterprise Risk Management, CIA, Dipl. Internrevisor, CRMA og CFE. Yara.

De fleste programvarer dekker flere områder innen «GRC», og tilpasser behovene gjennom ulike moduler som f.eks. risikostyring, revisjoner, leverandøroppfølging, styringsdokumenter etc. I en undersøkelse blant over 200 ulike virksomheter fremkommer det at de fleste investeringer forekommer i modulene risikostyring og risikoanalyser (42%), compliance (37%) og internrevisjon (36%)[2]. Kriterier for å velge løsning må tilpasses den enkelte virksomhet, men brukervennlighet, pris, funksjonalitet og muligheter for å konfigurere er kriterier som mange virksomheter trekker frem i denne undersøkelsen.

Leverandørmarkedet har vært drevet av noen store aktører som IBM, RSA Archer, og SAP, men det er også flere nisjeleverandører som tilbyr mange fleksible løsninger som MetricStream og Logicmanager[3]. I tillegg finnes det programvare for kun enkelte funksjoner som TeamMate for internrevisjon og Easyrisk for risikostyring. Analyseselskapene Forrester og Gartner gjør jevnlig analyse av aktuell programvare, og kan være et godt innspill til en vurdering av hvilke løsninger som kan undersøkes nærmere.

I IIA Norges medlemsundersøkelse 2016 ble det spurt om «Bruker din avdeling et GRC-verktøy?». I undersøkelsen svarte 55% av 250 respondenter ja. 31 av respondentene besvarte hvilket GRC-verktøy som ble benyttet og det var til sammen 12 ulike programvarer som ble nevnt. Tabellen under summerer opp programvarene og hvor mange virksomheter som har nevnt at det benyttes

Programvare	Antall virksomheter
Bwise	1
TeamMate	2
Grace	1
RSA Archer	2
Easyrisk	3
Wdesk	1
Corporater	1
STIR	1
SAP GRC	2
MetricStream	1
TQM	1
Pentana Vision	1

SIRK tok kontakt med fem av de som nevnte hvilken programvare de benyttet slik at de kunne dele sine erfaringer.

Marine Harvest

Renete Kaarvik, Compliance Officer

Hvilket GRC-verktøy har dere valgt?
Vi bruker Wdesk som vår GRC plattform. Her har vi samlet dokumentasjon relatert til internkontroll for finansiell rapportering. Siden vi er notert på New York Stock Exchange har vi lovkrav i SOX å forholde oss til, som blant annet betyr at vi foretar egen/management testing av våre internkontroller. Denne testingen dokumenteres også i Wdesk.

Når ble verktøyet implementert?
Wdesk er et system som settes opp med rettigheter og tilganger som gjør at flere kan jobbe i et dokument samtidig i tillegg til at det kan brukes for direkte filing til US Securities and Exchange Commission

[1] *Begrepet GRC er ikke et etablert og har i stor grad blitt definert av konsulentselskaper og softwareleverandører, jfr. "A Frame of Reference for Research of Integrated Governance, Risk & Compliance (GRC)" Nicolas Racz, Edgar Weippl, Andreas Seufert. August 2014*
[2] *Findings of the OCEG 2016 GRC Technology strategy, www.OCEG.org*
[3] *Deloitte 2014 "Governance, Risk and Compliance (GRC) software. Business needs and market Trends"*

(SEC). Vi anskaffet Wdesk i november 2014 og tok systemet i bruk i januar 2015 med det formål å skrive våre årsrapporter og kvartalsrapporter. I april i år startet jobben med å bygge opp SOX compliance/internkontrollrammeverket i Wdesk, og i juni var systemet klart til bruk for testing av SOX kontroller.

Hva var det viktigste kriteriet for valg av verktøy?
Et GRC verktøy må tilpasses oss, og ikke omvendt. Det er viktig at vi kan bygge systemet slik vi ønsker det, strukturerer dokumentasjon, endre oppsett og lage rapporter uten bruk av konsulenter/teknisk kompetanse. Med et så fleksibelt system som Wdesk er det nesten bare fantasien som setter begrensinger for hva man kan gjøre. Når vi i tillegg allerede hadde systemet tilgjengelig, var det også enklere å ta avgjørelsen om å bruke Wdesk som vår GRC plattform.

Hvem benytter seg av verktøyet?
Som et GRC verktøy brukes systemet per i dag blant annet for å dokumentere policier, risiko og kontrollmatriser, scoping og testing av SOX kontroller. I tillegg til våre egne «management SOX testers» er også internrevisor brukere av verktøyet. Eksternrevisor (både sentralt og lokale team) vil også kunne bruke verktøyet for å få tilgang til vårt internkontrollrammeverk samt våre testresultater.

Hva er de største fordelene ved å bruke verktøyet?
Fordelen med å ha et fleksibelt system er allerede nevnt. Systemet er fortsatt under utvikling, vi tar det i bruk til stadig nye dokumenter som kan kobles sammen og dermed få tidsriktig oppdaterte dokumenter. Brukergrensesnittet er kanskje ikke like sofistikert som i et mer etablert GRC verktøy men siden dette minner om Microsoft Office er terskelen for å ta i bruk systemet svært lav, noe som betyr minimalt behov for opplæring. Strukturen er logisk, man har tilgang på alle relaterte dokumenter på ett sted, ingen begrensninger i antall ord på felter/tekstbokser etc. Et annet pluss er at systemleverandør er svært opptatt av å utvikle systemet, og våre forbedringsforslag blir hensyntatt. I tillegg har vi en fast kontaktperson på kundestøtte som er svært kunnskapsrik og fleksibel både når det gjelder tidspunkt og type henvendelser. Dette betyr at vi får løst de fleste henvendelsene på dagen.

> Et GRC verktøy må tilpasses oss, og ikke omvendt.
>
> *Renate Kaarvik*

Har du noen synspunkter på hva som skal til for å lykkes med å implementere et GRC-verktøy?
Vi har en dyrekjøpt erfaring her, siden vi først implementerte et system uten helt å vite hva vi ønsket. Det er viktig at man vet hva man har behov for, og at man allerede har et etablert rammeverk man ønsker å strukturere i et system. Man må vite hva man anskaffer og ha den riktige kompetansen selv eller ha en god forståelse av hvor mye ekstern konsulentbistand man trenger for å tilpasse systemet eller bygge rapporter. Dedikerte ressurser og tid for å håndtere både implementering, drifting og evt opplæring av brukere. Det er også en fordel om man har mulighet til å snakke med andre virksomheter som har tatt systemet i bruk for å få deres erfaringer.

NAV

Terje Klepp, CAE

Hvilket GRC-verktøy har dere valgt?
Vi benytter revisjonsverktøyet TeamMate (TM) i Internrevisjonen. Alle revisorene (16) bruker verktøyet.

Når ble verktøyet implementert?
TM ble vurdert av ledergruppen høsten 2008, innkjøpt samme høst, og implementert mars 2009. I starten var det varierende bruk av systemet, første revisjonsprosjekt som benyttet TM fullt ut startet i slutten av april samme år.

Hva var det viktigste kriteriet for valg av verktøy?
Internrevisjonen ønsket å rendyrke en ensartet gjennomføring av revisjonsprosjektene. Likeledes var forbedring av tiltaksoppfølging et uttalt mål. I tillegg var behovet for styringsinformasjon et prioritert ønske, f.eks. monitorering av fremdrift, forbruk av tid og evaluering fra revidert enhet. Flere konkurrerende verktøy ble vurdert, og TM ble evaluert som det best egnede for våre behov.

Hvem benytter seg av verktøyet?
Internrevisjonen bruker 5 av 6 hovedmoduler. Alle statlige ansatte i NAV (ca. 15.000) kan i realiteten benytte modulen «TeamCentral» som er den delen av TM som benyttes til oppfølging av tiltak. Eier av tiltakene legger inn status for tiltak, eventuelle utsettelser og dokumentasjon av det som er implementert. I tillegg har Økonomi- og styringsavdelingen i direktoratet oppgaven å monitorere, dvs. følge opp og godkjenne lukking av tiltakene registrert i TeamCentral.

> Alle statlige ansatte i NAV kan i realiteten benytte modulen «TeamCentral»
>
> *Terje Klepp*

Hva er de største fordelene ved å bruke verktøyet?
- TM er et prosessverktøy som følger revisjonene «fra A til Å». Dvs. fra årsplanlegging, risikovurderinger, gjennomføring, til tiltaksoppfølging og lukking.
- All dokumentasjon er i ett system.
- Tiltaksoppfølging. Tidligere ble det brukt mye tid på å sette seg inn i 2-3 år gamle rapporter og tiltak, samt purre revidert enhet for ny status. I dag er dette automatisert ved at TM selv purrer tiltakseier som må legge inn ny status, samt dokumentere hva som er utført og implementert. Dette øker sikkerheten for at omforente tiltak blir tilstrekkelig fulgt opp.
- Stort, fleksibelt system som er modulbasert. Rapporter kan skreddersys til eget

behov og lages på tvers av enkeltoppdrag.
- TM er markedsledende innenfor sitt område (ca. 70 % av markedet basert på det vi har fått opplyst), hvilket tilsier at leverandøren har finansiell styrke til å vedlikeholde systemet i tråd med trender og utvikling innen revisjonsmetodikk.
- Brukt hensiktsmessig vil TM bidra til at organisasjonen får et samlet bilde av risiko og internkontrollen.
- Timeregistrering gir en enkel og effektiv oppfølging av de enkelte revisjonsprosjektene.
- Ledelsen kan monitorere fremdriften for de enkelte revisjonsprosjektene og få oversikt over hvordan man ligger an i forhold til årsplan.
- Driftssikkert system, lite nedetid.
- TM er integrert med Office produktene (Word, Excel etc.)
- Ulemper
  - Høy brukerterskel og lite intuitivt system, krever en del tid for å få systemet «inn under huden».
  - Krever teknisk kompetanse for å bruke fleksibiliteten f. eks. for å lage skreddersydde rapporter.
  - Utfordrende med tilgang til god support når vi må henvende oss til England/USA.

Har du noen synspunkter på hva som skal til for å lykkes med å implementere et GRC-verktøy?
- Opplæring helt avgjørende.
- Stor fleksibilitet krever høy kompetanse for å skreddersy systemet.
- Tenke igjennom på forhånd hvordan systemet skal benyttes til hva, og ha en ensartet forpliktende revisjonsmetodikk før systemet konfigureres.

TINE

Rune Moen, Konsern Risk Manager

Hvilket GRC-verktøy har dere valgt?
For kvalitativ risikostyring brukes EasyRisk Manager og for kvantitativ usikkerhetsanalyse brukes @risk for Excel. Ellers har vi dedikerte databaser i IBM NOTES for oppfølging av interne revisjoner og annen rapportering/oppfølging. Styringssystemet skal nå byttes ut med en ny løsning som ligger på O365 plattformen, noe som vil gi økte muligheter for integrert rapportering og oppfølging. Den mest operative delen av den kvalitative risikostyringen vil da sannsynligvis bli håndtert i et nytt verktøy.

Når ble verktøyet implementert?
2005.

Hva var det viktigste kriteriet for valg av verktøy?
Ønske om å kunne registrere og følge opp risikoer og tiltak i hele organisasjonen i ett system.

Hvem benytter seg av verktøyet?
TINE har svært mange brukere på alle nivåer, fra 1. linjeledere til konsernsjef. TINE anser det som viktig at verktøyet brukes til å følge opp risikoer og tiltak, noe som nødvendiggjør at alle risikoeiere og tiltaksansvarlige bruker verktøyet.

Hva er de største fordelene ved å bruke verktøyet?
Et verktøy som håndterer relasjoner mellom risikoer og tiltak er nødvendig dersom hensikten er å støtte risikostyringsprosessen. Verktøyet muliggjør tilordning av risikoer og tiltak til funksjoner og personer, samt nødvendig varsling og oppfølging av status. Verktøyet bør også støtte aggregering og eskalering av risikoer i organisasjonen. Dersom behovet kun er å rapportere et topprisikobilde til toppledelsen eller styret, kan Excel gjøre nytten.

> Verktøyet bør også støtte aggregering og eskalering av risikoer i organisasjonen.
>
> *Rune Moen*

Har du noen synspunkter på hva som skal til for å lykkes med å implementere et GRC-verktøy?
Fokus på rammeverk og prosess. Hensikten og tilnærmingen til risikostyring må inn i ryggraden til den enkelte leder. Verktøyet må så kunne settes opp slik at det støtter dette rammeverket og risikostyringsprosessen. Verktøy må ikke få for stor fokus, det skal kun være en støtte til effektivt risikostyringsarbeid, uavhengig av hva valgt fokus er i organisasjonen.

Nordea

Rune Johannessen, Senior Operational Risk Officer

Hvilket GRC-verktøy har dere valgt? Vi bruker en modifisert versjon av Bwise men kaller denne NORMS (Non-financial Risk Management System)

Når ble verktøyet implementert?
Vi har brukt dette verktøyet i nærmere 10 år men det er først de siste to årene som verktøyet har blitt brukt til andre formål enn hendelsesregistrering.

Hva var det viktigste kriteriet for valg av verktøy?
Verktøyet inngår som en modul i en større «pakkeløsning» som Nordea har. Bruk av verktøyet har derfor ikke påførte oss ytterligere lisenskostnader/var gratis, noe som var et tungtveiende for valg av denne løsningen.

Hvem benytter seg av verktøyet?
Både 1, 2 og 3 linjeforsvaret bruker dette verktøyet og vi snakker derfor om flere hundre brukere (flere enn 100 bare i IA funksjonen).

> Verktøyet inngår som en modul i en større «pakkeløsning» som Nordea har.
>
> *Rune Johannessen*

Hva er de største fordelene ved å bruke verktøyet?
- All informasjon lagres på ett sted, noe som gjør det lettere å standardisere, kvalitetssikre, aggregere, og rapportere informasjon.
- Bruk av et system gjør brukertrening og endringer/oppgraderinger enklere (både i forhold til trening og evt. synkronisering med andre systemer)
- Alle forholder seg til ett system og har forskjellige roller innenfor dette

systemet. Dette gjør av vi «snakker» samme språk, forholder oss til de samme standardiserte prosesser og har den samme forståelse av hva som er den enkeltes oppgaver og rettigheter på tvers av de ulike forsvarslinjene.

Har du noen synspunkter på hva som skal til for å lykkes med å implementere et GRC-verktøy?
Jeg mener at følgende punkter kan være aktuelle for lykkes i en slik prosess:

- Full støtte og lojalitet fra ledelsen i forhold til de valg som gjøres.
- En tilstrekkelig bemannet og kompetent brukerstøtte
- God informasjon og ikke minst at det settes av tid til ulike typer av opplæring for brukerne
- Gradvis utrulling og en justering av kurs hvor dette er nødvendig – ikke prøve å gjøre alt på en gang
- Et kontinuerlig arbeid med å forbedre og tilpasse systemet (lite trolig at man treffer på første forsøk) - basert på blant annet tilbakemeldinger og forslag fra brukerne om forbedring av funksjonalitet og bruk.

Gjensidige

Mazhar Ahmad, leder risikostyring

Hvilket GRC-verktøy har dere valgt?
Vi kaller ikke EasyRisk (levert av «norske» DNV GL) et GRC-verktøy, men et verktøy for risikostyring og internkontroll («operasjonell risikostyring»). Det understøtter våre prosesser rundt risikostyring og internkontroll i tilknytning til driftsmessige forhold på tvers av virksomheten. Dvs. der vi kartlegger at det er operasjonell risiko tilstede, så vil dette området være «in-scope» for rammeverket og understøttes av instrukser, prosesser og IT-støtte. I min verden er GRC et «altomfattende system» som utgjør mer enn dette - med gjensidige grensesnitt/knytninger mellom styrende dokumenter, testing, dokumentasjon, prosesskart og risikovurderinger på «alle» områder, inkludert andre styringsdimensjoner (oppfølging av KPIer/KRIer, risikovurderinger i tilknytning til nye produkter og systemer, risikoer og tiltaksoppfølging i prosjekter, revisjonsfunn, aktiviteter i tilknytning til kvalitetsarbeid, aktiviteter som har høy «frekvens» som sikkerhets-/IT-hendelser, forvaltningsoppgaver etc) og mye mer dynamisk enn et «standalone» system. Rent teknisk er det mulig å bygge infrastruktur rundt alle systemer, men det blir ofte dyrt og forholdsmessig krevende å vedlikeholde hvis et system ikke er designet for dette som formål.

Når ble verktøyet implementert?
Verktøyet ble anskaffet i 2012, men vi brukte faktisk et år å finne ut av om det opprinnelige scopet skulle utvides. Verktøyet ble i sin tid anskaffet for å understøtte våre prosedyrer rundt registrering av hendelser (et konsernfelles hendelsesregister).

Hva var det viktigste kriteriet for valg av verktøy?
At dette skulle være et «enkelt» produkt som likevel var «fleksibelt» i forhold til våre identifiserte behov og krav/forutsetninger. Vi ønsket en helhetlig leveranse fra en pålitelig leverandør med «track history» og gode referanser. Dessuten ønsket vi en leverandør som hadde lokal support og som ikke var for dyr i anskaffelse i første omgang, og videre at systemet hadde muligheter for utvikling.

> Verktøyet ble i sin tid anskaffet for å understøtte våre prosedyrer rundt registrering av hendelser
>
> *Mazhar Ahmad*

Hvem benytter seg av verktøyet?
Alle ledere i Gjensidige skal benytte systemet for å registrere og følge opp hendelser iht. instrukser godkjent av konsernsjef, risiko- og compliance koordinatorer i 1. linje, samt 2. linje (risikostyring og compliance) og 3. linje). Vi snakker om rundt 5-600 brukere. Det er stor variasjon i aktivitetsnivå. Vi i Risikostyring konsern er førstelinje support, tekniske forhold ruter vi selv videre til leverandør. Tekniske ting i selve applikasjonen må vi i Risikostyring håndtere selv. Driftsmessige forhold ordnes av vår IT-driftspartner Evry.

Hva er de største fordelene ved å bruke verktøyet?
Felles rammeverk og metode og at vi går bort fra løse Excel-ark. Enklere å kommunisere og utveksle informasjon.

Har du noen synspunkter på hva som skal til for å lykkes med å implementere et GRC-verktøy?
Implementeringsprosjektet er så vel et organisatorisk («snu organisasjonen» til å tenke på nye måter) som et ledelsesmessig grep («tone at the top» og support/forankring hos toppledelsen). Videre krever det involvering av nøkkelmedarbeidere (da prosjektet er ressurskrevende) og «risk champions» i linjen (som faktisk skal ta i mot løsningene), samt spesialistene internt i Risikostyring og Compliance som faktisk skal utvikle et rammeverk for å gjennomføre dette. Arbeidet ble organisert som et «program» bestående av mange enkeltprosjekter (organisert i «streams»/arbeidsstrømmer). Prosjektledere var primært ansatte i Risikostyring og Compliance med rapportering av status/fremdrift til både CRO og CCO, samt GRC (konsernets risikostyringskomite).

Vi valgte å få bistand fra eksterne i prosjektet. Jeg vil si at det tar rundt 2 år for store virksomheter å få på plass «basic» infrastruktur, og ytterligere 2 år før man begynner å høste noen frukter. Det tar lang til å utvikle en kultur som understøtter prosesser, metoder og verktøy, selv om disse også er viktige. Så kan man videreutvikle systemene for risikostyring og internkontroll, og dette stopper egentlig aldri opp.

Risikomatriser- forutsetninger og fallgruver

Av
Y. AYSE B. NORDAL
Fagansvarlig – risikostyring
Undervisningsbygg Oslo KF
MSC, BSC METU, Licentiat NHH
Sertifisert - Akkreditert Risk Manager QMCE

Ayse har vært medlem av arbeidsgruppen for utarbeidelse av Veileder for risikostyrings-funksjonen som blir utgitt av IIA Norge.

1. Bakgrunn

En modell er en forenklet fremstilling av variabler, forhold og relasjoner som vi møter i virkeligheten. Modellen kan være fysisk, symbolsk, matematisk, verbal eller grafisk. Uansett form er dens misjon å bidra til at vi forstår et fenomen, og dets påvirkning på andre forhold, slik at vi kan predikere disse variablenes fremtidige utvikling.

Risikomodeller har samme misjon. De bidrar til at vi forstår risikoene, prioriterer de viktigste og estimerer deres fremtidige utvikling. Det finnes ulike modeller i markedet med ulikt sofistikeringsnivå som benyttes for disse formål, eksempelvis finansielle risikomodeller, Monte Carlo simuleringer, Bow Tie analyser og beslutningstreet, men de fleste virksomheter velger en *risikomatrise* som «modell», siden denne representerer en enkel metode for å visualisere og prioritere risikoene. Utfordringer ved bruk av risikomatriser er forutsetningene som ligger til grunn, og som ofte ikke diskuteres med beslutningstakere.

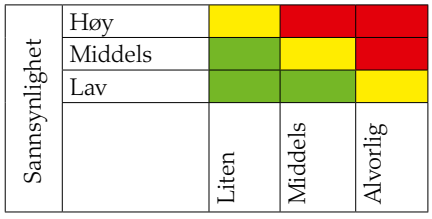
Hensikten med denne artikkelen er å synliggjøre forutsetningene som ligger bak ulike risikomatrisene og å oppfordre brukerne til å forstå, vurdere og akseptere disse før de tar matrisene i bruk.

2. Utfordringer ved bruk av risikomatriser

2.a.Fargeskalaen på risikomatrisen innebærer indirekte forutsetninger om virksomhetens risikoappetitt.

I følge ISO 31000 *«…uttrykkes risiko ofte som en kombinasjon av konsekvensene av en hendelse (inkludert endringer i omstendighetene) og den tilhørende muligheten for at den skal forekomme…»*[1]

Den vanligste tilnærmingen til risiko (R) er å definere den som R= Sannsynlighet * Konsekvens, selv om denne definisjonen innebærer flere svakheter siden den ikke tar hensyn til eksempelvis samvariasjonene mellom risikoene og de forsterkende snøballeffektene.



Figur 1

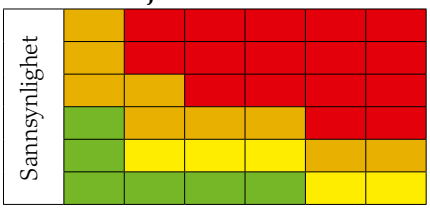
I samsvar med den ovennevnte definisjonen inneholder en risikomatrise en sannsynlighets- og en konsekvensskala. Området under matrisen klassifiseres som lav-, middels- og høyrisikoområder. Figur 1 beskriver den enkleste form av risikomatrise, der grønne, gule og røde celler fremstiller henholdsvis lav, middels og høyrisiko.

I markedet finnes det et stort antall risikomatriser med ulike egenskaper. Med referanse til K. Anderson opplyser Richard Jarrett and Mark Westcott at det er funnet mer enn 800 varianter ved en Google-søk. [4] Det blir enkelte ganger oversett at, til tross for et svakt teoretisk fundament, forsøker disse matrisevariantene å gi et visuelt uttrykk for virksomhetens *risikoappetitt*.

Risikoappetitt defineres som det nivå av usikkerhet en organisasjon er villig og har evne til å eksponere seg for å kunne gjennomføre sine aktiviteter og realisere sine mål. Risikomatrisen som Figur 1 beskriver forutsetter en *risiko-nøytral* innstilling. Matrisen inneholder like stort areal for lav-, høy- og middelsrisiko dvs. 33,33 %.

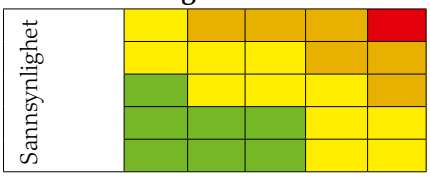
Matrisen i Figur 2 beskriver en helt annet innstilling til risiko. Kun 14% av arealet er grønt. Dvs. matrisen vil klassifisere brorparten av hendelsene som høy og middelsrisiko-hendelser som ville kreve tiltak.

Risikoaversjon



Figur 2

Stor risikovillighet



Figur 3

En slik matrise ville passe en virksomhet med høy risikoaversjon. Matrisen i Figur 3 fremstiller den motsatte innstilling til risiko. I denne matrisen vil veldig få hendelser klassifiseres som høy-risiko hendelser.

Enhver virksomhet som ønsker å benytte en risikomatrise for å identifisere, rangere og prioritere sine risikoer bør sette seg i matrisens egenskaper. Hvilke forutsetninger har matrisen? Blir sannsynlighet- og konsekvens vektet like i risikoberegningen? Innebærer matrisen prioriteringer vedrørende risikoappetitt eller er den risiko-nøytral? Hvilke antagelser ville passe best for den aktuelle virksomheten? Det, eksempelvis, ville være en stor feil å vurdere HMS-området med en matrise, som er beskrevet i Figur 3, som innebærer stor risikovillighet.

2.b. Risikomatrise samsvarer ikke med virksomhetens risikoforståelse og risikodefinisjon.

Tidligere ble begrepet risiko forbundet utelukkende med *uønskede hendelser* med negative konsekvenser. I dag defineres begrepet i samsvar med prinsippene for helhetlig risikostyring, med fokus på usikkerheten, som kan påvirke måloppnåelsen og gjennomføringen av virksomhetens strategi. ISO 31000 *definerer risikoen som virkningen av usikkerhet knyttet til mål. En virkning er avvik fra det forventede, positivt eller negativt.* [5]

COSO, Thought Leadership in ERM, «Risk Assessment in Practice» har i 2012 presentert risikomatrise med muligheter.[6]

Også det oppdaterte COSO- rammeverket som har nylig vært under høring forsøker en helhetlig tilnærming til risiko. *Risiko defineres som muligheten for en hendelse som kan påvirke oppnåelsen av virksomhetens strategi og målsetninger.* [7]

I sine strategidokumenter og målformuleringer forteller mange virksomheter at de ser på risiko som et begrep som innehar både opp-side og nedside. Usikkerheten kan resultere i uønskede hendelser, men den kan også bringe muligheter. Når det gjelder matrisevalg derimot velger de fleste de løsningene som identifiserer og rangerer kun de uønskede hendelsene. Få virksomheter tar i bruk matriser som er beskrevet i Figur 4, som gjør det mulig å kartlegge og rangere både positiv og negativ usikkerhet.

2.c Risikomatrise kan ha logiske brister.

Mange virksomheter er lite grundige når de definerer sannsynlighet- og konsekvensskalaene på risikomatrisen. I enkelte tilfeller kan begrepsbruken og skaleringen inneholde logiske brister.

Matrisen i Figur 5, som er i bruk i en rekke virksomheter er et slikt eksempel.

	Ubetydelig	Mindre alvorlig	Alvorlig	Meget alvorlig	Svært alvorlig
Svært s.					
Meget s.					
Sannsynlig					
Mindre s.					
Usannsynling					

Figur 5

På sannsynlighetsskalaen av denne matrisen blir det laveste nivået definert som usannsynlig. Dette er et vanskelig begrep å operasjonalisere. Begrepet usannsynlig kan tolkes som ikke sannsynlig. Skulle begrepet omfatte «null sannsynlighet» vil risikoen være et punkt på matrisen, dvs. origo. (R= null* konsekvens). Å definere «usannsynlig» risiko som et intervall som denne matrisen gjør ville da innebære en logisk brist.

Skulle begrepet inneholde minimal risiko som er større enn null, da vil den valgte fargeskalaen innebære en logisk brist, siden matrisen klassifiserer hendelsene med en veldig lav sannsynlighet men med svært alvorlige konsekvenser som hendelser med lav risiko. Dette er ikke realistisk. Eksempelvis, i bygg og anleggsvirksomheten er dødsulykkene heldigvis meget sjeldne. De har minimal sannsynlighet. Konsekvensene av slike ulykker i form av arbeidsmiljøkonsekvenser, erstatningskrav og omdømme tap derimot er veldig alvorlige. Det vil da være en logisk brist hvis matrisen i bruk skulle definere slike hendelser som lavrisiko hendelser.

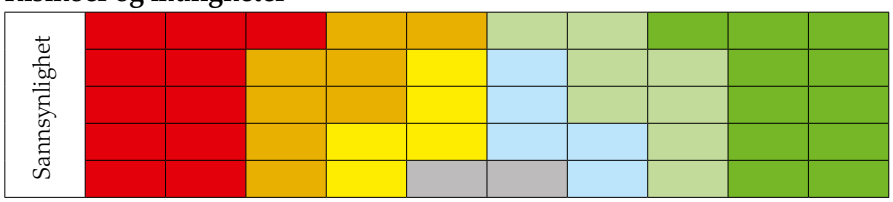
Konklusjon

En risikomatrise er et lavterskel verktøy, som er praktisk å bruke på risikoworkshop, for å definere og følge opp tiltak. Matrisen visualiserer virksomhetens risikoer og prioriteringer. Den representerer en lett forståelig dokumentasjon og utgangspunkt for rapportering.

Det er viktig at risk manager og internrevisor forstår forutsetningene av verktøyet som er i bruk, og det brukes med omhu. Alle instanser som benytter matrisen for analyse- og rapporteringsformål bør informere beslutningstakere om matrisens forutsetninger og mulige svakheter. Internrevisoren stiller vanligvis kritiske spørsmål om risikoformuleringene, risikohåndteringen og rapporteringsrutinene. Bør egnetheten av risikomatrisen som blir benyttet under risikovurderingen også komme til internrevisorens kritiske søkelys?

I egenskap å være den tredje forsvarslinjen i en virksomhet skal internrevisor gi styrende organer og toppledelsen en objektiv bekreftelse på internkontrollen og risikostyringen i virksomheten.

Risikoer og muligheter



Figur 4

Kilder:

[1]ISO, ISO 31000:2009, Risk management – Principles and guidelines, 2.1, MERKNAD 4 side: 2
[2] COSO (Committee of Sponsoring Organizations of the Treadway Commission) Internal Control Integrated Framework, Executive Summary, May 2013, side: 4
[3] Y. Ayse B. Nordal, «Modelling Risks – Limitations and Challanges» International May Conference on Strategic Management, 28. mai 2016, Technical Faculty at Bor, University of Belgrade.
[4] Richard Jarrett and Mark Westcott, Quantitative Risk. Dealing with Uncertainties in Policing Serious Crime, Australian National University, ANU-Press, 2010; side: 2
[5] ISO, log.cit. side: 2
[6] COSO, Thought Leadership in ERM" Risk Assessment in Practice", October 2012, side:15
[7] COSO ERM Aligning Risk With Strategy and Performance, June 2016, side: 9

Introducing a fresh approach and new medicine to tackle the constant headache of fraud and corruption (Part 1)

BY
NIGEL KRISHNA IYER
AND MARTINA MARMAI

Nigel Iyer 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 has written a number of films, plays and books based on his experiences, many of which are used in teaching worldwide. In addition to being one of the founder members of Hibis he is also a fellow of the University of Leicester School of Management.

Right from an early age Italian-Slovenian Martina Marmai wanted to play an active part in eradicating corruption and fraud. She continues this passion today at Hibis specializing in identifying red flags of corruption and understanding and investigating them across a wide range of countries and language-zones.

When it comes to corruption and fraud, it is logical to challenge how effective the past decade´s enormous efforts in Corporate Governance, Risk Analysis and Internal Controls have been. It seems from all the media reports, surveys and statistics that the cost and impact of fraud and corruption is in fact rising, not falling. In this article we propose that the power of teamwork combined with proactive fraud detection is a way both of saving costs and building up an organisation´s defences.

In connection with a speaking engagement on the subject of the early detection of fraud at a recent European Governance, Risk and Compliance conference we read in the conference brochure that the chairman of the organising committee expressed the opinion that *«GRC is the cure for the migraine and progress was being made». But he also added «the fog was clearing until along came the Panama Papers and gave us another headache».*

Governance Risk and Compliance (or «GRC» as it is known) may be a cure for some migraines but when it comes to fraud and corruption, we believe that a new medicine is needed. GRC is a preventative medicine, but there is only so much preventative medicine the patient can take; instead, proactive medicine is needed to be able to identify the fraud and corruption which is already there and to deal with it responsibly and efficiently thereby out-thinking the fraudsters at the earliest opportunity. Paying «lip-service» to fighting fraud and corruption by ticking off the formal GRC boxes is just not enough.

For organisations to succeed in stopping fraud and corruption, management should see its early discovery as good news rather than something to be afraid of. We believe management need to give their unequivocal backing to all those people in the organisation who are committed to finding fraud and corruption and removing its consequential cost and waste.

The dream: Teamwork against the common enemy of fraud and corruption

In our opinion the key to the early detection and eradication of fraud and corruption is teamwork and collaboration. This collaboration should involve people such as internal auditors, a number of people in finance and accounting, senior management (of course), legal and compliance, risk management, corporate security, HR and other willing participants. There are many people in an organisation who have either a mandate or an incentive to remove unnecessary and unethical costs and waste.

Whilst corruption and fraud have become as common as the common cold and nobody likes to be cheated, there is still a perception that it is a remote risk as far as «our» organisation is concerned. It's often dismissed as «something which happens to others».

But treating fraud and corruption as a remote risk is both naïve and dangerous. Many studies (including empirical and quasi-academic ones) place the total costs

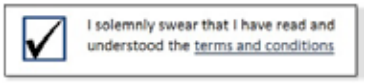
Foto: Lightspring/Shutterstock

associated with fraud and corruption (i.e. loss of money plus erosion of organisational culture plus damage to reputation) in the region of around 5% of an organization's annual turnover. In reality fraud and corruption is much more commonplace than we would like to think, but it´s supposed to be hard to spot. As a consequence it becomes a hidden cost for the organisation.

Based on our experiences one of the most important steps to counter fraud and corruption is to foster a spirit of teamwork against a common enemy and employ effective techniques which are successful in detecting fraud and corruption early.

Instead of waiting for someone else to spot the fraud and blow the whistle we have in recent months seen a number of examples where organisations were able to actively search for, identify and address typical red flags of fraud and corruption. Here are some recent examples of things that were found and resolved early:

- Numerous suppliers which take advantage of loopholes in the routines and controls and simply charge too much for what they do
- Sharp business partners, middlemen and consultants who take advantage of the organisation´s trust and behave unethically
- Customers who get excessive preferential treatment or prices
- Hidden connections between the organisation and Dirty Money Centres (the illegitimate side of tax havens)
- Bribes (sometimes cleverly disguised) which were paid as a shortcut to get business and so called «false bribes» (often just embezzlement by another name)
- «Creative numbers fraud» when sales figures are artificially inflated or costs are supressed
- Conflicts of interest where people on both the inside and the outside have their «fingers in many pies».



Asking people to tick boxes saying that they have read documents in the full knowledge that they will tick them blindly is not even real compliance, let alone a defence against corruption and fraud!.

The release of the Panama Papers and the «tip of the iceberg» that it revealed was just one more piece of evidence demonstrating that we need to take effective action against corruption and fraud.

Teamwork across departments, raising awareness and management empowering people such as internal auditors and security officers to take a more active role to help everyone look for the early warning signs could be the cure we were looking for. - and it needs everybody to be on board.

In Part 2 (to be published in the next issue) we will describe some of the most effective techniques by which everybody (including auditors) can find fraud and corruption before it finds them.

On the 19th January 2017, Nigel Iyer and Veronica Morino will be holding a course for IIA Norge and NKRF about how to find corruption and fraud early and effectively called «Oppdag korrupsjon, svindel og misligheter - raskt og tidlig!» See http://iia.no/aktiviteter/oppdag-korrupsjon-svindel-og-misligheter-raskt-og-tidlig/.

In every case where fraud and corruption was discovered early by a team approach, management felt they were prepared and was able to take immediate remedial action, first to stop any further unnecessary costs and waste, and then to find the most effective solution to resolve the matter and strengthen the robustness of the organisation for the future.

Amongst the most important additional benefits of teamwork in the early detection and resolution of and corruption were:

- The avoidance of internal squabbling over «who needs to take the blame for not finding it earlier?»
- People across the organisation feel confident to raise what they see as red flags, potential problems and cost saving opportunities because they know that this is what is expected of them (i.e. early discovery is good news)
- The creation of a new positive spirit in the organisation and a realisation that the days of «waiting for whistle-blowers» or only reacting to discoveries in the media were soon going to be over!

The example case in the box on this page, whilst in many ways an extreme case, illustrates important behavioural responses which are not as uncommon as we may at first think. It is understandable for management, at least at first, to be sceptical to any form of early detection of fraud and corruption. In their mind fraud and corruption does not happen to them, or they derive comfort from the fact that since nothing has been discovered so far then nothing will be uncovered in the future. A natural fear is that the process of looking could be disruptive and that in the event of a discovery the end result will be a painful investigation and possibly even a media scandal. We believe that all these fears can be dealt with and none of them have to be true. It is important however to address these fears in advance. Finding fraud and corruption early requires a solid business case (a financial «value proposition» to use another phrase), one which everybody supports and buys into.

Taking the next step and tuning up the organisation to be even more effective in eliminating the cost of fraud and corruption.

Whilst we believe that «Governance, Risk and Compliance» is not the ideal medicine for finding fraud and corruption early, we are by no means arguing for a complete dismissal of all organisational, regulatory and compliance measures; on the contrary, it is clear that complex organisations do need guidelines to establish their own controls. These must, however, be accompanied by proactive efforts to detect on-going fraud and corruption. A new internal regulation or a tick in a box is quite simply not enough.

A CASE IN POINT: WHY AND HOW TEAMWORK AND FINDING FRAUD EARLY IS GOOD NEWS FOR EVERYBODY - EXCEPT OF COURSE THE FRAUDSTERS!

A few months ago we assisted the internal audit department of a large Nordic company with a pilot review to look for red flags of fraud. It was a small project but among many of the examples and red flags identified one particular supplier stood out. At first glance, the invoices issued by this supplier looked fine: not a single detail was missing, from the unit price to the firm's logo, addresses, and contact details. This was a supplier from whom they had been sourcing large quantities of raw materials for over 10 years. Up to then there was no apparent reason to complain.

Yet a closer review of the invoices showed that something rather "odd" seemed to be going on. The supplier stated that they were the offshore branch of a company registered in a Dirty Money Centre (or DMC), and they requested payment in a different currency to an account in a slightly different name in yet another DMC. This on its own was not enough to convince the management that maybe something was wrong. Management repeated the argument that they had been using this supplier for many years, and no one had pointed out anything wrong before, they were getting the products at a good price and that they placed reliance on "compliance checks" that had been carried out. They referred to the supplier's almost flawless and detailed website which included a 10 page code of ethics, a whistle-blower line and a statement that the company´s management would welcome and not discriminate against whistle-blowers. Despite this the internal auditor trusted the analysis and his intuition and he was politely persistent. In order to get management´s attention further evidence was needed; evidence that the company´s website was only recently registered, the principal place of business was a law office employing four people with a permanent answerphone, and that no information could be found about the current true management and owners of the company whilst there was evidence that the former management had been the defendants in some serious criminal cases. Now management´s interest was aroused and they gave their full backing to the internal auditor to proceed to examine a little further. To cut a long story short, it was proven that this particular supplier was central to a complex scheme of shell companies controlled by a particular and well known organized crime group who had been working in this way for a relatively long period of time.

Management were quick now to appreciate that despite apparent cost-savings, the future risks to continue to buy from this supplier were too big to take. At the same time any further investigation or legal action against an organized crime group would likely be long and drawn-out, probably futile, and even counter-productive. A board decision was taken to politely sever the business relationship with this supplier. At the same time action was taken across the company to learn the lessons and put in place processes and training to prevent a similar situation arising in the future. Management and the board also commended the internal audit department for its proactive and timely action.

Styringssystem for sikkerhet

AV
CARSTEN RAPP

Carsten er senior manager i BDO Rådgivning, Sikkerhets- og beredskapstjenester. Han har vært sentral i utviklingen av regulatoriske krav, veiledere, håndbøker og kurs om bl.a. sikkerhetsstyring og sikringsrisikovurdering. Han har 12 års erfaring fra øverste ledergruppe i statlige virksomheter og 10 års erfaring med implementering, vedlikehold og revisjon av styringssystemer for sikkerhet. Carsten er utdannet jurist, sertifisert ISO 27001 Lead Implementer, og har tidligere jobbet i Nasjonal sikkerhetsmyndighet, Norges Bank, Etterretningstjenesten, Datatilsynet og Forsvarets overkommando.

Innledning

I en verden der omgivelser og forutsetninger endres med stadig nye muligheter, trusler og sårbarheter, er det krevende å holde tritt i sikkerhetsarbeidet. Det stilles høyere krav til sikkerhet enn tidligere fra både myndigheter, kunder og publikum. De seneste rapportene fra Nasjonal sikkerhetsmyndighet, Riksrevisjonen og internasjonale aktører, viser med tydelighet økt behov og økte forventinger til et systematisk arbeid med sikkerhet i offentlige og private virksomheter. I tillegg har det de siste årene skjedd endringer i og harmonisering av nasjonale og internasjonale standarder for styringssystemer, eller ledelsessystemer som er betegnelsen Standard Norge har valgt å bruke. I denne artikkelen grunngis hvorfor virksomheter bør ha et styringssystem for sikkerhet og det beskrives hva et slikt styringssystem for sikkerhet går ut på. Videre redegjøres det for likheter og forskjeller mellom styringssystemer for sikkerhet i forhold til andre former for styringssystemer. Til slutt omtales integrasjon og samordning av styringssystemer. Fokuset i artikkelen er sikring mot tilsiktede uønskede handlinger, altså viljestyrte hendelser. Mye vil imidlertid være felles med sikkerhet mot utilsiktede hendelser som naturkatastrofer, ulykker og ubevisste feil.

Hvorfor bør bedrifter ha et styringssystem for *sikkerhet*?

Alle virksomheter har behov for å sikre sine verdier. Det sentrale målet er å sikre at viktige ressurser kan benyttes av bedriften når det er behov for det (tilgjengeligheten) og at data ikke er skadet eller manipulert med (integriteten). For informasjonsverdier kan det også være et mål at taushetsbelagte opplysninger ikke kommer uvedkommende i hende (konfidensialiteten). Andre mål kan være at det for viktige transaksjoner skal bekreftes at avsender eller mottaker er den vedkommende gir seg ut for å være (autentisering).

Hvilket sikkerhetsnivå og hvilke typer sikkerhetstiltak som velges i ulike bedrifter varierer veldig. Ofte er det påfallende store ulikheter i sikringsnivået mellom bedrifter i samme bransje og marked. Det aktualiserer flere spørsmål og problemstillinger. Hvordan skal man kunne vite at tiltakene faktisk er de riktige? Hvordan skal man kunne vite at tiltakene er implementert hensiktsmessig? Eller kanskje enda viktigere; hvordan skal man kunne vite at det som var den riktige dimensjoneringen og kombinasjonen av tiltak i fjor (eller i går) fortsatt er den riktige nå (og i morgen)?

Sikkerhetstiltak koster. De kan påvirke bedriftens handlingsrom, og kan utgjøre inngrep overfor medarbeiderne og omgivelsene som oppfattes negativt. Sikkerhet kan imidlertid også medføre et konkurransefortrinn og åpne for muligheter som bedriften ellers ikke ville eller burde satset på. Det er uansett viktig at sikkerhetstiltakene er tilpasset risikobildet og er kostnadseffektive.

I BDO ser vi ofte at virksomheter etterspør bestemte typer sikkerhetstiltak, som i beste fall er tilpasset risikobildet der og da, men som lett får et statisk preg. Flere tenker nok at hvis de har anskaffet og implementert et håndfast teknologisk tiltak, slipper de å tenke mer på sikkerhet på en god stund. Teknologiske tiltak er imidlertid bare én kategori av tiltak. Trusselaktørenes teknologi endres og tilpasses kontinuerlig for å finne og utnytte sårbarheter.

Alle bedrifter påvirkes av utviklingen i omgivelsene så vel som av endringer internt - planlagte eller ikke. Akkurat som at markedet kontinuerlig er i endring, er risikobildet innen sikkerhet svært dynamisk.

Enkelte bedrifter har god og oppdatert oversikt over trusler og farer, som er vel og bra. Risikoen består imidlertid av mer enn bare trusler og farer. I hvilken grad bedriftens *viktigste innsatsfaktorer og ressurser (verdier) er sårbare* mot uønskede hendelser, er vel så sentralt. Det er tross alt egne sårbarheter bedriften primært selv kan påvirke. Med en rivende teknologisk utvikling, spesielt innen IT der «alt» etter hvert kobles til Internett,

TRUSLER OG FARER

Klimaendringer fører til at faren for naturgitte hendelser også endres. Teknisk svikt i infrastruktur er ofte årsak til driftsstans eller ulykker. Hvem som blir utsatt for naturrelaterte hendelser og andre ulykker er uforutsigbart, og som oftest utenfor egen kontroll.

Også når det gjelder terrorhandlinger og sabotasje er uforutsigbarheten stor. Terrorhandlinger og sabotasje er ikke lenger bare relevant for virksomheter med tilstedeværelse i ustabile land, og hvem som blir mål skifter stadig.

Cyberangrep er en annen stor trussel mot samfunnets og enkeltbedrifters IT-systemer. Manglende evne til å hindre informasjonstyveri eller sabotasje av IT-systemer kan føre til blant annet dårligere konkurranseevne, erstatningsansvar overfor tredjeparter, sanksjoner fra myndighetene eller svekket omdømme.

Empiri viser at mange uønskede hendelser er forårsaket eller muliggjort av egne ansatte. Disse kan være et resultat av en enkelt ansatt sine bevisste handlinger. Motivet kan være alt fra egen vinning til press fra andre eller gjengjeldelse. All verdens teknologiske tiltak vil ikke hjelpe mot en innsider som benytter sine lovlige tilganger til å skade bedriften.

En vesentlig kilde til sikkerhetsbrister er uønskede hendelser forårsaket av manglende bevissthet og manglende kunnskap om risikofaktorer og sikkerhet.

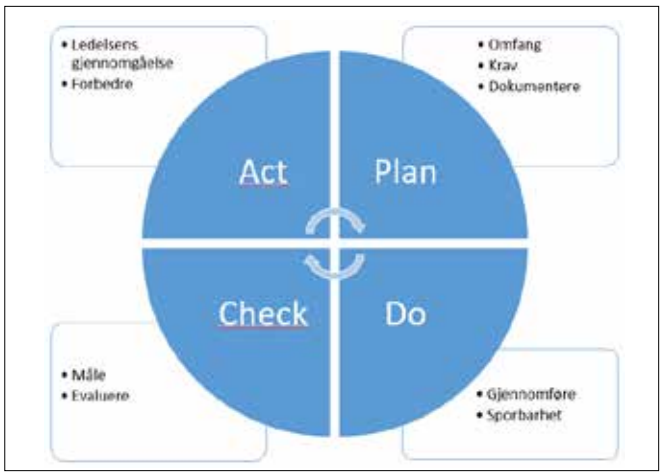
er endringstakten stor. Denne endringstakten gjelder også sårbarheter i bedrifters IT-systemer. Ikke bare IT-systemer for beslutningsstøtte, men også driftskontrollsystemer for infrastruktur, produksjonsutstyr og tekniske sikringssystemer. Eksisterende sårbarhetsvurderinger og sikkerhetstiltak mister dermed sin relevans over tid. Gode prosesser for kontinuerlig forbedring og utvikling innen sikkerhet er derfor viktig.

Hva har styringssystemer for sikkerhet til felles med andre styringssystemer?

Tidligere ble formålet med risikostyring sett på som primært å unngå tap. Senere har risikostyring blitt ansett som vel så mye et middel til å håndtere usikkerhet. I de nyeste versjonene av flere ISO-standarder, er risiko definert som *virkningen av usikkerhet knyttet til et mål*[1]. God risikostyring reduserer usikkerheten i beslutningsgrunnlaget om egne verdier, trusler, sårbarheter og påfølgende sikringstiltak. Det er i prinsippet ikke det å ta risiko som er utfordringen, men det å ikke identifisere og vurdere risikoen før viktige beslutninger tas.

Så hvordan holde tritt med utviklingen i et dynamisk trussel- og sårbarhetsbilde? Hvordan unngå feilinvesteringer i sikkerhetstiltak, at opprinnelig gode tiltak går ut på dato, og at tiltak endres først etter at det har gått virkelig galt? Hvordan redusere usikkerhet? Det er her styringssystem for sikkerhet kommer inn.

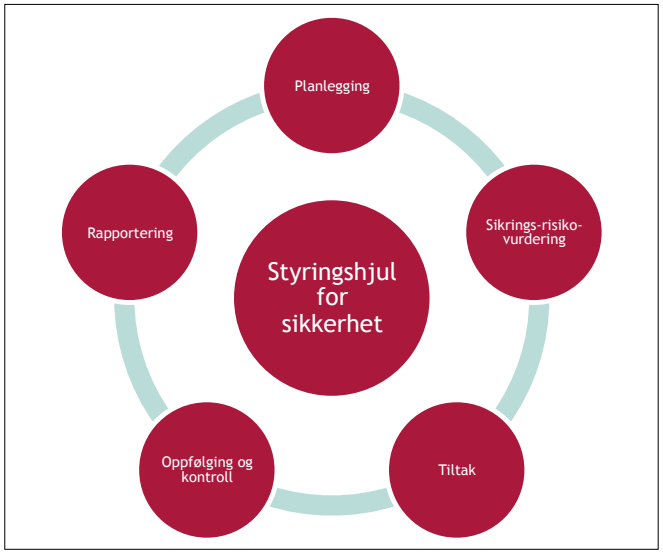
Det finnes flere definisjoner av styringssystem, eller ledelsessystem som det nylig er omdøpt til i norske standarder. I ISO-standardene benyttes følgende definisjon, oversatt til norsk; *sett av beslektede eller samvirkende elementer i en organisasjon for å etablere policyer, mål, og prosesser for å oppnå disse målene.* I sin opprinnelige og enkleste form består modellen av et styringshjul med hovedelementene «PDCA»; Plan, Do, Check, Act – altså *planlegge, utføre, evaluere og korrigere (figur 1)*. Formålet er å oppnå *kontinuerlig forbedring.* Opprinnelig for å oppnå forventet kvalitet ved utvikling og produksjon av varer og tjenester, altså kvalitetsstyring, men senere er prinsippene utvidet til å gjelde for styring av også andre forhold.



Figur 1: Forenklet versjon av kvalitetshjulet, med utgangspunkt i Demings sirkel.

PDCA-modellen utgjør fortsatt kjernen i ulike norske og internasjonale standarder om ledelsessystemer, herunder innen kvalitet, informasjonssikkerhet, ytre miljø og arbeidsmiljø. Også rammeverkene COSO[3] og COCO[4] for styring og kontroll, samt flere veiledere utgitt av staten om alt fra generell internkontroll til økonomistyring og sikkerhet, har store likhetstrekk med PDCA-modellen (figur 2). Modellene i disse rammeverkene og veilederne har imidlertid en mer helhetlig tilnærming til virksomhetsstyringen, og er ofte delt opp i noen flere hovedelementer enn PDCA. Blant annet er det en sterkere synliggjøring av kontrollmiljøet (konteksten), risikostyring og ekstern rapportering, enn det som har vært vanlig innen kvalitetssystemer for produksjon.

[1] *Jf. bl.a. SN-ISO Guide 73:2009 pkt 1.1, NS-EN/ISO 9000:2015, 3.7.9, NS-ISO 31000:2009 pkt 2.1 og NS-ISO/IEC 27000:2016 pkt 2.68.*



Figur 2: Styringshjulet i NSMs veileder om sikkerhetsstyring (201)

Et velfungerende styringssystem for sikkerhet sørger for at sikkerhetsarbeidet skjer på en *planlagt, systematisk og dokumentert* måte. Systemet skal virke både *proaktivt* (grunnsikring og beredskap) og *reaktivt* (hendelseshåndtering). Styringssystemet for sikkerhet kan fungere som et selvstendig styringssystem, spesielt hvis virksomhetsstyringen i bedriften for øvrig er umoden. Optimalt sett bør systemet imidlertid integreres i den øvrige styringen og kontrollen i bedriften («GRC-funksjonene»; Governance, Risk & Compliance).

Hva skiller et styringssystem for sikkerhet fra andre former for styringssystemer?

Sikkerhet beskrives ofte som en tilstand som må gjenskapes hver dag. En statisk tilnærming vil føre til at sikkerhetstilstanden gradvis forvitrer og mister sin relevans opp imot sikkerhetsbehovet. Et styringssystem for sikkerhet skal bidra til god og målrettet styring av sikkerhetsrisiko. Systemet skal også fremskaffe et informasjonsgrunnlag for å vise om sikringsrisikostyringen har fungert etter hensikten.

I utgangspunktet er det som tidligere nevnt de samme hovedelementene i et styringssystem for sikkerhet som for andre styringssystemer. Så hva er spesielt for et styringssystem for sikkerhet, og da spesielt sikring mot tilsiktede uønskede handlinger?

Én forskjell er at metodene for risikovurdering er tilpasset og i større grad operasjonalisert for å anvendes innen sikkerhet. I stedet for generelle prosessbeskrivelser for risikovurdering som i NS-ISO 31000:2009, brukes prosessbeskrivelser og terminologi tilpasset sikkerhetsområdet. I sikkerhetsstandardenes beskrivelse av risikovurderingsmodeller, har f. eks. vurdering av *verdi, trussel og sårbarhet* en sentral plass . BDO har utviklet en forenklet modell av prosessbeskrivelsene i NS 5831:2015, som vist i figur 3.

En annen forskjell er fokuset på sikring av verdiers konfidensialitet, integritet og tilgjengelighet (KIT). KIT er riktignok et element i de fleste former for styringssystemer. Det er imidlertid et betydelig sterkere fokus på KIT i styringssystemer for sikkerhet mot tilsiktede uønskede handlinger, og det er et viktig mål for sikkerhetsarbeidet.

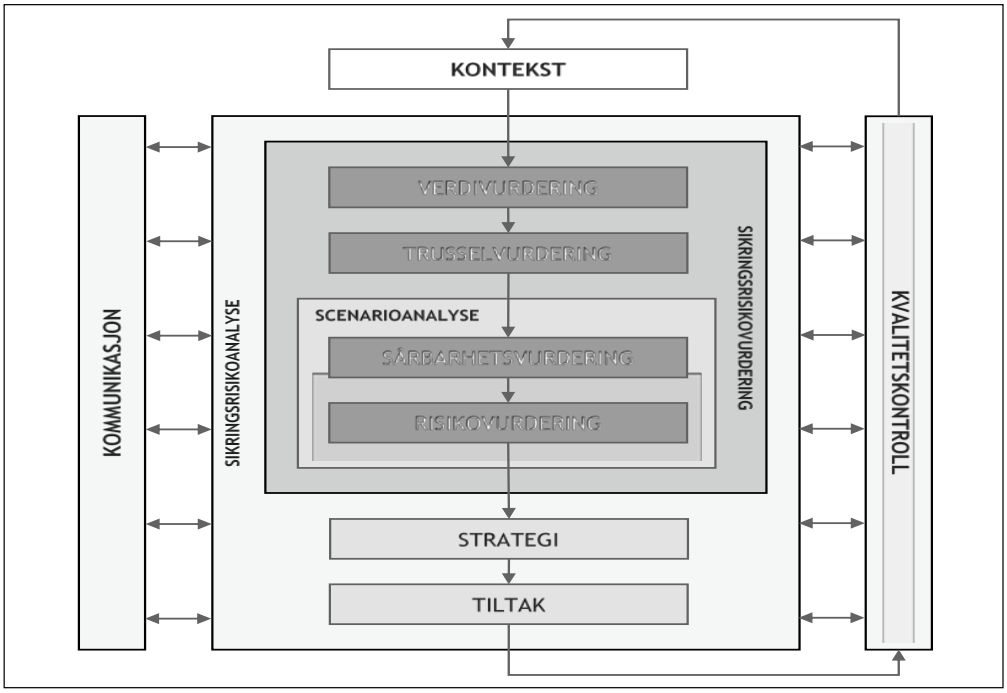
Sikkerhet kan oppnås gjennom tiltak av menneskelig, teknologisk eller organisatorisk art. Menneskelige tiltak skal gjøre ledere og medarbeidere i bedriften kompetente og robuste, f. eks. mot sosial manipulasjon. Teknologiske tiltak i det fysiske eller digitale rom kan f. eks. være sensorer som registrerer og varsler om fysiske bevegelser eller kryptering av informasjon. Organisatoriske tiltak består av prosedyrer og dokumentasjon som skal bidra til at fremgangsmåten i oppgaveløsningen ivaretar sikkerheten, f. eks. beskrivelse av ansvar og roller innen sikkerhet. Den mest effektive sikringen skjer ofte ved å kombinere tiltak fra disse ulike kategoriene. Det er imidlertid ikke et skarpt skille mellom nevnte kategorier og ett og samme tiltak kan ivareta flere hensyn. Et tiltak som

STYRINGSSYSTEMER

Prinsippene i regulative krav og standarder om styringssystemer, er i stor grad basert på forsknings- og utviklingsarbeidet til amerikanerne Walther Shewart (1891-1967) og W. Edward Deming (1900-1993). PDCA-modellen kalles derfor også «Demings sirkel». Modellen ble utarbeidet primært med sikte på forbedring av industriell produksjon. Modellen ble så videreutviklet av spesielt japansk industri, som i etterkrigstiden la modellen til grunn for sin kvalitetsstyring, og som Deming da var rådgiver for.

Deming ville senere erstatte uttrykket Check med Study, for å bedre få frem viktigheten av å analysere og evaluere basert på et bredere informasjonsgrunnlag enn avvikskontroll og revisjon. Videre argumenterte han etterhvert for at uttrykket kontinuerlig forbedring (eng: improvement) kunne erstattes med kontinuerlig utvikling (eng: development). Dette for bedre å få frem dynamikken med ytre rammefaktorer, men også for å passe bedre til andre områder enn kvalitetsstyring. Disse begrepsjusteringene fra Deming har ikke ført til endringer av begrepene i standardene for styringssystemer, men har trolig fått betydning for utviklingen og forståelsen av innholdet i standardene. Demings arbeid har også fått innflytelse på teorier om ledelse generelt[2].

[2] *The Essential Deming: Leadership Principles from the Father of Quality, by W. Edwards Deming, edited by Joyce Nilsson Orsini, published by MacGraw-Hill Education, 2012.*
[2] *The Essential Deming: Leadership Principles from the Father of Quality, by W. Edwards Deming, edited by Joyce Nilsson Orsini, published by MacGraw-Hill Education, 2012.*
[3] *The Committee of Sponsoring Organizations of the Treadway Commission (COSO)*
[4] *Criteria of Control (COCO)*



Figur 3: BDOs forenklede modell av sikringsrisikoanalyse etter NS 5831:2015

f. eks. kryptering vil kunne ivareta både konfidensialitets- og integritetshensyn, mens et kompetanseprogram kan være et tiltak av både menneskelig og organisatorisk art.

Sikringstiltak kan bestå av barrierer, deteksjon, verifikasjon og reaksjon. Ingen barriere kan motstå ethvert angrep. Målet for sikring av viktige verdier er ofte at innen barrierene er forsert, skal bedriften ha rukket å oppdage forseringsforsøket, undersøke eller bekrefte hva trusselen består av, for så å reagere før skaden inntrer eller blir for stor.

Akseptansetest og evaluering er viktige elementer i alle styringssystemer. Enkelte metoder for akseptansetest og evaluering innen sikkerhet forutsetter imidlertid spesialkompetanse og spesialverktøy som en internrevisor i bedriften normalt ikke besitter. Eksempler er inntrengingstesting av IKT-systemer, teknisk sårbarhetsskanning eller simulering av eksplosjonsvirkninger mot bygninger.

Det er normalt frivillig for en bedrift om den vil ha et kvalitetssystem for produksjon, med mindre en kunde stiller det som krav ved en anskaffelse. For styringssystemer for sikkerhet er det annerledes. Det finnes en rekke eksplisitte regulative krav, både i Norge og andre land, som pålegger virksomheter å ha et styringssystem for sikkerhet, med egne tilsynsorgan og strenge sanksjonsregler; det være seg som del av risikostyring og internkontroll generelt eller for sikkerhet spesielt. Eksempelvis innen finansvirksomhet, arbeidsmiljøvern, personopplysningsvern og nasjonal sikkerhet. I tillegg er det enkelte kunder som ved virksomhetskritiske anskaffelser eller før utlevering av sensitiv informasjon, krever at leverandøren etterlever ISO/IEC 27001 om informasjonssikkerhet, eller endog er sertifisert. Det er altså få bedrifter som kan unnlate å ha et styringssystem for sikkerhet.

[5] *Jf. NS-EN ISO/IEC 27005:2011 kap. 8.2 og NS 5832 kap. 5.*

Ineffektivitet og integrasjonsbehovet

Fremveksten av regulatoriske krav til og standarder for styringssystemer for ulike forhold er i utgangspunktet positivt. I hvert fall så lenge omfanget skal være risikobasert og kan skaleres etter bedriftens størrelse. Utfordringen i mange bedrifter er likevel at ulike interne fagmiljøer i mellomstore og store bedrifter ofte, og naturlig nok, har et eierforhold til kun styringssystemer for sine «egne» fagområder. Et slikt fokus skaper «siloer» og resulterer ofte i at det etableres flere parallelle styringssystemer med liten eller ingen sammenheng og derav manglende synergieffekt.

Parallelle styringssystemer vil lett kunne overlappe hverandre, noe som ofte medfører unødvendig og kostnadsdrivende byråkrati. Parallelle styringssystemer kan i tillegg føre til uklare ansvarsforhold, f. eks. der en og samme prosess eller tiltak kan håndtere flere risikoer i ulike styringssystemer, eller der ett tiltak ikke er forenlig med et annet. Videre vil parallelle styringssystemer sjelden gi en samlet og ordnet oversikt over alle typer avvik og uønskede hendelser. På strategisk nivå blir det da vanskelig å presentere et helhetlig risikobilde, på samme format og med omforente kriterier, for virksomhetsledelsen. Konsekvensen er at *prioritering* mellom risikoer som bør håndteres og mulige synergier av tiltak vanskeliggjøres, om det i det hele tatt skjer en bevisst prioritering.

Bedrifter bør søke å *integrere prinsipper og prosesser av felles art* gitt i regulatoriske krav og standarder relevante for bedriften, inn i et balansert og helhetlig styringssystem. I det minste for alle former for sikkerhet (HMS, informasjonssikkerhet, sikring av eiendeler og personer osv.), men helst også integrert med virksomhetsstyringen for øvrig. Omfanget bør skaleres og innholdet tilpasses virksomhetens størrelse og risiko. I store og mellomstore bedrifter bør alle roller med en styrende og kontrollerende funksjon for styringssystemer samles i en felles enhet for GRC-funksjonene, mens de utøvende funksjonene i styringssystemet er distribuert ut i bedriftens linjeorganisasjon. En slik tilnærming vil gi bedre og mer kosteffektiv styring og kontroll i bedriften enn parallelle systemer.

Hvorfor bør styret stille tydeligere krav til risikostyringen?

AV
OLE MARTIN KJØRSTAD

Ole Martin Kjørstad er Senior Manager i BDO Advisory der han har hovedansvar for internrevisjon. Som prosjektleder har han bred erfaring fra ulike fra revisjons- og rådgivningstjenester, primært innenfor risiko- og virksomhetsstyring. Han er opptatt av at risikostyring skal være et målfokusert og reelt ledelsesverktøy, med fokus på praktiske løsninger og gode kommunikasjonsmekanismer. Ole Martin er også del av arbeidsgruppen som på vegne av IIA Norge utarbeider en Veileder for Risikostyringsfunksjonen.

Styret i en virksomhet har et lovfestet ansvar for å sørge for forsvarlig drift av virksomheten. Dette omfatter ansvaret for virksomhetens risikostyring, som til dels er definert i mer detalj av ulike organisasjoner og bransjespesifikke reguleringer. Blant annet presiserer NUES 10[1] at styret selv må danne seg en oppfatning av virksomhetens internkontroll, basert på informasjon som blir forelagt styret. Andre føringer, slik som Finanstilsynets veiledning til forskrift om risikostyring og internkontroll[2], sier først og fremst noe om rapportering fra ledelsen til styret. Dette er i seg selv bra, men verdien av slik rapportering er unektelig betinget av ledelsens evne og mulighet til å fange informasjon som er vesentlig for styret. Videre må man spørre seg om periodisk rapportering er tilstrekkelig for å sikre tidsriktig håndtering av potensielt vesentlige risiki.

Når man som styremedlem har ansvar for å sørge for forsvarlig drift har man i siste instans også ansvar for alt som skjer i virksomheten – inkludert forhold man ikke kjenner til. Når det er tilfellet, burde ikke god risikostyring handle om noe mer enn å vurdere virksomhetens risiko basert på den informasjonen man blir forelagt?

Jeg mener at et styre som skal ivareta dette ansvaret aktivt må se til at det etableres mekanismer som er egnet til å identifisere og kommunisere vesentlig informasjon til rett nivå i organisasjonen. For styrets del skal dette gi trygghet for at informasjon som er vesentlig for dem å ta stilling til blir kommunisert løpende. Med andre ord er det vel så viktig å ta et eierskap til den metodikken ledelsen og selskapet jobber etter, som å stille krav til innholdet i periodisk rapportering. Skal risikorapporteringen gi trygghet som beslutningsgrunnlag, må styrets medlemmer også føle seg komfortable med at den er så fullstendig, presis og nyansert som mulig.

Hva kjennetegner god risikostyring?

God risikostyring handler ikke om hvor mange analyser som er gjennomført eller hvor ofte man rapporterer. Det handler om mer enn å vurdere sannsynlighet og konsekvens knyttet til uønskede hendelser. God risikostyring handler om å legge til rette for at organisasjonen skal kunne ta velinformerte beslutninger og fokusere på de aktivitetene som maksimerer måloppnåelsen. Kort sagt kan man si at det handler om å skape trygghet for at virksomhetens strategi operasjonaliseres på best mulig vis samtidig som man ivaretar gjeldende interne og eksterne krav.

Dette bør som nevnt stå svært høyt på styrets agenda. Men hvordan skal man vurdere hvorvidt virksomheten har mekanismer som ivaretar dette på en god måte? Dette er lettere sagt enn gjort og vil fortone seg svært forskjellig avhengig av bransje og selskap. Jeg mener likevel det er noen nøkkelfaktorer som er generiske. Dette tegner selvfølgelig ikke et fullstendig bilde av hva som kjennetegner god risikostyring. Temaene kan imidlertid være til hjelp når man som styremedlem eller internrevisor skal vurdere hvordan risikostyringen i virksomheten er organisert og ivaretatt.

Organisering og tydelige roller med reelt mandat og ansvar

Vi har en tendens å umiddelbart tenke på metodikk for risikovurderinger og rapportering når det er snakk om risikostyring. Minst like viktig er imidlertid hvordan man organiserer arbeidet. Roller og ansvar må defineres på et vis som sikrer ivaretakelse av risikostyringsprosessen, hensiktsmessige rapporteringslinjer og nødvendig integritet i arbeidet. Dersom dette ikke er på plass, er det vanskelig å

[1] *Norsk utvalg for eierstyring og selskapsledelse (NUES) www.nues.no*
[2] *Finanstilsynet, Rundskriv 3/2009 - Veiledning til forskrift om risikostyring og internkontroll*

implementere en risikostyringsprosess som tilfører virksomheten verdi.

Selve ansvaret for virksomhetens risikostyring og internkontroll kan ikke delegeres bort fra styret og daglig leder. Det operative ansvaret for selve prosessen er imidlertid en krevende oppgave i seg selv. Dette ansvaret må derfor være reelt og ligge på tilstrekkelig høyt nivå i virksomheten. Videre bør det være direkte rapporteringskanaler til toppledelsen og til styret. Uten disse kanalene vil man kunne begrense verdien av løpende rapportering. Tett dialog er avgjørende for at arbeidet skal kunne skje i tråd med styrets og ledelsens forventninger. Dersom avstanden blir for stor øker sannsynligheten for at fokuset til funksjonen ikke fullt ut støtter virksomhetens målsetninger.

Mange virksomheter har ikke rom for en dedikert Risk Manager. I slike tilfeller er det viktig at det likevel vies tilstrekkelig ressurser og oppmerksomhet til rollen. Dette handler vel så mye om hvordan ledelsen følger opp arbeidet, som hvilken stillingsbrøk som formelt blir allokert. Dersom resultatet av arbeidet som gjøres ikke brukes som et reelt beslutningsunderlag, er det lite trolig at arbeidet blir viet mye oppmerksomhet. Dette forutsetter så klart at informasjon som tilflyter styret og ledelsen er matnyttig. Av nettopp denne grunn er det viktig at styret og toppledelsen legger nødvendige føringer for hva de ønsker å få ut av risikostyringsarbeidet. Ofte blir det for raskt fokus på rapportering oppstrøms, uten at det er brukt tilstrekkelig tid på føringer og prinsipper for hvordan informasjon sammenstilles og rapporteres på ulike nivåer. Dersom styret og ledelsen ikke gir slike føringer, kan de heller ikke forvente at rapporteringen er tilpasset deres ønsker og behov.

Foto: Olivier Le Moal/Shutterstock

Et mål med risikostyring er å allokere ressurser best mulig i virksomheten. Den som har øverste ansvar for risikostyringsarbeidet bør derfor ha dette for hele virksomheten, for å unngå suboptimale beslutninger. Dette forutsetter at ansvaret ligger hos en som har tilstrekkelig kompetanse og kapasitet til å ha overblikk over virksomhetens samlede aktiviteter. Videre må den ansvarlige ikke ha insentiver som knytter egeninteresse tettere til resultatet i enkelte deler av virksomheten.

Foto: ImageFlow/Shutterstock

Omforent metodikk og prinsipper for rapportering

Skal risikostyringen gi verdi er et viktig premiss at informasjon om risiko systematiseres på et vis som gjør det mulig for styret og ledelsen å bruke dette som beslutningsgrunnlag. Dette forutsetter at beslutningstagere raskt kan tolke informasjonen og forstå hva som ligger bak. Skal man få til dette må det rapporteres etter prinsipper som er like for alle i virksomheten. I tillegg må det jobbes etter en felles metodikk som skaper forutsigbarhet og integritet i rapporterte data.

Identifikasjon og kvantifisering av risiko

Rapporteringsform har liten verdi dersom det underliggende arbeidet ikke er godt. Det som gjør rapporteringen verdifull, er strukturen man jobber etter for å identifisere og evaluere risiko. Måten man fanger informasjon og kvantifiserer risiko er derfor avgjørende. Hvordan man konkret kvantifiserer risiko skal jeg ikke gå nærmere inn på i denne artikkelen. Det finnes ingen universell fremgangsmåte som passer for alle. En bank beregner for eksempel kredittrisiko anderledes enn en anleggsvirksomhet rangerer HMS-risiko, og mange bransjer har egne standarder og normer for hvordan risikovurderinger skal gjøres. Den vanligste presentasjonen av risiko er en matrise som viser produktet av sannsynlighet og konsekvens. Bak dette kan det imidlertid også ligge indikatorer eller beregninger som dikterer hva som utgjør de ulike nivåene i matrisen.

Dette påvirker også hvordan man innhenter informasjon om risiko. Noen har mulighet til å hente mye informasjon direkte fra kilder som regnskap og fagsystemer, mens noen virksomheter utelukkende baserer seg på kvalitative analyser. Hva som er best vil avhenge av både ambisjonsnivå og tilgjengelighet til gode data. Ofte kan en kombinasjon være mest hensiktsmessig, men dette medfører

også et behov for gode modeller for datafangst og -prosessering. Dette er ofte nødvendig for å dekke ulike aspekter som inngår i risikoanalysen. Som eksempelet i figur 1 viser, er det ofte vanlig å vurdere risiko i lys av ulike konsekvensområder.

Uavhengig av valgt metode, er det viktig at prinsippene for hvordan man kvantifiserer er tydelige og omforent. I et konsern der man rapporter på ulike nivåer, bør det benyttes skalaer som gjør at informasjonen blir relevant for de respektive nivåene. Ledere på ulike nivåer vil ha behov for informasjon med ulik detaljeringsgrad. Det som er svært vesentlig for en avdeling eller et datterselskap er ikke nødvendigvis like alvorlig for konsernet samlet sett.

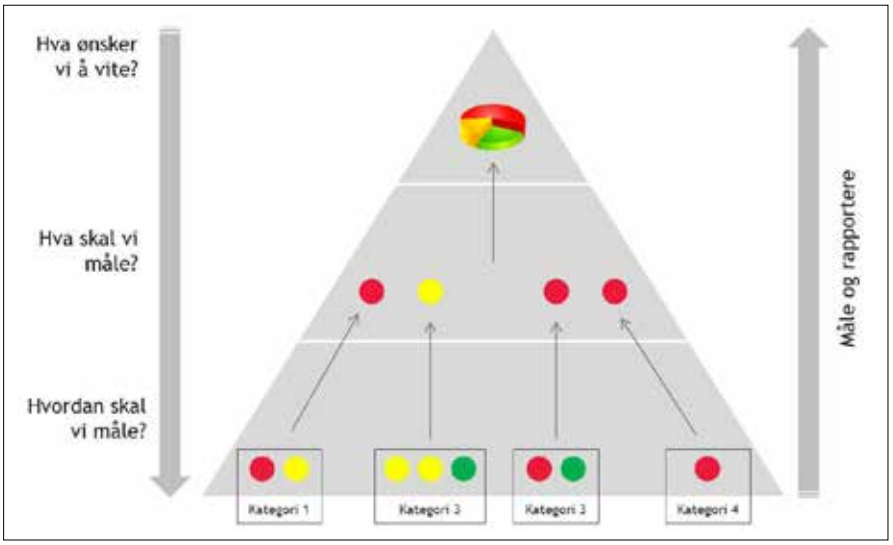
Figur 1

Presentasjon

Når det gjelder rapportering til styret og ledelsen bør man også vurdere å presentere risiko i form av et statisk sett kategorier. Til sammen bør disse kategoriene utgjøre de forholdene som er essensielle å ivareta for at virksomheten skal styres i tråd med definerte krav og målsetninger. Ved å velge en slik tilnærming kan man lettere se utviklingen i risikobildet over tid. Samtidig er det mindre risiko for at områder med et høyt antall risikoer tar uforholdsmessig mye plass i rapporteringen. Dette kan overskygge risiki som er mindre sammensatt, men potensielt mer vesentlige.

En slik tilnærming fordrer at det er definerte prinsipper for hvordan det som rapporteres under hver enkelt kategori aggregeres. Også her vil det variere hva som er mest hensiktsmessig. For noen vil det være mest interessant å se de høyeste risikoene i hver kategori, mens andre vil ha mest interesse av et vektet gjennomsnitt. Dersom man bruker sistnevnte bør rapporteringsmekanismene imidlertid være slik at mindre enkeltforhold som i seg selv kan være svært kritiske likevel blir rapportert direkte. Igjen forutsetter dette at styret og toppledelsen er involvert i utviklingen av disse prinsippene.

Figur 2 viser et enkelt eksempel på rapportering på ulike nivåer. I dette eksempelet er det den høyeste risikoen innenfor hver kategori som dikterer verdien som blir rapportert videre.



Figur 2

Risikoappetitt og -aksept

En god risikovurdering skal ta utgangspunkt i virksomhetens krav og målsetninger, og evaluere hvorvidt dagens strategi og internkontroll i tilfredsstillende grad ivaretar disse. For at virksomheten skal kunne gjennomføre slike vurderinger, må styret og ledelsens risikoappetitt være definert. Risikoappetitten sier noe om hvor mye risiko virksomheten er villig til å ta for å nå sine målsetninger.

Virksomheter som driver med kapitalforvaltning kan definere og operasjonalisere sin risikoappetitt i form av investeringsmandater. I de fleste virksomheter er det imidlertid svært vanskelig å kvantitativt definere føringer som sier hvor mye risiko ulike ledere kan forplikte virksomheten til. I disse tilfellene kan en systematisk tilnærming til risikoaksept, i form av tydelige akseptkriterier, være et godt hjelpemiddel for å overvåke at virksomhetens aktiviteter er innenfor styret og ledelsens risikoappetitt.

Når man definerer slike kriterier må man huske at målet er at risikoeksponeringen skal stå i stil med de målsetningene som er satt for virksomheten. Dersom man sier at det skal være automatikk i at risiko over et visst nivå ikke er akseptabel og derfor må reduseres kan man skape uheldige ringvirkninger. Det kan skape motstand mot selve metodikken og bidra til å skape distanse mellom risikostyrings- og strategiarbeidet. Videre kan det bidra til insentiver for å underrapportere reelle forhold. Jeg mener derfor at kriteriene som settes ikke bør være absolutte, men heller tydelig si

noe om hvem som kan akseptere ulike nivåer av risiko. For eksempel bør det være definerte nivåer som linjeleder kan akseptere før vurderingen heves til daglig leder og eventuelt direkte til styret. På denne måten blir rapporteringen også en mulighet for de med et operasjonelt ansvar til å «få aksept» fra ledelsen og styret for den risikoen som er assosiert med deres ansvarsområde. Slik kan man skape mer effektiv transparens mellom strategiske valg og de ulike risikoene valgene innebærer. Dersom en strategisk beslutning medfører vesentlig risikoeksponering i en begrenset del av virksomheten kan et slikt regime øke sannsynligheten for at informasjon raskt tilflyter styret og ledelsen. Ved å synliggjøre risikoeksponeringen som følger av virksomhetens ulike aktiviteter, mener jeg også at man kan oppnå et sterkere resultat- og oppgaveeierskap i organisasjonen.

Figur 3

Systematisk oppfølging og evaluering av utviklingstiltak

Det er en grunn til at det heter risikostyring og ikke bare risikoanalyse. Arbeidet som gjøres for å identifisere og analysere risiko er til for å gi et bedre grunnlag for å prioritere ressurser til de viktigste tiltakene og mest verdiskapende utviklingsaktivitetene – se eksempel på styringssystem i figur 3. Dersom virksomheten ikke evner å implementere og følge opp de initiativene som besluttes på bakgrunn av identifisert risiko, vil arbeidet heller ikke gi den ønskede effekten.

En god metodisk tilnærming til risikostyring inkluderer derfor tydelige prinsipper for hvordan man følger opp utviklingsarbeid i virksomheten. Metodikken bør også legge opp til en vurdering av ressursene et tiltak krever opp mot den forventede effekten. I tillegg til tydelig delegering av ansvar bør alle tiltak forankres på det nivået som er nødvendig for å sikre at tilstrekkelige ressurser faktisk blir allokert. Dette for å at tiltak skal få nødvendig fokus, hindre at ressurser brukes på tiltak som ikke realiseres og sikre at tiltak som ikke anses hensiktsmessige heller ikke igangsettes.

Når et tiltak er vedtatt implementert bør det være en fast systematikk i hvordan fremdrift følges opp, og ikke minst hvordan effekten av tiltaket evalueres når det er ferdigstilt. En slik systematikk skal gi styret trygghet for at nødvendige utviklingstiltak faktisk blir gjennomført og at effekten blir evaluert. Denne tryggheten mener jeg er et premiss for effektiv ivaretagelse av styrets tilsynsansvar.

Foto: ESB Professional/Shutterstock

Samordning med andre styringsaktiviteter

De fleste virksomheter har i ulik grad allerede etablert ulike mekanismer for ledelses- og styrerapportering. Noen har kanskje implementert balansert målstyring eller andre arbeidsmetoder som overvåker virksomhetens forretnings- og støtteaktiviteter. Risikostyringsarbeidet bør koordineres og samkjøres med slike aktiviteter. Å se på

dette som helt separate funksjoner vil være sløsing med ressurser ettersom fokuset ofte i stor grad vil overlappe. Både risiko- og målstyring handler tross alt om hvordan man fanger informasjon om forhold som påvirker usikkerhet knyttet til topp- og bunnlinjen i virksomheten. Dette skal igjen være grunnlaget for å se hvordan denne usikkerheten best håndteres.

Riktig bruk av støtteverktøy

Alle kan være enige om at enkel tilgang til fullstendig informasjon ved beslutninger samt strukturert oppfølging av utviklingstiltak i en virksomhet er bra. Begge deler er imidlertid lettere sagt enn gjort og krever administrative ressurser. Det krever innsats, eierskap og involvering fra flere parter. For at bedre risikostyring ikke skal være synonymt med økt administrasjon, er det viktig å bruke tilgjengelige verktøy på best mulig vis. For mange vil dette innebære å bruke eksisterende rapporteringsverktøy og -systemer mer effektivt. Noen vil også kunne dra nytte av å anskaffe et eget system som støtter opp om risikostyringsaktivitetene.

Det utvikles flere slike systemløsninger i dag. Noen av disse er dedikerte risikostyringsverktøy, mens andre er bygget med tanke på blant annet kvalitetsledelse. Det finnes også løsninger som i stor grad er skalerbare og skal kunne dekke alle fagområder under paraplyen GRC (Governance, Risk & Compliance). Dersom et system skal videreformidle informasjon til styret og ledelsen som gir noen reell verdi, må det legge til rette for at informasjon blir registrert og behandlet korrekt. Videre bør man sørge for at systemet er egnet til å automatisere oppfølging av enkle administrative oppgaver, slik som å holde oversikt over roller og ansvar for risikovurderinger samt sende påminnelser om statusoppdateringer for pågående tiltak.

Dette stiller krav til brukervennlighet og ofte mulighet for integrasjon med andre systemer. Ved en anskaffelse bør man derfor være svært bevisst på hvordan ulike interessenter i virksomheten skal benytte systemet. Systemet bør være praktisk innrettet og ikke innebære at informasjon som allerede registreres i ett system mål registreres dobbelt. Som bruker bør det være enkelt å få oversikt over status på oppgaver som man selv har ansvar for eller som omhandler eget ansvarsområde i virksomheten.

Foto: ImageFlow/Shutterstock

Risikostyring – styret og ledelsens verktøy for en mer robust virksomhet

God risikostyring handler altså om mye mer enn det å gjøre gode risikoanalyser. Det handler om å legge til rette for effektiv informasjonsflyt, tydeliggjøring av roller og ansvar, gode beslutningsmekanismer, riktig prioritering av ressurser og felles forståelse for virksomhetens målsetninger, krav og verdier. Et godt system for risikostyring representeres av summen av de aktivitetene som legger til rette for dette. Styret bør derfor aktivt søke informasjon fra ledelsen om hvordan arbeidet er organisert og følges opp, fremfor kun å etterspørre periodisk orientering om risikobildet. Gjennom dette kan styret oppnå trygghet for at relevant informasjon raskt tilflyter rett nivå og vurdere om etablerte prosesser for å identifisere, evaluere og håndtere risiko er gode nok.

For styret og toppledelsen bør risikostyring være et verktøy som skaper trygghet for at virksomheten organiseres og drives på en måte som støtter opp om definerte mål og krav. De må være komfortable med at måten det jobbes på er egnet til å fange opp, håndtere og kommunisere forhold på rett nivå i organisasjonen.

Det er dette, og ikke risikoanalysen eller rapporteringen i seg selv som skaper en mer robust organisasjon. Nettopp derfor bør styret stille tydeligere krav til krav til risikostyringen.

> Både risiko- og målstyring handler om hvordan man fanger informasjon om forhold som påvirker usikkerhet knyttet til topp- og bunnlinjen i virksomheten.

Revisjon i en digital verden

«Den digitale revolusjon» er under oppseiling, og dette påvirker de fleste virksomheter vi reviderer og hele revisjonsbransjen. Mange mener vi står overfor et paradigmeskifte i samfunnet, men det er få som kan konkretisere hva dette innebærer, eller hvordan dette påvirker vår bransje. En ting er sikkert, og det er at vi må endre oss for å være relevante for de virksomhetene vi skal revidere, og for å yte verdifulle tjenester overfor de reviderte enhetene og deres styrer og ledelse. En annen ting som også er sikkert, er at kravene til revisor øker, og det samme gjør forventningene til hvordan vi jobber, hva vi leverer og hva våre tjenester omfatter.

Av
SIV IRENE AASEN
Partner IT-risikotjenester,
BDO AS og medlem i arbeidsutvalget for IT-nettverket i IIA Norge

Den digitale revolusjon

Veldig mange virksomheter er i gang med å utvikle digitale strategier og å implementere tiltak for å møte kravene til effektiv interaksjon med kunder og samarbeidspartnere, og for å automatisere prosesser og arbeidsoppgaver. Omfanget av elektroniske transaksjoner som genereres er større enn noen gang. Den elektroniske utvekslingen av transaksjoner mellom virksomheter øker, og ofte genereres transaksjonene andre steder enn hos den virksomheten vi reviderer. Omfanget av informasjon er formidabelt, og derfor er det veldig viktig å sikre at vi behandler riktig, fullstendig og relevant informasjon

Heldigvis har de analytiske verktøyene utviklet seg i parallell, og har en helt annen kapasitet enn for noen få år siden. Dette øker mulighetsrommet for å utføre avviks- og trendanalyser på store datamengder (big data).

Den teknologiske utviklingen har pågått i mange år, men det har i nevneverdig grad ikke påvirket hvordan vi revisorer har organisert oss i forhold til dette, eller måten vi har arbeidet på. Etter hvert som graden av elektronisk samhandling har økt, og teknologien har modnet, har det vokst frem behov for å tilpasse oss til disse endringene og dra nytte av de mulighetene de gir. Spørsmålet vi står overfor er imidlertid hvordan dette bør gjøres.

Hvordan revidere i en digital verden?

Slik jeg vurderer det, er det normalt tre måter å tilnærme seg den digitale revolusjonen i revisjonssammenheng. Den første måten er gjennom å nyttiggjøre seg av den elektroniske informasjonen som virksomheten forvalter selv. Den andre måten er gjennom å automatisere selve revisjonsprosessen. Og den tredje måten er ved å sikre at fundamentet hvor den elektroniske informasjonen initieres, behandles og lagres er underlagt tilstrekkelig sikkerhet og kontroll.

Effektiv utnyttelse av elektronisk informasjon

Det å nyttiggjøre seg av elektronisk informasjon som virksomhetene forvalter selv stiller krav til at virksomheten har en dataarkitektur som kan etterprøves. Mange virksomheter benytter IT-systemer hvor det er innebygde kontroller for å sikre fullstendig og nøyaktig transaksjonsbehandling og løpende avviksrapportering over alle de transaksjonene som ikke oppfyller bestemte kriterier. Hvorvidt avviksrapporteringen følges opp og korrigeres gjennom manuelle eller automatiske rutiner varierer i forhold til størrelse og modenhet i organisasjonen. Det har i mange år vært snakk om GRC-løsninger (Governance – Risk – Compliance) og «continuous auditing», men det er et fåtall norske virksomheter som har klart å implementere dette på en god måte. -Noe av grunnen til dette er at arbeidet med å definere og implementere kontrollene i IT-systemene krever betydelige ressurser fra virksomhetene, spesielt fordi de større virksomhetene ofte har ERP-løsninger med stor grad av tilpasning. Implementeringskostnaden har derfor blitt større enn hva en normal norsk virksomhet har tatt seg råd til.

Trenden i dag er at de store ERP-leverandørene satser på standardiserte løsninger, hvor spesialbehovene leveres i

egne tilleggsmoduler. Dette innebærer at ERP-systemene kan defineres med standard GRC-funksjonalitet med innebygde kontroller og løpende avviksrapportering for unormale transaksjoner. I dag kan ERP- leverandørene forvalte virksomhetenes data i en skybasert løsning, hvilket gir tilgang til nye funksjoner. Når virksomhetens data ivaretas hos en sentral systemleverandør vil alle virksomheter kunne «benchmarkes» mot hverandre med hensyn til bruk av systemet, omfang av avvikende transaksjoner og kvalitet på internkontroll. . Fordelen med dette er at også revisoren kan bygge opp sin kompetanse på tvers av selskaper og systemleverandører.

Som revisor har det ofte vært aktuelt å implementere analyseverktøy eller trekke ut store mengder data hos den reviderte enheten for å utføre analyser av transaksjonsbehandlingen, og for å avdekke unormale transaksjoner. Denne rollen vil nok revisor også inneha en god stund fremover, da det vil ta lang tid før virksomhetene er over på IT-løsninger som gjør dette automatisk. Revisor vil også ha en viktig rolle for å påvirke etableringen av automatiske kontroller og avviksrapportering hos de reviderte enhetene, både overfor interne IT-organisasjoner og eksterne systemleverandører. Frem til disse fremtidige løsningene er på plass, er det normalt et krav fra virksomhetene om at revisor skal kunne bidra med denne typen analyser og oppfølging av transaksjonsbehandlingen som en siste skanse i forsvarsmekanismene. Derfor vil både internrevisorer og eksternrevisorer oppleve en forventning om at dette kan gjøres effektivt overfor den reviderte enheten. Kravet til at analysene og avviksrapporteringen skal være i sanntid øker også. Dette innebærer at revisors grensesnitt mot den reviderte enhetens IT-systemer må være kontinuerlig, og ikke bare skje en til to ganger i året.

En slik siste forsvarsskanse vil fremdeles kunne oppleves som nyttig for en virksomhet i en tid fremover, og vil være med på å skape merverdi gjennom trygghet for at transaksjonsbehandlingen ikke inneholder vesentlige feil. Spørsmålet man imidlertid må stille seg, er hvorvidt revisors rolle i en slik sammenheng blir å

Fremtidens revisor? Foto: agsandrew/Shutterstock

anse som en uavhengig part, eller om revisor blir en del av internkontrollfunksjonen i virksomheten? Dette opplever jeg at bransjen ikke har tatt noe klart standpunkt til, men for at vi skal oppleves som relevante for kunden er det viktig at vi deler den kompetansen vi har. Etter hvert som kravene om rapportering til Skattemyndighetene på transaksjonsnivå innføres gjennom SAF-T, vil revisor også kunne være gi en trygghet før overlevering av data til myndighetene.

En annen måte revisor kan nyttiggjøre seg av den elektroniske informasjonen på er gjennom sammenstilling av virksomhetens informasjon mot eksterne kilder. Økt grad av utveksling av elektroniske data mot eksterne samarbeidspartnere, kunder, banker og offentlige myndigheter danner et stort grunnlag for å samle og behandle data som kan utnyttes på et bredere grunnlag. Dette vil gi muligheter for å generere bransjeinformasjon, foreta trendanalyser og markedsanalyser, avdekke systematiske svindelforsøk og avdekke signaler i forhold til misligheter eller hvitvasking. Etter hvert som de elektroniske sporene gjennomsyrer all aktivitet som skjer mellom virksomheter vil de på sikt kunne benyttes for å avdekke uregelmessigheter, eller unormale transaksjoner, i det de inntreffer. Dette vil gi en samfunnsøkonomisk gevinst, og samtidig gi merverdi til virksomhetene ved at de legitimerer sin interaksjon med andre samarbeidspartnere.

Automatisering av revisjonsprosessen

Den andre måten revisor bør utfordre seg selv på er hvordan selve revisjonen utføres. Det å etablere effektive verktøy for å planlegge, gjennomføre, konkludere og rapportere et revisjonsoppdrag vil være et fortrinn. Dette gir mulighet til å automatisere handlinger knyttet til innhenting og bearbeiding av informasjon. Evaluering av resultater, dokumentasjon og rapporteringspunkter vil også kunne genereres automatisk. Den manuelle behandlingen i revisjonen blir redusert, samtidig som revisor frigjør tid til å benytte sin profesjonelle kompetanse og vurderingsevne på en bedre måte.

Effektivisering av prosessen innebærer et potensiale for å optimalisere ressursbruken knyttet til revisjonsfunksjonen og samtidig bidra til økt verdiskapning i virksomheten. Dette er et krav som har vært stilt overfor alle virksomheter de siste årene, og som har medført at mange virksomheter har utkontraktert hele, eller deler av, funksjoner i sin virk-

somhet. Dette gjelder blant annet IT-, logistikk-, regnskap- og lønnsfunksjoner. Kravene til at også revisor kan vise til resultater på dette området øker, noe som innebærer at sammensetningen av en profesjonell og kvalitativ tjeneste utført på en effektiv måte er en selvfølge. For å være i stand til å utvikle verktøy og automatisering av revisjonsprosesser er man avhengig av at revisjonsfunksjonen gjør investeringer på området, og det kan være utfordrende for mindre revisjonsenheter. Det vil derfor overraske meg om ikke internrevisjonsfunksjonen i de fleste virksomhetene vil utføres i en kombinasjon av ressurser som har inngående kjennskap til virksomheten, og innleie av eksterne ressurser som bistår med gjennomføringen ved bruk av automatiske verktøy og spesialkompetanse knyttet til systemer og cyber-security.

Fundamentet for revisjonen og cyber-security

Det tredje området vi må berøre når vi snakker om revisjon i en digital verden gjelder selve fundamentet for den digitale informasjonen som vi ønsker å benytte i revisjonen. Etter hvert som det meste av informasjonen vi ønsker å bygge på er elektronisk, er vi avhengig av at vi kan stole på kvaliteten av denne. Dette innebærer at vi må utføre revisjonshandlinger rettet mot initieringen av elektroniske transaksjoner, behandlingen og rapporteringen. Hvorvidt disse handlingene er utført i et miljø hvor det er etablert god internkontroll i virksomheten vil være en del av dette bildet. Dette oppnås gjennom gode kontroller rundt tilgangsstyring, endringshåndtering og prosessering av data – de såkalte generelle IT-kontrollene i virksomheten. De generelle IT-kontrollene har vært en del av revisjonsmetodikken siden lenge før tusenårsskiftet, men det er nå behov for å utvide begrepene. Det som er minst like viktig i det digitale samfunnet vi er en del av, er sikkerheten knyttet til systemer, data og integrasjoner i et større perspektiv. Da beveger vi oss inn i det vi gjerne kaller cyber-security.

Cyber-security er en videreføring av kjente begreper som IT-sikkerhet og informasjonssikkerhet. I forhold til cyber-security må vi ta innover oss at

Interaksjon på tvers av grenser. Foto: sdecoret/Shutterstock

sikkerheten knyttet til systemer, data og integrasjoner ikke bare er avhengig av sikkerheten hos den virksomheten vi reviderer, men at virksomheten er en del av en et større bilde med samarbeidspartnere, leverandører, kunder og myndigheter. Dette gjør at bildet over hvor informasjonen befinner seg og hvilke faktorer som kan påvirke integriteten i denne, blir mer komplisert.

Som revisor må vi gjøre handlinger for å forsikre oss om at cyber-security er forvaltet på en trygg og forsvarlig måte hos virksomheten og deres samarbeidspartnere, og at de har gjort nødvendige tiltak for å sikre sine informasjonsverdier. Informasjonsverdiene vil være blant annet systemer, data og integrasjoner. I revisjonssammenheng er vi ikke bare interessert i at virksomheten har beskyttet sensitiv og kritisk informasjon, men også at de har sikret at integriteten i informasjonen opprettholdes, og at den til enhver tid er tilgjengelig.

Vi bør begynne med å vurdere hvordan virksomheten har identifisert og klassifisert sine informasjonsverdier. Deretter må vi vurdere kvaliteten på de risikovurderingene som er gjennomført, hvilke sikkerhetstiltak som er gjennomført og hvordan disse er implementert og opererer i den operasjonelle driften. Det bør også gjøres tester av sikkerheten i virksomheten for å kunne gi verdifulle innspill til status på området, og hva som bør utbedres av ytterligere sikkerhetstiltak. I en verden med økt interaksjon med samarbeidspartnere må vi også vurdere hvordan disse sikrer informasjonen som de forvalter på vegne av virksomheten.

Revisor må derfor sikre seg tilstrekkelig kompetanse for å foreta vurdering av cyber-security i den reviderte enheten og deres relaterte samarbeidspartnere. I den grad revisor ikke selv har den nødvendige kompetansen, må det nødvendigvis leies inn ressurser som kan supplere på de aktuelle områdene. Sikkerheten hos samarbeidspartnere må også omfattes av de revisjonene vi utfører.

Hvordan kan revisor overleve i den digitale verden?

Avslutningsvis ønsker jeg å oppsummere de områdene som jeg har berørt ovenfor. Den digitale revolusjonen utfordrer revisjonsbransjen og vår relevans i forhold til de tjenestene vi utfører. Revolusjonen kommer først og fremst ikke som noen overraskelse på oss. Vi har hatt mange år til å omstille oss og levere nye, relevante tjenester til virksomhetene, både i internrevisjonssammenheng og eksternrevisjon. Utviklingen har imidlertid eskalert den siste tiden, og for at vi skal kunne være en verdiøkende funksjon må revisjonen fornyes. Dette innebærer hva vi gjør, hvordan vi utfører det, og hvordan vi rapporterer til virksomheten. Jeg vil derfor oppsummere revisjon i en digital verden med tre nøkkelord som vi må kunne levere på for å overleve som profesjon i fremtiden; sanntidsrevisjon, automatisering og cyber-security.

Ny fellesavtale på internrevisjon for statlige virksomheter

Statens innkjøpssenter har som mål kunngjøre en konkurranse om en ny statlig fellesavtale for internrevisjon innen utgangen av året, og implementere avtalen våren 2017.

Av
RIITTA LAUSAMO
Prosjektleder, Direktoratet for forvaltning og IKT (Difi)

Statens innkjøpssenter ble etablert i Difi 1. januar i år med oppdrag *«å effektivisere offentlige anskaffelser ved å inngå og forvalte statlige fellesavtaler for statlig virksomheter»*. Fellesavtalene som inngås og forvaltes er obligatorisk for statlige forvaltningsorganer i sivil sektor.

Etter første innkjøpsrådsmøte den 01.09.2016, ble det bestemt at Statens innkjøpssenter skulle inngå og forvalte en fellesavtale på internrevisjon. (Les mer om hva innkjøpsråd er på web 4) Internrevisjon er en uavhengig, objektiv bekreftelses- og rådgivningsfunksjon som har til hensikt å tilføre merverdi og forbedre organisasjonens drift.

Behovet for internrevisjon blant statlige virksomheter (statlige forvaltningsorganer) har sin opprinnelse i at Norge ble anbefalt av internasjonale organisasjoner som OECD og IMF (International Monetary Fund) å vurdere mer utstrakt bruk av internrevisjon i staten.

I 2013 utpekte Finansdepartementet en arbeidsgruppe som skulle utrede «bruk av internrevisjon i staten» (web 1), og som et resultat av dette ble alle statlige virksomheter med inntekter eller utgifter over 300 mill kroner pålagt å vurdere behovet for internrevisjon i egen virksomhet (Finansdepartementet, R-117, ref.14/3305, dato 20.05.2015)..

Før 2015 hadde 22 virksomheter etablert internrevisjon, og etter R-117 har 45 av 72 statlige virksomheter etablert, eller planlagt å etablere internrevisjon i løpet av de neste to årene (web 2). For staten, sett som et hele, betyr dette en økning på over 100% i antall virksomheter med *behov for internrevisjon.*

Statens innkjøpsgruppe for internrevisjon ble etablert den 1. oktober i år. Innkjøpsgruppen er ledet av Riitta Lausamo og består av et tverrfaglig team av åtte personer med solid kompetanse fra offentlige anskaffelser, juridisk fagkompetanse og/eller kompetanse fra internrevisjon i statlig forvaltning.

Innkjøpsgruppens medlemmer kommer fra virksomheter som Universitetet i Oslo, Politiet, Høgskolen i Oslo og Akershus, Difi og DFØ. I tillegg, har flere virksomheter som NAV, Skatteetaten, Tolldirektoratet, Garantiinstituttet for eksportkreditt (GIEK), Helse Midt-Norge RHF, Metrologisk institutt, metrologisk institutt og Norges miljø- og biovitenskapelige universitet (NMBU) meldt seg inn som en del av referansegruppen, som skal kommentere konkurransegrunnlaget før kunngjøring. Gjennom hele innkjøpsprosessen har de hatt tett dialog med DFØ og IIA Norge, i tillegg til at de har åpnet dialog med Riksrevisjonen.

Bak fra venstre: Karen-Inger Verket (Difi), Pål Cato Andersen (Politiets fellestjenester), Knut Riise (Difi), Riitta Lausamo (Difi/Statens innkjøpssenter).
Foran fra venstre: Barbro Bottheim (Difi/Statens innkjøpssenter), Jacob M. Landsvik (Universitetet i Oslo).
Ikke til stede: Kristin Kahrik (Difi/Statens innkjøpssenter), Tore Dæhlin (Høgskolen i Oslo og Akershus), Ola Otterdal (Direktoratet for økonomistyring - DFØ).

Innkjøpsgruppen har nettopp fullført første runde med leverandørkonferanse (27.10.2016), og en-til-en møter med potensielle leverandører. Likevel oppmuntrer vi flere små og mellomstore virksomheter til å melde sin interesse, og ta kontakt for et møte. I tillegg til å kartlegge markedets muligheter, har innkjøpsgruppen også vært i dialog med statlige brukere og bestillere av denne type tjenester for å kartlegge deres brukerbehov. Utfordringene er flere og kompleksiteten er stor ettersom det er flere behov som skal dekkes gjennom en felles avtale. Likevel er det dette som gjør nettopp denne fellesavtalen interessant å arbeide med, og vi oppfordrer alle potensielle leverandører om å følge nøye med på den videre utviklingen.

Målet er kunngjøring innen 2016, med implementering av avtalen våren 2017. Likevel understrekes det at avtalens kvalitet vil være avgjørende for kunngjøring før eller etter nyttår.

Web 1: https://www.regjeringen.no/contentassets/586b1b12486c4d-45adc698514c840f80/utredning.pdf
Web 2: https://dfo.no/fagomrader/intern-revisjon/aktuelt/oppsumme-ring-av-statlige-virksomheters-vurde-ring-av-behovet-for-internrevisjon/
web 3: https://www.anskaffelser.no/nyhet/2016-09-01/innkjopssente-rets-avtaleliste-er-klar
web 4: https://www.anskaffelser.no/statens-innkjopssenter/statlige-innkjopere

Hva kan vi forvente av blokkjede-teknologien på kort sikt?

Av
ESA LEPORANTA
Systems Audit Manager
Nets Branch Norway

SIRK 01/2016 hadde en innførende artikkel til blokkjede-teknologien: «Hvordan bruke blokkjedet i finansnæringen?» I mellomtiden har flere aktører annonsert nye løsninger som det kan være interessant å kjenne til.

Forventninger

Don Tapscott, som ble rangert som den fjerde mest innflytelsesrike tenkeren i verden i 2015, mener at blokkjede-teknologien fundamentalt vil endre muligheten for hva mennesker kan oppnå i fremtiden. Han påstår at uansett hvilken industri vi velger, så vil blokkjede-teknologien ha et stort potensial til å kunne forstyrre den, såfremt vi klarer å etablere liknende systemer til det vi i dag har for styring av Internett[1].

Den eksperimentelle fasen

I mars i år testet 40 av R3CEVs medlemsbanker fem ulike blokkjedeteknologier[2]. Et av målene med testingen var å sammenligne de ulike teknologiske løsningene med hverandre, siden det på det tidspunktet ikke fantes noen egne verktøy for det. To måneder senere søkte R3 finansiering på opptil 200 MUSD fra sine medlemsbanker[3]. Ifølge media[4] var ikke alle europeiske banker tilfreds med dette, men kort tid senere holdt de fem nordiske R3 bankene sitt første møte[5] i Stockholm for å diskutere hvordan de kunne samarbeide videre. I begynnelsen av juli annonserte seks russiske banker at de skulle etablere en liknende konsortium i Russland for å konkurrere med det New York baserte R3 kollektivet[6]. Ifølge en analyse av konsulentselskapet Bain & Company[7] er det ikke godt nok med slike innledende «eksperimenter». De påstår at bankene på kort sikt risikerer å miste mer enn 150 milliarder dollar av sin omsetning blant annet på grunn av svakheter i deres håndtering av internasjonale betalingsoverføringer.

Førstemann til mølla...

Som svar på tiltale annonserte Santander UK kort tid senere at de skal lansere en blokkjede-basert applikasjon som kan gjennomføre internasjonale betalingsoverføringer 24 timer i døgnet[8]. I en annen undersøkelse foretatt av IBM hevdes det at omtrent 30 banker har planer om å implementere komplette blockchain-baserte løsninger i full skala i 2017 og at hele 130 banker regner med å kunne tilby det samme innen de neste 3 år[9]. Det er flere grunner til det. De som kommer først i gang kan være med å etablere og utvikle nye standarder og forretningsmodeller som senere legges til grunn av fremtidige konkurrenter. De som er først ute, vil normalt også ha bedre forutsetninger til å forutse potensielle forstyrrelser, som vil hjelpe de i å bekjempe nye aktører[10].

Globale aktører satser tungt

Det viser seg at mange kjente aktører er i full gang med å teste nye blockchain-baserte løsninger. I midten av mars annonserte et London basert meglerfirma, ICAP, at de har distribuert forretningsdata til ni av deres kunder med hjelp av teknologien som støtter bruk av Bitcoin[12]. Et par måneder senere opplyste Deloitte at de skal etablere et blokkjedesenter i Dublin for 50 utviklere og designere. Som et resultat av denne satsningen, presenterte Deloitte Luxemburg i juli en ny løsning for rapportering av derivattransaksjoner, som anvender blockchain-baserte smartkontrakter[13]. Like før

[1] *http://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world*
[2] *http://www.coindesk.com/r3-consortium-banks-blockchain-solutions/*
[3] *http://www.thepaypers.com/default/r3-seeks-usd-200-mln-from-big-bank-backers/764326-0?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+thepaypers%2FcfKW+(The+Paypers+Headlines)*
[4] *http://finanswatch.dk/Finansnyt/article8672426.ece?utm_source=Feed&utm_medium=top*
[5] *http://www.nordea.com/fi/palvelut/cashmanagement/cash-management-news/cash-management-news-archive/2016/01-06-2016-r3-cev-nordic-blockchain-meetup.html*
[6] *https://www.finextra.com/newsarticle/29135/russian-banks-create-blockchain-consortium*
[7] *http://www.bain.com/about/press/press-releases/150-billion-dollars-at-risk-for-banks-that-cannot-overcome-hurdles-of-digital-currency.aspx*
[8] *http://www.reuters.com/article/us-santander-blockchain-idUSKCN0YH1UZ*
[9] *https://www.finextra.com/newsarticle/29514/banks-ready-for-real-world-blockchain*
[10] *Ibid*
[11] *http://www.dn.no/grunder/2016/04/23/1326/Finansteknologi/-haugevis-av-nye-aktrer-nsker--gjre-det-vi-gjr*
[12] *http://www.reuters.com/article/us-icap-markets-blockchain-idUSKCN0WH2J7*
[13] *http://deloittekilden.no/gjor-kontrakten-sikker-med-blockchain/*

informerte IBM at de skal åpne deres første innovasjonssenter for blokkjedet i Singapore. Som en del av denne satsningen, skulle IBM samarbeide med verdens største havn for containeromlastning, Port of Singapore Authority, for å etablere et nytt handelssystem[14]. I begynnelsen av september kunngjorde CGI at de som den første kommersielle aktøren tar i bruk teknologien til Ripple Labs, som skal kunne behandle internasjonale og nasjonale transaksjoner i realtid[15]. I oktober presenterte VISA sin nyeste løsning for betalingsformidling, B2B Connect. I denne løsningen skal blokkjede-teknologien tilby bedriftskunder en raskere måte å utveksle sine betalinger over hele verden[16]. I midten av november lanserte PwC et nytt nettsted[17], Vulcan Digital Asset Services, for å tilby sine kunder digitale valutatjenester. På samme tidspunkt annonserte Deloitte og SETL, et London-basert finansteknologiselskap, at de har utviklet et kontaktløst smartkort som kan anvendes for å betale innkjøp i butikker. Hele prosesseringen og avregningen mellom kunder og butikker skal kunne gjennomføres ved hjelp av blokkjede-teknologien[18].

> «Kanskje kan man si at man kan klare seg i to-tre år til slik man har holdt på fordi det fremdeles er reguleringer som sperrer for nye aktører. Men det vil kun være der en liten stund til»
>
> *Chris Skinner, forfatteren til bok Digital Bank*[11]

Barrierer

I lys av disse eksemplene kan det virke som overraskende at ikke flere virksomheter har kastet seg over denne bølgen. Morgan Stanley har undersøkt hvilke barrierer det finnes for implementering av blokkjede-teknologien. For å overvinne en stor del av disse vil det kreve at aktørene samarbeider med lokale myndigheter. Mange av reglene som skal regulere bruk av denne nye teknologien er ikke engang skrevet[19]. Samtidig har eksisterende reguleringer i noen tilfeller tvunget nylig oppstartede virksomheter til å samarbeide med de mer etablerte aktørene, som igjen har bremset utviklingen[20]. Frem til nå har det ikke eksistert blockchain-baserte løsninger som klarer å håndtere tilstrekkelig store transaksjonsmengder, men dette er nå på vei til å endres med løsningen til SETL, som skal kunne behandle flere titusener transaksjoner per sekund[21]. Mange av dagens banker har i tillegg eldre IT systemer og forretningsprosesser som må moderniseres for at de skal bli kompatible med nye krav. Ved fusjoner mellom bankene blir IT systemene sjelden harmonisert, hvilket skaper ytterligere utfordringer[22].

Manglende fokus på back-office tjenester?

I en artikkel publisert av CIO hevdes det at bankene så langt har investert mesteparten av ressursene sine i kunderettede systemer, og at en stor del av deres back-office funksjoner fremdeles er papirbaserte. I den grad dette stemmer, så vil slike banker møte en tøff konkurranse fra aktører som kun opererer med digitale løsninger. Videre påstås det at en gjennomsnittlig bank opererer med mer enn 1 000 ulike applikasjoner i ulike siloer, hvilket begrenser deres evne til å få en oversikt over systemene på samme måte som en digital konkurrent kan bli i stand til. Derfor bør bankene ha det som et mål å kunne operere med vertikalt integrerte digitale løsninger som dekker alt fra kundebehandling til back-office funksjoner[23].

Aktiviteter i Norden

I Norden har bankene forberedt seg til disse endringene på ulike måter. I desember 2015 møtte de første robotene på jobb hos SR banken i Rogaland for å behandle søknader fra kunder som vil gjøre endringer på sine lån[24]. I april i år ble vi kjent med at Danske Bank kan bli den første av store danske bankene som tilbyr sine investeringskunder robotrådgivning[25]. Få dager senere ble det opplyst at Handelsbanken skal investere 700 MSEK til digitalisering av sine tjenester[26]. To måneder etterpå ble det annonsert at Nordea skal fornye alle sine IT systemer for grunnleggende banktjenester for 1,1 mrd euro og OP Financial Group, Finlands største finansgruppe, skal iverksette en liknende prosess med en estimert prislapp på opptil 2,0 mrd euro[27].

Oppsummering

Gjennomgangen av rapporter og artikler viser at det er store forventninger til blokkjede-teknologien. De fleste store aktørene eksperimenter med ulike løsninger og ifølge Morgan Stanley underestimerer markedet de fordeler dette gir. Finansielle institusjoner i verden forventes å investere over 1 mrd USD for blockchain-relaterte prosjekter i 2017. Det er identifisert flere barrierer som må løses, men de forventes ikke å stoppe utviklingen[28]. Aktivitetene i Norden viser at de største bankene kommer til å bruke svimlende beløp for å digitalisere sine tjenester.

[14] *http://www-03.ibm.com/press/us/en/pressrelease/50163.wss*
[15] *http://www.cgi.com/en/cgi-advances-blockchain-adoption-implementation-ripple-validator-node*
[16] *http://www.businesswire.com/news/home/20161021005212/en/*
[17] *http://www.ibtimes.co.uk/pwc-launches-vulcan-digital-asset-services-bloq-libra-netki-1591476*
[18] *https://setl.io/*
[19] *https://www.ft.com/content/a1fc3522-314b-11e6-bda0-04585c31b153*
[20] *http://www.bain.com/Images/BAIN_BRIEF_Distributed_Ledgers_in_Payments.pdf*
[21] *https://setl.io/*
[22] *http://www.cgi.com/en/practical-innovation-using-cutting-edge-technology*
[23] *http://www.cio.com/article/3096125/outsourcing/big-banks-big-applications-big-outsourcing.html*
[24] *http://www.hegnar.no/Nyheter/Boers-finans/2015/11/SR-Bank-har-ansatt-roboter*
[25] *http://finans.borsen.dk/artikel/1/323115/medie_danske_bank_vil_maaske_tilbyde_robotraadgivning.html*
[26] *http://www.mkse.com/2016/04/21/handelsbanken-satsar-700-mkr-pa-digital-transformation*
[27] *http://www.hs.fi/talous/a1466306691851 (på finsk)*
[28] *http://www.the-blockchain.com/docs/Morgan-Stanley-blockchain-report.pdf*

Intervju med Frede Aas Rognlien om korrupsjon

INTERVJU MED
FREDE AAS ROGNLIEN,
LEDER AV GROUP COMPLIANCE, SEB NORGE

Av
MARTIN STEVENS
Gjensidige Forsikring

Compliance-funksjonen er relativt ny i Norge og det er ikke noen klar og entydig karrierestige for de som skal jobbe i en slik funksjon. Kan du fortelle kort om din vei til å bli leder av Group Compliance i Norge for SEB. Hva synes du er det som har betydd mest fra din utdannelse, bakgrunn og erfaring til den stillingen du i dag besitter?

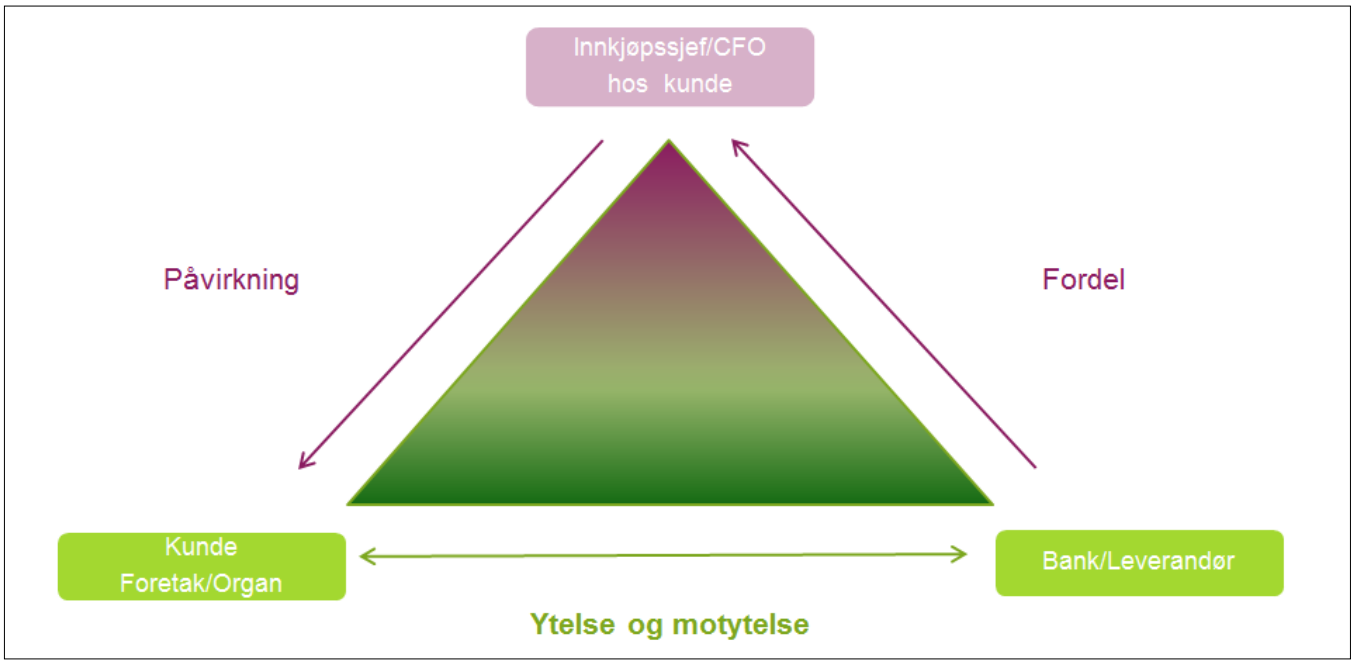
Jeg fikk min utdannelse som jurist. Etter et kort opphold i Finansdepartementet praktiserte jeg noen år som advokat før jeg i 1990 ble ansatt i det som nå heter Verdipapirforetakenes Forbund. Dette var temmelig tidlig i regelverksutviklingen for verdipapirmarkedene og jeg fikk anledning til å være med på hele denne reisen, inklusive utviklingen av bransjenormer og selvdømmefunksjoner, samt internasjonalt arbeid. Jeg fikk vel da en så bred og interessant kompetanse at SEB Enskilda, som et av de første meglerhusene som skulle styrke den juridiske og compliance kompetansen, så meg som en potensiell kandidat – og jeg var interessert. Så fulgte endringene i SEB i Norge med tettere integrasjon og fellesfunksjoner og senere fusjoner av selskaper. Da fikk jeg det overordnede compliance-ansvaret i SEB Norge. Kompetansen fra hele regelverksutviklingen kombinert med praktisk erfaring som advokat har nok vært det viktigste for å gjøre meg i stand til å fylle rollen. Om jeg har lykkes får andre vurdere.

Alle har hørt om korrupsjon og man kjenner instinktivt at det er noe negativt og ødeleggende for bedriften og samfunnet, men kan du hjelpe oss med en enkelt definisjon av hva korrupsjon egentlig er?

Korrupsjon oppstår når f eks en leverandør søker å oppnå en fordel (eksempelvis en kontrakt) gjennom å påvirke en innkjøpsansvarlig hos en leverandør til å få dette til. Man tilbyr noen en eller annen fordel for at denne i kraft av sin stilling hos en annen skal få denne andre til å agere slik man ønsker, jfr illustrasjonen (figur 1). Et eksempel kan være å invitere en analytiker i en bank på en attraktiv reise for å søke å oppnå at analytikeren skriver fordelaktige analyser på vegne av banken. Men bedriftsbesøk og reiser kan meget vel også ligge innenfor det akseptable så her kan det være vanskelige grenseoppganger. Hovedproblemet er at slikt skjer i det skjulte uten at arbeidsgiver kjenner til forholdet. Om det er åpenhet mellom alle vil nok risikoen for straffbar korrupsjon reduseres.

Kan du gi noen eksempler på hva som kan være en utilbørlig fordel i lovens forstand? I din mening er rettspraksisen entydig?

En utilbørlig fordel er noe kvalifisert klanderverdig, dvs at ikke enhver ytelse er utilbørlig, og det er lov til å gjøre ukloke ting uten at man skal bli straffet for dette. Begrepet utilbørlig har intet eksakt innhold og vil variere over tid. Det vil også kunne være avhengig av graden av åpenhet. Typiske fordeler kan være verdioverføringer, gaver, reiser og middager (ekstravagante), men også rabatter, veldedighet, sponsing i andres navn, formidling av innsideinformasjon, deltakelse i andres økonomiske virksomhet. Kanskje vanskeligere å vurdere er trainee-ordninger og ansettelser, seminarer og studieturer. Jeg tror nok mange vil kjenne på seg selv hvor grensen går, men også at mange ikke helt har under huden at holdningene har endret seg kraftig de seneste årene slik at det som var akseptabelt for 15 år siden ikke nødvendigvis er OK i dag.



Figur 1

Hvilke rutiner bør en bedrift ha på plass for å beskytte seg mot rettsforfølgelse?
Man bør ganske enkelt ha en instruks som viser hva selskapet mener er akseptabelt, så vel verdimessig som forretningsmessig. Videre må man i denne ha klare retningslinjer for hvordan man behandler «gifts & entertainment», med tilstrekkelig eskalering slik at ledelsen vet hva som foregår og kan ta avgjørelser. Og endelig så bør man sikre åpenhet om hva man mottar eller vil tilby. Unngå f eks tredjepartsproblemet og inviter den reelle kunden og ikke dennes representant. Ta klart stilling til hva som ikke er akseptabelt, f eks rene pengegaver (inkl. substitutter for penger). Moderasjonskrav er nok en fordel og så må man ha en kontroll- og rapporteringsmessig oppfølging. Instruksen bør være tilgjengelig for alle og man må drive aktiv opplæring og oppfølging.

I en norsk virksomhet som opererer internasjonalt skal man etter din mening ha de samme strenge (norske) krav til tiltak mot korrupsjon eller skal man kunne akseptere at kutymen er annerledes i andre land for ikke å støte fra seg forretningsforbindelser?
Man må forholde seg til de norske kravene. Det er de som er styrende for norske virksomheter også i forhold til det som gjøres i andre land. Kutymer i andre land kan også endres og det er vanskelig å vurdere hva som er riktig og galt til enhver tid, ikke minst der regimer endres osv. men det er klart noen store dilemmaer her i forhold til f eks å delta i utviklingen i enkelte land gjennomsyret av korrupsjon.

Er korrupsjon noe som stort sett foregår i utlandet eller er vi i Norge for naive? Hvordan skal vi kunne få løftet ....
Korrupsjon er et problem i Norge. Det har vi sett i en rekke saker både i forhold til det offentlige, men også det private næringsliv. Jeg antar det er mange saker som aldri når offentlighetens lys. Personlig tror jeg vi har «lullet» oss inn i en tro på at korrupsjon bare er noe som skjer i andre kulturer, men den nærhet vi har til mange beslutningstakere i et lite land, i en liten kommune, i en liten eller stor bedrift kan gjøre det lett å gi og motta slike fordeler, som jeg nevnte, uten at man tenker på om dette faktisk kan være en utilbørlig fordel. For å gjøre noe med dette må man erkjenne at det er, eller kan være, et problem. Så må man snakke om det slik at man bygger en bevisst og robust kultur mot korrupsjon.

Til slutt har du noen tips til internrevisoren, compliance officer eller risk manager på hvordan de kan få ledelsens oppmerksomhet på korrupsjonsrisikoen og forebyggende tiltak?
Det kanskje enkleste er å ta tak i en del tilfeller man har sett i Norge og sette de inn i ens egen virksomhetskontekst for å vise hvor lett problemet kan oppstå i ens egen virksomhet. Er man interessant å bestikke eller kan man være interessert i å bestikke andre for å øke salg, rennomme eller være suksessfull i jobben? Gjennom risikovurderinger kan man vise at selv om risikoen for korrupsjonsaktivitet kanskje er liten i selskapet, er det likevel betydelige konsekvenser for rennommeet om ett tilfelle skulle inntreffe. Med så mange kjøpere av produkter og tjenester som etter hvert har meget lav toleranse for korrupsjon er det også en høy kommersiell risiko knyttet til selv mindre overtredelser eller «videreføring» av tradisjoner. Det er også en betydelig finansiell risiko knyttet til mulige foretaksstraffer, selv om denne risikoen kan reduseres gjennom gode rutiner og reell oppfølging.

Ny personvernforordning - Gjensidiges forberedelser

AV
HANNE CORNELIUSSEN
Compliance officer,
Compliance konsern Gjensidige

Hanne Corneliussen har vært ansatt som compliance officer i Gjensidige Forsikring ASA siden 2010, og er nå teamleder for konsernfunksjonen. Før dette jobbet hun 11 år i Finanstilsynet, både med forsikring og verdipapir, og har også erfaring fra departementet. Hanne er utdannet cand. jur. fra Universitetet i Oslo.

I denne artikkelen vil jeg peke på de viktigste endringene med ny personvernforordning, og redegjøre for hvordan Gjensidige forbereder seg på implementering av de nye personvernregler i organisasjonen.

Status

Ny personvernforordning trer i kraft i mai 2018. Det er varslet at et lovforslag for gjennomføring i norsk rett skal sendes på høring i mai 2017. Forordningen inneholder noen praktisk viktige overgangsregler. Datatilsynet har uttalt at behandlinger som er påbegynt skal bringes i samsvar innen to år etter ikrafttredelsesdatoen, avgitt samtykke som er i henhold til gjeldende direktiv skal fortsatt gjelde og konsesjoner vil gjelde inntil de endres, erstattes eller oppheves.

Forordningsteksten gir stort rom for fortolking og det foreligger foreløpig lite veiledning fra EU og Datatilsynet. Datatilsynet er likevel tydelig på at virksomhetene har et selvstendig ansvar for å tolke regelverket, og starte forberedelsen til nytt regelverk.

Hva er nytt i Personvernforordningen?

Når man leser fortalen til forordningen og forordningsteksten er det mye som i stor grad samsvarer med gjeldende regelverk, herunder regler om internkontroll og behandlingsgrunnlag. De nye reglene gir imidlertid flere og strengere plikter enn før for virksomheten og flere rettigheter for den registrerte.

Personvernforordningen inneholder en ny bestemmelse om dataportabilitet. Formålet med denne bestemmelsen er å styrke forbrukerens stilling og stimulere til økt konkurranse i marked hvor det håndteres store mengder personopplysninger. Dette vil typisk kunne være i forsikringsmarkedet. Dataportabilitet betyr at den registrerte kan kreve å få flyttet egne personopplysninger fra en behandlingsansvarlig til en annen i et vanlig brukt filformat. Det er et vilkår at dette er teknisk gjennomførbart.

Videre gis den registrerte en styrket rettighet til å motsette seg noen typer behandling. Et eksempel på dette er utarbeidelse av personprofiler, der formålet er direkte markedsføring.

Reglene om sletting og retting viderefører i stor grad gjeldende rett. Retten til å bli glemt lovfestes. Bestemmelsen lovfester en dom i EU-domstolen som ga borgere av EU og EØS muligheten til å be søkemotorselskaper som var etablert med kontorer i EU-området om å slette lenker til sider som inneholder informasjon som er «utilstrekkelig, irrelevant eller utdatert, eller overdreven». Med ny forordning vil dette også gjelde virksomheter som holder til utenfor Europa, men som tilbyr tjenester til borgere i EU/EØS.

Personvernforordningen innfører begrepene «privacy by design» and «privacy by default». Databeskyttelse gjennom design vil si at det skal iverksettes tekniske og organisatoriske tiltak for å sikre et godt beskyttelsesnivå i alle utviklingsfaser av et system eller en løsning. Dette er ikke et lovkrav i dag, men Datatilsynet har i flere år hatt sin anbefaling «Syv steg til innebygd personvern». Privacy by default betyr databeskyttelse gjennom standardinnstillinger,

og at standardinnstillinger skal ligge på det mest personvernvennlige nivået. Fortalen til forordningen gir som et eksempel at et tiltak for å etterleve dette vil være å minimere behandlingen av personopplysninger.

Reglene om avvikshåndtering vil bli strengere. Det er flere avvik som skal meldes til Datatilsynet, meldingen skal sendes innen 72 timer og det er krav om underretting til de berørte uten unødig forsinkelse. Det er ingen slik varslingsplikt til de berørte i dag, men det er grunn til å tro at dette likevel gjøres etter konkrete vurderinger.

Risikobaserte krav til etterlevelse innføres. Det skal identifiseres behandlinger som kan medføre en stor risiko for personvernet. Behandling av sensitive personopplysninger antas å være eksempel på dette. Der behandlingen vil resultere i stor risiko, plikter virksomheten å gjennomføre en vurdering av personvernkonsekvensene (PIA), og Datatilsynet skal involveres i forhåndsdrøftelser.

For de virksomhetene som i dag har en konsesjonsplikt, vil denne opphøre. Det innføres i stedet krav til bransjenormer, standarder og sektorvis utforming av retningslinjer. Datatilsynet skal godkjenne bransjenormer.

I dag er det mange virksomheter som har personvernombud, men dagens ordning er frivillig. Nå innføres det et krav til personvernombud for alle offentlige og private virksomheter, som regelmessig og systematisk overvåker personer i stort omfang eller behandler sensitive personopplysninger i stort omfang. Ombudets uavhengighet og posisjon i virksomheten styrkes i de nye reglene. I tillegg stilles det strengere krav til ombudets faglige kunnskap og evne til å utføre oppgavene sine.

Brudd på personvernlovgivningen vil kunne få store økonomiske konsekvenser. Datatilsynet vil få hjemmel til å utstede bøter i størrelsesordenen opp til EUR 20 mill. eller 4 % av global årlig omsetning mot maks ca 850 000 kroner i dag. For konsern som opererer i flere land kan bestemmelsen om global omsetning, reise et interessant spørsmål. Vil brudd på personvernregler i et land virksomhetene opererer i, utløse bøter regnet av global omsetning, eller vil man avgrense beregningsgrunnlaget for boten? Det er nærliggende å tro at dersom avviket kan isoleres til virksomheten i det enkelte land, vil beregningsgrunnlaget for boten isoleres. Dersom avviket derimot avslører gjennomgående dårlig internkontroll i konsernet, vil det være større risiko for at man legger global omsetning til grunn ved beregningen.

Gjensidiges forberedelser til nye personvernregler

Gjensidige er et forsikringskonsern som forvalter en mengde personopplysninger, også sensitive. Det betyr at arbeidet med personvern er svært viktig både overfor dem vi behandler personopplysninger på vegne av, kunder og ansatte, og i forhold til myndigheter. At kunder oppfatter at vi behandler personopplysninger på en ryddig måte, vil også gi et konkurransefortrinn. Risiko for manglende etterlevelse av personvernforordningen innebærer derfor en betydelig compliancerisiko for oss.

> Dataportabilitet betyr at den registrerte kan kreve å få flyttet egne personopplysninger fra en behandlingsansvarlig til en annen i et vanlig brukt filformat.

I Gjensidige er det nedsatt en intern arbeidsgruppe som har som formål å få oversikt over regelverket, gjennomføre en gap-analyse både i henhold til dagens lovkrav og i henhold til nytt regelverk. identifisere løsninger som krever IKT-utvikling av systemer kontra regler som bare krever endringer i styrende dokumenter, rutiner og organiseringer. Prosjektet skal også foreslå tiltak som skal gjennomføres på forretningssiden.

På dette tidspunktet er det en utfordring at forordningsteksten gir stort rom for fortolkning, og det finnes lite veiledning for hvordan man skal innrette seg for å etterleve reglene. Det mest krevende i dette arbeidet er å kartlegge hva som kreves av våre IT-systemer for å ivareta kravet til for eksempel dataportabilitet og innebygd personvern, og så utføre disse IKT-utviklingene. Dette er en øvelse som vil være ressurskrevende.

For konsern som har virksomhet i flere land, vil ulik modenhet på behandling av personopplysninger i de ulike geografiene gi noen utfordringer når nye personvernregler skal implementeres i organisasjonen. Virksomheter som har kunder og spesielt de som behandler sensitive personopplysninger, vil ha større utfordringer og vil måtte sette av mer ressurser enn virksomheter som ikke har det. En av Gjensidiges uttalte strategier er å være en innsiktsbasert og analytisk virksomhet. Med økende digitalisering følger det med vekst i datamengde. Gjensidige har for eksempel kommet langt i å utnytte offentlig tilgjengelig geografi- og bygningsdata på tvers av alle prosesser, som bidrar til bedre prising, kunde- og risikoseleksjon og mer effektivt skadeoppgjør. Når data identifiseres på personnivå vil dette være personopplysninger, og kravene i personforordningen inntrer.

Datatilsynet har gitt noen råd om hva man allerede nå bør gjøre for å etterleve kravene som kommer; skap bevissthet innad i organisasjonen, få oversikt over kilder, sjekk hvorvidt dere behandler personopplysninger om barn, kartlegg informasjonsflyt, oppdater rutiner, gjennomfør risikovurderinger, dokumenter, men det er viktig å ikke glemme implementeringen - opprett personvernombud og bruk nettverket for å finne beste praksis. Lykke til!

Hvitvaskingsloven og eiendomsmeglere

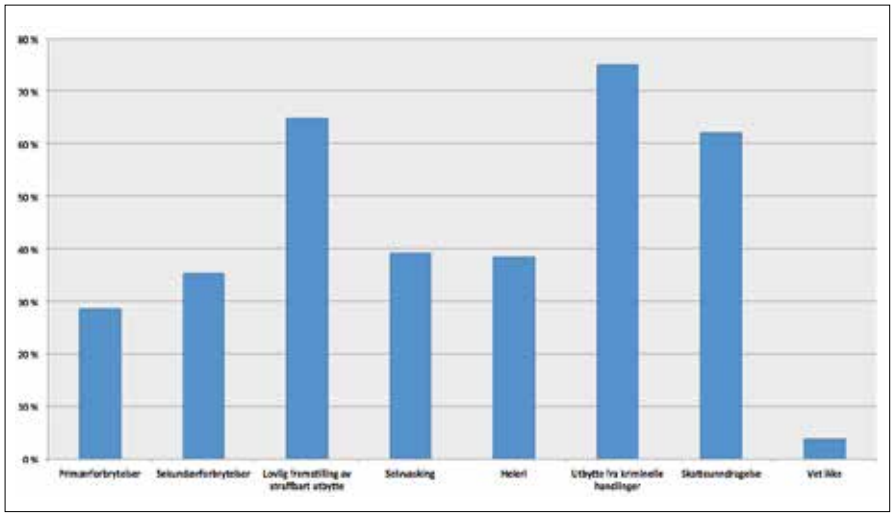
AV
JENNY MARIE DØLI
OG PEDER OLSBØ

Jenny Marie og Peder mottok NEF-Help stipendet fra Norges Eiendomsmeglerforbund og Help Forsikring høsten 2015 for å skrive sin Master Thesis på BI. Oppgaven ble levert 1. september 2016.

Økonomisk kriminalitet er fortsatt et dagsaktuelt tema, og vi ser stadig eksempler på økonomisk kriminalitet av betydelig omfang i Norge og internasjonalt, både i privat og offentlig virksomhet. Økonomisk kriminalitet utgjør en stor trussel mot samfunnet, finanssystemets integritet, økonomiens virkeområde og rettstaten. I 2014 la The Financial Action Task Force frem en rapport som første av sitt slag i Norge. Analysen og rapporten viste at det i Norge er et klart forbedringspotensial med tanke på å motvirke hvitvasking og terrorfinansiering, og at behovet og risikoen for dette er større enn den oppfatningen som er rådende innenfor forskjellige bransjer.

I vår Master Thesis så vi nærmere på hvitvaskingsloven og hvordan den dekker eiendomsmeglere, samt deres holdninger til undersøkelses- og rapporteringsplikten. Eiendomsmegleres forståelse av hvitvasking som fenomen og i hvilke former den kan forekomme er også kartlagt. Videre ble forskjeller mellom praksis hos meglere og foretak på tvers av banktilknytning, markedet de opererer i og regioner belyst.

NEF har bidratt med intervjuobjekter og tilgang til sin medlemsmasse, hvilket har vært avgjørende for våre analyser og observasjoner. Vi reiste rundt i Norge og intervjuet nøkkelpersoner i bransjen, ØKOKRIM, Finanstilsynet og Eiendom Norge for å høre deres synspunkter av hvitvasking i eiendomsmeglingsbransjen. Gjennom disse intervjuene fikk vi et innblikk i hvordan hvitvasking oppfattes av meglere, forekomsten av fenomenet i bransjen og hvordan en eiendomsmegler kan bli utnyttet i en hvitvaskingsprosess. På bakgrunn av disse dybdeintervjuene lagde vi en større, anonym spørreunder-



I spørreundersøkelsen svarte 95% at de hadde en god forståelse av begrepet hvitvasking. Da respondentene ble bedt om å velge de alternativene de kategoriserte som hvitvasking, endte vi opp med følgende svar som vist i figuren, hvor to av de tre mest hyppige alternativene er feil.

> Økonomisk kriminalitet utgjør en stor trussel mot samfunnet, finanssystemets integritet, økonomiens virkeområde og rettstaten.

søkelse som ble sendt ut til alle NEF sine medlemmer. Svarene fra undersøkelsen ble behandlet i Excel og statistikkprogrammet Stata, slik at vi kunne trekke ut viktige observasjoner.

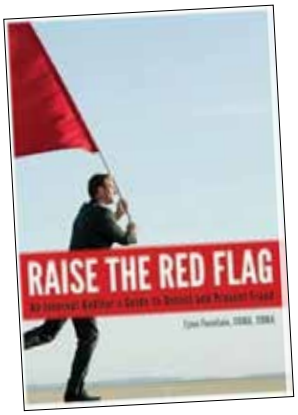
Resultatene og observasjonene fra intervjuene og spørreundersøkelsen er svært interessante, og viser flere elementer vi mener det burde fokuseres på i bransjen. Kvalitetsforskjellene mellom interne retningslinjer og rutiner fremstår som store på tvers av selskaper. Terskelen for rapportering praktiseres som høyere enn lovteksten tilsier, og svært mange finner regelverket uklart. Eiendomsmegleres kunnskap om hvitvasking og hvordan de kan bli utnyttet oppfattes som lavere enn ønsket. I følge våre undersøkelser er det mange eiendomsmeglere som ikke vet hva begrepet betyr og hvordan det kan forekomme i deres bransje.

Vi mener bransjen har behov for økt kunnskap om hvitvasking, regelverket og en bevisstgjøring av eiendomsmeglers rolle i en potensiell hvitvaskingsprosess. Vi håper at oppgaven kan skape et godt grunnlag for diskusjon og et felles økt fokus på bekjempelse av hvitvasking hos eiendomsmeglere.

RAISE THE RED FLAG - AN INTERNAL AUDITOR'S GUIDE TO DETECT AND PREVENT FRAUD. LYNN FOUNTAIN (2015)

Institute of Internal Auditors Research Foundation (IIARF)

Av
ESA LEPORANTA
Systems Audit Manager,
Nets Norway Branch



Boken presenterer praktiske metoder og prosedyrer for å evaluere, identifisere og redusere risikoen for misligheter.

Fountain innleder boken sin med å diskutere hvilket ansvar internrevisjonen har for å identifisere misligheter.

Ved å lese IIAs standard 2120.A2 kan det oppfattes at internrevisjon skal foreta overordnede mislighetsevalueringer på *bedriftsnivå*. Ifølge Fountain kan det hevdes at IIAs standard 2210.A2 forplikter internrevisjonen til å vurdere sannsynligheten for vesentlige feil og misligheter på *prosessnivå* ved utarbeidelsen av revisjonsoppdragets målsetninger. Poenget med dette er å vise at det må avklares med virksomhetens revisjonsutvalg hvordan internrevisjonen skal foreta mislighetsevalueringer.

IIAs standard 1210.A2 forutsetter at internrevisorene har tilstrekkelig kunnskap til å vurdere risikoen for misligheter. Fountain mener videre at revisorer bør ha en spørrende tilnærming og vurdere mottatte revisjonsbevis kritisk for å innfri kravene i denne standarden.

Kapitlet avsluttes ved å vektlegge behovet for å avklare og kommunisere hvilken rolle internrevisjonen skal ha ved en eventuell mislighetsgransking. Som kjent er det virksomhetens ledelse som har hovedansvaret for å identifisere misligheter i bedriften.

I det neste kapitlet viser Fountain hvordan ansattes *kontrollbevissthet* (jfr. definisjon av internt kontrollmiljø i COSO 2013[1]) kan knyttes til å bekjempe misligheter. For å redusere muligheten for misligheter (jfr. mislighetstriangel til Cressey[2]), har internrevisjonen tradisjonelt evaluert styrken av interne kontroller. Gjennom å etablere en åpen, ærlig og rettferdig atmosfære på arbeidsplassen, kan organisasjonen redusere ansattes rettferdiggjørelse av uetiske handlinger.

Ifølge Fountain er det heller ikke nok av ledelsen å si at det ikke er identifisert og/eller rapportert noen misligheter eller gjort noen reelle mislighetsfunn. Ved å bruke en tradisjonell prosessmodenhetsmodell (jfr. *Internal Audit Capability Model*[3]) kan ledelsen istedenfor skape åpenhet og øke sin forståelse rundt organisasjonens arbeid for å forebygge misligheter.

Ved en eventuell mislighetsgransking er det kritisk at internrevisjonen har etablert en prosess som sikrer at selve granskingen kan gjennomføres med største forsiktighet og flid. Ved minste usikkerhet rundt dette, anbefales det å ta kontakt med eksterne spesialister.

Økt kompleksitet i samfunnet har gjort det mer krevende å se for seg hvilke mislighetsrisikoer organisasjonen kan bli utsatt for. Ved vurderingen av slike risikoer, blir det først anbefalt å vurdere organisasjonens kultur. Deretter bør det tas stilling til på hvilket nivå i organisasjonen det skal foretas slike risikovurderinger. Resten av kapitlet tilbyr flere ulike forslag til maler som kan benyttes for å gjennomføre slike risikoanalyser.

I et av bokens avsluttende kapitler gis det en kort innføring i hvordan internrevisjonen kan bruke data-analyser ved identifisering av misligheter.

Boken viser hvordan internrevisjonen kan hjelpe organisasjonens ansatte med å bekjempe misligheter gjennom å tilby et helhetlig rammeverk og verktøy for bekjemping av misligheter.

En av fordelene med boken er at den viser hvordan internrevisorer kan begrunne sine valg med henvisning til IIAs standarder. Videre er det i boken gjennomgående tatt med eksempler som viser hvordan revisorer kan møte ledelsens argumenter og dermed redusere deres effekt på sitt arbeid.

[1] *http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf – Page 2*
[2] *Cressey, Donald R. 1953. Other People›s Money: A Study in the Social Psychology of Embezzlement,. Belmont, California: Wadsworth.*
[3] *The Institute of Internal Auditor's Research Organization. 2009. Internal Audit Capability Model (IA-CM) for Public Sector, Altamonte Springs, Florida*

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. IIA i Norge har en historie som går tilbake til 1951, men det første medlemsblad ble utgitt i 1993. Bladet het Internrevisoren frem til 2011, da det skiftet navn til SIRK.

I 2003 fusjonerte Norsk Finansrevisorforening inn i IIA Norge. Foreningen begynte sitt liv i 1921 som Norsk Bankrevisorforening. Medlemsbladet deres het først Bankrevisoren før det skiftet navn til Finansrevisoren.

For 20 år siden – så det heller ikke så lyst ut for økonomien

Den tiden på året vi nå er inne i er hvor vi tenker fremover i forhold til risikobildet i virksomheten og planlegger relevante revisjoner. I et år med Brexit-avstemming i England og Trumpvalg i USA er politisk risiko høyt på agendaen og hva det kan bety for verdensøkonomien. Heller ikke for 20 år siden var man spart for økonomisk usikkerhet – forskjellen fra den gang til nå er vel det mektige oljefondet Norge har greidd å bygge opp. Fra redaksjonens spalte til julenummer 1996 står det å lese følgende:

«Den nye finansministeren advarte i høst fra Stortingets talerstol om at varsellampene igjen blinker for norsk økonomi. Konjunkturoppgangen er i ferd med å gå ut av kontroll og ende med overoppheting og inflasjon. De fleste kommentatorer mener at faren er reell. Der stopper enigheten.

Historien gjentar seg aldri, den dukker alltid opp i nye versjoner med en ny miks av kjente og overraskende elementer. Derfor kan ingen legge blåkopi av gårsdagens løsninger på fremtidige problemer. Dessuten er det til og med få som kan bli helt enige om hva som egentlig skjedde sist, og hva man derfor burde kopiere. Er det riktig å stabilisere kronekursen, eller skal pengepolitikken brukes til å stabilisere inflasjon og konjunkturer, eller er det opposisjonens økte bevilgningsforslag som er avgjørende?

Som interne revisorer har vi litt andre problemstillinger å bale med. Linken til samfunnsutviklingen generelt er imidlertid relevant for de fleste virksomheter. Hvor ligger risikoen? Hva er tiltakene? Det eneste som nesten er helt sikkert er at «noen» også i fremtiden vil gå på større og mindre smeller. For interne revisorer blir hovedutfordringen å medvirke til at det ikke blir våre virksomheter.»

Er det riktig å stabilisere kronekursen, eller skal pengepolitikken brukes til å stabilisere inflasjon og konjunkturer, eller er det opposisjonens økte bevilgningsforslag som er avgjørende?

For 40 år siden – Hvor står revisjonssjefen?

I desember 1976 utgaven av Bankrevisoren var det gjengitt et svar fra Tidsskrift for revisjon og regnskap. Det var statsautorisert revisor 0. Solberg-Johansen, revisjonssjef i Bergen Bank, som hadde svart på følgende spørsmål «Det har vært diskusjon i vår bank om hvem som har det største personlige ansvar av disse: Kontorsjef, hovedbokholder, hovedkasserer aller revisjonssjef, og i hvilken rekkefølge disse rangerer?». Tittelen til artikkelen er «Hvor står revisjonssjefen?».

I konklusjonen av artikkelen kan man lese at en revisjonssjef (i en sparebank) «er der i en selvstendig og uavhengig stilling. Hans nærmeste overordnede er representantskapet/forstanderskapet.

Hvem som rangerer fremst osv. av kontorsjef, hovedbokholder eller hovedkasserer kan avhenge av stillingsinstruksen m.v. i vedkommende bank. Men kanskje aller mest av selve bankens størrelse, form og innhold. Dette får disse slåss om på kammerset.

Men hold revisjonssjefen utenom.»

Vi liker å tro at vi har kommet så langt i utvikling i løpet av de siste 40 år, men selv i våre dager ser vi tendenser i bankvesenet til å rekke pekefingeren først mot leder av internrevisjon før noen andre i organisasjonen blir gjort ansvarlige.

Martin Stevens

KURS OG NETTVERKSAKTIVITETER VÅREN 2017

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

Medlemsmøte på BI – tema: Endringer i standardene

12. januar, 14.30 – 16.30

De internasjonale standardene for utøvelse av internrevisjon har vært igjennom en lang reviderings- og høringsprosess og er nå klar i ny utgave. På møtet går vi igjennom hva som er nytt og hva dette vil si for internrevisor.

Praktisk kurs: Oppdag korrupsjon, svindel og misligheter raskt og tidlig

19. januar, 09.00 – 17.00

Kurset tar for seg teknikker og metoder for å oppdage når leverandører tar seg til rette, grådige mellommenn og konsulenter, regnskapssvindel, kunder som får for mye, interessekonflikt og andre former for uetisk adferd. Hvordan man oppdager røde flagg og utvikler strukturerte tester for avdekking av disse er en del av kurset.

Medlemsmøte: Compliance & kaffe

25. januar, 8. mars og 3. 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.

Kurs: Introduksjon til internrevisjon

28. februar, 09.00 – 17.00

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. Innholdet i kurset er nødvendig basiskunnskap for kurset Praktisk Internrevisjon.

Medlemsmøte: Varsling - daglig-dagse utfordringer

1. februar, 08.30 – 10.30

Nettverksgruppen for misligheter inviterer til erfaringsutveksling rundt dagligdagse utfordringer i mottak og vurdering av varsler. Temaer som organisering av arbeidet, innledende vurderinger rundt mottak av varsler, informering av ledelsen og ivaretagelse av anonymitet, vil bli dekket. Etter innledningen vil det bli satt av tid til gruppediskusjoner rundt utvalgte tema.

LES MER OM ALLE KURSENE OG MELD DEG PÅ VIA VÅR NETTSIDE WWW.IIA.NO.

Kurs: grunnkurs excel og dataanalyse

17. februar, 09.00 – 17.00

Kurset starter med grunnleggende Excel, men går relativt fort over til mer avanserte metoder for å gjennomføre dataanalyser. Kurset skal gi deltakerne en plattform å bygge videre på, samt et innblikk i handlinger og teknikker ved anvendelse av analyseverktøy ved gjennomføring av revisjonsarbeidet.

Kurs: Intervjuteknikk

13. - 14. juni, 09.00 – 16.00

Gjennom kombinasjon av teori, eksempler, analyser og flere praktiske øvelser fra deltakernes virkelighet, skal deltakerne få en forståelse for hva som skal til for å beherske intervjusituasjonen, forberede og ta kontroll over intervjuet og på den måten tilegne seg relevant viten på en effektiv og formålstjenlig måte i en revisjon. Det finnes ingen fasit på hvordan man gjennomfører et godt intervju, men kurset gir deltakerne innsikt i en utprøvd metodikk og hvordan den kan anvendes i praksis. Kurset tar for seg intervjuet som sjanger, hvordan en stiller de gode enkeltspørsmålene, hvordan en hindrer avsporinger eller ufrivillige sporskifter og hvordan en bestemmer mål og strategi for intervjuet.

Humor i særklasse

Av
ASBJØRN NYGÅRD
Statsautorisert revisor

Statsautorisert revisor Asbjørn Nygård (42) fra Kvernaland liker å utfordre seg selv. I 2012 syklet han Norge på langs og debuterte som forfatter med bok om turen. Kombinasjonen sykkel og bok ga tydeligvis mersmak. For i 2013 laget han sitt eget Tour de France og 2014 sitt eget Giro d'Italia. Også disse sykkelturene endte opp mellom to permer. Mett på sykkelopplevelser så Nygård seg høsten 2015 om etter nye utfordringer.

Tiden var inne for å rette fokus mot revisjonsfaget. Fortjent eller ufortjent har revisorene fått rykte på seg for å være grå, kjedelige og uten humor. Revisorhumor er derfor et begrep som skurrer litt for de aller fleste. For ordene revisor og humor passer liksom ikke sammen. Men det var akkurat det som inspirerte Nygård til å forsøke å lage en bok om revisorhumor. Med friskt mot begynte han arbeidet med å samle inn muntre revisorhistorier og – vitser. Han sendte e-poster til 5.000 revisorer og regnskapsførere med spørsmål om hjelp til å finne de gode historiene, men den store responsen uteble. Det var således ikke uten grunn at Norges Interne Revisorers Forening omtalte bokprosjeket som «Det umulige prosjektet» i et forsøk på å få internrevisorene til å komme med sine bidrag. Men heller ikke fra den kanten var det særlig å melde.

Nygård nektet imidlertid å gi opp og klarte til slutt å fullføre det umulige prosjektet. At boken ble tynn (56 sider) er kanskje ingen overraskelse, men iht. forfatteren er boken den eneste og derfor også den tykkeste boken i verden om revisorhumor. Boken ble lansert den første uken i november og allerede før første opplaget var levert fra trykkeriet, var alle bøkene utsolgt. Det er derfor ikke utenkelig at noen av bøkene også vil bli å finne under juletreet.

Avslutningsvis en liten smakebit

Lenge leve livet

Haukeland universitetssykehus, rundt årtusenskiftet.

En kvinne fikk den fryktelige beskjeden fra legen om at hun kun hadde seks måneder igjen å leve.
Fortvilet spurte kvinnen om det ikke var et eller annet hun kunne gjøre, hvorpå legen svarte at hun alltids kunne gifte seg med en revisor.
Kvinnen stusset litt over det merkelige svaret og etter en kort tenkepause spurte hun om det faktisk var slik at å gifte seg med en revisor ville medføre at hun kunne leve lenger enn de tilmålte seks månedene.
– Nei, svarte legen, men det vil føles slik.

Generalsekretæren informerer

AV ELLEN BRATAAS

Styret har denne høsten hatt stort fokus på strategi og revitalisering av foreningens visjon og handlingsplaner, og har også startet prosessen for å se om foreningen skal endre navn. Enn så lenge er det besluttet å benytte IIA Norge, så får vi ta en runde med medlemmene på neste generalforsamling før nytt navn endelig besluttes. I oktober inviterte styret inn ledere av tillitsvalgtapparatet til en sesjon for å diskutere forventninger og ambisjonsnivå i alle foreningens nettverk og komiteer. Det var et veldig nyttig møte for alle parter og Programkomiteen fulgte opp med et felles koordineringsmøte for å sette alle aktiviteter inn i et årshjul for neste år. Vi håper at dette kan bidra til å skape et mer helhetlig perspektiv for koordinering av aktiviteter og samarbeid på tvers av nettverk og komiteer. Målet er også å bidra til å utnytte synergier og sørge for at alle trekker i samme retning som den vegen strategien peker.

STATUS INTERNREVISJONER I STATLIG SEKTOR

72 statlige virksomheter har vurdert behovet for etablering av internrevisjon etter at Finansdepartementet besluttet at alle statlige virksomheter med inntekter eller utgifter over 300 millioner skulle vurdere dette behovet. Pr. 20. juni var resultatet som følger:

- 23 etater har allerede internrevisjon
- 24 skal ikke etablere en funksjon
- 22 nye virksomheter skal etablere internrevisjon innen 2018

Av de nye funksjonene skal 6 etablere en enhet med fast ansatte internrevisorer, mens 8 kommer til å outsource hele funksjonen. Dette betyr at 49 % av statens totale utgifter blir dekket av internrevisjon (tall fra juni 2016).

Forståelsen for internrevisjonens rolle og oppgaver er varierende blant de som nå skal etablere. Behovet for opplæring og erfaringsutveksling blir ikke mindre i tiden som kommer. Foreningen erfarer også at Offentlighetsloven tolkes forskjellig og praktiseres ulikt når det gjelder offentliggjøring av revisjonsrapporter. Også på dette området ville det vært hensiktsmessig med en generell uttalelse/tolkning/redegjørelse fra Justisdepartementet e.l.

Med økt etterspørsel etter internrevisjon i statlig forvaltning har Statens innkjøpssenter (Difi) fått i mandat å etablere felles rammeavtale for kjøp av internrevisjonstjenester. Tanken er god, men ikke like lett å omsette i praksis. Difi har som mål om kunngjøring allerede før jul, men det er i skrivende stund ikke klart om det blir en eller flere forskjellige avtaler, eller eventuelt en dynamisk innkjøpsordning med miniavrop.

AKADEMIA

IIA Norge tok denne høsten kontakt med flere universiteter og høyskoler i Norge med utgangspunkt i at utviklingen gjør at det er behov for flere kandidater med tilstrekkelig innsikt og erfaring i risikostyring, internkontroll og internrevisjon. Det er viktig 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. Vi mottok positiv respons fra flere akademiske miljøer som ønsker dialog. Pt. har vi allerede hatt et møte med Høyskolen i Oslo og Akershus. Vi fortsetter dialogen med akademia i året som kommer.

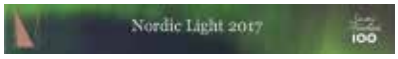
VEILEDER FOR RISIKO-STYRINGSFUNKSJONEN

Nettverk risikostyring har laget et utkast til «Veileder for risikostyrings-funksjonen» som er sendt på høring til rundt 30 virksomheter og organisasjo-ner. Det hårete målet om å lansere veilederen før jul har måttet vike for tiden det tar å innarbeide høringssva-rene som har kommet. Nytt realistisk mål er derfor å kunne gi ut veilederen 1. kvartal 2017.

Veilederen beskriver risikostyringsfunk-sjonens hensikt, ansvar og oppgaver, samt forutsetninger og suksesskrite-rier på tvers av bransjer. Prinsippene i veilederen kan også være nyttige for virksomheter som mangler en egen Risk Manager, men som ivaretar lig-nende arbeidsoppgaver under en annen stillingsbetegnelse.

KONFERANSER VERDT Å MERKE SEG

Nordic Light, 9. og 10. februar 2017, Helsinki, Finland



IIA Norges årlige konferanse, 29. og 30. mai 2017, Fornebu, Bærum
IIAs International Conference, 23. – 26. juli 2017, Sydney, Australia

ECIIA Conference, 21. og 22. september 2017, Basel, Sveits

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

OPPDATERING AV ANBEFALING TIL EIERSTYRING OG SELSKAPSLEDELSE

KPMG har på vegne av NUES gjennomført en analyse av hvordan anbefaling for eierstyring og selskapsledelse brukes i redegjørelser fra virksomheter på OSE/OBX. NUES› mål med undersøkelsen var å skaffe kunnskap om bruken av anbefalingen for å vurdere anbefalingens gjennomslag i markedet og vurdere behov for endringer. Funnene i undersøkelsen og lovarbeider som er på gang både i Norge og EU, tilsier at det er grunn til å endre anbefalingen for eierstyring og selskapsledelse. I den forbindelse har NUES åpnet døren for en videre dialog og innspill fra IIA Norge når kapittel 10 om risikostyring og intern kontroll skal gjennomgås til neste år.

SVAR PÅ HØRINGER GJENNOM ÅRET

Det er mange høringer som kommer gjennom et år og foreningen forsøker å besvare alt som er relevant. Tusen takk til enkeltmedlemmer, komiteer og nettverk som har bidratt til følgende høringssvar:

a) Forskrift om styringssystem i helse- og omsorgstjeneste, januar 2016

b) Digital sårbarhet – sikkert samfunn (NOU 2015:13), mars 2016

c) Comments to the Exposure Draft – Changes to the International Standards, april 2016

d) Høring om endringer i arbeidsmiljølovens regler om varsling, september 2016

e) Comments to the ERM Framework Update Approaches: Aligning Risk with Strategy and Performance, september 2016

f) Utkast til endringer i personopplysningsforskriftens regler om melde- og konsesjonsplikt, november 2016

VI GRATULERER FØLGENDE MEDLEMMER

Diplomert Intern Revisor (Dipl IR)
Under behandling – kunngjøres samlet i neste SIRK.

Certified Internal Auditor (CIA)
Mads G. Kristensen, Norges Bank
Mireille Morkos Ramberg, Nordea Bank Norge ASA
Frode Øverli, Nordea Bank Norge ASA

The Institute of Internal Auditors | Global

Fra 1. januar 2017 trer den oppdaterte versjonen av de internasjonale standardene i kraft. Du kan laste ned både den nye utgaven og standardene der du ser hvilke endringer som er gjort, fra nettet.

Implementation Guides (IG) and Practice Advisories (PA) assist internal auditors in applying the Standards. They collectively address internal auditing›s approach, methodologies, and consideration, but do not detail processes or procedures. IGs will be developed to replace the existing PAs. IG will be more comprehensive than PA in guiding practitioners toward conformance to the International Standards for the Professional Practice of Internal Auditing (Standards). Here are the new IGs since the last edition of SIRK:

IG1100 Independence and Objectivity (August 2016)
IG1110 Organizational Independence (August 2016)
IG1111 Direct Interaction with the Board (August 2016)
IG1120 Individual Objectivity (August 2016)
IG1130 Impairment to Independence or Objectivity (August 2016)
IG2000 Managing the Internal Audit Activity (October 2016)
IG2010 Planning (October 2016)
IG2020 Communication and Approval (October 2016)
IG2030 Resource Management (October 2016)
IG2040 Policies and Procedures (October 2016)
IG2050 Coordination and Reliance (October 2016)
IG2060 Reporting to Senior Management and the Board, (October 2016)
IG2500 Monitoring Progress (July 2016)
IG2600 Communicating the Acceptance of Risks (July 2016)

Supplemental Guidance (PG) provides detailed guidance for conducting internal audit activities. These include topical areas, sector-specific issues, as well as processes and procedures, tools and techniques, programs, step-by-step approaches, and examples of deliverables. You can download all the PGs from www.globaliia.org.

The newest PG Audit Reports: Communicating Assurance Engagement was released in October 2016 and offers guidance to audit practitioners on how to effectively communicate the results of internal audit engagements to stakeholders. The guide addresses key considerations such as tailoring the report to multiple audiences, structuring the report to maximize impact, and accounting for follow up and corrective action.

REVISING COSO ERM – ALIGNING RISK WITH STRATEGY AND PERFORMANCE

The revised Framework updates the core definitions of risk and enterprise risk management as well as the components of enterprise risk management. One of the most significant enhancements is the introduction of principles that reflect the evolution of risk management thinking and practices. Also the cube will be replaced with a new model. The updated ERM Framework will be available medio 2017.

The new new model replacing the cube

Ugler i mosen

Dette året har vi vært vitne til hvordan internrevisjonen er kommet i fokus i Norges største bank. Etter medias avsløringer om potensielt ulovlig skatterådgivning gjennom Panama papers, har styre og konsernledelse vist manglende evne til å ta ansvar for denne delen av bankens virksomhet. De har isteden søkt etter syndebukker internt i banken.

Den som leter, han skal finne! Og gjett hva styret og konsernledelsen fant? De fant internrevisjonsfunksjonen i banken og syntes tydeligvis det var et godt funn! Naturligvis tenker man på svikt i styring og kontroll og, hvis man «hopper over styring», da gjenstår bare «kontroll». Da må det være bankens interne kontrollfunksjon som har sviktet i sin kontrolloppgave. Kanskje internrevisjonen konsentrerte bruk av sine ressurser på andre områder med høy risiko, sett med datidens briller? Styret og ledelsen ante jo ikke at bankens aktivitet knyttet til rådgivning og bistand til skatteunndragelse for utvalgte kunder via skatteparadis kunne bli oppfattet som en lite lojal etterlevelse av loven. Langt mindre ante de at dette skulle bli avdekket i media. Forklaringen om svikt i internrevisjonsfunksjonen syntes å være anvendbar og ble tydeligvis ansett som «spiselig» for alle bankens interessenter. For å få bekreftet forklaringens godhet, ga styret advokatfirma Hjort et oppdrag (med hemmelig mandat, riktignok!) som i praksis dels gikk ut på å granske fadesen.

Som ventet, reiste rapporten fra Hjort ingen alvorlig kritikk av manglende risikostyring eller manglende oversikt og kontroll over bankens aktiviteter – hverken mot styret eller konsernledelsen. Man aner en viss kritikk av konsernets internrevisjon og dens daværende leder, dog er den dempet i forhold til uttalelser fra styrelederen da saken først kom opp våren 2016. Den sterke kritikken som var rettet mot den separate internrevisjonsfunksjonen ved kontoret i Luxemburg som fremgikk av den opprinnelige utredning som banken selv hadde utarbeidet, var ikke gjentatt i rapporten fra Hjort. De to internrevisjonsfunksjonene blir således heller ikke renvasket i Hjort rapporten og mistanken som hadde festet seg ved disse funksjonene henger fortsatt ved.

Er det mulig at en så stor og tilsynelatende kompetent virksomhet ikke forstår at styret, ved å legge all skyld på internrevisjonen, har skutt seg selv i foten – og erkjent uvitenhet om corporate governance og styreansvar?

Det er grunn til å minne om at gjennom lov og forskrifter er Internrevisjonen i banker organisert direkte under styret. Styret har ansvar for å sikre at internrevisjonen har tilstrekkelig ressurser og kompetanse god nok til å utføre sine oppgaver som styrets kontrollorgan. Styret skal minst årlig vurdere bankens risikoprofil og fastsette en adekvat arbeidsplan for internrevisjonen. Styret mottar alle internrevisjonsrapporter og skal følge opp at nye identifiserte risiko-områder og avdekkede svakheter i etterlevelse av fastsatt kontrollnivå blir håndtert av virksomhetens ledelse.

De fleste av oss «innenfor menigheta» og heldigvis mange utenfor - er både forundret, forskrekket og opprørt over bankens håndtering av ovennevnte sak. Risikoen for å tape ansikt ved å innrømme manglende oversikt og handlekraft relatert til denne noe tvilsomme tjenesten i bankens regi, vurderes åpenbart som større enn risikoen for å fremstå som et styre og en ledelse med manglende kompetanse på styring og kontroll. Snakk om svikt i risikovurderingsevne!

Slik adferd fra styret og ledelsen vil medføre at internrevisjonsansvar i virksomheter fremstår som en ren risikosport og tiltak bør følgelig settes inn. Ett tiltak bør være at risikopremie og fallskjerm inngår som egne elementer i lønnsdiskusjoner for ansvarlige internrevisorer.

Men for øvrig slutter vi oss til en norsk artist som på nyåret vil turnere Oslo med en konsert med følgende tittel: «Kan nokon gripe inn?»

Uhuuu….

Returadresse
IIA Norge
Postboks 1417 Vika
0115 Oslo

DE BESTE LØSNINGENE FOR DEG

I BDO er vi opptatt av å kombinere internrevisjonserfaring med spesialistkompetanse innen de fagfeltene som preger risikobildet norske virksomheter står overfor i dag.

Gjennom tverrfaglige team bidrar vi til en løsningsorientert internrevisjon, med fokus på det som virkelig betyr noe for virksomheten. Enten vi ivaretar internrevisjonsfunksjonen eller bistår i gjennomføring av enkeltoppdrag, gir vi alltid våre kunder tilgang på spiss-kompetansen som behøves for å løse nettopp deres problemstillinger. Slik bidrar vi til å skape merverdi og trygge, gode løsninger for deg.

Virksomhets-styring | **Gransking og compliance** | **IT-revisjon og IT-risiko** | **Sikkerhet og beredskap** | **Transaksjons-rådgivning**

For mer informasjon om våre tjenester og hva vi kan hjelpe deg med, se www.bdo.no

Revisjon | Advokat | Rådgivning | Regnskap

BDO