NORGES INTERNE REVISORERS FORENING

SIRK

Styring – Internrevisjon

Risiko – Kontroll

Nummer 2, vinter 2014, 22. årgang

Hva bør styret kunne om nettsikkerhet?

Lean auditing | Hvordan sveve på en rosa sky | Compliance – beste praksis

REDAKTØRENS SPALTE

Å arbeide frem en ny utgave av SIRK er en like spennende oppgave hver gang. Jeg håper at det blir like spennende for dere som åpner opp bladet i disse førjulstider. Vår målsetning er å komme med gode artikler som spenner over de områdene som SIRK skal stå for (Styring, Internrevisjon, Risiko og Kontroll). Det er ingen radikale endringer i stilen denne gangen. Utover dette har det vært et mål å kunne tilby flere nyheter om utviklingen internasjonalt.

Under temaet "virksomhetsstyring" har vi satt nettsikkerhet samt misligheter og korrupsjon på dagsordenen. For å skape størst mulig verdi for våre lesere har vi lettfattelig presentert nye og aktuelle temaer og deretter henvist til andre kilder for ytterligere detaljer og informasjon.

Under temaet «kontroll» er det presentert to artikler om compliance og etikk. Til slutt er det lettet på alvorets slør med en artikkel om brettspill som trekker på COSO.

Under temaet «internrevisjon» ønsker jeg spesielt løfte frem en undersøkelse om internrevisjonsinstruksen, som er gjennomført her i Norge. Artikkelen setter fokus på et område som med stor sannsynlighet bør oppdateres jevnlig i virksomheter med en internrevisjonsfunksjon. Undersøkelsen er basert på en prosjektoppgave innlevert i forbindelse med internrevisjonsstudiet på BI. Det er mange interessante oppgaver som produseres, og vi vil gjerne med dette invitere flere tidligere og fremtidige studenter til å publisere deres funn i fremtidige SIRK utgaver. Videre har vi et intervju med internrevisjonssjefen i Australian Taxation Office hvor han forteller om hvordan en ekstern kvalitetsvurdering kan benyttes på en hensiktsmessig måte til å forbedre prestasjoner.

I tillegg har vi artikler som dekker områdene ERM, finans, det offentlige og kompetanseutvikling i egne rekker. Til slutt har vi også en bokanmeldelse av boken skrevet av selveste CEO i IIA internasjonalt som viser en mann som til tross for sin høy posisjon har så absolutt revisjonsbeinene plantet på bakken.

Ja, når vi avslutter bladet med informasjon fra den norske foreningen sammen med en oppdatering om nye publikasjoner fra internrevisjonsmiljøer internasjonalt, tør vi håpe at det er noe i dette nummeret for enhver smak. Vi ønsker at SIRK oppleves nyttig og relevant for deg, og vi i redaksjonen setter stor pris på din tilbakemelding – ros og ris for å bli enda bedre.

REDAKSJONS KOMITEEN

Ansvarlig for dette nummeret av SIRK

Martin Stevens
Gjensidige Forsikring
M: 957 50 192
martin.stevens@gjensidige.no

Jan Wilhelm Kavli,
Utlendingsdirektoratet
jaka@udi.no

Reidar Døli
Oslo Børs
reidar.doli@oslobors.no

Esa Leporanta
Nets Norway AS
elepo@nets.eu

Cira Holm
Yara International ASA
Cira.holm@yara.com

Se mer info på www.iia.no

Innhold

Travel høst

Vi har hatt en travel høst med mange viktige saker.

Utredningen om internrevisjon i staten
I oktober ga NIRF høringssvar til Finansdepartementets utredning om internrevisjon i staten. Formålet med utredningen har vært å skape mer forutsigbare rammer, videreutvikle det statlige økonomiregelverket samt tilrettelegge for faglige standarder og annen støtte for internrevisjon. Hensikten var å legge til rette for beste praksis og mer effektivt samarbeid mellom ekstern- og internrevisjon.

I motsetning til hva som er vanlig i EU, har vi i Norge så langt ikke innført noe krav om at statlig sektor skal ha internrevisjon. NIRF støttet i høringssvaret anbefalingene til beste praksis fra OECD og IMF. OECD har uttalt at Norge ligger i ytterkant av internasjonal praksis når ansvaret for internrevisjonsordningen er lagt til etatene. Norge ble anbefalt å inkludere departementene. OECD viste videre til at den internasjonale hovedtrenden for internrevisjon er «dualrapportering» - dvs rapportering både til minister og til departement- og/eller etatsledelse. Selv om utredningen er et skritt i riktig retning, synes vi i NIRF den på viktige områder er for vag:

- Det bør fastsettes objektive kriterier for hvilke statlige virksomheter som skal etablere internrevisjon. Dette spørsmålet er for viktig til at det blir personavhengig.
- Det bør ikke være svakere krav til å ha internrevisjon i staten enn i finanssektoren, helsesektoren eller arbeids- og velferdsforvaltningen, som har fått slike krav. Skattebetalernes penger er ikke mindre viktige enn investorers. Regelverk bør harmoniseres.
- Fra 2014 krever økonomiregelverket at ledelsen skal gi uttalelse om styring og kontroll i årsrapporten. Forslaget burde stilt krav til at internrevisjonens årlige rapport skulle relateres til ledelsens uttalelse om styring og kontroll.
- Primært skal internrevisjon gjennomføre uavhengig revisjon. Den skal gi uttalelser om styring og kontroll til det øverste ledelsesnivået. Finansdepartementet foreslår å unnta departementene i kravet om å vurdere internrevisjon. NIRF mener internrevisjonsmodellen i forsvarssektoren er god. OECD har anbefalt Norge å ha internrevisjon i departementene. Funksjonen kan innhente rapporter fra underliggende enheters internrevisjoner.

Ny utgave av Norsk anbefaling til eierstyring og selskapsledelse (NUES)
NUES-anbefalingen er oppdatert. OECD har pekt på at til tross for flere oppdateringer i den norske anbefalingen siden 2006, er den ikke vesentlig endret etter store skandaler som Enron. Den reflekterer i for liten grad hva som kan læres av finanskrisen. Norske selskaper utnytter ikke potensialet i risikostyring godt nok. Om lag 90 % av børsnoterte selskap har ikke internrevisjon, noe som er svært uvanlig internasjonalt.

NIRF ga innspill utover de mindre forslagene til endringer, samt åpnet for diskusjon av mer prinsipiell karakter:

Sammenlignet med anbefalinger til god governance i andre land, både i og utenfor EU, er den norske anbefalingen relativt snever. Den dekker hovedsakelig kravene til foretaksstyring sett fra eier og ledelsens perspektiv. Det vil være god praksis å inkludere også krav til governance fra ansatte, brukere, leverandører, kunder og samarbeidspartnere. Likeledes vil prinsippet om å ikke ta med lovfestede emner i NUES anbefalingen medføre at anbefalingen på sikt vil bli kort.

NIRF viste også til rapporten «Corporate Governance Codes on Internal audit: current status in the EU (2012)». Den konkluderte med at bortsett fra Litauen, Polen og Portugal, inneholder samtlige av EU-lands governance-koder enten et krav til internrevisjon, eller til at styret skal begrunne hvorfor dette ikke er nødvendig.

Compliance og anti-korrupsjon
Det har i høst vært flere saker om misligheter og korrupsjon i media: JP Morgan, RTC/Tinn Kommune og sist Telenor. NIRF har bidratt inn i arbeidet med Transparency International Norges nye utgave av *Antikorrupsjonshåndbok for næringslivet.*

Vi har også deltatt i et prosjekt med Snøball Film, som lager tre kortfilmer om anti-korrupsjon for Aftenposten. Hensikten er å skape debatt i det offentlige rom. Foruten NIRF, er Norges Kommunerevisorforbund, Finansmarkedsfondet, Selmer og TI Norge bidragsytere i prosjektet.

Vårt compliance-nettverk er en felles møteplass og arena for erfaringsutveksling for de som jobber med compliance i Norge. Nettverket er nå i sluttfasen med å utarbeide en bransjeuavhengig veiledning til beste praksis for compliance-rollen i Norge.

Kvalitetssikring
Vår satsning på å bistå medlemmene med kvalitetssikring er styrket. Vi har i høst tilbudt medlemmer kurs for å etablere kvalitets- og forbedringsprogram og forberede ekstern kvalitetskontroll. Vi har engasjert oss i den europeiske QA-gruppen, som gir NIRF / IIA mulighet til å sette opp internasjonale QA team.

Til slutt vil jeg takke alle i NIRF som i høst har bidratt til å bringe oss videre. Vårt arbeid har gitt resultater. Vi har ny medlemsrekord med over 800 medlemmer. Sammen bidrar vi alle til bedre styring og kontroll i offentlig og privat sektor i Norge.

Jeg ønsker dere alle en gledelig jul og et godt nytt år.

Jørgen Bock
President NIRF
@jorgeniia

Vi vokser

Deloitte er et av de ledende internrevisjonsmiljøene i Norge. Vi bidrar til å skape resultater for våre kunder gjennom en strategisk tilnærming til utfordringer, men også gjennom praktiske handlinger og gjennomføringsevne.

Vi har i dag over 100 rådgivere som leverer tjenester innenfor internrevisjon, strategisk og taktisk risikostyring, intern kontroll, corporate governance, compliance, informasjonssikkerhet og granskning.

Deloitte er verdens største leverandør av profesjonelle tjenester med over 200.000 medarbeidere i over 150 land, hvorav ca. 1.250 i Norge.

Ønsker du å vite mer om våre tjenester eller være del av et dynamisk og innovativt miljø, kontakt oss gjerne for en hyggelig samtale.

Stein Ove Songstad, *Partner*
ssongstad@deloitte.no
Tlf. 915 56 161

Eivind Skaug, *Partner*
eskaug@deloitte.no
Tlf. 915 18 997

Helene Raa Bamrud, *Partner*
hbamrud@deloitte.no
Tlf. 974 23 678

Deloitte.

Foreningen gratulerer følgende medlemmer med ny tittel siden forrige nummer av SIRK:

Diplomert Intern Revisor (Dipl IR)
Kathrine W. Boge, NAV
Silje Evjen Hansen, Forsvarsdepartementet
Turid Adamsen Husvæg, Aibel AS
Per Anders Kongsvik, NAV
Liss Johansen Vallestrand, Norsk Folkehjelp
Bjørn Ole Kristiansen, Helse Nord RHF
Monika Sverdrup-Thygeson, Statkraft AS
Sonja Dar, Oslo kommunerevisjon
Hilde Ludt, Oslo kommunerevisjon
Camilla Svae, DNB
Jorun Andreassen, Oslo kommunerevisjon
Tore Dæhlin, Høgskolen i Oslo og Akershus
Tuva Elgaaen, Vestre Viken HF
Brit Gagnat, Riksrevisjonen
Kari Hesjedal, KPMG
Ingvild Lundin Nordahl, Omsorgsbygg
Randi Bolsø Hardy, Forsvarsstaben
Mery Mehrnaz Zadeh, Eika Gruppen AS
Vibeke Vestbø, Forsvarssjefens internrevisjon
Hilde Tanggaard, NIRF

Certified Internal Auditor (CIA)
Ewa Grabarczyk, Statoil
Sissel Kristiseter, Oslo kommune, Byrådslederens kontor
George Turk, Telenor

Certified Government Auditing Professional (CGAP)
Ida Thorsrud, Forsvarsdepartementet
Arne Torgersen, Forsvarsdepartementet

NIRF og IIA globalt gratulerer!

Oppdatert UK Corporate Governance Code

September 2014

The Financial Reporting Council (FRC) i UK har utgitt en oppdatert utgave av UK Corporate Governance Code som utvider kravet til kvaliteten av informasjon som investorer får om selskapenes langsiktige overlevelsesevne og strategi i børsnoterte selskaper, og som stiller større krav til risiko-styring.

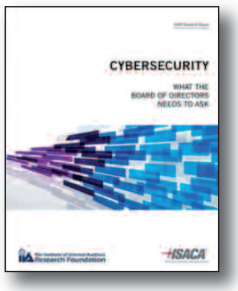
Sammen med de nye kravene i selve koden er det utgitt en oppdatert "Guidance on Risk Management, Internal Control and Related Financial and Business Reporting " – retningslinjer om risikostyring og intern kontroll med rapportering. Fra dette dokumentet er det flere områder som kan være av interesse for internrevisorer som for eksempel på områdene bedriftskultur, debatt og utfordringer i styrerommet og styrets behov for bekreftelser (assurance).

For videre informasjon se https://www.frc.org.uk/News-and-Events/FRC-Press/Press/2014/September/FRC-updates-UK-Corporate-Governance-Code.aspx

Og NIRF sitt blogg http://www.iia.no/no/nyhetsblogg/

Rapportanmeldelser

Av Esa Leporanta



Forskningsrapport til IIARF

NETTSIKKERHET – Hva bør styret spørre om selskapets nettsikkerhet

Et hovedbudskap i denne rapporten er at selskapets styre ikke bør delegere nettsikkerheten til IT-avdelingen. Selskapets styre skal selv ta en aktiv rolle ved styringen av selskapets nettsikkerhet.

I en separat spørreundersøkelse som er delvis gjengitt i forskningsrapporten, oppgir mer enn 65 % av respondentene at risikoene innen nettsikkerhet er på høyt nivå og har økt. Samtidig gir kun 14 % av respondentene uttrykk for at de har vært aktivt involvert i tiltak hvor målet har vært å forbedre virksomhetens nettsikkerhet.

Rapporten presenterer fem prinsipper som kan anvendes for å forbedre oversikten over virksomhetens nettrisikoer:

1) Styrets medlemmer bør se nettsikkerhet som en del av virksomhetens totale risikostyring, og kreve årlig rapportering om organisasjonens arbeid innen nettsikkerhet.
2) Styrets medlemmer bør forstå cyberrisikoene som er knyttet til virksomhetens tredjeparts-leverandører, og sikre at organisasjonen følger gjeldende lovgivning på feltet. I tillegg skal styret bli informert om alle alvorlige dataangrep på selskapet.
3) Styret bør møte selskapets datasikkerhetsleder årlig for å få en oppdatering om selskapets nettsikkerhetsarbeid. Videre bør styret sikre at selskapets ledelse har etablert kontakt med relevante myndigheter innen nettsikkerhet.
4) Styret bør forvente at selskapets ledelse har i bruk et helhetlig risikorammeverk som inkluderer nettsikkerhetsrisikoer, og sikre at datasikkerhetslederen rapporter til riktig ledelsesnivå i organisasjonen.
5) Styret bør møte selskapets risikoleder årlig for å evaluere alle risikoer, og bekrefte at selskapets forsikringer har tilstrekkelig dekning for å adressere potensielle cyberrisikoer.

Videre kan følgende spørsmål hjelpe selskapets styre til å forberede seg til samtaler med ledelsen og revisjonsledelsen:

1) Bruker virksomheten et helhetlig sikkerhetsrammeverk?
2) Hvilke er selskapets fem viktigste nettsikkerhetsrisikoer?
3) Hvordan er virksomhetens ansatte bevisstgjort om deres rolle for nettsikkerheten?
4) Har selskapets eksterne og interne trusler blitt analysert og vurdert ved planleggingen av nettsikkerhetsaktiviteter?
5) Hvordan er selskapets sikkerhetsledelse organisert?
6) Ved eventuelle datainnbrudd, har ledelsen etablert robuste løsninger for å kunne håndtere situasjonen tilfredsstillende?

Forskningsrapporten til IIARF viser klart at styret forventes å ha en aktiv rolle ved ledelsen av selskapets nettsikkerhet. Ved å stille spørsmålene presentert over, kan styret ta de kritiske første stegene for å kunne fungere som virksomhetens fjerde forsvarslinje innen nettsikkerhet.

European Cybersecurity Implementation: Oversikt

Denne oversiktsrapporten er en av totalt fem publikasjoner i ISACAs serie om *European Cybersecurity Implementation Series*, og tilbyr en overordnet fremstilling om hvordan selskapene kan oppnå en tilfredsstillende kvalitet innen nettsikkerhet.

Innledningsvis presenterer rapporten tre viktigste årsaker som forklarer hvorfor vi bør ha økt fokus på nettsikkerhet. Deretter viser rapporten en oversikt over de seneste nettsikkerhetsprogrammer og initiativer som er introdusert i Europa og som kan brukes som kilder til en verdifull informasjon.

Selskapene anbefales å skille mellom informasjonssikkerhet og nettsikkerhet. Utover dette visualiseres forskjellen mellom informasjonssikkerhets- og nettsikkerhetstrusler og risikoer med et PESTLE-diagram.

Ifølge rapporten er mange selskapene fremdeles ikke kjent med at nye automatiserte angrepsmetoder kan nesten som tilfeldig sjekke sårbarheten i virksomhetenes datasikkerhetsløsninger. Dermed anbefales det at selskapene i stedet for å vurdere sannsynligheten for at de vil bli angrepet, legger til grunn at det er sannsynlig at dette vil skje.

For å kunne møte dagens krav innen nettsikkerhet, er det anbefalt å utvikle en *business case* som identifiserer og analyserer effekten og konsekvenser av nettkriminalitet. Dernest bør selskapet etablere et målebilde for sitt nettsikkerhet. Avslutningsvis skal det lages egne målekort for nettsikkerhetens ulike delområder, som deretter fordeles mellom selskapets ulike avdelinger.

I slutten av rapporten blir leserne påminnet om at nettkriminaliteten ut fra sin natur krever kontinuerlige justeringer, vurderinger og forbedringer i hele verdikjeden. Dette forutsetter i sin tur at selskapet adopterer en langsiktig cyberstrategi, som inkluderer dynamiske og fleksible løsninger, inkludert kontinuerlig oppdatert informasjon om kvaliteten i eksisterende nettsikkerhetsløsninger med tilhørende indikatorer og nøkkeltall.

Avslutningsvis viser rapporten hvordan virksomhetene kan organisere arbeidet sitt med hensyn til bekreftelser fra internrevisjon, og viser videre til andre kilder.

Oversiktsrapporten fra ISACA kan anbefales, da den tilbyr verdifull informasjon til alle relevante interessenter i virksomhetene. Dette gjør den gjennom å skape et felles begreps- og forståelsesgrunnlag for fremtidige diskusjoner om nettsikkerhet. Revisorer anbefales også tre andre rapporter i serien, som handler om risikoveiledning, bekreftelse og revisjons program innen nettsikkerhet.

Hvordan sveve på en rosa sky

Bjørn Chr. Borgen, CISA, ITIL, leder Sikkerhet & Teknologi hos RSM

Kent Kvalvik, CIA, Dipl. IR, CRMA, CRISC, CGEIT, partner Risk & Advisory Services hos RSM

Skytjenester og lagring

De siste årene har det har vært mange endringer på teknologien som ligger til grunn for vår bruk av IT-systemer.
En av de mer omtalte er inntoget av såkalte skytjenester, nettskyer og cloud computing - eller rett og slett nettbaserte tjenester. Kort forklart omfatter dette dataprosessering og datalagring som skjer på store og sentrale datasentre tilknyttet Internett. Det er vanlig å skille på private og kommersielle tjenester. De private er forbeholdt eierens bruk og deles ikke med andre virksomheter, mens de kommersielle deles av mange virksomheter og brukere.

Skytjenester er bygget med stor kapasitet for databehandling og datalagring som deles av alle brukerne Målet er å redusere kompleksitet og investeringsbehov for den enkelte virksomhet ved at hver av kundene kan leie nødvendig kapasitet.

De mest kjente skytjenestene er plassert i store datasentre hvor hver enkelt kunde har mulighet til dynamisk skalering etter sine behov for datakraft og datalagring. For eksempel er det virksomheter som har ekstreme behov for datakraft i kortere perioder. Med tradisjonelle løsninger måtte slike virksomheter investert store beløp i infrastruktur for å kunne ha tilstrekkelig kapasitet selv. Med skytjenester kan de ganske enkelt bestille ønsket kapasitet for de timene, dagene eller ukene de trenger det.

Med ny teknologi følger nye muligheter. Med muligheter følger også nye risikoer og verdien av infrastrukturen vil forandre seg. For eksempel vil tilgang til Internett bli viktigere for virksomheten, mens lokale servere kanskje kan reduseres i antall og størrelse. Å være klar over nye og endrede risikoer og sårbarheter er essensielt for å understøtte virksomhetens måloppnåelse.

Mange virksomheter har lenge vurdert slike skytjenester med stor skepsis. Det har per dags dato ikke vært rapportert om tap av data eller større sikkerhetshendelser hos leverandører som Amazon, Google, Microsoft eller Salesforce. Når dette skrives har Apple lagt til rette for såkalt to-faktor autentisering i sin skylagringsløsning – iCloud, etter at flere avslørende og private bilder har blitt stjålet fra brukerkontoer med dårlig sikkerhet. Om dette tyveriet skyldes at brukerne hadde for svakt passord eller Apple hadde for dårlig sikring vil sikkert bli diskutert i lang tid fremover.

Kanskje har din virksomhet tatt i bruk skytjenester allerede? Eller kanskje det er oppe til vurdering? Kanskje har det vært vurdert som for risikabelt? Uavhengig av bruk og utbredelse er skytjenester noe alle virksomheter må forholde seg til. Kanskje er det allerede ansatte som har tatt i bruk de samme tjenestene på jobb som de benytter privat. Det er jo så lettvint å flytte dokumenter mellom hjemmekontor og jobb med skytjenester. Dermed har kanskje virksomheten i praksis skytjenester i bruk uten at de er vurdert i forhold til behov og bruk, eller i forhold til trusler og risiko. I verste fall kan det være snakk om mindre sikre tjenester hvor det oppbevares personsensitiv og virksomhetskritisk informasjon uten at ledelse, sikkerhetsansvarlig og IT-avdelingen er klar over utbredelsen.

Bruk av skytjenester utgjør dermed en potensiell og ofte reell risiko for at data kan komme på avveie. En annen risiko er at data blir oppbevart på en måte som ikke tilfredsstiller norsk lovgivning. Blant annet stiller Personopplysningsloven og Bokføringsloven krav til hvor og hvordan elektronisk lagret informasjon skal oppbevares.

Selskapets styre og daglig leder har ansvar for å ivareta sikkerheten og tilrettelegge for forsvarlig drift. Mye av dette handler om å vite hvilke verdier og trusler som finnes og iverksette tekniske og organisatoriske tiltak for å håndtere dette. Kanskje er det på tide med en gjennomgang av verdier, trusler og risikoer, eller kanskje det er på tide å gjøre en ny vurdering av behovene virksomheten har til nye tjenester.

Det er vanskelig å styre bruk av skytjenester fordi det eneste som kreves er

en helt ordinær nettleser. Virksomhetene må ha et bevisst forhold til skytjenester og følge med på bruk av slike løsninger. Et virkningsfullt tiltak er å arbeide med bevisstgjøring og opplæring av de ansatte. Retningslinjer for bruk av IT-systemer og behandling av informasjon må gjøres kjent gjennom opplæring av ansatte og gjentas jevnlig.

Skytjenester har kommet for å bli, i hvert fall til det dukker opp andre løsninger og teknologi som kan gjøre arbeidshverdagen vår enda mer effektiv. Er det ikke blitt gjort noe relatert til slike tjenester, så er tiden kanskje kommet?

Bevisstgjøring og opplæring av sikre ansatte

Tidligere var det systemene og den tekniske infrastrukturen som var gjenstand for dataangrep, men i dag er ikke brannmurer, antivirus og oppdatert programvare nok for å sikre elektroniske verdier i virksomheten. Det er ikke lenger tilstrekkelig at IT-avdelingen sørger for at uønsket datatrafikk blir stoppet på vei inn via Internett og andre elektroniske kanaler. Dette kan være i form av e-post med uønsket innhold eller uønsket programvare, eller det kan være reklame på nettsider som blir besøkt. Selv om de fleste har hørt om farene ved å klikke på lenker og bilder i mistenkelig e-post eller på internettsider, er det fortsatt mange som gjør nettopp det. Det er derfor bevisstgjøring og opplæring av de ansatte bør fokuseres på.

Målet for angriperne kan være å få tilgang til informasjon om brukernavn og passord slik at de kan hente ut informasjon, eller plassere eget utstyr inn i virksomhetens infrastruktur. Angriperne er nesten alltid ute etter å tjene penger på informasjonen de får tilgang til.

Det har vært flere eksempler på at ansatte er den nye inngangsporten for hackere. Blant annet ble energisektoren i Norge utsatt for et større angrep i august i år. Utvalgte ansatte mottok falsk e-post hvor klikk på lenker eller vedlegg installerte en spionprogramvare på PC-en. Budskapet i e-posten var troverdig, og angrepet var godt organisert og nøye planlagt.
Formålet med slike angrep er ofte å tilegne seg virksomhetskritisk informasjon, bedriftshemmeligheter og utvidede tilganger til IT-systemer.

Angrepet viser at det blir benyttet mer og mer sofistikerte metoder og at angriperne tenker strategisk for å nå sine mål. Angrepene kan gjennomføres over lengre tid uten at ansatte, IT-avdeling eller samarbeidspartnere vil være i stand til å skjønne at de faktisk er under angrep. Dette kan gjøres gjennom å infisere mye brukte nettsteder og underleverandører, samt med forskjellige former for sosial manipulering (social engineering) mot utvalgte ansatte.

Ettersom angrepet går mot de ansatte og ikke de tekniske elementene virksomheten har kontroll på, er ikke gode rutiner og teknisk sikkerhet tilstrekkelig for å hindre slike angrep. Det må stilles krav til at brukerne vet hva de kan og bør gjøre når de oppdager mistenkelig aktivitet i forbindelse med IKT-systemene.

Det er virksomhetens ledelse som har ansvar for å tilrettelegge for sikring av informasjon og verdier. I dette ligger også å sikre at de ansatte får tilstrekkelig opplæring. Det bør også etableres rutiner og retningslinjer for bruk av IT-systemene og hvordan eventuelt sensitiv og virksomhetskritisk informasjon skal behandles.

For en potensiell angriper vil de ansattes brukernavn og passord være en mulig vei til informasjon. Hvor lett det er å få tilgang til dette for en angriper avhenger blant annet av om de ansatte har fulgt rådene som blir gitt. Har de for eksempel forskjellig passord på alle nettsteder? Etterhvert som vi stadig tar i bruk flere tjenester både privat og på jobb blir det viktigere å sørge for at passordene vi bruker er forskjellige. Det blir med andre ord ikke lettere å være bruker i den digitale verdenen med det første. Fortsatt er det nok mange som har det samme passordet sitt på jobb-PC og private PC. Skulle en ansatt i virksomheten for eksempel miste passordet til Facebook-kontoen sin ville det være uheldig om det er det samme passordet som er brukt på alle IT-systemene på jobb også.

Tap av brukernavn og passord er noe som går igjen ved flere sikkerhetshendelser i år. Senest i september ble det lekket en fil med 5 millioner brukernavn og passord til Google-kontoer. Google påstår selv at de ikke har hatt noen brudd på sikkerheten, så brukernavnene i filen er sannsynligvis samlet inn via phishing angrep (falske kopier av nettsider) mot brukere og fra andre nettsteder. Dette viser hvor viktig det er å ha forskjellig passord på forskjellige tjenester.

Enkle tiltak for å redusere risikoen for tap av passord kan være:

- Bruk av forskjellige passord på forskjellige tjenester. Skill i det minste på jobb og privat. Det finnes elektroniske passordsafer som kan gjøre hverdagen med mange passord litt mer overkommelig.
- Benytte en form for to-faktor autentisering der det er mulig. Flere og flere tjenester tilbyr dette på en fornuftig og enkel måte. Også skytjenester som Google, iCloud Drive, LinkedIn og Dropbox har støtte for dette, men det krever at brukerne velger å ta det i bruk.
- Å innta en kritisk holdning til mail hvor du blir avkrevd for personlig informasjon. Regelen er å aldri oppgi brukernavn og passord eller annen personlige informasjon via en e-post.
- Undersøke merkelige eller uventede beskjeder på mail nærmere før de åpnes. Ikke klikk på lenker eller bilder i disse mailene før du er helt sikker på at det er trygt. Det samme gjelder "hyggelige" meldinger om premier du har vunnet i konkurranser du ikke har deltatt i.

At de ansatte i din virksomhet vil bli forsøkt angrepet via e-post eller tjenester på Internett er sannsynlig.

Et tiltak som vil være med på å avdekke hvilke risikoer de ansatte og virksomheten er utsatt for er å gjennomføre en risikoanalyse. En risikoanalyse vil gi svar på hvilke trusler virksomheten står overfor, hvilke verdier som må beskyttes, hvilke konsekvenser en sikkerhetshendelse kan få og hvor sannsynlig det er at den inntreffer. Dette vil ikke bare være med på å beskrive behovet for opplæring i virksomheten, men også hvilke andre tiltak som bør treffes for å oppnå ønsket nivå på sikkerhet innenfor IT-området.

Avdekking av misligheter ved hjelp av dataanalyser

Jeanette Vatnemo Rasmussen

Senior Associate, Forensic, KPMG Advisory

Magnus Digernes

Senior Manager, Internal Audit, Risk and compliance Services, KPMG Advisory

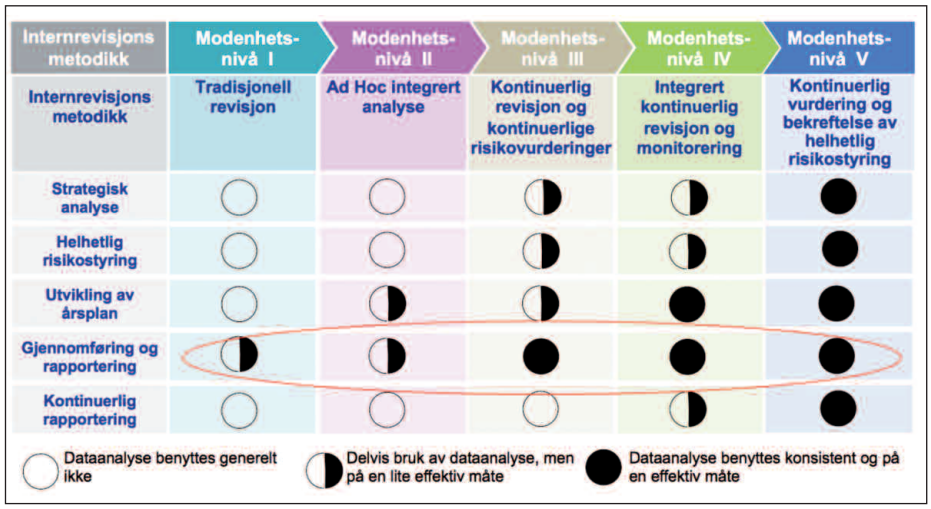
I KPMGs årlige lederundersøkelse[1] opplyser en av tre ledere at deres virksomhet, gjennom de siste fem årene, en eller flere ganger har vært utsatt for en eller annen form for økonomisk kriminalitet. Undersøkelsen viser at det er økonomisk utroskap, underslag, regnskapsmanipulasjon og korrupsjon som rammer norske virksomheter oftest. Det meldes om mange hendelser og forsmedelige tap.

Hvordan kan internrevisjonen avdekke misligheter gjennom dataanalyse?

Internrevisorer spiller en viktig rolle i avdekking av misligheter i selskaper og organisasjoner. I en undersøkelse gjennomført av Association for Certified Fraud Examiners ("ACFE") fremkommer det at 14,1 % av mislighetssakene innrapportert til ACFE i 2014 ble avdekket av internrevisjon[2].

En internrevisjon kan bruke dataanalyse i flere sammenhenger og i alle deler av internrevisjonsmetodikken. Figur 1 illustrerer at dataanalyse benyttes ulikt avhengig av modenhet på internrevisjonsmetodikken.

I det følgende vil vi redegjøre for hvordan internrevisor kan benytte dataanalyse i gjennomføringsfasen for å avdekke røde flagg og eventuelle misligheter i virksomheters regnskapsdata. Dette kan gjøres som kontrollhandlinger i et tradisjonelt internrevisjonsprosjekt, som enkeltstående mislighetsrevisjoner eller kontinuerlige revisjoner og oppfølging /monitorering.



Figur 1

Ulike verktøy kan benyttes for å gjennomføre dataanalyser med fokus på å identifisere røde flagg og misligheter, slik som IDEA, ACL, SQL og i2 Analyst's Notebook for å gjennomføre nettverksanalyser.

Noen av dataanalysene som kan gjennomføres blir nærmere beskrevet nedenfor.

Analyse av inngående fakturaer

Ved å analysere selskapets inngående fakturaer for en tidsbegrenset periode kan man identifisere en rekke røde flagg ved selskapets utbetalinger, som eksempelvis;

- Duplikate fakturanummer, leverandør og beløp for å avdekke mulig dobbeltfakturering fra leverandør
- Fakturaer med feil/mangelfulle data på fakturaen
- Fakturaer med ikke-verifiserbare tjenester

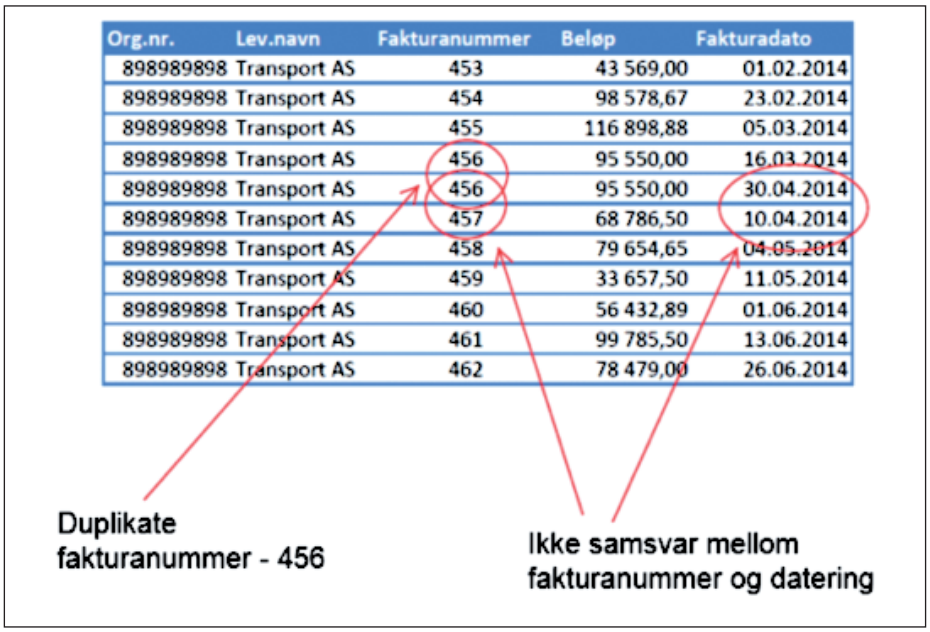
[1] *KPMGs lederundersøkelse 2014 med nærmere 200 norske ledere. Se KPMG.no*

[2] *Association of Certified Fraud Examiners: Report to the nations on occupational fraud and abuse, 2014 Global Fraud Survey*

- Fakturaer med betaling til skatteparadis
- Fakturaer med ulogisk fakturanummerering
- Fakturaer med runde beløp

Listen over hvilke analyser man kan gjøre er lang, og vi vil ikke nevne alle her. Analysene man gjør av inngående fakturaer er spesielt for å avdekke falske fakturaer uten tilsvarende leveranse eller tjeneste som brukes for å skjule for eksempel utbetalinger som er bestikkelser, underslag eller hvitvasking. Omposteringer og korrigeringer kan benyttes for å skjule utbetalinger som skjer uten reelt grunnlag.

Et reelt eksempel fra en dataanalyse gjennomført for en stor norsk kunde avdekket betydelige avvik i selskapets inngående fakturaer. Ved søk på duplikate fakturanummer ble det avdekket flere treff. Det viste seg at det var foretatt utbetalinger flere ganger til samme leverandør. Videre viste det seg at flere fakturaer til samme leverandør var lagt inn med fakturadato som ikke stemte overens med fakturanummeret. Selskapet hadde gjort flere utbetalinger til leverandør med utgangspunkt i uriktige fakturaer. Ved nærmere innsyn i saken viste det seg at de uriktige fakturaene var registrert inn i regnskapssystemet av en ansatt som hadde relasjoner til leverandøren. I dette tilfellet hadde den ansatte kunnet gjennomføre disse transaksjonene på grunn av svakheter ved selskapets internkontroll. Eksempelet er illustrert i figuren 2 nedenfor.



Figur 2: Eksempel inngående fakturaer (fiktive data).

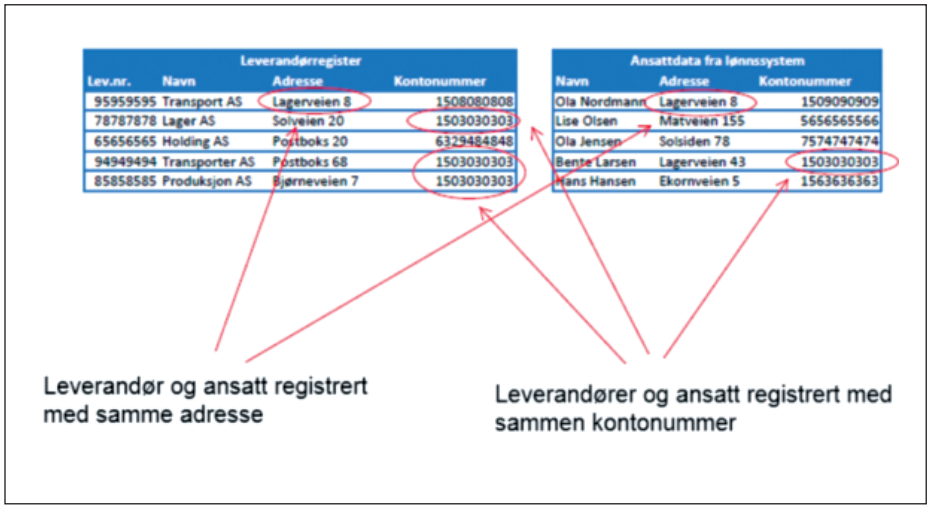
Leverandører

Det kan avdekkes flere røde flagg og misligheter ved å utføre dataanalyser av virksomheters leverandørdata, som eksempelvis leverandører uten eller med ugyldig organisasjonsnummer, duplikate leverandører og fiktive leverandører.

Det at ulike leverandører har identisk bankkontonummer i leverandørregisteret er et rødt flagg, og gir risiko for at ansatte i kommunen har opprettet fiktive leverandører og gjennomført utbetalinger til eget, eller tilknyttede personers, bankkontonummer.

I forbindelse med kryssjekk av data fra leverandørregisteret mot data fra lønnssystemet, ble det avdekket at flere av leverandørene hadde samme bankkontonummer som en ansatt i selskapet. En ansatt i selskapet hadde utarbeidet uriktige fakturaer med fiktive leverandørnavn i selskapets regnskapsdata. Deretter hadde det blitt ubetalt penger til de fiktive leverandørene som hadde et kontonummer som var identisk med den ansatte i selskapet. Eksempelet er illustrert i figuren 3:

Vær oppmerksom på at en ansatt eksempelvis kan endre leverandørens kontonummer for en kort periode for å underslå midler. Denne fremgangsmåten avdekkes ikke gjennom en statisk gjennomgang av master data.



Figur 3: Eksempel fiktive leverandører (fiktive data).

Anskaffelser

Misligheter knyttet til anskaffelser er mest sannsynlig den vanligste formen for misligheter i norske virksomheter. Dette kan omfatte uvanlige anskaffelser, innkjøp utenfor rammeavtale, fakturaer uten tilhørende innkjøpsordre og "budrigging". Uvanlige anskaffelser er innkjøp av varer eller tjenester som ikke inngår i selskapets normale drift og er et rødt flagg som virksomheten bør se nærmere på.

Innkjøp gjennomført uten godkjenning i henhold til virksomhetens fullmaktsmatrise er verdt å følge opp. Store innkjøp gjennomført uten å innhente priser fra flere leverandører kan være et rødt flagg som må ses nærmere på. Andre røde flagg er at anskaffelsen blir delt opp i mindre innkjøp for å komme innunder terskelverdi for innkjøp i virksomheten.

De fleste prosesser og transaksjoner har et naturlig og logisk forløp. Dersom for eksempel en ordredato ligger etter dato for inngående faktura vil det være viktig å følge opp. Innkjøpet kan da være gjort uten at man hadde fått godkjent innkjøpsordre internt.

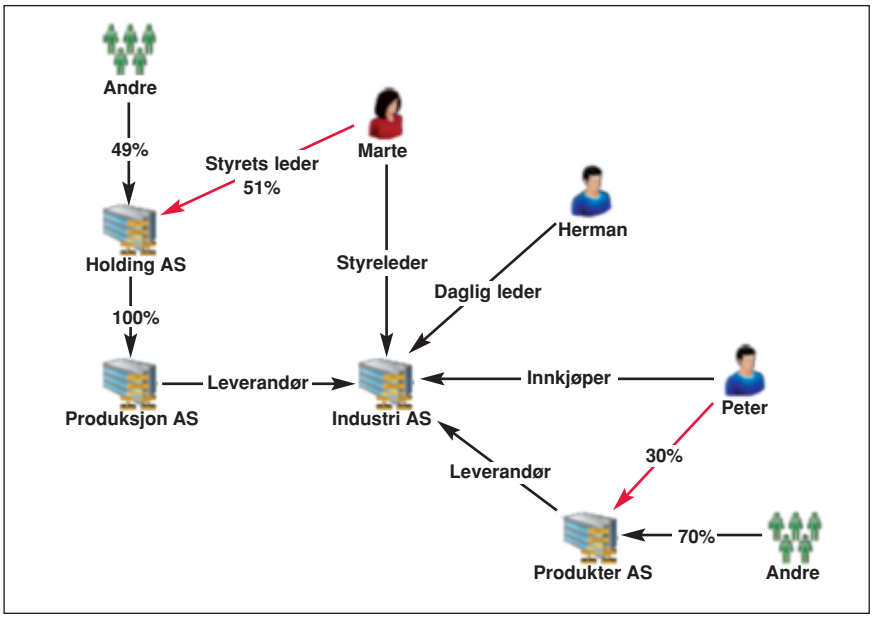
Et annet varselsignal er bruk av mellommenn, konsulenter og tilretteleggere som i tillegg får store honorarer. Slike tjenester kan være reelle, men det kan også være en måte å skjule korrupsjon og bestikkelser på.

Nærstående relasjoner

Transaksjoner med nærstående parter kan innebære en stor mislighetsrisiko. Revisors plikter vedrørende kontroll av nærstående parter er definert i ISA 550. En mulig problemstilling er at personer med ledende posisjoner i et selskap (dvs. daglig leder, styret, hovedaksjonær mv.) kan sette sine personlige interesser foran selskapets interesser og misbruke roller og innflytelse. En statsansatt kan ikke ha bierverv, styreverv og annet lønnet oppdrag som er uforenlige med arbeidsgiverens legitime interesser. De fleste norske selskaper har også egne retningslinjer for innrapportering av verv og mulige interessekonflikter i eksempelvis etisk regelverk.

I Norge er det flere eksempler på vennskapskorrupsjon eller krysstjenester, hvor vi ofte ikke ser direkte linker. Et eksempel kan være at person A kjøper tjenester av en bekjent B sitt selskap til høy pris i bytte mot at person B kjøper produkter på vegne av sitt selskap til høy pris fra selskapet til person A sin kone.

Ved å innhente data fra Brønnøysundregistrene og informasjon om selskapets leverandører og nøkkelansatte, slik som innkjøpsansvarlige, kan vi kjøre analyser for å avdekke hvorvidt det er relasjoner mellom selskapets nøkkelansatte og relevante personer (eiere, styremedlemmer) hos selskapets leverandører.



Figur 4: Nærstående relasjoner (fiktive data).

Figur 4 over viser et eksempel avdekket hos et selskap hvor styreleder i det aktuelle selskapet også var styreleder i holdingselskapet til selskapets leverandør. Videre ble det avdekket at en av de innkjøpsansvarlige i selskapet var deleier i en av leverandørene til selskapet. Den innkjøpsansvarlige hadde vært leder av anskaffelsesprosessen hvor det ble besluttet å inngå avtale med den aktuelle leverandøren. Dette var et klart eksempel på en interessekonflikt og et klart brudd på selskapets retningslinjer.

Lønn

Det kan også forekomme misligheter knyttet til virksomhetens lønnssystem. Vi har sett på at ansatte kan opprette fiktive personer i lønnssystemet og hvorpå disse legges inn med eget kontonummer med påfølgende betalinger. Andre eksempler er at man utelater å fjerne ansatte som har sluttet i virksomheten, for deretter å endre sitt eget kontonummer med påfølgende utbetalinger.

Dataanalyser kan benyttes for å avdekke uvanlige lønnstransaksjoner og til å se på lønnsdata opp mot andre data, som eksempelvis inngående fakturaer eller leverandørdata. Et tips er å analysere hvilke endringer som er gjennomført i faste data, slik som bankkontonummer og adresse, samt hvem som kan og har gjort endringer i lønnsdata. Nærmere bestemt kan man gjennomføre følgende analyser:

- Dobbeltregistrering av ansatte
- Dobbeltregistrering av bankkontoer
- Sammenligne lønnsdata mot ulike datoer
- Store overtidsutbetalinger
- Se på lønnsutbetalinger mot den ansattes HR-data for å avdekke fiktive ansatte

Dette er bare noen av dataanalysene man kan gjennomføre for å avdekke misligheter i virksomheters regnskapsdata og svakheter i virksomheters internkontroll.

Mislighetssaker kan svekke troverdigheten og omdømmet til en virksomhet. Det er derfor viktig at virksomheten tar risikoen for misligheter på alvor. Internrevisjonen har en unik mulighet til å avdekke flere misligheter gjennom en effektiv bruk av dataanalyse.


Foto: Shutterstock

Det er en usikker verden der ute

Ny teknologi og økende globalisering har skapt en verden der spillereglene og risikobildet stadig endres. Gale beslutninger kan fort påvirke omdømme, tillit og økonomiske resultater. Er du derimot godt forberedt, kan du både redusere risikoen og åpne for nye muligheter.

RSM tilbyr tjenester innenfor helhetlig risikostyring, internkontroll og informasjonssikkerhet for både små og store virksomheter, nasjonalt og internasjonalt. Det handler om å beskytte verdier, ta de riktige beslutningene og være forberedt . Det vil både du og dine kunder sette pris på.

RSM – LOKAL KUNNSKAP I ET GLOBALT NETTVERK

RSM er medlem av RSM International, et av verdens ledende tilbydere av revisjons- og rådgivningstjenester. I Norge har vi kontorer i Oslo, Bergen og Voss. Les mer på **www.RSMI.no**

Kontakt *Kent Kvalvik, mobil 965 19 700, e-post kk@rsmi.no*

RSM Audit • Tax • Advisory Celebrating 50 years 1964 - 2014

Korrupsjon og foretaksstraff – Hva forventes av norske virksomheter?[1]

Av Christine Wendt, Contract Advisor, Aker Solutions

I stortingsmeldingen «Næringslivets samfunnsansvar i en global økonomi»[2] slår regjeringen klart og tydelig fast at det forventes at norske bedrifter motarbeider korrupsjon, etablerer varslingsmekanismer og utvikler interne regler og retningslinjer. Det følger også av bestemmelsen om foretaksstraff at opplæring, kontroll og andre tiltak skal vektlegges i avgjørelsen av om selskapet skal straffes, men om hva som kreves av slike tiltak er forarbeidene tause.

Det forventes altså at bedriftene regulerer seg selv strengt, men uten noen direkte plikt til internregulering og uten klare retningslinjer.

Risikoen for korrupsjon er stor, og det samme er konsekvensene for de involverte selskapene. Ikke bare bøter og rettighetstap, men også tap av omdømme kan koste et selskap mye. Korrupsjonsbekjempelse blir dermed ikke bare en juridisk forpliktelse og et etisk standpunkt. Det er også i bedriftenes egeninteresse å ta avstand fra og forsøke å unngå korrupsjon.

Foreign Corrupt Practics Act (FCPA)[3] og UK Bribery Act (UKBA)[4] er interessante lover da de i hovedtrekk er svært like de norske bestemmelsene om korrupsjon og foretaksstraff. Dette gjelder både hva man kan straffes for, og vilkårene for at straff inntreffer. UKBA skiller seg ut ved at den pålegger britiske myndigheter å fremlegge retningslinjer som selskapene må følge, dersom de skal unngå foretaksstraff for korrupsjon.

Det britiske justisdepartementet har utgitt en guide med seks prinsipper som er ment som retningslinjer som bedrifter skal følge for å unngå korrupsjon. Disse seks prinsippene er kort fortalt; «Proportional Procedures» – tiltakene må være utformet og tilrettelagt ut fra bedriftens risiko; «Top-level Commitment» – tiltakene må springe ut fra bedriftens ledelse; «Risk Assessment» og «Due diligence» – det må fortløpende foretas risikovurderinger av samarbeidspartnere, land, ansatte etc.; «Communication and Training» – fokus på opplæring og treningsprogrammer for å heve bevisstheten og kunnskapen til ansatte og til sist «Monitoring and Review» – som pålegger selskapet å holde følge med forandringer i regelverk og kutymer på områder hvor de opererer.[5]

FCPA stiller ingen lignende krav om retningslinjer, men blant annet er varslervern gitt betydelig oppmerksomhet i deres kamp mot korrupsjon. En egen lov, «The Sarbanes-Oxley Act» (SOX) fra 2002, regulerer varsling av økonomisk kriminalitet. Denne loven gjenspeiler i stor grad de norske reglene om varsling i arbeidsmiljøloven, men norsk lov gir her et bredere vern enn SOX. Amerika strekker seg likevel lenger på et punkt. I 2006 fastsatte det amerikanske skattevesenet, IRS, at mellom 15 og 30 % av straffebeløpet i korrupsjonssaker skulle tilfalle varsleren, såkalt «insentivbasert varsling». Dette kan sies å gjøre Amerika til et av landene med bredest varslervern i verden og tilsier i prinsippet at man kan tjene penger på korrupsjon man selv har medvirket til.

Store endringer i flere lands lovverk og det nye fokuset på korrupsjonsbekjempelse førte til Transparency Internationals (TI) utgivelse av «The Business Principles for Countering Bribery» i 2003. «Beskytt din virksomhet! Håndbok i antikorrupsjon for norsk næringsliv» bygger på disse prinsippene og ble utgitt av TI-Norge i 2009. TI-Norge oppfordrer alle norske bedrifter til å følge disse prinsippene for å etablere og opprettholde anti-korrupsjonsprogrammer. TIs prinsippene går ut på det samme som UKBA, men på noen områder strekker TI seg enda lenger.

Ifølge TI er det særlig viktig med fokus på åpenhet som en del av et godt anti-korrupsjonsprogram, både når det gjelder selve programmet, etiske syn, økonomi og organisasjonsopplysninger.[6] I og med at korrupsjon er noe som foregår i det skjulte, vil større åpenhet vanskeliggjøre at korrupsjon forekommer, samt bygge tillit hos ansatte, forretningspartnere, investorer og ikke minst hos myndighetene. TI fremhever også nytten ved å kommunisere konsekvensene av korrupsjon og mener det burde komme tydelig frem at overtredelse er uakseptabelt og vil medføre disiplinærtiltak. Videre vektlegger TI også at det må være enda større fokus på varsling og et sunt varslingsmiljø i bedriften.[7]

TIs prinsipper gir en god oversikt over hva selskaper burde tenke på når de igangsetter anti-korrupsjonstiltak. Prinsippene er likevel bare veiledende og ikke lovpålagte retningslinjer utgitt av myndighetene, slik som i Storbritannia hvor selskapene vet hva de har å forholde seg til dersom de ønsker å beskytte seg mot foretaksstraff.

---

[1] Denne artikkelen springer ut av min masteroppgave «Korrupsjon og foretaksstraff – Betydningen av forebyggende tiltak i «kan»-vurderingen i strl. § 48a ved korrupsjonstilfeller, og behovet for klarere retningslinjer på området» fra UiB våren 2014. Oppgaven er i sin helhet publisert på nettsidene til Transparency International Norge. Se http://www.transparency.no/2014/09/10/korrupsjon-og-foretaksstraff/ .

[2] Stortingsmelding om «næringslivets samfunnsansvar i en global økonomi», nr. 10 (2008-2009).

[3] Foreign Corrupt Practices Act 1977, amerikansk korrupsjonslovgivning.

[4] UK Bribery Act 2010, korrupsjonslovgivning i Storbritannia.

[5] Det britiske justisdepartementets «guidance» s. 21-31.

[6] TI-Norge sin undersøkelse «åpenhet i selskapsrapportering» s. 126-127.

[7] «Beskytt din virksomhet! Håndbok i antikorrupsjon for norsk næringsliv» s. 36-41.

I Norge er det Økokrim som fungerer som både etterforsker og påtalemyndighet i saker om økonomisk kriminalitet. Økokrim har utarbeidet en egen sjekkliste, bygget på momenter fra norsk rettspraksis, over hva rettssystemet forventer av foretakene for at de skal kunne slippe straff selv om korrupsjon har funnet sted. Førstestatsadvokat Arnt Angell i Økokrim har uttalt at «om foretaket har alt på stell, så er det ikke noen mening å straffe bedriften».[8] Denne listen blir slik sett et viktig holdepunkt for selskaper som ønsker å beskytte seg.

Momentene Økokrim trekker ut fra norsk rettspraksis har store likhetstrekk med prinsippene i UKBA og TIs håndbok. Det stilles således allerede i praksis strenge krav til selskapenes anti-korrupsjonsprogrammer for at de skal få betydning i formildende retning. Tiltakene skal ifølge Økokrim også være grundig implementert, og krever tett oppfølging. Det kreves stor åpenhet og velvillighet fra selskapers side for å få gjennomført alle tiltak.

Av norsk rettspraksis på området finnes det per dags dato kun en Høyesterettsdom, den såkalte Norconsult-dommen. Selskapet ble til slutt frikjent i Høyesterett, men spørsmålet om selskapet hadde gjort nok for å forebygge korrupsjon ble til tross for frikjennelsen besvart negativt av flertallet. Selskapet ble frikjent med hovedvekt på den lange tiden som hadde gått, og at selskapet i mellomtiden hadde innarbeidet grundige anti-korrupsjonsprogrammer. Flertallet i dommen er tydelig på at det kreves klare og konkrete retningslinjer innad i selskapet, rutiner for håndtering av korrupsjonsspørsmål og en jevn oppfølging av disse og risikoutsatte områder.[9]

Også annen rettspraksis på området for foretaksstraff er av betydning. En gjennomgang viser at de samme kravene til forebyggende tiltak går igjen i de fleste dommer de siste 30 årene. Dommene viser at det stilles strenge krav til retningslinjer, instrukser, gjennomføring, oppfølging og opplæring av de ansatte. Selskapene må sørge for etterlevelse, samt foreta risikovurderinger av bedriften selv, områder det opererer på og av mulige samarbeidspartnere. Det stilles også krav om effektiv internkontroll, samt sanksjoner innad i selskapet ved brudd.

Det er mye som taler for at Norge burde etablere retningslinjer, tilsvarende det Storbritannia har fått i UKBA, for å få det klart på papiret hva som kreves. Samtidig ser man at de samme krav til forebygging og tiltak som man finner både i UKBA, TI-Norges prinsipper og Økokrims sjekkliste også ligger til grunn for Høyesteretts momenter i norsk rettspraksis på området.

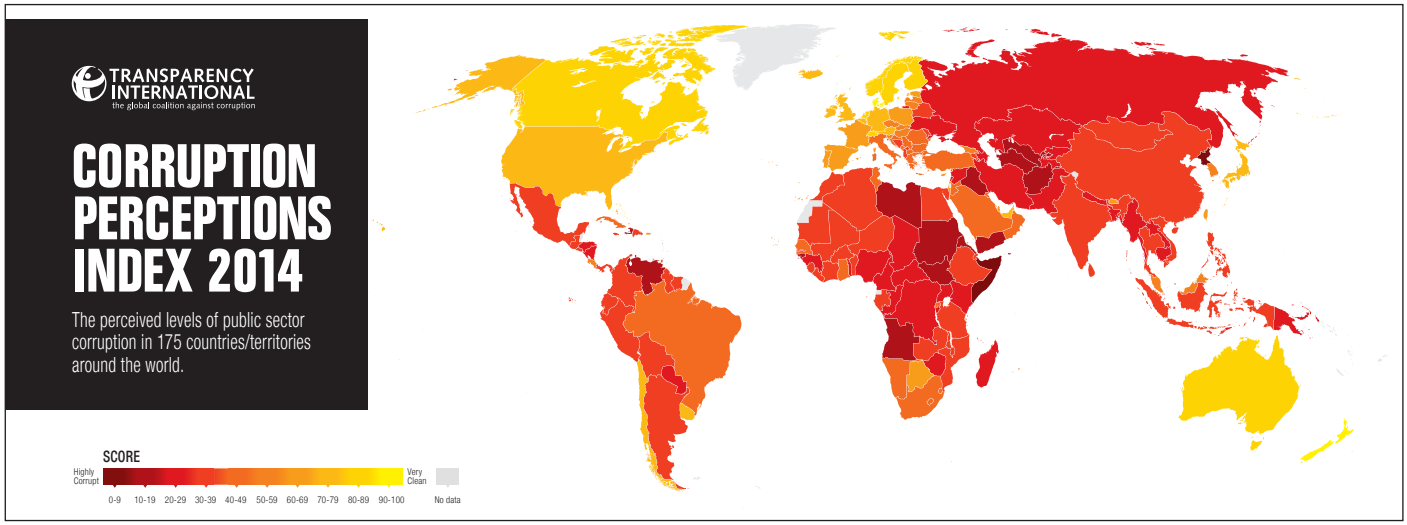
Slik sett kan ikke selskapers krav til forutberegnelighet sies å bli tilsidesatt. Rettspraksis er allmenn tilgjengelig informasjon, som i hvert fall større bedrifter med internasjonal virksomhet relativt enkelt burde kunne få fatt i.

Når de nye bestemmelsene i 2005-straffeloven trer i kraft vil det bli enklere for Økokrim å pålegge selskaper foretaksansvar. Den nye § 48b bokstav h) tilsier at korrupsjon blir en typisk overtredelse som taler for at foretaksstraff skal ilegges. I tillegg blir det etter den nye korrupsjonsbestemmelsen § 27 ikke lenger et krav om at det må være utvist noen form for skyld. Det kan da bli enda viktigere med klare og konkrete retningslinjer til bedriftene å følge for å kunne verne seg mot foretaksstraff.

Dagens kamp mot korrupsjon tilsier også at myndighetene burde utarbeide klarere retningslinjer, rett og slett fordi iverksettelse av dyptgående anti-korrupsjonsprogrammer vil vanskeliggjøre at korrupsjon forekommer og slik sett støtte opp om straffebudenes ønskede preventive effekt. Dersom det for eksempel ble stilt større krav til åpenhet rundt selskapsform og selskapets økonomi, ville det blitt vanskeligere å bedrive korrupsjon.

Korrupsjonsproblemet skyldes langt på vei manglende vilje, heller enn manglende kunnskap. Innføring av dyptgående og gode anti-korrupsjonsprogrammer vil kunne bidra til å oppnå en holdningsskapende og holdningsendrende effekt på både ledelse, styre, ansatte, samarbeidspartnere, varslere og resten av samfunnet. Ikke minst ville slike programmer bidratt til å få et sunnere varslingsmiljø, der varsling anerkjennes som den samfunnsnyttige handlingen den faktisk er. Med et nytt syn på varsling ville flere korrupsjonshandlinger komme frem i lyset, kanskje også i tide til å kunne forhindre at ugjerningene blir gjennomført.

[8] *Uttalt på PwCs seminar om forebygging av korrupsjon og misligheter (april 2014).*
[9] *Rt-2013-1025 s. 69.*



Gjengitt med tillatelse fra Transparency International Norge

Grov økonomisk kriminalitet i 1 av 4 norske virksomheter

Martha C. W. Lind er jurist i Ernst & Youngs granskingsavdeling med spesialkompetanse innenfor områdene compliance, antikorrupsjon, antihvitvask og integrity due diligence.

Hanne Oppen Bieker er siviløkonom fra NHH og manager i Ernst & Youngs granskingsavdeling med spesialkompetanse innenfor områdene forebygging og gransking av misligheter, compliance, risikoanalyse, antikorrupsjon og antihvitvask.

Mange tror at korrupsjon, underslag og andre økonomiske misligheter i liten grad skjer i norske virksomheter. Resultatene av EY Global Fraud Survey som ble publisert i juni 2014[1] viser noe annet. I undersøkelsen kommer Norge langt opp på lista over land med høy andel av grov økonomisk kriminalitet de siste to årene. Hvilke ulike faktorer kan forklare dette resultatet, og hva kan gjøres for å forbedre situasjonen?

I EY Global Fraud Survey ble 2700 ledere av selskaper[2] i 59 land verden over, hvorav 50 norske, intervjuet om sitt syn på misligheter, korrupsjon og bestikkelser. Et resultat som vekket særlig oppmerksomhet var at hele 26% av de spurte norske lederne svarte at deres virksomhet hadde opplevd grov økonomisk kriminalitet i løpet av de siste to årene. Den høye prosentandelen plasserer Norge på en overraskende 6. plass av 59 land, foran land som for eksempel Russland (16%), Colombia (12%) og Kina (8%). Resultatet er også langt over gjennomsnittet i både Vest-Europa[3] og globalt, som begge er på 12%.

Resultatet er overraskende og det er vanskelig å si noe om årsaken. En mulig forklaring kan være økt bevissthet som følge av relativt stort mediefokus på økonomisk kriminalitet og korrupsjon i Norge de senere årene, samt at det er stadige bedre kontroll- og varslingsordninger i virksomhetene som har ført til at flere saker oppdages og rapporteres.

Et annet interessant resultat i undersøkelsen er forholdet mellom antatte og opplevde misligheter / korrupsjon. Så mye som 40% av lederne på global basis mener at korrupsjon og bestikkelser er et problem i eget land, mens bare 12% opplyser at deres virksomhet har opplevd grov økonomisk kriminalitet de siste to årene. I Norge opplyser kun 14% at de anser korrupsjon som et problem, mens altså hele 26% opplyser å ha opplevd grov økonomisk kriminalitet. Nå inkluderer riktignok begrepet «økonomisk kriminalitet» mer enn bare korrupsjon og bestikkelser, men resultatet er likevel interessant. Det kan blant annet tyde på at definisjonen av korrupsjon og oppfatningen av korrupsjonshandlingenes grovhet varierer mellom ulike land. Det kan være et utslag av at misligheter i større utstrekning avdekkes i Norge sammenliknet med mange andre land.

Vår erfaring fra granskingsenheten i EY, er at det er særlig tre områder som peker seg ut i arbeidet for å forebygge og avdekke økonomiske misligheter;

- en effektiv varslingskanal,
- et virksomhetstilpasset anti-mislighetsprogram, inkludert anti-korrupsjonsprogram, samt
- ledelsens fokus på å bygge en god etisk kultur i virksomheten, blant annet gjennom en klar "tone at the top"

En effektiv varslingskanal får mislighetssakene opp i lyset

Det fremkommer av undersøkelsen at hele 82% av norske virksomheter har innført en varslingsordning. Dette er langt over gjennomsnittet i Vest-Europa som ligger på 53%. At så mange norske virksomheter har etablert varslingskanal skyldes nok primært at den norske arbeidsmiljøloven gir arbeidstaker rett til å varsle om kritikkverdige forhold på arbeidsplassen og pålegger arbeidsgiver en plikt til å tilrettelegge for slik varsling[4].

Association of Certified Fraud Examiners (ACFE) gjennomfører annethvert år en undersøkelse hvor de blant annet kartlegger hvordan misligheter oppdages[5]. Siden 2002 har resultatene vist at tips er svært effektivt for å avdekke misligheter. I de siste tre ACFE undersøkelsene har tips stått for oppdagelsen av over 40% av mislighetssakene, mens internrevisjonen til

---

[1] *Overcoming compliance fatique - reinforcing the commitment to ethical growth*
http://www.ey.com/Publication/vwLUAssets/EY-13th-Global-Fraud-Survey/$FILE/EY-13th-Global-Fraud-Survey.pdf

[2] *Selskapene som er med i undersøkelsen representerer relativt sett store selskaper i hvert land, fordelt på ulike bransjer.*

[3] *Vest-Europa er definert som Østerrike, Belgia, Finland, Frankrike, Tyskland, Hellas, Irland, Italia, Luxembourg, Nederland, Norge, Portugal, Spania, Sverige, Sveits og Storbritannia*

[4] *Arbeidsmiljøloven §§ 2-4, 2-5 og 3-6*

[5] *Report to the Nations on Occupational Fraud and Abuse. 2014 Global Fraud Study*
http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

sammenligning avdekker rundt 14% og IT-kontroller 1%.

Tilsvarende er det forventet at virksomheter som tilrettelegger for varsling på en god og hensiktsmessig måte også avdekker flere tilfeller av misligheter. En effektiv varslingsordning vil derfor være en fornuftig investering for å få potensielle saker opp i dagen. Varslingen bør også kunne skje anonymt via telefon, post eller en sikker elektronisk løsning. Videre må behandling av innkomne varsler ivareta alle relevante lovkrav.

Et virksomhetstilpasset anti-mislighetsprogram må gjenspeile selskapets faktiske risiko

Misligheter er en operasjonell risiko, og håndtering av misligheter bør inngå som en del av virksomhetens overordnede system for risikostyring og internkontroll. Alt arbeid med å forebygge misligheter bør være risikobasert i den forstand at man har fokus på de områdene som anses mest kritiske for virksomheten, og hvor risikoen er størst.

De siste årene har det vært flere store økonomiske straffesaker i Norge som har fått mye medieoppmerksomhet. Den hyppigst forekomne formen for økonomiske misligheter er underslag/ økonomisk utroskap. Det er ofte betrodde personer med god kompetanse og mulighet til å tilsløre mislighetene som begår handlingene. Av saker som har fått bred omtale i media siste året kan nevnes saken hvor en finansdirektør i et kjent forlagshus urettmessig overførte millionbeløp til seg selv. Den påfølgende granskingen skal ha avdekket at finansdirektøren gjennom en større mengde transaksjoner over flere år hadde underslått til sammen 9,4 millioner kroner. Saken ble avdekket ved en tilfeldighet internt i forlaget.

I tillegg til de mer tradisjonelle økonomiske mislighetene som underslag/ økonomisk utroskap, ser flere og flere norske selskaper nødvendigheten av å sette korrupsjonsrisiko på dagsorden. Korrupsjon medfører ikke bare omdømmetap, eventuelle tap av kontrakt eller utestengelse fra offentlig anbud og straffereaksjoner overfor individer, men også risiko for foretaksstraff. Både norske og utenlandske myndigheter strammer i økende grad grepet med strengere korrupsjonslovgivning og håndheving. Selskapet Yara ble nylig ilagt et forelegg på 295 millioner kroner for bestikkelser av høytstående offentlige tjenestemenn i Libya og India, samt bestikkelser av en leverandør i Russland. Til sammen dreier det seg om avtaler om bestikkelser for cirka 12 millioner USD. Forelegget er akseptert av selskapet og er det største som hittil er utstedt i Norge. Av andre saker kan nevnes rettssaken (som startet høsten 2014) mot flere tidligere ledere i det kommunalt eide selskapet Unibuss, deriblant den tidligere administrerende direktøren. Saken dreier seg i hovedsak om bestikkelser i forbindelse med kjøp av busser, inkludert privat oppussing utført av underleverandører som ved fiktiv fakturering ble betalt av Unibuss. Så langt er 11 personer tiltalt, siktet eller dømt i denne korrupsjonssaken. I 2011 viste EY Global Fraud Survey at 14% av norske ledere mente det var akseptabelt med rene pengegaver for å vinne eller beholde kunder dersom det hjalp virksomheten i økonomiske nedgangstider. I 2014 hadde andelen som syntes pengegaver var akseptabelt falt til 4%. I samme tidsperiode hadde andelen ledere som bekreftet at de hadde gjennomført anti-korrupsjonsopplæring økt fra 30% til 74%. Dette kan tilsi at økt oppmerksomhet, kunnskap og bevisstgjøring om korrupsjon har stor påvirkning på ledernes oppfatning av hva de oppfatter som akseptabelt. Som følge av dette vil de i større grad enn tidligere kunne gjenkjenne korrupsjonsscenarier og hvilke konsekvenser disse kan ha for egen person og virksomheten.

***Tone at the top* - essensielt for å bygge en helhetlig integritets- og compliancekultur**

I følge EY Global Fraud Survey 2014 opplyser 94% av de norske respondentene at deres virksomhet har et internt anti-korrupsjonsregelverk. Videre fremgår at 92% av virksomhetene har klare sanksjoner for brudd på slikt regelverk. Det fremgår også at i 90% av de norske virksomhetene hadde ledelsen tydelig kommunisert forpliktelsen om å etterleve anti-korrupsjonsregelverk.

Både styret og ledelsen bør spille en sentral rolle i etableringen av grunnleggende kjerneverdier, etisk regelverk og effektive complianceprogrammer, eksempelvis innen anti-korrupsjon. Styret og ledelsens integritet og etterlevelse av virksomhetens etiske verdier påvirker kulturen i virksomheten, og hvilke rutiner og regler som blir fulgt, omgått eller ignorert. I følge ACFE er det en klar sammenheng mellom uklar eller fravær av *tone at the top* og risikoen for misligheter i virksomheten[6].

Gjennom opplæring og trening må det videre sikres en omforent forståelse hos virksomhetens ansatte av hva som er forventet for å bygge en kultur med høy etisk standard. Effektive sanksjoner for dem som bryter normene, samt det å motivere de ansatte til å varsle dersom de mistenker overtredelser, er også viktig.

En virksomhets etiske regelverk/complianceprogrammer søker typisk å definere hva som er akseptabel og forventet adferd av virksomhetens ansatte i ulike situasjoner. Et omforent begrepsapparat er viktig for at de ansatte skal definere korrupsjon på samme måte og tolke situasjoner tilnærmet likt. Eksempelvis det å forstå at de er i en situasjon hvor de blir avkrevd en fasiliteringsbetaling, og å vite hvordan de skal håndtere dette i henhold til virksomhetens interne regelverk.

Virksomheter som definerer lovlig og ulovlig praksis, sørger for et omforent begrepsapparat i virksomheten, og skaper en compliancekultur for årvåkenhet med hensyn til hvilke handlinger som er i henhold til internt regelverk og gjeldende lovgivning, legger til rette for at kritikkverdige og ulovlige handlinger vil kunne bli avdekket og rapportert.

Avslutning

Store selskaper kan være bedre rustet enn små og mellomstore selskaper til å avdekke misligheter, fordi de kan sette av mer ressurser til forebyggende og avdekkende handlinger. På den andre siden har store selskaper gjerne mer uoversiktlig struktur, prosesser og tilgangskontroller, flere nivåledere samt høyere omsetning, slik at uregelmessigheter enklere kan gå under radaren enn i et mer transparent og mindre selskap. Uansett størrelse er det imidlertid vår erfaring er at en helhetlig integritets- og compliancekultur der ledelsen og styret setter den etiske standarden både i ord og handling, tilrettelegger for en varslingskultur, samt etablerer et effektivt og virksomhetstilpasset anti-mislighetsprogram er en grunnleggende suksessfaktor i bekjempelsen av økonomisk kriminalitet og misligheter.

[6] *Jf. Association of Certified Fraud Examiners, www.acfe.com*

Beste praksis på compliance-området

Izabella Salicath, Compliance Manager, Abbvie

”Compliance” er en foretaksfunksjon som vokser frem i stadig flere bransjer. Dog synes det ikke å foreligge noen klart etablert generell og bransjeuavhengig compliancemetodikk. Med utgangspunkt i et historisk tilbakeblikk på utviklingen av funksjonen kan man se at to ulike sektorer har vært viktige drivere for compliancefunksjonen, dog med noe ulikt utgangspunkt. En av disse er finansbransjen og spesielt verdipapirsektoren – der compliancefunksjonen er en del av konsesjonskravene for foretakene. Den andre er industrisektoren – hvor for eksempel antikorrupsjons-regelverk som FCPA (Foreign Corrupt Practices Act) og UK Bribery Act trigger behovet for et velfungerende compliance-program. Er det mulig å finne noen kjennetegn i de ulike bransjene som jobber med compliance og som kan danne et utgangspunkt for en generell compliancemetodikk?

Finansindustrien og Verdipapirforetak

Risikostyringsforskriften er det nærmeste vi kommer en generell hjemmel for en compliancefunksjon innen finans i Norge. Merk at begrepet ”compliance” ikke nevnes i forskriften. Formålet med forskriften er å bedre foretakenes risikostyring og internkontroll gjennom å utdype styrets og ledelsens ansvar utover det som følger av selskapsrettslige regler og regler i særlovgivningen. Forskriften er generelt utformet og presiserer at foretakenes risikostyring og internkontroll skal tilpasses virksomhetens art, omfang og kompleksitet.

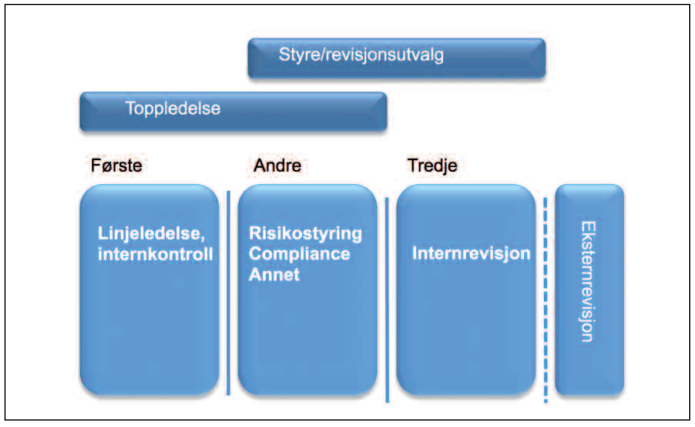
Det er særlig implementeringen av MiFID som har formalisert kravene til compliancefunksjonen i verdipapirforetak. I tillegg til de omfattende operasjonelle adferdskravene som følger av MiFID, er MiFIDs krav til organisering av virksomheten inntatt i verdipapirhandelloven. I Norge har vi derfor særskilte lovhjemler for compliance i verdipapirfondsselskaper og verdipapirforetak. For verdipapirforetakene ble, som en direkte konsekvens av implementeringen av MiFID, kravet til opprettelsen av compliancefunksjonen hjemlet i verdipapirhandelloven med tilhørende retningslinjer i verdipapirforskriften. Finanstilsynet har kommet med omfattende retningslinjer for tolkningen av kravene til compliancefunksjonen gjennom offentliggjøring av tilsynsrapporter (http://www.finanstilsynet.no/ offentlige brev).

Compliance i industri, særlig fokus på anti-korrupsjon

Det er økende fokus på arbeidet med å bekjempe korrupsjon. Myndighetene i flere land har de siste årene fått øyene opp for at korrupsjon er noe som må bekjempes, og da med større involvering fra myndighetenes side. Arbeidet mot korrupsjon tydeliggjøres særlig med implementeringen av FCPA i USA i 1977, og nå også UK Bribery Act, ”UKBA”, i Storbritannia, vedtatt i 2010. Regelverkene har noe ulik tilnærming til straffbarhetsnorm. Eksempelvis er «facilitation payments» straffbart etter UKBA, men ikke etter FCPA. Hovedprinsippene i regelverkene er dog temmelig like. Norge var også tidlig ute med å likestille privat og offentlig korrupsjon. Interessant å merke seg er at FCPA og UKBA regelverket klargjør krav til forebygging som kan beskytte mot ansvar, altså vil et godt compliance-program beskytte mot ansvar. Det er blitt publisert en rekke ulike veiledere som tar for seg hvordan regelverkene skal implementeres, og kanskje aller viktigst, hvordan et compliance-program bør bygges opp, og hva som skal til for at man skal kunne si at man har et velfungerende compliance-program og hvordan compliancefunksjonen skal arbeide. Noen av veilederne som kan nevnes er FCPA Guidelines 2012 (FCPA-veilederen) og Bribery Act 2010 Guidelines (UKBA-veilederen). I tillegg finnes det OECDs 2009 Anti-korrupsjonsanbefalinger kapittel II, *Good Practice Guidance on Internal Controls, Ethics, and* Compliance, publisert i 2010.

Compliancefunksjonens plass i organisasjonen

Når vi snakker om en compliancefunksjon, er det naturlig å se på koblingen mellom risikostyring og internkontroll, og compliancefunksjonen. Det er også nærliggende å se på



Kilde: FERMA / ECIIA ”Veiledning for styrer og revisjonsutvalg”

koblingen mot internrevisjonen. Det kan være en utfordring å finne compliancefunksjonens plass blant ulike funksjoner innenfor kontroll- og risikostyring, samt å finne en hensiktsmessig organisering for å sikre en effektiv arbeidsfordeling mellom disse. Figuren som viser de tre forsvarslinjene er flittig brukt. Kort oppsummert viser figuren at risikoene selskapet møter skal håndteres av de operative ansatte. Støttefunksjonene, deriblant compliance, skal sørge for overvåkning.
I tillegg kommer internrevisjon som tredje linje for å sørge for en uavhengig bekreftelse til styret.

Likheter mellom finans og industri
Utgangspunktene for begge regelverksområdene er en generell utforming. Lovgiver har et ønske om en compliancefunksjon som er tilpasset den enkelte virksomhet. Dette er også bakgrunnen for at det oppstår tolkningsspørsmål. Praksisen til Finanstilsynet med å offentliggjøre tilsynsrapporter gir mer detaljert input på hvordan compliancefunksjonen bør organisere sitt arbeid. Tilgang til den type informasjon er noe knappere i forhold til etterlevelsen av FCPA og UKBA. Topplededelsens engasjement og ansvar i forhold til å gå foran med godt eksempel er et felles moment. Denne faktoren forenkler compliancefunksjonens arbeid med å skape et miljø i organisasjonen hvor compliance blir fremhevet som viktig og noe organisasjonen prioriterer. Det skapes et miljø som er et godt utgangspunkt for de ansattes holdninger, integritet og sunne etiske verdier.

Ut fra en risikovurdering skal selskapets policyer og opplæringsprogram tilpasses selskapets kompleksitet. Risikotilnærmingen er særlig presisert i veilederne til FCPA og UKBA, men også innen verdipapirområdet er det presisert at regelverket skal tilpasses foretakets vurdering av egen virksomhet.

Oppfølging av effektiviteten av complianceprogrammet er momenter som går igjen i begge bransjer. Oppfølging av etterlevelse av policyer og retningslinjer er viktige virkemidler til å kunne avdekke områder som kan virke uklare og ikke etterleves, rapportere på avvik og foreta justeringer. Det er dog ulike tilnærminger til oppfølging.

Begge bransjene har krav til en complianceansvarlig som har autoritet og nok ressurser til å kunne fungere optimalt. I følge korrupsjonsregelverkene skal complianceansvarlig være en av ”top management”. Samtidig har finansbransjen en klar føring på kravene til uavhengighet og objektivitet. Dette er ikke like klart i veilederne til UKBA og FCPA. Arbeidet skal rapporteres og rapporteringen skal være hensiktsmessig. Den skal tilpasses virksomhetens omfang. Art, kompleksitet og rapporteringslinjene, detaljnivå og hyppighet skal tilpasses virksomheten. Dette viser også viktigheten ved å ta utgangspunkt i en risikovurdering av virksomheten. Veilederen til FCPA er noe mer presis i forhold til hvem compliance skal rapportere til og nevner bla. direkte tilgang til styret eller revisjonskomiteen.

Ulikheter?
På verdipapirområdet presiserer regelverket viktigheten av compliancefunksjonens objektivitet og uavhengighet. Dette legger også Finanstilsynet vekt på i sine rapporter. Dette er et moment som ikke blir omhandlet i like stor grad i veilederne til FCPA og UKBA. Det presiseres dog at compliancefunksjonen skal plasseres på riktig sted i organisasjonen for å kunne utøve sitt arbeid på en velfungerende måte. Kan man si at en organisasjonsmessig plassering som sikrer objektivitet og uavhengighet er en forutsetning for en velfungerende compliancefunksjon? I BS 10500:2011 (Specification for an anti bribery management system) kan man lese under punkt 5.2 ”Internal Audit” at det skal innføres interne kontroller for å bla. kunne teste dårlig eller manglende etterlevelse av policyer og retningslinjer på området. Det presiseres at dette skal gjennomføres av en objektiv part slik at man beholder uavhengigheten til den som blir kontrollert. Det er nærliggende å tro at dette punktet viser til en internrevisjonsfunksjon gitt overskriften. Dette punktet presiserer dog videre at objektive kontroller også kan/skal gjennomføres av compliancefunksjonen:

”5.2.6 To ensure the objectivity and impartiality of the audit program, the organization shall so far as is reasonable ensure that the audit is undertaken by:

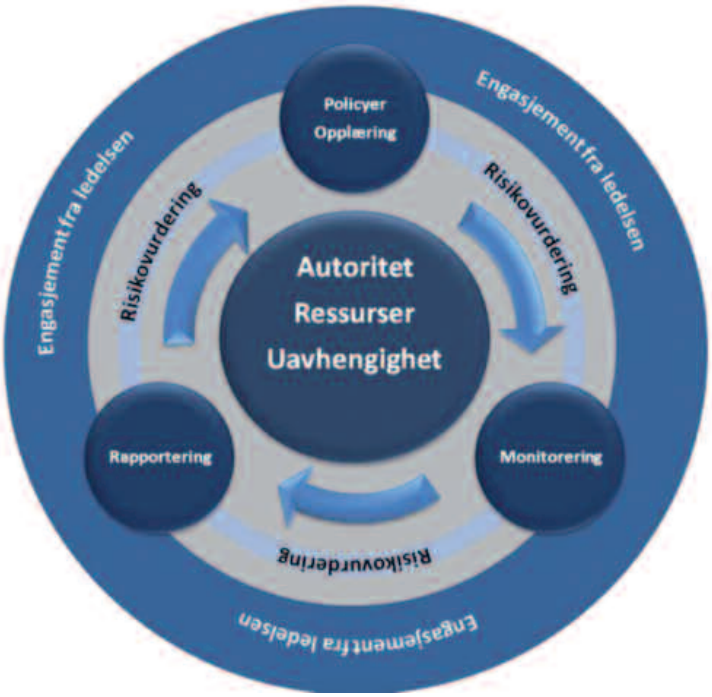
a) an independent function or person within the organization established or appointed for this process; or

b) the compliance manager (unless it is the compliance manager’s own actions which are being audited); (...)”

Det er dog ikke like klart som på verdipapirområdet hvordan arbeidet skal fordeles mellom compliance og internrevisjonen. Det som er viktig å legge merke til, er at kontrollene skal gjennomføres av en uavhengig og objektiv part.

Konklusjon
Driverne bak etableringen av compliancefunksjoner i henholdsvis verdipapir- og industrisektoren er noe ulik. Innenfor verdipapirsektoren er formålet bak rammeverket å sikre markedet effektiv tilgang på kapital gjennom et regelsett som hindrer diskriminering av investorer. Her har altså ønsket om et velfungerende kapitalmarked medført at compliancefunksjonen har blitt en grunnstein i konsesjonsgrunnlaget for foretakene. Innenfor industrisektoren oppstår compliancefunksjonen som en konsekvens av et strengt regelverk som skal etterleves, men det er ikke nødvendigvis en betingelse for å operere i markedet. Selv om enkelte momenter er strengere praktisert i den ene eller den andre sektoren, finnes det noen felles grunnprinsipper som bør kunne danne utgangspunktet for en mer generell compliancemetodikk. En felles compliancemetodikk kan illustreres i figuren under. Egenskapene en stilling som f.eks. en Compliance Officer må ha illustreres i sirkelen i midten.
Det er kritisk for en compliancefunksjon å ha tilstrekkelige ressurser, autoritet og uavhengighet. Dette blir presisert av myndighetene innen begge bransjer. Oppgavene som gjennomføres av en Compliance Officer skal være utarbeidelse av policyer, opplæring, oppfølging og rapportering. Disse illustreres ved hjelp av sirklene rundt kjerneegenskapene. Det er oppgaver som skal gjøres kontinuerlig og som ofte henger sammen. ☞

Compliance Officer skal utarbeide policyer og lære opp de andre i organisasjonene. Deretter skal etterlevelse oppfølges og rapporteres. Ut fra resultatene fra oppfølgingen vil Compliance Officer kunne danne seg et bilde av hvor mye opplæring som kreves. Dårlig etterlevelse kan tyde på vanskelig tilgjengelige policyer og/eller for dårlig opplæring. Det som danner grunnlaget for alt arbeidet er en risikovurdering. Det er risikovurderingen som bestemmer hvilke policyer selskapet skal ha, hvilke områder opplæringen skal fokusere på, og hvilke områder Compliance Officer bør oppfølge særskilt. Rapporteringen er også avhengig av risikovurderingen; høy risiko tilsvarer hyppigere rapportering. Det viktigste av alt er ledelsens engasjement. Uten fokus fra ledelsen mister man ikke bare tilgang på nok ressurser, men mangler god kultur hvor etikk og integritet er i fokus.



NIRF om eksterne evalueringer

Ekstern evaluering handler om å bidra til forbedring av internrevisjonsleveransen. Vi søker å identifisere områder som kan utvikles slik at dere kan fortsette å i enda større grad skape merverdi i virksomheten. Den eksterne evalueringen fungerer også som en bekreftelse til ledelsen og styret på om internrevisjonen er organisert på en optimal måte. I følge Standard 1312 skal en ekstern evaluering av internrevisjonsavdelingen utføres minst hvert femte år. Evalueringen utføres av en uavhengig kontrollør utenfor organisasjonen. Denne eksterne evaluering kan være i form av en full ekstern evaluering eller en egenevaluering med uavhengig ekstern validering. Se våre nettsider www.iia.no/no/ekstern_evaluering/ for mer informasjon om forskjeller i de ulike oppdragene.

Hvorfor NIRF
NIRF er internrevisjonsprofesjonens egen interesseorganisasjon med formål å styrke den faglige og etiske utviklingen innenfor internrevisjon. Vi tilbyr medlemmer et nøytralt og uavhengig alternativ for utførelsen av den eksterne evalueringen.
I utøvelsen av kontrollene benyttes en kombinasjon av faste ansatte og egne medlemmer med god erfaring fra internrevisjonsfunksjoner. NIRF har gjennomført eksterne evalueringer av internrevisjoner fra statlig, privat og finansiell sektor.

Hva kan man forvente
Gjennomgangen vil foruten å bekrefte hvorvidt internrevisjonsavdelingen er i overensstemmelse med standardene, gi en oppsummering av vårt inntrykk av om enheten er organisert på en hensiktsmessig måte, slik at den får utnyttet de ressurser og kompetanse den disponerer for å levere verdiskapende tjenester i tråd med virksomhetens strategier og målsettinger. NIRF ønsker å fremheve profesjonen og dens positive påvirkning i en organisasjon. Vi ønsker å bidra til å belyse for styret og ledelsen hvilken nytte de kan ha av internrevisjonen. Dette kan være en mulighet til å løse opp i eksisterende utfordringer.
NIRF har en konstruktiv tilnærming til oppdraget og søker å skape god kommunikasjon underveis, slik ta det ikke skal være noen overraskelser i rapporten. Samtidig kan en ekstern evaluering være utfordrende. Vi vil bringe med oss ideer og forslag basert på tidligere gjennomganger for å gi verdi og forbedringer til internrevisjonen.

Hvordan
Vår gjennomgang tar utgangspunkt i kvalitetsmanualen fra IIA; *Quality Assessment Manual for the Internal Audit Activity* som vi har tilpasset norske forhold, samt at vi har utviklet egne verktøy som benyttes under gjennomgangen.

Kvalitetssikring av oppdraget
NIRF har etablert en egen overordnet kvalitetskontrollgruppe for å sikre konformitet i alle kontroller og en mest mulig lik vurdering av kriterier og tolkning av standardene. Fire inneværende internrevisjonssjefer utgjør denne gruppen, og rapporten blir gjennomgått og kvalitetssikret av dem.

For mer informasjon ta kontakt med
Hilde Tanggaard, rådgiver i NIRF
E-post: hilde.tanggaard@iia.no
mob: 41107296

COSO i jakten på den forsvunne diamant

Av Hilde Tanggaard, rådgiver i NIRF

COSO 2013 skal gjøre enheter bedre i stand til å tilpasse seg endringer i forretningsmiljø, redusere risikoer til akseptable nivåer og støtte oppunder en hensiktsmessig beslutnings- og styringsprosess. Dette skal bidra til at de når sine mål. Den oppdaterte versjonen av COSO rammeverket understreker behovet for bruk av skjønn og en tydelig link mellom mål, risiko, og tiltak.

Den forsvunne diamant er et brettspill for 2-5 deltakere fra 7 år og oppover. Handlingen utspiller seg i Afrika, i et konkurransepreget miljø med store muligheter og risikoer som røvere, dobbelt gevinst ved diamantfunn på Gullkysten, og insentiver som bonus til første spiller som når Cape Town. Hvilken verdi kan COSO ha i jakten på den forsvunne diamant?

Uten regler fungerer ikke spillet, altså må man etablere et kontrollmiljø. Ikke bare må reglene finnes og være kjent, de må også etterleves. Hvordan sørger man for dette? I dette tilfellet; ved full åpenhet. Det sikrer blant annet at antall plasser man forflytter seg samsvarer med gitt terningkast, riktig turtaking, og at alle pengene blir levert banken ved røverfangst. Videre har en av oss ansvar for banken som forsyner hele Afrika, i tillegg til å være bankkunde. Roller er fordelt. Manglende etterlevelse etterfølges av høylytte protester og umiddelbar korreksjon.

Det er et relativt tøft miljø å operere i - diamantbransjen er en svært konkurransepreget bransje. Det er seier for kun en part. Den store hvite diamanten er hovedmålet. Den finnes under en brikke, et sted i Afrika, og brikken må bli snudd. Hvis dette inntreffer, eller rettere sagt når dette inntreffer, må man hurtig kaste seg rundt. Har man diamanten må man komme seg til mål for å vinne. Har man ikke diamanten, må man finne et visa og så komme seg først i mål. Situasjonen inntreffer, men man vet ikke for hvem eller når. Man kan være i en posisjon langt fra mål, uten penger og langt fra potensielle visabrikker. Hvordan håndterer man denne usikkerheten?

I dette konkurransepregete miljøet er det stor sannsynlighet for både nye muligheter og risikohendelser. Sannsynligheten er svært stor for at du flere ganger kommer til å miste alle pengene dine. Det er imidlertid også svært sannsynlig at du kommer til å oppnå ny opptjening ganske raskt. Mulighetene og farene må vurderes opp mot hovedmålet; diamanten. Man kan i teorien vandre rundt i jungelen, i ørkenen, eller på savannen, og aldri snu en brikke. Det vil imidlertid innebære at man aldri vinner. Og trolig blir du heller ikke invitert til Afrika for å jakte diamanter igjen.

Hvis man velger å gå sjøveien, som man må betale for, er det en fare for at man blir utsatt for røveri på St. Helena, og dermed må stå over ett kast. Er det verdt å ta denne kostnaden og akseptere denne risikoen? Er sjøveien raskeste vei til Cape Town? Vil man dit før de andre? Finnes det heller flere brikker i nærheten som øker muligheten til diamantfunn?

Hvilke trekk gjør de andre? Stor usikkerhet og et stadig skriftende miljø krever kontinuerlig risikovurdering for å kunne fatte beslutninger som sikrer måloppnåelse.
Vi flyr, betaler 3000 dollar, tar sjøveien, betaler 1000 dollar, mottar forskjellig gevinst etter grønt, gult eller rødt diamantfunn. Jeg kan velge å kaste eller å betale for å snu brikker. Når velger jeg å betale? Når vi jakter på samme brikke? Hvem når frem først? Har jeg penger? Har jeg altfor mye penger? Det er spennende, og vi koser oss.

Så hva med muligheten for misligheter; går det an å jukse med så mye åpenhet? Det er behov for en ny skive leverpostei til kveldsmat. En part forlater rommet for å fremskaffe proviant, mens den andre blir igjen i stua med full tilgang til banken og til å lette på brikker. Tillit blir utvist. Muligheten for mislighet er tilstede. Men som typisk norsk hersker det en god porsjon naivitet som gjør at slike kontrolltiltak ikke en gang vurderes. Imidlertid kan det tenkes det bør vaie et rødt flagg om det kommer flere bestillinger fra stua, som sylteagurk og melk.

Samtidig som det er konkurrerende parter og en hard virkelighet i Afrika, er det likevel rom for å utøve en god porsjon samfunnsansvar som ikke går på bekostning av muligheten til seier, men som på sitt vis bidrar til verdiskapning. I et konkurransepreget miljø står det ikke tilbake for at røverfangst etterfølges av en latter med et visst snev av skadefryd hos motparten. Imidlertid kan man selv ha som policy å heie på motparten ved funn av rød diamant, og sympatisere ved tap av aktiva.

Og så har vi alltid muligheten for at det inntreffer en svart svane. Melkeglasset. Det er sølete. Vi må starte på nytt.

Fokus på etikk og compliance

Helene Raa Bamrud
Partner og leder av Enterprise Risk Services i Deloitte Norge.

Endre Fosen
Partner i Enterprise Risk Services.

Line N. Dahl
Manager i Enterprise Risk Services.

Compliance blir stadig viktigere for selskaper på grunn av økte regulatoriske krav og forventninger om etisk atferd fra kunder, investorer og samfunnet for øvrig. Dette medfører at virksomheter må etablere tiltak for å etterleve disse kravene og forventningene, og gjennom det redusere risiko knyttet til omdømmetap, økonomiske tap eller i verste konsekvens foretaksstraff. Dersom selskapene kan vise til at de har implementert et helhetlig compliance- eller antikorrupsjonsprogram, viser tidligere rettsavgjørelser at dette kan være formildende med hensyn til straff.

En rekke norske selskaper har de senere år erfart at det kan være en betydelig risiko knyttet til forretningspartnere, noe som har medført at flere ser nødvendigheten av å implementere forebyggende tiltak knyttet til tredjeparter. Internasjonale retningslinjer og guidelines som UK Bribery Act, FCPA og World Bank Integrity Guidelines har i stor grad vært retningsgivende for complianceprogram.

Deloitte inviterte i september til et seminar hvor resultatene fra to undersøkelser relatert til etikk og compliance ble presentert. En for å kartlegge status i Norge og en for å kartlegge beste praksis internasjonalt, basert på intervjuer med seks globalt ledende selskaper innenfor etikk og compliance. Undersøkelsene ble gjennomført våren og sommeren 2014. Begge undersøkelsene peker på at et robust og helhetlig complianceprogram er basert på en sterk etisk bedriftskultur hvor ledelsen leder an gjennom sine handlinger, samtidig som det er implementert et solid internkontrollsystem som bidrar til å redusere de viktige compliancerisikoene til et akseptabelt nivå. I denne artikkelen presenterer vi utvalgte funn fra nevnte undersøkelser.

Den norske compliancesurveyen viser at norske selskaper har utfordringer knyttet til etterlevelse, og at det investeres for lite i compliancefunksjonen både med hensyn til antall ressurser og budsjett[1]. Den norske undersøkelsen viser i tillegg at teknologi og verktøy må benyttes for å få et mer effektivt complianceprogram. Hele 81% av de norske selskapene viser til at de gjennomfører risikovurderinger årlig eller oftere. De compliancerisikoene som selskapene har størst utfordringer med er tredjeparter, oppfølging av etterlevelse av policy og prosedyrer, samt administrasjon av disse.

Kultur og tonen på toppen

Styret og ledelsens engasjement for å gjøre etiske retningslinjer og compliance til en del av bedriftskulturen er av kritisk betydning for et effektivt complianceprogram. Det er ikke tilstrekkelig at ledelsen snakker om viktigheten av etikk og compliance, de må også vise sitt engasjement gjennom handlinger og beslutninger. Undersøkelsen av internasjonale selskaper viser at compliance og etikk må være kriterier i ledelsens insentivordning og årlige evaluering for å forsterke ledernes handlinger[2]. «Tonen på toppen» har innvirkning på kulturen i selskapet, som videre er toneangivende for atferden til ansatte og retningsgivende for hva som er riktig og galt i organisasjonen. Av den grunn er kulturen sentral for et effektivt complianceprogram. Norske selskaper mener selv at de har en sterk bedriftskultur som bygger på etiske verdier.

Det er styret i selskapet som har det overordnede ansvaret for at compliancefunksjonen har tilstrekkelige ressurser, og de bør være engasjert i evalueringen av effektiviteten til complianceprogrammet. Styret bør delegere myndighet til en person, *Compliance Officer* eller lignende, som

[1] *Deloitte: The Norway Compliance Survey – Risk assessment, August 2014*

[2] *Deloitte og Telenors undersøkelse av beste praksis innen etikk og compliance, 2014*

er ansvarlig for å styre, overvåke og evaluere complianceprogrammet. Selskapet bør etablere en prosess som sikrer at styret er informert om alle brudd på retningslinjer av vesentlig størrelse, og at alle brudd og mistanker om brudd blir rapportert og håndtert. God praksis tilsier at *Compliance Officer* har direkte tilgang til styret ved behov.

Risikovurderinger og internkontroll
Det er avgjørende at virksomheten gjennomfører jevnlige risikovurderinger som omfatter hele virksomheten. Selskaper bør ha etablert en prosess som sikrer at risikovurderingen gjennomføres i alle selskapets enheter, og at identifisert risiko på lokalt nivå løftes til den sentrale delen av organisasjonen. Risikovurderingen utgjør grunnlaget for beslutningen om å etablere risikoreduserende tiltak. God praksis tilsier prosedyrer som klart definerer roller og ansvar i prosessene, hovedaktiviteter med krav og retningslinjer, risikovurdering og tilhørende nøkkelkontroller. Etablering av konkrete nøkkelkontroller i arbeidsprosessene er god praksis og i mange tilfeller helt nødvendig for å sikre etterlevelse.

Det er viktig at risikovurderingen gjennomføres og oppdateres jevnlig, da risikobildet endrer seg kontinuerlig. 81% av norske selskaper sier at de gjennomfører risikovurderinger årlig eller oftere, men det er nok mer varierende hvor mange som knytter risikovurderingene til effektive tiltak og nøkkelkontroller i arbeidsprosessene. Ledende internasjonale selskaper innen compliance har risikovurdering knyttet til compliance som en del av ERM-systemet[3], og har et tett samarbeid mellom funksjonene risk, intern revisjon og compliance.

Håndtering av tredjeparter
Det området norske selskaper sier de har størst utfordring med er compliance knyttet til tredjeparter. For selskaper som opererer internasjonalt er det sentralt å vurdere korrupsjonsrisikoen til leverandører. Det er god praksis å etablere en prosess for å kontrollere og gjennomføre bakgrunnssjekker av forretningspartnere for å avdekke og redusere risikoen knyttet til tredjeparter.
Selskaper med risiko knyttet til leverandører bør i tillegg vurdere å ha egne etiske retningslinjer som gjelder spesielt for tredjeparter. Samtidig bør det utarbeides avtaler om forsvarlig forretningsdrift som blant annet inneholder retten til å inspisere leverandør, til å benytte sanksjoner og til å terminere kontrakt ved brudd.
Ledende internasjonale selskaper gjennomfører trening også av sine forretningspartnere, som for eksempel dilemmatrening og opplæring i etiske retningslinjer.

Et fullverdig compliance-program skal sikre at selskapet er rustet for å forebygge, avdekke og håndtere alle misligheter og brudd på eksterne og interne retningslinjer.

Testing og overvåkning av styringssystemet og compliance programmet
En kritisk suksessfaktor for et effektivt etikk- og complianceprogram er testing og oppfølging av implementering og etterlevelse. Alle policyer, prosedyrer og nøkkelkontroller som er utviklet for å redusere risiko er irrelevante hvis de ikke brukes. Selskapet må sikre at alle ansatte er kjent med og følger selskapets policyer og prosedyrer ved å gjennomføre jevnlig trening og opplæring.

Den globale undersøkelsen til Deloitte viser at det er effektivt at linjeledere og geografiske ledere har ansvaret for implementering i sine enheter. Selskaper som er best i klassen innen compliance har egne treningsprogram for ansatte i land hvor for eksempel risikoen for korrupsjon anses som høy. Selskapet må ha etablert solide kontroller som blir jevnlig testet og overvåket. Dette er viktig for å kunne gjennomføre tiltak for å fjerne avvik og for å sikre kontinuerlig forbedring av programmet.

Undersøkelsen viser også at norske selskaper i liten grad benytter verktøy og teknologi innen complianceområdet. God praksis er å benytte teknologi og verktøy for å jobbe effektivt, sikre implementering, etterlevelse, god kontroll og rapportere til ledelsen og styret.

Et fullverdig complianceprogram skal sikre at selskapet er rustet for å forebygge, avdekke og håndtere alle misligheter og brudd på eksterne og interne retningslinjer. Norske selskaper har en lang vei å gå for å komme på nivå med de beste internasjonale selskapene – men det er en positiv utvikling – og flere selskaper ser nå behovet for å videreutvikle sin compliancefunksjon og sitt complianceprogram.

[3] *Enterprise Risk Management*

Auditing ERM

Interview with Vasilka Bangeova, internal auditor, Swiss Re

By Martin Stevens, internal auditor, Gjensidige

On 31st October we in NIRF were fortunate to receive a visit from Vasilka Bangeova, internal audit director in Swiss Re in London. Vasilka is head of the risk management audit team in Swiss Re.

Vasilka, many people say that it is important to define what the organisation means by risk and risk management – what is your experience from Swiss Re?
In Swiss Re the ERM philosophy is all about more adaptive and intuitive approach to risk. Swiss Re's ERM program is focused on intelligent protection: through understanding planned risks, supporting the taking of good risks and top-down management of the biggest threats. The business is shifting from a strategy of "blanket" protection or 'zero tolerance' to encouraging educated and transparent risk-taking and seizing the opportunity aspect of risk. The ultimate objective is to enable better commercial decisions, without incurring unsustainable cost, thus improving competitive advantage.

How did you find moving to a third line role when you moved from working in Capital and Risk Management to Internal Audit?

Coming from the first or second line gives an appreciation of the complexity and challenges Risk Management faces to strike the optimal balance between educating, challenging and enabling the risk takers who own the core business execution. This is not an easy cultural shift: compliance is no longer only about following rules, but is also about applying knowledge and experience contextually and interpreting risk accordingly. The demand now is for the Risk Management function to focus less on controlling the day-to-day decisions and look more strategically across the business, e.g.: to give an independent perspective and enhance the risk and return profile of the business, influence product development, investment decisions, etc.

In your speech at the Norwegian Business school you identified a further category of audit planning beyond cyclical planning and risk based planning could you explain what you mean by this.

We call this further category ERM internal audit planning. This approach builds on the internal audit's universe of enterprise risks and the key themes from management's top-down risk assessment. ERM planning ensures that risks critical to the business strategy are covered and are adequately mapped to the corresponding business processes. In addition, it allows the flexibility to re-prioritize the audit work and adjust the audit plan in real time as the business and its environment change. Cost optimization and business value come as a by-product of this planning approach as audit resources are reallocated to 'hot spots' and are fully utilized.

Some people have said that the internal auditor's role in a developed governance system is to ensure the second line of defense is working do you agree with this?

I find such a view only partially valid because risk management is a responsibility of everyone in a company and this includes core business execution in the first line as well as activities related to strategy setting, business planning, performance measurement, oversight and reporting. Under Swiss Re's Risk Management Standards the risk management function acts as the risk controller. However, the risk owners and takers reside with the first line of defense and have shared responsibilities for risk identification (including horizon scanning), implementation of controls, monitoring of identified risks, and validation and maintenance of risk models, etc. Internal audit is responsible to provide assurance over the activities of both the 1st and 2nd lines of defense.

In Norway it is common for the internal audit to report either semi-annually or quarterly to the Board but I understand in Swiss Re you have a monthly reporting. Could you explain briefly the content of such a report and who receives it ?

We produce a Monthly Risk Assessment (MRA) business summary, which supports our proposals to the Group Audit

Swiss Re
The Swiss Re Group is a leading wholesale provider of reinsurance, insurance and other insurance-based forms of risk transfer. Dealing direct and working through brokers, its global client base consists of insurance companies, mid-to-large-sized corporations and public sector clients. From standard products to tailor-made coverage across all lines of business, Swiss Re deploys its capital strength, expertise and innovation power to enable the risk taking upon which enterprise and progress in society depend.

Premiums earned in 2013 USD 28.8 bn.
Employees worldwide. 11,500

Committee for changes to the Annual Audit Plan. .The report includes an overview of management and organizational change per business unit and corporate function, significant business developments, changes in the market and regulatory environment, operational incidents and key risk themes under monitoring. The MRA is information sharing mechanism for the audit directors and a business educational tool for the broader internal audit team as it condenses the findings from hundreds of relationship meetings, reviews of committees' packs, specialist publications and intranet posts.

An overview of internal audit in Swiss Re
85 employees located in the USA, Continental Europe, the United Kingdom and Asia.
Reporting lines are organized by business area but operation follows a matrix logic whereby subject matter experts lead or contribute to audits where the audit scope creates demand for their particular skill.

The Risk management audit team comprises three specialists in financial, actuarial and other insurance risk and capital management. It is complemented by 'Risk Management ambassadors' - a virtual team of co-opted auditors from other teams who have local business knowledge and are trained in various risk management topics.

In the auditing standards it is stated that the internal audit should assess whether appropriate risk responses are selected that align risks with risk appetite. Do you have any suggestions as to how an internal auditor might plan such an audit?

In each audit at Swiss Re we report explicitly on the quality of the management's self-assessment of residual risk. We look for evidence that our auditees are familiar with the risk appetite statement relevant for their area of responsibility. We audit the governance process for making decisions on management response to risk (e.g. control, accept or transfer). We test how risk exposure is measured against appetite; we also assess the quality of related monitoring data and the validation of underlying models and measurement methodologies. In addition, we audit the group-wide process for setting risk appetite, for communicating it to business units and for 'translating' it into a set of limits and key risk indicators.

In your speech you presented a two lens approach to auditing ERM. Could you give a brief explanation of these two approaches and what in your opinion are the main challenges for internal audit ?

The two lens approach analyzes ERM into organizational and individual (human) components. Then for each component internal audit considers both the 'tangible' characteristics (i.e. capabilities one can measure) and the 'soft' attitudes and behavior (i.e. motivation). The organizational view captures policies and standards, risk appetite and limit setting, as well as the 'soft' risk culture: corporate values and tone from the top. The individual view looks at employees' skills and competences and how employees' controls related behaviors are influenced by remuneration policies and career management practices.

The main challenges for internal audit arise from the need for new skills and higher flexibility in stakeholder management. For example, in an ERM environment we now need experts in complex quantitative techniques to audit causal models but also specialists in behavioral psychology who can assess how people anticipate and influence risk outcomes. Audit methodology and the assurance products also need to evolve: judgmental areas do not lend themselves to sample testing; it is also a very delicate balancing act to remain independent and deliver business value, especially when assessing ERM's role in steering business performance and resilience (as opposed to hazard avoidance).

How is internal audit work aligned and coordinated with that of the second line without breaching internal audit's independence?

Swiss Re's Group Internal Audit (GIA) operates an Integrated Assurance Framework (IAF) together with Operational Risk Management (ORM) and Compliance. This is a platform for information exchange supporting coordinated risk assessment, assurance planning, and issue monitoring and reporting. The IAF uses common risk heat maps, which capture senior management's top-down risk assessments and link to key strategic initiatives. GIA opines on the effectiveness of the activities performed by the 1st and 2nd lines of defense, however GIA leverages management's risk and controls self-assessment, the key ORSA conclusions and the findings of ORM and Compliance risk reviews. GIA's independence is maintained via its reporting line and budget approval by the Audit Committee, 'operational immunity' in recruitment and remuneration policies, clear mandate definition and observance of professional standards.

Vasilka Bangeova
Vasilka is a qualified accountant with 13 years post-qualification experience and a student of the UK Institute & Faculty of Actuaries. Prior to joining Swiss Re, Vasilka headed the aggregation of Group available economic capital of a global listed insurer and led a Solvency II Model Validation team. She has 16 years of experience in insurance, pensions and banking in various roles with Big 4 firms, boutique consultancies and internal audit functions. Vasilka has led large cross-border projects for re-engineering of business process, development of IT strategies, financial due-diligence, private placements and AIM listings. Vasilka has also advised regulators in Eastern Europe and Central Asia on the implementation of IFRS and Basel II.

Finally I believe this was your first time in Norway. We apologise for the dreary late autumn weather, but apart from that what were you first impressions of Norway and its inhabitants.

Well, I am very well trained by the British weather, so the rain in Oslo did not deter me from indulging into my other passions: modern architecture and sculpture. I enjoyed the vibrant vibe of the city but could also relate to its reflective coastal views. Everyone I have met and spoken to on my first visit to Norway met me with a smile, openness and curiosity, I felt welcome and comfortable and am definitely coming back in the spring to experience the fjords.

Thank you Vasilka and we hope that you may visit us again soon when the weather will be hopefully a bit more on the sunny side.

Internrevisjonsinstruksen

Hilde Tanggaard, rådgiver i NIRF

Silje Evjen Hansen, seniorrådgiver i Forsvarsdepartementets internrevisjon

I forbindelsen med studiet *Internrevisjon; Governance - Risikostyring - Intern styring og kontroll* på Master of Management på BI har vi foretatt en empirisk undersøkelse av internrevisjonsinstrukser i norske virksomheter, for å undersøke i hvilken grad internrevisjoner i Norge oppfyller kravene til instruksen i standard 1000, og hvorvidt man følger anbefalinger til beste praksis beskrevet i Practice Advisory 1000-1. Disse er utformet for å ivareta internrevisjonens uavhengighet, og for å sikre levering av verdiskapende tjenester. Vår analyse av datamaterialet viser at det er et forbedringspotensial når det gjelder oppfyllelse av krav i standarden, og at det også er et stykke igjen før internrevisjoner i Norge har integrert anbefalt beste praksis. Analysen har også medført refleksjoner om utforming av mal til instruks, og om proaktive løsninger oppdaget i datamaterialet.

Det ble sendt en spørreundersøkelse til internrevisjonssjefer kjent for NIRF på daværende tidspunkt, og svarene ble koblet mot innholdet i tilsendte instrukser. Vi rettet oss mot internrevisjoner i Norge som sier at de anerkjenner definisjonen av internrevisjon, etiske regler og standardene til *the Institute of Internal Auditors*, og har minst en internrevisor ansatt i virksomheten. Totalt gjennomgikk vi 26 instrukser.

Det funksjonelle rapporteringsforholdet

Vi ser at de aller fleste er organisatorisk korrekt plassert for å ivareta uavhengigheten, med rapporteringslinje til øverste myndighet. Det er imidlertid tidvis uklart i flere instrukser hva som inngår i det funksjonelle rapporteringsforholdet for internrevisjonen i virksomheten, og dermed om rapporteringsforholdet i tilstrekkelig grad ivaretar uavhengigheten. Enkelte har stadfestet i instruksen at man rapporterer *funksjonelt* til øverste myndighet, og andre har i instruksen inkludert flere av forholdene tolkningen til standard 1100 nevner som eksempler på hva som kan inngå i et funksjonelt rapporteringsforhold. I og med at standardene kun gir eksempler, er det rom for selv å betegne hva dette forholdet innebærer for den enkelte virksomhet. Et funksjonelt rapporteringsforhold kan variere fra internrevisjon til internrevisjon, og noen elementer kan være viktige enn andre. Det som er nyttig å reflektere rundt er hvordan disse elementene (tilstede eller fraværende) kan påvirke uavhengigheten til internrevisjonen. Er dette klart for alle involverte parter? Og er det tilstrekkelig uttrykt i instruksen?

Hvordan gjør vi det?

Dersom man i virksomheten har valgt å rette seg etter det eneste anerkjente internasjonale rammeverket for internrevisjon, skal dette i følge standard 1010 være nedfelt i instruksen. Vår undersøkelse viser at det er 9 av 26 som ikke har dette riktig beskrevet i instruksen, til tross for at dette kravet er lett å innfri. Ved å vise at man følger IIAs rammeverk er det visse elementer som allerede er definert i rammeverket og visse elementer som er omtalt som skal, for eksempel at man skal ha en ekstern evaluering av en uavhengig kvalifisert part minst hvert femte år (standard 1312). Dermed er det grunnlag til å henvise til rammeverket ved behov fremfor å overøse instruksen med beskrivelser og definisjoner. I utarbeidelsen og vurderingen av instruksen kan det være nyttig å reflektere over *hva* man tar med i instruksen og *hvorfor.* Selv om det er visse krav til hva som skal være omtalt i instruksen, er det ingen fasit for hvordan den utformes eller hva annet man beskriver i instruksen. Hva kan være nyttig å inkludere i instruksen i din virksomhet?

Gjennomgang og kommunikasjon

Det er et krav at man periodisk skal gjennomgå innholdet i instruksen for å vurdere om den i tilstrekkelig grad reflekterer de faktiske forholdene i

Internrevisjonsinstruks

- Hvem er vi?
  - Hva er vårt formål?
  - Hva er vårt ansvar?
  - Hva er vår myndighet?
  - Hvordan sikrer vi vår uavhengighet?
- Hva gjør vi?
  - Hvilke typer bekreftelsestjenester leverer vi?
  - Leverer vi bekreftelser til parter utenfor virksomheten?
  - Hvilke typer rådgivningsoppdrag gjør vi?
- Hvordan gjør vi det?
  - Følger vi IIAs standarder, etiske regler, definisjonen av internrevisjon?

Uansett hvordan man velger å beskrive internrevisjonens formål, ansvar og myndighet i instruksen, så er det viktig at den er oppdatert for å gjenspeile de faktiske forhold, noe som sikres gjennom en periodisk gjennomgang og kommunikasjon med styret og toppledelsen.

virksomheten. Flere oppgir i spørreundersøkelsen at de ikke oppfyller dette kravet. Verken standarden eller PA-1000 definerer hvor ofte dette bør gjøres. Hvis man velger å utføre en årlig gjennomgang kan det gjøres for eksempel i forbindelsen med årsrapporteringen eller årsplanleggingen. Samtidig kan det også være nødvendig å løpende vurdere endringer som kan påvirke internrevisjonens formål, fullmakt og ansvar. I PA 1000-1, som er anbefalt beste praksis, står det at resultatet av gjennomgangen av instruksen også skal kommuniseres til toppledelsen og styret. Analysen vår viser at dette følges opp i varierende grad.

Om vi ser på kombinasjonen av oppfyllelse av kravet om periodisk gjennomgang, og utøvelse av anbefalt beste praksis for kommunikasjon av denne, er det 10 av 26 som gjennomfører dette, og dermed sikrer at toppledelsen og styret er informert om forholdene som er vurdert. Hvordan er det i din virksomhet? Når kan være et naturlig tidspunkt å sette dette på agendaen?

Proaktiv løsning?
NIRF vil på grunnlag av kunnskap fremkommet blant annet på bakgrunn av oppgavens analyse, utarbeide en mal for instruks som kan være nyttig både for etablerte og nye internrevisjoner. Vi ser for eksempel en økning i nyetablerte, små enheter som ikke trenger å finne opp kruttet på nytt. En inspirasjon inn i dette videre arbeidet, er hva vi liker å kalle for en proaktiv løsning i noen av instruksene i datamaterialet. I gjennomgangen ble det observert at to instrukser omtalte beste praksis. Dette er ikke en del av kravene til hva som skal være nedfelt i instruksen, men ettersom det ikke finnes en fasit for utforming av en instruks, så kan nettopp det å nedfelle beste praksis av instruksen bidra til å sikre nettopp det.

Vi håper at disse funnene og refleksjonene rundt instruksen vil bidra til at flere internrevisjoner innfører beste praksis. Instruksen er et grunnleggende dokument som man kanskje ikke tenker på i det daglige, men som uansett bør være et *levende* dokument.

Helt til slutt, vil vi benytte anledningen til å takke alle internrevisjonssjefer som har bidratt til datainnsamlingen og dermed også bidratt til foreningens arbeid. Tusen takk!

Høringskommentarer fra ECIIA

Internrevisjon er ikke en del av kontrollsystemet.

Oktober 2014

The European Banking Authority's (EBA) sitt forslag til retningslinjer for felles prosedyrer og metodikk til bruk for banktilsynsmyndigheter mangler klarhet i beskrivelsen av internrevisjonens rolle i virksomhetsstyringen, sier the European Confederation of Institutes of Internal Audit (ECIIA).

ECIIA svarer på høringsrunden EBA initierte på sitt dokument *Draft Guidelines for common procedures and methodologies for the supervisory review and evaluation process under Article 107 (3) of Directive 2013/36/EU,* ECIIA uttalte at EBA tok feil i å beskrive internrevisjon som en del av finansinstitusjonenes internkontrollsystem.

"Internrevisjonens oppgave er ikke å utføre kontroller, men i hovedsak å revidere kontrollfunksjonene og gi bekreftelse på status og kvalitet av disse til styre og tilsynsmyndighetene" sier ECIIA.

ECIIA mener dette skillet er grunnleggende fordi det gjenspeiler at kjernevirksomheten til internrevisjon er, på styrets vegne, å overvåke alle de andre funksjoner i en bank fra sitt enestående uavhengige ståsted.

"Ettersom fremtidige internasjonale tilsynsinspektører vil komme til å benytte seg av dette meget nyttige dokumentet, er det viktig å klargjøre forskjellen mellom kontrollsystemer og internrevisjonsfunksjonen" sier presidenten i ECIIA Thijs Smit.

For videre informasjon se http://www.eciia.eu/our-current-views/responses-to-consultation/

Internrevisjonens uavhengighet må tydelig defineres i Solvency II

September 2014

Internrevisjon må være utvetydelig uavhengig skal det spille en effektiv rolle under det nye tilsynssregimet for forsikringsselskaper som går under navnet av Solvency II - dette ifølge ECIIA.

Retningslinjer for implementering av Solvency II utgitt av the European Insurance and Occupational Pensions Authority (EIOPA) krever eksplisitt ansvarsskille mellom de ulike virksomhetsstyringsfunksjoner, noe som ECIIA hilser velkommen. Imidlertid bør dokumentet der ansvarsoppgavene er nedfelt uttrykke mer detaljert hvordan internrevisjonens uavhengighet skal oppnås.

"En av hovedoppgavene til internrevisjon er å revidere virksomhetsstyringssystemet" sier ECIIA i sitt svar til høringsdokumentet. "Dette inkluderer en rolle i å revidere andre nøkkelfunksjoner som risikostyrings-, compliance- og aktuarfunksjoner og derfor må internrevisjon holdes adskilt fra disse funksjonene."

Nøkkelen til internrevisjonens uavhengighet er sitt forhold til revisjonsutvalget – kommunikasjonen må kunne skje direkte og konfidensielt der dette er nødvendig – og retten til å revidere hvilket som helst område i forsikringsvirksomheten uten begrensninger og påvirkning fra ledelsen. Internrevisjonen må rapportere funksjonelt til styret og operasjonelt til organisasjonens daglig leder, skrives det i kommentaren til høringsutkastet fra EIOPA. For videre informasjon se http://www.eciia.eu/our-current-views/responses-to-consultation/

LEAN AUDITING

– using lean techniques to enhance added value and reduce waste

By James C Paterson. PIIA, Director, Risk & Assurance Insights Ltd

When I was Chief Audit Executive (CAE) for Pharmaceuticals company AstraZeneca PLC, I became increasingly interested in two key questions about internal auditing:

- How could I be sure the internal audit function was adding the maximum value it could?
- How could I be sure the internal audit function was as efficient as it could be – moving beyond benchmarking and going back to first principles?

One of my audit team alerted me to lean manufacturing (which revolutionized the Japanese motor industry in the 1960s and 1970s) and suggested we could adapt this to internal auditing. After an initial review we agreed that lean techniques could help us and thereafter we worked to apply these to what we did, creating a lean auditing approach and obtaining positive recognition internally and externally, and also driving efficiency improvements of around 20%.

Several years later I started to work as a freelance consultant and took what I had learned at AstraZeneca and applied and enhanced it with my clients. I also started to run training on lean auditing for the IIA UK and thereafter gained interest overseas in Belgium, Sweden, the Middle East, South Africa and as far afield as Canada and Australia.
In 2013 I was approached by John Wiley & Sons, Ltd and asked if I would write a book on lean auditing (due for release early in 2015). I was aware that some of the ways of working that I would be proposing would be challenging to some internal auditors, so I decided to discuss the principles and practices with a range of heads of audit, some of whom were my clients and some not, to validate and enhance what I was planning to write. In addition to interviews with more than twenty heads of audit, I was also lucky enough to interview Richard Chambers the CEO of the IIA in the USA, Norman Marks, a leading thought leader in GRC in the US and also Chris Baker the technical manager of the IIA UK.

What is lean and what can it offer us?
The label "lean" was first used in 1987 by John Krafcik, a student at that time of the Massachusetts Institute of Technology (MIT) who examined the Toyota Production System that had revolutionized their production methods and observed: "It needs less of everything to create a given amount of value, so let's call it lean."

Lean techniques have now been successfully applied in a range of sectors outside of motor manufacturing (e.g. in white goods and pharmaceuticals manufacturing) and, increasingly, in service sectors (e.g. airlines, healthcare). Typical benefits obtained from lean ways of working include:

- Reductions in: Defects, Lead times, cost, inventory and waste
- Improvements in: Customer satisfaction, Productivity, Capacity, Responsiveness and Quality

Lean ways of working have also been used in relation to finance, HR and IT. And the application of lean to internal auditing can be thought of as just a continuation its application. However, the key to success is to understand how to intelligently apply these principles and techniques whilst respecting key IIA standards.

Key principles of lean
The 5 key principles of lean can be summarized as:

- Specify value from the point of view of the customer
- Identify the value stream
- Create activities that Flow
- Pull through "just in time"
- Always strive for perfection

It is important to recognize therefore that lean is not simply about reducing costs although managing and reducing costs is a by-product of lean ways of working. This also means that working in a lean way is often a much more positive thing than most people realize and is something that regularly is told to me during the lean auditing workshops I run.

Of course, which lean tools to apply and how apply them needs to be situation specific and appropriately tailored to internal audit work.

The consequences and benefits of using a lean auditing approach
The benefits from using these tools and techniques can range between each audit function and will depend on the extent to which best practices are already in operation. One of my interviewees makes a key point:

Illustrasjonsfoto: Scanstock photo

"I think that there can be issues around peoples' understanding of lean auditing. People can easily see it as just finding an efficient way of doing an audit. In other words, it is the methodology that is related to lean, not the focus of the audit and the outcome. They might think it's meant to relate to cutting out unnecessary administration and trying to avoid long drawn-out audit reports and taking ages to get your audit report produced. This probably comes from the layman's understanding of lean which is that its about cutting things back to their bare bones.

Of course lean has an element of this but its not just about cutting out unnecessary activities, its just as much about getting the focus of the audit right and using the time more wisely and more effectively".

Thus the key benefits from a progressive, lean audit approach are manyfold for both internal audit and the wider organization but can include:

- The creation of an audit culture that is focused on delivering value add
- An audit plan that is more closely, and demonstrably, aligned with the key value drivers of the organization on an ongoing basis
- An audit function that plays a key role in understanding the overall risk assurance landscape of the organization
- An audit plan that is scheduled and delivered with the minimum of delays or difficulties
- Audit findings, reports and other forms of communication, that are short, insightful and recognize the wider context of the organization and the challenges it is facing
- An audit function that is able to highlight appropriate efficiency opportunities in the wider organisation, including instances where the streamlining of compliance and control processes would be beneficial
- A function that can clearly demonstrate a positive return on its cost

Final reflections

Many more detailed practices and insights are contained within the lean auditing book. These have given me encouragement that there is a considerable body of progressive, value adding, practice in the internal audit profession across a range of countries and sectors. However, it is clear from my research that many audit functions can do more to improve their value add contribution and/or improve their efficiency and will therefore gain benefit from the practices outlined in the book.

Of course making progress in driving forward more progressive audit practices requires leadership and judgment from heads of audit and auditors. As one head of audit explained:

"It takes confidence and courage to say no, I'm not doing any more audit work. It takes confidence and experience to say I'm not going to drill down any further. I've got my point. Management have said yes, we agree, we've got an issue, we need to do something about it."

My hope is that the greater understanding of lean principles can help us as a profession to become more confident in making these judgments, without feeling like we are "cutting corners".

Profesjonens puls

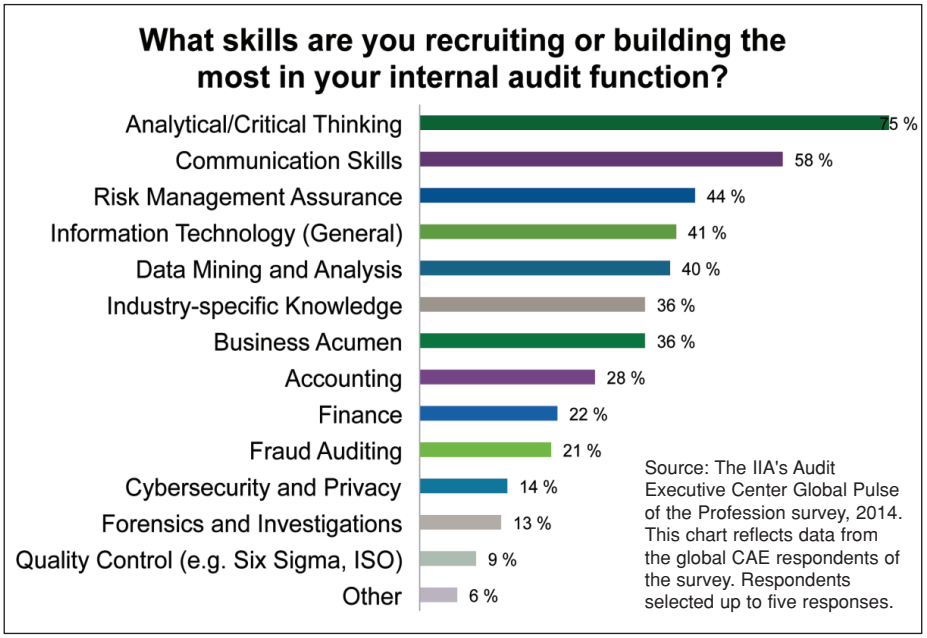
Hvert år utgir IIA en rapport om utviklingstrender i internrevisjon kalt "The Pulse of the Profession". En slik rapport er også laget i 2014 basert på en global undersøkelse som ble besvart av 1935 internrevisorer fra hele verden, og konklusjonene er sammenstilt med relaterte undersøkelser utført av KPMG, PwC og Protiviti samme år. Rapporten kan lastes ned på IIA global sin webside https://global.theiia.org/knowledge/services/Pages/Global-Pulse-of-the-Profession-Study.aspx

Av Martin Stevens, redaktør SIRK

Det første som slo meg i rapporten var at forretningsstrategi var identifisert som et like viktig område for planlagte revisjoner som regnskap/økonomi. For ikke mange år siden var regnskap/økonomi hovedfokusområde, uten tanke på forretningsstrategi. Nå har sannelig internrevisjon utvidet horisonten sin.

Et annet interessant spørsmål som ble stilt, var om det var godt definerte avgrensninger mellom internrevisjon og 2.linjeforsvarsfunksjoner som feks compliance og risikostyring. Her responderte kun en tredjedel at det var meget klare grenser mellom disse rollene. Dette viser at selv om den treforsvarslinjemodellen har nådd allmenn anerkjennelse, er man fortsatt usikre på den praktiske delingen av arbeidet. Dette kan ingen være tjent med og svaret må blant annet ligge i en god og regelmessig dialog mellom partene.

Til slutt synes jeg det er interessant å se nærmere på listen over ønsket ferdigheter ved ansettelse og videreutvikling av internrevisjonsfunksjonen. Evnen til å tenke analytisk og kritisk som internrevisor scorer høyst med 75%, etterfulgt av kommunikasjonsferdigheter og kunnskap om risikostyring. Langt nede på listen med en score på 28% kommer regnskapskompetanse. Det er ikke tvil om at rapporten illustrerer at internrevisjonsprofesjonen har definitivt har /utviklet seg. Stemmer kompetanseønskelisten med den utarbeidet i din internrevisjonsavdeling?



@IIA_Norge

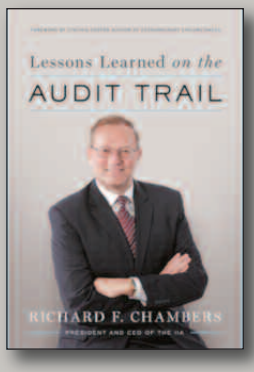
NIRF

Norges Interne Revisorers Forening

nirf_iianorge

Lessons learned

Bokanmeldelse av Esa Leporanta



IIAs Research Foundation

Richard F. Chambers - Lessons Learned on the AUDIT TRAIL

Boken til Richard F. Chambers blir innledet med et kapittel som gir en helhetlig oversikt over den lange og hendelsesrike karrieren hans som CEO, CAE og internrevisor.

I de neste 15 kapitlene deler han åpenhjertig sine erfaringer med lesere, hvilket gjør denne boken til et relevant informasjonskilde både for erfarne og mindre erfarne revisorer.

I et av bokens første kapitler beskriver Chambers hvilke egenskaper han anser som viktige for å lykkes i rollen som revisor. Deretter belyser han hvorfor det er så kritisk å kjenne til hva våre viktigste interessenter forventer av oss som revisorer.

Lengre frem i boken blir verdien og betydningen av revisjonsplanleggingen fremhevet. Chambers påstår at dårlig planlegging er den første og største feilen vi kan gjøre som revisorer. Selv om viktigheten av planleggingen normalt ikke vektes like høyt i andre lærebøker, vil en erfaren revisor kunne si seg enig med forfatteren.

Chambers forteller oss videre hvordan vi som revisorer kan gjennomføre effektive intervjuer og hvilke grep det kan foretas for å øke effektiviteten i revisjoner. Det blir gitt råd om hva man ikke bør skrive i revisjonsrapporter og hvordan vi kan møte klienter som er generelt skeptiske til internrevisjon. Rådene omfatter også hva vi kan gjøre for å få revisjonsoppdraget på rett kjøl, dersom vi holder på å spolere hele *oppdraget.*

Det som skiller denne boken fra de fleste andre er enkelte av Chambers egne refleksjoner. I utvalgte tilfeller er han enig med oss lesere at det ikke er lett å innfri hans forventninger. Samtidig guider han oss videre for å vise at det er mulig følge anbefalingene og at vi uansett ikke må stoppe å utvikle oss videre.

Gjennom hele boken viser Chambers sine 35 viktigste erfaringer i separate tavler, hvilket gjør det lettvint å repetere bokens innhold.

Når vi sjonglerer mellom ulike revisjonsoppgaver, vil vi ikke til enhver tid huske hele den kompleksiteten og alle de detaljene, som Chambers har samlet i boken sin, men boken tjener da som et utmerket oppslagsverk.

Ved å dele sine erfaringer med oss, står Chambers også frem som et lysende eksempel på en menneske som forsøker å leve etter det fremragende mottoet vi har innen vårt fagfelt: *«Progress through Sharing».*

Alt i alt, vil jeg gjerne anbefale denne boken til alle som vil lære seg mer om hva som kjennetegner en profesjonell internrevisjon. Her finnes det noe nytt for hver og en av oss!

God leselyst!

Frank Alvern om sertifisering

Forsvarsdepartementet har etablert en kompetansepool på ti personer. Med disse ti ansatte leveres internrevisjonstjenester til tre av Forsvarsdepartementets etater – Forsvarsbygg, Forsvarets forskningsinstitutt og Nasjonal sikkerhetsmyndighet – i tillegg til at departementet revideres, Forsvaret (koordinert med Forsvarssjefens internrevisjon), samt mer og mer sektorprosesser og aktiviteter/prosjekter som er felles over hele sektoren. Endelig forvaltes varslingskanalen i departementet samt at det er gitt et sektoransvar i den sammenhengen.

Av Hilde Tanggaard, rådgiver NIRF

Frank Alvern internrevisjonssjef i Forsvarsdepartementets internrevisjon har fokus på kompetansebygging, herunder sertifisering, av sin stab og er stolt over teamet sitt. Frank svarer følgende på spørsmål om sertifisering:

Hvor mange ansatte har du, og hvilke sertifiseringen innenfor internrevisjonsfaget innehar teamet?
Etter en bevisst satsing er status akkurat nå at vi i teamet har fire CIA, seks CGAP, tre CRMA, to CISA, en CCSA samt fire som er Dipl. I.R. De fleste har mer enn en sertifisering, en kjapp beregning gir akkurat to i gjennomsnitt!

Er det krav, sterk oppfordring til eller frivillig for den ansatte å bli sertifisert?
Jeg tror medarbeiderne vil lande på «sterk oppfordring» her. Vi ser klart etter sertifisering når vi rekrutterer, og prioriterer sertifisering både med tid og penger i hvert budsjett.

Hva betyr det for deg som internrevisjonssjef å ha sertifiserte ansatte?
I forsvarssektoren er det å synliggjøre kompetanse virkelig satt i system gjennom graden uniformen viser. I Internrevisjonen er vi kun sivilt ansatte, og internasjonale faglige sertifiseringer er en måte for sivilistene å vise at man har gjennomført et kompetanseløp som har resultert i sertifisering/diplomering. Vi har laget en liten «brosjyre» hvor vi presenterer oss i internrevisjonen, og i denne har vi inkludert en beskrivelse av de enkelte sertifiseringene og diplomeringen. En annen viktig faktor for meg er at sertifiseringene bidrar til å sikre at vi står på den samme faglige grunnmuren for å si det slik. Man må skjønne standardene for å oppnå sertifisering/diplomering! Til slutt vil jeg legge til at standardene jo er ganske klare i sin anbefaling på dette området også – og instruksen vår er å følge IIA her.

> ***Sertifiseringene bidrar til å sikre at vi står på den samme faglige grunnmuren.***

Hva tror du det betyr for den enkelte medarbeider å være sertifisert?
Jeg opplever at det er lett «å selge» en innsats mot å oppnå en sertifisering. Når det kommer til stykket så er en sertifisering noe som den enkelte medarbeider eier, og tar med seg videre uansett om det er hos oss eller andre steder etter hvert. Jeg vinkler det som et konkurransefortrinn for den enkelte.

Hva tror du sertifiseringsmuligheten har å si for motivasjonen til den enkelte medarbeider?
I forlengelsen av det forrige spørsmålet – vårt sertifiseringsprogram viser for den enkelte at vi er villige til å prioritere investering i faglig vedlikehold og kompetansebygging i en travel hverdag.

Utover sertifisering og annen formell utdannelse, hva er de tre viktigste egenskapene du ser etter i en internrevisor?
Analytisk, logisk tenkende er definitivt der – det er her vi skal bygge uavhengige bekreftelser. Så er kommunikasjonsevner særdeles viktige, så den er med i min topp tre. Endelig vil jeg ta med lagspilleren som noe jeg ser etter. Særdeles viktig når vi har bygget en slik ressurspool som vi har i vår sektor.

EXECUTIVE MASTER OF MANAGEMENT

INTERN REVISJON

– Governance – Risikostyring – Intern styring og kontroll

Oppstart
høsten 2015
bi.no/emm

Få en inngående forståelse for samspillet mellom virksomheters etablerte strategier og mål, og hvordan du kostnadseffektivt sikrer at målene oppnås gjennom god virksomhetsstyring. Programmet tar utgangspunkt i aktuelle aspekter av virksomhetsstyring som kan bidra til at toppledelsen og styret får relevant informasjon om organisasjonens situasjon. Programmet gir kunnskap og innsikt i hvordan bruk av intern revisjon, aktiv risikostyring og god intern kontroll gir en nøkkel til god måloppnåelse. Du lærer også hvordan den interne revisor i samspill med andre kan utøve sin funksjon.

Programmet er utviklet og blir gjennomført i samarbeid med Norges Interne Revisorers Forening (NIRF).

NORGES INTERNE REVISORERS FORENING

TYNGDEN DU TRENGER BI

So you think you are good – How do you get better?

Interview with Greg Hollyman, Chief Internal Auditor for Australian Taxation Office

By Hilde Tanggaard, advisor, NIRF

Greg Hollyman, the Chief Internal Auditor at the Australian Taxation Office, held a presentation at the global Conference in London earlier this year, called: So you think you are good – how do you get better? Greg found himself in the difficult position of taking over as CAE on the retirement of his predecessor who earlier had undergone an external quality assessment which concluded that the department was world-class. In his presentation in London Greg shared his experience of the challenges he had in developing and improving the function further. For those of you who missed that presentation, Greg visited Oslo on 3rd July for a seminar on Quality together with a group of other Heads of Internal Audit from Australia and New Zealand all of whom had been invited by IIA Norway to present and contribute to the seminar. For those of you who missed that too – get a grip! Note for the future - pay closer attention to all the inspiring seminars and courses IIA prepares for your participation.

As it is we also took the opportunity after the seminar to ask Greg a few questions about external quality assessment (QA), which we would like to share here with you SIRK reader. Specifically we sought his opinion on the QA requirement in the IIA International Professional Practices Framework and whether he sees it as a natural part of a modern internal audit function and as an opportunity for advancing its work.

- ***What value can be derived from being subject to a QA?***

  In my opinion there are two key advantages from a QAR, the first is to obtain the assurance that your team is in fact in conformance with the standards, the second one, which I obtain the most benefit from, is the opportunity to receive some ideas from my peers as to what better practices or ideas I can implement into my function to take it up another notch.

The most important thing in my opinion is selling the reason as to why we, as an organisation, benefit from a QAR rather than just saying that we are having one because the standards say we must.

- ***The requirement in Standard 1312 is to undergo a QA every five years, what do you think is the best practice time interval?***

  I think that five years feels about right, though I would suggest that functions do not leave it until the last second but plan for it to be convenient to your timing. What I mean is that we all have our peaks and troughs so book it to be in one of your troughs as it will take time from your side and the last thing you want is to be working towards other deadlines then having a QAR at the same time. I would also suggest requesting one when you take over a function if one was not done immediately prior to you taking over (as it was in my case) as it gives a good feel of where the function actually is and where further enhancements can be made.

- ***Some internal auditors might feel uncomfortable having a QA, why do you think that is? And what is your advice to them?***

  It is natural to feel uncomfortable about a team coming in from the outside, looking at your work then telling you how to do it better, but consider this, is this not we do when we do audits? A QAR is in fact an audit of what we do so it provides us with the opportunity to see what it is like for the areas we audit. My advice is to embrace this experience as there is nothing better than to experience what our clients go through so as to increase our empathy to what we put them through.

- ***Sometimes it may be difficult to communicate to the stakeholder the value/importance of getting a QA performed? If so, how would you handle this situation?***

  The most important thing in my opinion is selling the reason as to why we, as an organisation, benefit from a QAR rather than just saying that we are having one because the standards say we must. As mentioned earlier there are the two aspects that can be "sold", the first is to provide assurance to the key stake-

holders that the function is abiding as per the international professional standards, the other is the aspect that we are getting better practice advice as well to improve the function even more.

- ***A complete Program for Quality Assurance and Improvement also includes ongoing and periodic internal assessments. Can you describe what internal assessment activities you perform in your internal audit function, and in what ways they are interconnected to or support the results of the QA (i.e. in regard to the outcome of the QA.)***

  We periodically examine the various standards to see if we are abiding to them through a self-assessment approach. We have also recently commenced a comprehensive quality review process of a sample of our files where we check that they are completed in line with our methodology and documentations standards. We have already developed our methodology in close alignment to the standards so this also provides us assurance that we are in alignment with the standards. This gives me a continual assurance that our function is working in general conformance to the standards and will feed in as evidence to the QA team to support their review.

- ***In choosing between the two: a Self-assessment with an Independent Validation or a full External Assessment, which would you choose, when and why?***

  There is no right or wrong answer here as it is really up to what works best for a function and organisation. Both approaches have their differing advantages. In our organization we prefer to have a full external assessment as I prefer to have that full detailed look at our function, but that is a personal preference, which is shared by my Audit and Risk Committee.

- ***What do the stakeholders, the board and management, often perceive as the greatest value from QA of their internal audit function?***

  Similar to what I mentioned earlier our Audit and Risk Committee likes to receive external assurance that the Internal Audit function is indeed in general conformance to the IPPF, though they do not have reservations that we are. In addition they also appreciate the aspect of obtaining advice as to how the IA function can further improve itself as we should never believe that we are truly as great as what we often say we are.

- ***Any advice for those who are about to have a QA or who are considering to put it in on their plan for next year?***

  Firstly it is going to take some time from your side as well so be prepared for that as you collate all the information required for the QA team. Secondly book it in for a quitter period for yourself so that you can focus on it. Finally and most importantly, treat the QA team in the way that you would wish to be treated as an auditor, it is a bit of a role reversal – we know what we require from our clients, now we are the clients.

Greg Hollyman, CIA, CCSA, CFSA, CGAP, CRMA, Chief Internal Auditor, Australian Taxation Office.

Greg has over 20 years of experience and numerous qualifications in the internal audit and risk management fields. He has been recognized nationally and internationally, including through his association with the global Institute of Internal Auditors. He currently holds the position of Chairman of the Institute Relations Committee of the Global IIA and is a past Chairman of the Victoria Chapter of that Institute. He was previously the Chairman of the Global Public Sector Committee, President of the Institute in South Africa and has also been the Vice Chairman of the Global Ethics Committee. In addition Greg has spoken on internal audit, governance and risk management topics at national and international conferences.

Aktuelt fra ledernettverk for Finans

Ledernettverket for Finans gjennomførte sitt høstseminar på Bjørvika Konferansesenter den 15. oktober med et tyvetalls deltakere. Arbeidsutvalgets leder Vidar Hansen fra Sparebanken Sør ønsket velkommen og presenterte programmets hovedbolker. Programmet inneholdt en rekke aktuelle tema for alle som interesserer seg for internrevisjon innen finansforetak.

Av Reidar Døli, medlem av arbeidsutvalget

Are Jansrud fra KPMG fortalte om de viktigste endringer som følger av inntredenen av Finansforetaksloven. Utkastet til lov er oversendt Stortinget med forventet behandling i Finanskomiteen i november. Loven vil erstatte Sparebankloven, Forretningsbankloven, Finansieringsvirksomhetsloven samt at store deler av Forsikringsvirksomhetsloven oppheves. Lovutkastet inneholder flere bestemmelser relatert til finansforetakenes risikostyring og internkontroll, blant annet at alle finansforetak skal ha uavhengige funksjoner for risikostyring, compliance og internrevisjon. Loven stiller nye kapitaldekningskrav til forsikring og innebærer i praksis en innføring av Solvency II i Norge. Videre gis det nye regler mht. utkontraktering samt om utveksling av kundeinformasjon mellom konsernforetak. For øvrig vil kravet til Kontrollkomitèer avvikles. Dessuten forventes det at bankenes kontanthåndtering skal avstemmes med kundenes forventninger og behov. Are Jansrud refererte avslutningsvis til at det er varslet at det vil komme en ny forskrift om virksomhetsstyring, til erstatning for dagens forskrift om risikostyring og internkontroll. Den vil ha vesentlig påvirkning for den funksjon som forsamlingen representerer.

Neste foredragsholder var **Joachim Bernhardsen fra Nordea.** Han skisserte et bilde av den fremtidige makrosituasjonen, som slett ikke er fri for utfordringer. Hans presentasjon tok forsamlingen over i Finanstilsynets foredrag som denne gang ble presentert av **Ingvild Eide Sanden.** Hun bidro med status i innføringen av CRD IV og andre nyheter. EU har vedtatt CRD IV som setter regler for rapportering av kapitaldekning, kvantitative likviditetskrav, uvektet kapitalkrav mv. Når forordningen er på plass vil CRD prinsippene legges til grunn i utformingen av de norske forskriftene som vil erstatte en rekke av dagens gjeldende regulering. Sanden kom deretter nærmere inn på bestemmelsen som er gitt i Finansieringsvirksomhetsloven § 2-9b om at «Institusjonen skal ha et risikoutvalg oppnevnt av styret». Uavhengighetsproblematikk kan oppstå hvis samme person leder revisjons- og risikoutvalget. Sanden bekreftet til slutt Finanstilsynets arbeid med en ny forskrift til erstatning for Forskrift om risikostyring og internkontroll. Nettverket ga uttrykk for at det ser frem til å bli involvert i arbeidet med den nye forskriften.

Åsfrid Betten fra DNB presenterte hvitvaskingsregelverket og forslag til hvordan internrevisor kan innrette sin tilnærming. Lovens formål er å forebygge og avdekke transaksjoner med tilknytning til hvitvasking og terrorfinansiering. Den skal hindre at finansinstitusjoner brukes som kanal for hvitvasking og terrorfinansiering øke oppdagelsesrisikoen og være kriminalitetsforebyggende. Utgangspunktet for etterlevelse av Hvitvaskingsloven og Anti Money Laundering (AML) arbeidet er en risikobasert tilnærming. Finanstilsynet har i sitt rundskriv nr. 8/2009 presisert at det er meget viktig at den rapporteringspliktige overfor tilsynet klart kan påvise at den operasjonelle risikoen som hvitvasking og terrorfinansiering innebærer er konkret vurdert og tilstrekkelig tatt hensyn til ved omfanget og intensiteten av kundekontrolltiltakene. Fra internrevisjonens ståsted er det derfor vesentlig å påse at de AML-rutiner som er etablert er risikobaserte. Betten fremhevet at det er viktig at terskelen er mest mulig lik gjennom hele finansbransjen, ellers vil de kriminelle søke seg dit hvor det er enklest å etablere et kundeforhold. Alvorligheten understrekes av de saker som har vært gjennom rettsapparatet internasjonalt hvor bøtene har kommet opp i et flertalls MRD USD.

Trygve Sørlie var invitert til å fortelle om nytt fra IIA internasjonalt. Deltakerne fikk god anledning til å relatere det øvrige de hadde fått presentert gjennom dagen til «IIA's vision, mission and motto». Det er arbeidet frem et forslag til endringer i International Professional Practices Framework som er på høring frem til 3. november. Helt nytt denne gang er at det fremsettes et forslag til «Mission of Internal Auditing» som er formulert som følger: «To enhance and protect organizational value by providing stakeholders with risk-based, objective and reliable assurance, advice and insight». Nytt i forslaget er også «12 Core Principles for the Professional Practice of Internal Auditing». Det arbeides med å lage en modell for å presentere de foreslåtte endringer som sammen med oppdaterte versjoner av definisjonen, standardene og de etiske retningslinjer skal utgjøre det nye rammeverket. Sørlie delte til slutt sine erfaringer fra bruken av en modenhetsmodell i en virksomhet og som verktøy for internrevisjonen. Modellen baserer seg på CoCo regelverket. Den dokumenterer virksomhetsledelsens innstilling til hvilken modenhet som forventes nå og i fremtiden på prosesser for internkontroll, risikostyring og virksomhetsstyring. Bruken av slike modeller spås å ville tilta fremover. Seminaret ble avsluttet med middag i historiske omgivelser ved Akershus festning. Symboleffekten i valg av spisested var fra arbeidsutvalget side ikke helt tilsiktet, men like fullt en fulltreffer tatt i betraktning at nettverket representerer en forsvarslinje med lange tradisjoner og et stort behov for å fortelle anekdoter fra oppdrag i felten.

Ledernettverk for finans har linjer tilbake til 1967 og stiftelsen av Revisjonssjefkretsen. Nettverket ble innlemmet i NIRF i 2012. Det har i dag medlemmer fra alle typer finansforetak som har ansatt leder av internrevisjonen. Felles for medlemmene er at de fleste er ansatt i virksomheter som er underlagt Finanstilsynets forskrift om Risikostyring og internkontroll. I følge mandatet er nettverket en møteplass for medlemmene for bearbeiding av faglige tema og for diskusjoner av mer strategisk art. Nettverket fungerer også som et bindeledd mellom bransjen og Finanstilsynet i forbindelse med arbeid med nytt regelverk.
Aktiviteten i nettverket har igjen tatt seg opp da det skjer endringer på flere fronter som berører reguleringen og innholdet i funksjonen.

En høst med regulatoriske endringer på agendaen

Av: Ellen Brataas, generalsekretær

Det har vært en aktiv høst der høringer i både privat og offentlig sektor har stått på agendaen. Her kommer en oppsummering av de viktigste sakene NIRF har engasjert seg i.

Finansdepartementets rapport «Bruk av internrevisjon i statlig sektor»
Finansdepartementet har avgitt en rapport der formålet og mandatet med utredningen har vært å etablere mer forutsigbare rammer for bruk av internrevisjonen i staten. De viktigste grepene de foreslår er å videreutvikle økonomiregelverket og tilrettelegge faglige standarder og annen støtte for internrevisjonen. Arbeidsgruppen bak rapporten har gjort grundig research av internrevisjonsordninger i norske statlige virksomheter, og sett til andre europeiske land for å kartlegge hvordan de har løst det der. Rapporten fremmer forslag om organisering, kompetanse og rekruttering, bruk av anerkjente standarder, rapportering og dialog, eventuelt krav til vurdering av bruk av internrevisjon og eventuelt krav om bruk av internrevisjon.

NIRF synes det er bra at internrevisjon i statlig sektor er satt på agendaen og støtter flere av de forslagene Finansdepartementet foreslår i rapporten. Men det er også noen punkter vi skulle ønske var formulert annerledes: NIRF konstaterer at arbeidsgruppen anbefaler at det *ikke* innføres krav om at statlige virksomheter skal bruke internrevisjon. I stedet foreslår de at spørsmålet vurderes igjen om noen år, på grunnlag av erfaringer med et eventuelt pålegg om å *vurdere* bruk av internrevisjon. Rapporten anbefaler at det skal være opp til virksomheten (i praksis dermed virksomhetsleder) å vurdere behovet for etablering av internrevisjon, og føyer til at det er naturlig at denne vurderingen blir tema i styringsdialogen med overordnet departement.

Den 20. juni 2014 la Finansdepartementet ut forslag til ny Finansforetakslov (Prop. 125), der det legges opp til etablering av internrevisjon i **alle** finansforetak, uavhengig av størrelse. NIRF mener god forvaltning av fellesskapets midler er like viktig som interessene til investorer og aksjonærer, og *anbefaler at det innføres objektive kriterier for hvilke statlige virksomheter som skal etablere internrevisjon,* på lik linje med lovkravene i finanssektoren, helsesektoren og arbeids- og velferdsforvaltningen.

De fleste medlemsstatene i EU har krav om internrevisjon i statlig sektor. Objektive kriterier for hvilke statlige virksomheter som skal ha internrevisjon hindrer at dette viktige spørsmålet avgjøres av de personlige preferansene til den enkelte virksomhetsleder. I henhold til Riksrevisjonens *Practice Note* til ISSAI 1610 (INTOSAI), tillegges det vekt at internrevisjonsordningen er etablert ved lov når Riksrevisjonen vurderer å bygge på internrevisjonens arbeid. Norge har en stor og mangfoldig statlig sektor som ivaretar fellesskapets midler.

Departementene er etter NIRFs vurdering det viktigste leddet i et godt styrings- og kontrollmiljø for forvaltning av fellesskapets midler. OECD har på sin side anbefalt Norge å forankre internrevisjonsordningen i departementene. Arbeidsgruppen foreslår imidlertid at *departementene ikke inkluderes* i et pålegg om å vurdere bruk av internrevisjon i egen virksomhet. *NIRF er uenig i dette.* Vi er også uenige i premisset om at internrevisjon ikke passer inn i den norske styrings- og forvaltningsmodellen, herunder ansvarsdelingen mellom departement og underliggende virksomhet. Vi slutter oss til OECDs anbefaling til Norge. Det ville styrke departementene å ha en internrevisjon som gir uavhengige uttalelser og proaktive bidrag til god styring og kontroll innenfor departementets ansvarsområder.

Norsk anbefaling for eierstyring og selskapsledelse (NUES) – en oppdatering
Den norske anbefaling for eierstyring og selskapsledelse ble 30. oktober 2014 lansert i en oppdatert utgave. Lanseringen ble gjort på NUES-forum, der over 100 deltakere hadde samlet seg for å markere 10-årsdagen for lanseringen av den første utgaven av anbefalingen. Endringene er, i følge NUES, mindre omfattende og neppe særlig kontroversielle.

NIRF hadde ingen særskilte kommentarer til de foreslåtte endringene. Derimot har vi benyttet anledningen til å komme med noen ytterligere innspill, samt åpne opp for diskusjon av en mer prinsipiell karakter.

Sammenlignet med anbefalinger til god governance i andre land, både i og utenfor EU, er NIRF av den oppfatning at innholdet i den norske anbefalingen er relativt snevert. Den norske anbefalingen dekker hovedsakelig kravene til foretaksstyring sett fra eier og ledelsens perspektiv. Det vil være god praksis å inkludere også øvrige interessenter, som eksempelvis ansatte, brukere, leverandører, kunder og samarbeidspartnere, sine krav til god governance i en nasjonal anbefaling. Likeledes vil prinsippet om å ta ut de emner som blir lovfestet fra den norske anbefalingen, medføre at anbefalingen på sikt vil bli ganske kort. Vi mener det vil være en fordel for styrer, revisjonsutvalg, revisorer, regnskapsbrukere, investorer og andre interessenter at en norsk anbefaling er helhetlig med hensyn til hva som forventes og kreves i forhold til anbefalinger, krav og prinsipper knyttet til governance.

Eksempelvis er internrevisjon i liten grad lovregulert i Norge, men en rekke bransjer er underlagt krav om internrevisjon gjennom Finanstilsynets forskrift om risikostyring og internkontroll. I veiledningen til forskriften fremheves internrevisjonens betydning i styrets overvåking av risikostyring og internkontroll.

Rapporten «Corporate Governance Codes on Internal audit: current status in the EU (2012)» gir et overblikk over bruk av statlig internrevisjon i EU. Rapporten viser at governance-kodene i flertallet av EU-landene enten inneholder et krav om etablering av internrevisjon, eller et krav om at virksomhetens styre skal begrunne hvorfor en slik internrevisjonsfunksjon ikke er hensiktsmessig. I siste fall kreves henvisning til at internkontroll og risikostyring blir ivaretatt på andre måter. NIRF mener at det ville styrket også den norske anbefalingen for eierstyring og selskapsledelse dersom det fremgikk av punkt 10 at «Dersom virksomheten ikke har internrevisjon bør styret årlig evaluere om et slikt behov er til stede». NIRF ønsker å utfordre til debatt rundt behov for at det utvikles en helhetlig norsk anbefaling om god governance som kan brukes av alle interessenter, og samtidig drøfte konklusjonene i rapporten fra OECD. Fortsettelse følger…

Finanstilsynets høringsnotat om «Meldeplikt ved utkontraktering»
Finanstilsynet ba om kommentarer til høringsnotatet «Meldeplikt ved utkontraktering av virksomhet fra foretak under tilsyn», hvor NIRF kun kommenterte på forslagene som gjaldt internrevisjonstjenester.

NIRF er enige i Finanstilsynets vurdering om at internrevisjon er en funksjon som anses som viktig og derfor skal omfattes av meldeplikten. Vi støtter også tilsynets forslag om at meldingen om utkontraktering må inneholde opplysninger om avtalepart og avtalens art, omfang og varighet. Ved utkontraktering av internrevisjonsfunksjonen bør meldingen også omtale hvorvidt utkontrakteringspartneren legger de internasjonale standarder for profesjonell utøvelse av internrevisjon til grunn for sitt arbeide. NIRF mener det er fornuftig, slik tilsynet legger til grunn, at det i meldingen opplyses om hvordan foretaket vil følge opp sitt ansvar for den utkontrakterte virksomheten.

Håndbok i antikorrupsjon for næringslivet
NIRF fikk i oppgave å formulere et utkast til oppdatering av kapittel 9.3 *Intern kontroll og revisjon* i Transparency International Norges håndbok i antikorrupsjon. Deretter har vi kommentert på hele den oppdaterte versjonen av håndboken, som skal lanseres på den årlige antikorrupsjonskonferansen i desember.

Det er vanskelig å få med seg alt i en hektisk og veldig variert hverdag, derfor blir vi i sekretariatet alltid glad for tips til post@iia.no dersom medlemmer ser at det kommer utkast til lovendringer, reguleringer og annet der foreningen bør reise sin stemme.

Revisjon av virksomhetsstyring

Av Therese Johnsen, ekspedisjonssjef i Riksrevisjonen

Kjennetegn ved virksomhetsstyring
Virksomhetsstyring betegner virksomhetens interne styring, som blant annet omfatter krav til myndighets- og ansvarsstrukturer, styringsprosesser og intern kontroll. For å skape større sikkerhet for at vesentlige mål nås, er det i reglementet og bestemmelsene for økonomistyring for staten innført prinsipper om at **risikostyring og intern kontroll** skal integreres i mål- og resultatstyringen. Mål- og resultatstyringen er hovedprinsippet i den statlige virksomhetsstyringen.

Virksomhetsstyringen skal kjennetegnes ved gode styringsprosesser tilpasset virksomhetens risiko og egenart. Risikostyringen skal gi større sikkerhet for at vesentlige mål nås gjennom å identifisere risiko og iverksette tiltak for å redusere denne.

Alle virksomheter skal etablere ***intern kontroll*** tilpasset risiko og vesentlighet. Intern kontroll omfatter de prosesser, systemer og rutiner som er etablert for å gi rimelig sikkerhet for god måloppnåelse, god kvalitet, effektiv drift, pålitelig rapportering og økonomiforvaltning og overholdelse av lover og regler.

Topplеder og andre ledere har et særlig ansvar for å fremme en internkultur som vektlegger kvalitet i alt arbeid som utføres i virksomheten. Dette gjøres gjennom strategiarbeid, kommunikasjon, arbeids- og ansvarsrutiner og beskrivelser, evalueringer og gode rutiner for tilbakemelding og læring.

Disse prinsippene og aktivitetene utgjør virksomhetsstyringen og skal inngå i virksomhetens styringshjul.

Få revisjoner hvor virksomhetsstyringen er saksforholdet
Riksrevisjonen har gjennomført få revisjoner hvor hovedtyngden i saksforholdet som revideres er virksomhetsstyring. Det kan være mange forklaringer på hvorfor det er slik. Alt fra manglende kompetanse hos revisor på helheten i virksomhetsstyringen, og derfor problemer med å identifisere risiko som gjelder hele virksomhetsstyringen, til manglende tradisjon for å revidere virksomhetsstyringen som et eget saksforhold. En tredje forklaring kan være revisjonens metoder for risikovurderinger. Oppmerksomheten har vært rettet mot sektormålene og de mer tradisjonelle virkemidlene som tilskudd, lover, handlingsplaner og investeringer, og virksomhetsstyringens betydning for gode resultater og måloppnåelse har ikke blitt tilstrekkelig vektlagt av revisor.

Denne praksisen kan også henge sammen med at Riksrevisjonen rapporterer til Stortinget som er opptatt av de strategiske temaene som rettssikkerhet og god samfunnsmessig måloppnåelse på ulike områder, mens det ligger mer i forvaltningens rolle "å holde orden i eget hus". Det er imidlertid en sammenheng mellom profesjonaliteten i virksomhetsstyringen og virksomhetens bidrag til de samfunnsmessige målene, herunder effektiv ressursbruk, som revisor må være oppmerksom på. Virksomhetsstyring er også et kjerneområde for internrevisjoner, og det gjøres nå vurderinger i forvaltningen av hvorvidt denne funksjonen skal brukes mer systematisk.

Elementer av virksomhetsstyring inngår i mange revisjoner under lignende problemstillinger som: Hva kan forklare svakheter i resultatoppnåelsen? Dette var tilfelle i en nylig gjennomført undersøkelse av NAVs arbeidsrettede oppfølging av personer med nedsatt arbeidsevne. Her var problemstillingen: Hva kan forklare svakheter i brukerrettet oppfølging og manglende overgang til arbeid? Riksrevisjonen konkluderte med at det var svak styring av kvaliteten i oppfølgingsarbeidet ved NAV-kontorene. For eksempel hadde ingen av de undersøkte kontorene gjennomført kvalitetskontroller av de aktivitetsplaner som er en del av oppfølgingsarbeidet. Denne revisjonen kan bidra til at NAV forsøker å forbedre elementer i virksomhetsstyringen, men den gir ikke innspill til en mer helhetlig vurdering av virksomhetsstyringen i NAV. Ulike mangler i virksomhetsstyringen blir ofte brukt som en forklaring på svake resultater uten at revisor er 100 prosent sikker på årsakssammenhengen.

Risikovurdering av virksomhetsstyring
For revisor er et aktuelt spørsmål: Hvilke forhold er kjennetegn på svak virksomhetsstyring og utgjør dermed risiko for at den ikke sikrer at virksomheten gjennomfører oppgavene effektivt og når sine mål? Uten å påstå å være uttømmende, mener jeg følgende forhold kan gi indikasjoner på svak virksomhetsstyring: Mange og skiftende mål, svak måloppnåelse over tid, liten konsistens mellom mål og rapportering, liten opplevd nytte av styringsinformasjonen internt i virksomheten, manglende risikostyring og svak internkontroll. Hver for seg blir ikke disse svakhetene vurdert til å representere tilstrekkelig risiko til å starte en helhetlig revisjon av virksomhetsstyringen, men hvis revisor har indikasjoner på svakheter ved virksomhetsstyringen, må flere elementer ved virksomhetsstyringen kartlegges. Det vil gi revisor et bredere grunnlag til å vurdere risiko ved virksomhetsstyringen og behovet for og nytten av å gjennomføre en revisjon hvor virksomhetsstyringen utgjør saksforholdet.

Vesentlighet er også en utfordring ved risikovurdering av en virksomhet. Vesentligheten skal blant annet vurderes ut fra hvilken betydning virksomheten har, og om forbedringer i virksomhetsstyringen vil påvirke virksomhetens resultater positivt.

Som tidligere nevnt har Riksrevisjonen gjennomført få revisjoner hvor virksomhetsstyringen har vært hovedproblemstillingen i saksforholdet. Vi gjennomførte

en slik revisjon av Helsedirektoratet i 2013. I denne revisjonen var målet å vurdere helheten i virksomhetsstyringen. Helsedirektoratet har stor vesentlighet, da det er en stor organisasjon som legger premisser for tjenesteutforming innenfor helsesektoren.

Den finansielle revisjonen hadde gjennom flere år tatt opp mangler ved regnskapsføringen, budsjetteringen, tilskuddsforvaltningen og saksbehandlingstidene. Det var godt dokumentert risiko som utløste denne revisjonen hvor virksomhetsstyringen var saksforholdet sammen med departementets etatsstyring av direktoratet.

Et annet eksempel er revisjonen av Bufetat som Riksrevisjonen gjennomførte i 2008. Også den etaten har stor vesentlighet, særlig fordi den har viktige oppgaver knyttet til barn og unge i vanskelige livssituasjoner. Tidligere regnskapsrevisjoner hadde vist at det ikke var etablert gode systemer og rutiner for intern styring, og at det var vesentlige feil og mangler i etatens etterlevelse av sentrale statlige regelverk. Samtidig var måloppnåelsen svak på flere områder. I denne revisjonen var virksomhetsstyringen saksforholdet sammen med en vurdering av etatens resultater og departementets etatsstyring.

Eksemplene over illustrerer at erfaringer fra tidligere revisjoner kan gi viktige innspill til risikovurderingene. Revisor får også ofte innspill til risikovurderinger av virksomhetsstyring fra virksomhetens interne styringsdokumenter, virksomhetsstatistikk og eksterne evalueringer, i noen tilfeller også fra intervju med ansatte i virksomheten, samarbeidende virksomheter eller brukere/brukergrupper. Det er først og fremst de interne dokumentene og intervjuene som vil synliggjøre om manglende resultater kan knyttes til svakheter i virksomhetsstyringen. Det er som regel gjennom intervju at revisor får innblikk i problemer knyttet til virksomhetskulturen, kontrollmiljøet og internkontrollen, for eksempel mangelfull informasjon om vesentlige oppgaver hos virksomhetens ledelse.

Revisjonskriterier for virksomhetsstyring

For statlige virksomheter har vi et godt grunnlag for å utlede revisjonskriterier. Økonomireglementet, Bestemmelser om økonomistyring i staten, Bevilgningsreglementet og forvaltningsloven er gode kilder. Som grunnleggende styringsprinsipper gjelder at det skal fastsettes mål- og resultatkrav. Videre skal virksomheten drives i tråd med gjeldende lover og regler, herunder krav til god forvaltningsskikk, habilitet og etisk atferd.

Statlige virksomheter skal etablere systemer og rutiner som har innebygd intern kontroll, blant annet for å sikre at ressursbruken er effektiv. Videre har virksomhetens ledelse ansvar for å påse at styringen og internkontrollen er tilpasset virksomhetens risiko og egenart.

Virksomhetsstyringen skal være innrettet slik at den gir tilstrekkelig styringsinformasjon til å følge opp aktivitetene og resultatene. Informasjon fra virksomhetens økonomisystem skal sammen med statistikk, analyser, evalueringer og andre relevante systemer kunne belyse om virksomheten drives effektivt når det gjelder kostnader og fastsatte mål- og resultatkrav. Ledelsen har også et ansvar for å prioritere innenfor eget ansvarsområde.

Ifølge Bevilgningsreglementet skal utgiftsbevilgningene disponeres slik at ressursbruk og virkemidler er effektive i forhold til de forutsatte resultatmålene. Og det er virksomhetsleders ansvar å sikre at nødvendige rutiner og systemer er på plass, at ansvar og myndighet er forstått og at planer og mål følges opp.

Gjennomføring av en revisjon av virksomhetsstyring

En revisjon av virksomhetsstyring krever i likhet med revisjon av andre saksforhold god planlegging og en metodisk tilnærming som tar høyde for den antatte risikoen. En revisjon av virksomhetsstyring kan bli svært omfattende. Virksomheten kan ha problemer med å oppfylle målkravene, styringsinformasjonen kan mangle eller være mindre relevant, og det kan være usikkert om virksomheten har effektiv drift. Revisjon av virksomhetsstyring innebærer både en resultatorientert, en systemorientert og en problemorientert tilnærming. Som regel krever revisjonen at man har en metodisk tilnærming hvor systemet vurderes fra flere nivåer i organisasjonen, både et top-down og et bottom-up perspektiv.

Virksomhetsstyring innebærer at det skal være etablert et system for å styre både på kort og lang sikt. Det betyr at virksomheten bør ha mål som er rettet mot effektene av tjenesten eller produksjonen, men den må også ha informasjon som forteller hvordan det går i det daglige arbeidet. For eksempel: Når virksomheten saksbehandlingstidene, og har den effektive arbeidsprosesser? Har den rutiner for å følge opp at arbeidsprosessene er effektive, og er det en systematisk læring i organisasjonen som sikrer kontinuerlige forbedringer? Har virksomheten systemer som sikrer at ressurser omfordeles dersom uforutsette hendelser skulle oppstå? Revisjonen må vurdere om virksomheten har en balansert styring hvor sammenhengen mellom de kortsiktige og de langsiktige målene er ivaretatt.

Revisjonen må også sjekke ut at virksomheten kan begrunne hvorfor den har valgt det styringssystemet den har. Styringssystemet skal være tilpasset virksomhetens egenart og risiko, og så er det opp til revisjonen å vurdere om styringssystemet er tilstrekkelig ut fra revisjonskriteriene. Ikke minst er det også viktig at informasjon fra styringssystemet brukes til å forbedre arbeidsprosessene og måloppnåelsen.

Siden en revisjon av virksomhetsstyring fort kan bli meget omfattende, må revisor ofte erkjenne at man ikke rekker å se på alt. Det er derfor nødvendig å velge ut områder, organisatoriske enheter og/eller aktiviteter som skal studeres nærmere i revisjonen. I tillegg til å gjøre et utvalg blant virksomhetens primæroppgaver, må man også se på om administrative støttefunksjoner understøtter en effektiv oppgaveløsning. Det er viktig at revisjonen velger ut områder som hver for seg og samlet er vesentlige for virksomheten. Ved å gjøre dette er det på vesentlige områder mulig å undersøke om styringen er tilpasset områdets risiko og egenart og om etatens virksomhetsstyring samlet sett ivaretar de krav som stilles til gode styringsprosesser og god intern kontroll. Med et godt metodisk design kan revisor med rimelig sikkerhet si noe om hvorvidt virksomheten har effektiv drift, om kvaliteten i oppgaveløsningen overvåkes og om virksomheten har rutiner og kultur som bidrar til læring og utvikling.

Mange virksomheter har på plass elementer i virksomhetsstyringen, men elementene henger ikke alltid godt nok sammen. For eksempel ser vi ofte at styringsinformasjon ikke blir brukt til læring, eller at virksomheten har større ambisjoner når det gjelder hva den ønsker å styre på enn hva den har kapasitet til å gjennomføre.
Jeg tror at gode og mer helhetlige revisjoner av virksomhetsstyringen vil kunne være nyttige innspill til forbedringer i den enkelte virksomhet.

Nyheter fra sekretariatet, IIA og andre samarbeidspartnere

Av Ellen Brataas, generalsekretær

Veiledning i beste praksis for Compliance-funksjonen

Nettverk compliance har ferdigstilt utkast til en veiledning til beste praksis for organisering av compliance-funksjonen. Planen er at utkastet skal sendes på høring i desember og forhåpentligvis kan veiledningen lanseres primo 2015. Veiledningen er en overordnet beskrivelse ment til bruk for nye compliance-funksjoner, eller ledere som vurderer å etablere en compliance-funksjon. Veiledningen er bransje-uavhengig. Som vedlegg til veiledningen har nettverk compliance som formål å lage diverse maler som skal være til støtte og fri benyttelse for compliance-funksjon.

Foreslåtte endringer i rammeverket (IPPF) for profesjonen

Som flere kanskje har lagt merke til, har IIA kommet med forslag til endringer i strukturen i rammeverket for profesjonen, IPPF. Forslaget har ligget ute på høring denne høsten, og alle medlemmer, institutter og interessenter har fått muligheten til å gi tilbakemelding. Jeg har hørt rykter om at det har kommet inn rundt 3 000 kommentarer som IIA skal gå igjennom på Mid-year meeting i Orlando i desember. Det er ikke selve standardene som skal endres i denne omgang, men det forslås å lage en «mission» som skal forklare internrevisjon på en enkel måte, utarbeide prinsipper som de prinsippbaserte standardene skal tuftes på samt gjøre om i hierarkiet til practice advisories, position papers og practice guides.

COSO har satt i gang et prosjekt for å oppdatere COSO ERM

COSO-rapporten "Intern kontroll et integrert rammeverk" (COSO 1) ble oppdatert i 2013. Nå er turen kommet til COSO ERM "Helhetlig risikostyring – et integrert rammeverk" (COSO 2), som første gang ble utgitt i 2004. Verden er i konstant endring, og rammeverkene må oppdateres for å være relevante. Akkurat nå kan du gi innspill til nåværende rammeverk og forslag til forbedringer via en undersøkelse på COSOs hjemmesider, www.coso.org. Dette vil danne grunnlaget for første utkast til oppdatert rammeverk.

Konferansedatoer verdt å merke seg

NIRFs årskonferanse, 31. mai – 2. juni 2015, Trondheim, Norge
CAE Nordic Light, 11. – 12. juni 2015, Stockholm, Sverige
IIAs International Conference, 5. – 8. juli 2015, Vancouver, Canada
ECIIA Conference, 19. – 22. september 2015, Paris, Frankrike

The Institute of Internal Auditors | Global

Nye veiledninger fra IIA siden forrige nummer av SIRK:

Practice Guide: Business Continuity Management

Business continuity management (BCM) is a risk management approach based on business value. It matches business continuity capabilities and risks. The goal of BCM is to enable any organization to restore critical operational activities, manage communications, and minimize financial and other effects of a disaster, business disruption, or other major events. This practice guide specifically discusses the definitions of Business Continuity Management (BCM) and Crisis Management (CM), the activities that may be performed by internal audit before, during, and after a crisis and internal audit's evaluation of key BCM elements. Also, practice aids are provided in the appendices.

Practice Guide: Auditing Anti-bribery and Anti-corruption Programs

The IIA's new Practice Guide: *Auditing Anti-bribery and Anti-corruption Programs* offers internal audit practitioners insight on the nature of bribery and corruption in organizations throughout the world. It discusses the current business landscape and stresses that no organization, regardless of whether it is public, private, large or small is immune from the devastating impacts bribery and corruptions bring. The guide provides an overview of the key components necessary to effectively audit prevention and deterrence programs.

Policy Setting for Public Sector Auditing in the Absence of Government Legislation

This Global Public Sector Insight will assist government organizations for which legislation has not been developed in relation to audit activities or is relatively narrow in scope. This publication navigates audit practitioners and their key stakeholders in a practical way to develop suitable policies and procedures for the entire organization in the absence of government legislation.

The five-step process shared in this report for developing all-encompassing policies and procedures could be beneficial to any organization and its audit activity.

Independent Audit Committees in Public Sector Organizations

Independent audit committees help public sector organizations meet taxpayers' increasing demands for transparency and accountability by providing oversight of management practices in key governance areas such as risk management, internal audit, value and ethics, governance, financial stability, and others. Strong audit committees build public trust and confidence in how organizations are managed and strengthen the independence and value of the internal audit activity. This Global Public Sector Insight is designed to communicate the importance of independent public sector audit committees, the value they provide, and how an organization can properly establish an audit committee.

New Research Reports from The IIA Research Foundation:

Internal Audit Capabilities and Performance Levels in the Public Sector

Internal Audit Capabilities and Performance Levels in the Public Sector, provides a global bird's-eye view of public sector internal audit activities. Co-authored by the lead researcher and principal author of the Nine Elements Required for Internal Audit Effectiveness in the Public Sector, Elizabeth MacRae, CGAP, this new report analyzes the survey responses of public sector chief audit executives (CAEs). As part of The Global Internal Audit Common Body of Knowledge (CBOK) Study, this report provides the first-ever public sector-specific analysis of its kind, delivering a snapshot of what public sector internal audit activities are doing well, what they could improve upon, and what the main differences are by region.

High-level takeaways from the report include:

- Internal auditors' perception of how they can, or should, add value to their organizations.
- The most common activities undertaken by internal audit functions and the tools used to carry them out.
- A demographic profile of internal auditors.

Cybersecurity – What the Board of Directors Needs to Ask

The overwhelming number of cybercrime incidents in recent months has forced boards of directors to ask strategic and thoughtful questions directed toward management and internal audit. Boards need to take a more proactive role in cybersecurity or face the possibility of lawsuits in the event of a security breach. Yet in The IIA Audit Executive Center's "Pulse of the Profession 2014" survey, when asked how involved the board was during the last fiscal year in regard to specific action or requests on cybersecurity preparedness, only 14% responded they were actively involved.

The IIA Research Foundation, in partnership with ISACA, commissioned the research report, Cybersecurity: What the Board of Directors Needs to Ask, to:

- Help directors know how they should react to cybersecurity breaches and what to do.
- Understand that cybersecurity is an enterprisewide issue, not just an IT issue.
- Know what the IT auditor's role is in helping the Board of Directors address the issue.

The report also outlines the NACD's five principles for the board, and provides a list of top questions every board needs to ask.

Internal Audit Around the World

This research report provides an in-depth analysis of the factors and rationale behind the development of the profession and seeks to identify opportunities for the transfer of success stories to the rest of the internal audit community. To perform the analysis, the researchers initially analyzed the 2010 CBOK results, comparing the data for each region. Where the 2010 and 2006 survey questions were comparable, a temporal comparison was conducted to analyze those trends.

The Value of Quality and Improvement Programs: A Global Perspective

Researched and developed by IIA–France, this research provides an overview of the current state of Quality Assurance and Improvement Programs (QAIPs) around the world. The report, which incorporated responses from more than 1 000 practitioners in 46 countries, offers practical information about leading QAIP practices and specifically addresses:

- Added value specific to the internal audit function.
- The most commonly cited challenges to building and sustaining a QAIP.
- Ways in which respondents believe the QAIP has added value to their organization.

This can be used to identify key factors for successfully implementing QAIPs and communicate the benefits of QAIPs to audit committees and boards. To assist in this process, the report also includes suggestions for CAEs as to how they can engage stakeholders in a meaningful dialogue about internal audit's value.

Promoting internal audit in European corporate governance

The ECIIA has worked hard over the last twelve months to promote the value of internal audit in European corporate governance. One of ECIIA's key messages has been that good coordination between internal and external audit adds real value and increases the effectiveness of corporate governance. It published its *position paper Improving cooperation between internal and external audit* during the year to illustrate best practice in this area. It explored this theme further with the European Organisation of Supreme Audit Institutions (EUROSAI) in a joint study on better cooperation between internal auditors and supreme audit institutions.

With audit reform on the agenda of the European Commission, ECIIA was involved in thought leadership activities too. For example, it organised a round table discussion on the topic at the European Parliament.

☞

ECIIA had regular meetings with the European Insurance and Occupational Pensions Authority (EIOPA) to review the impact of Solvency II and the role of internal audit; and it reinforced its collaboration with EUROSAI by signing a new agreement with them on 19 June 2014 in The Hague.

"Twenty-fourteen was a busy year for us, but 2015 promises to be even more important," Thijs Smit, ECIIA President says. "We will continue to represent the profession, ensuring that the role of internal audit and best practice are properly understood and taken into consideration."

Ny veiledning fra ECIIA (the European Confederation of Institute of Internal Auditors) med titteleen "Audit and Risk Committees"

Endring i lovgivning gir behov for etablering av risikoutvalg innen finansielle virksomheter – dette vil være noe som kan bli aktuelt også for andre virksomheter

ECIIA og FERMA (the Federation of European Risk Management Associations) har samarbeidet om å utarbeide en veiledning til styrer for å hjelpe med tilpasninger til den siste utviklingen i selskapslovgivning i EU, med blant annet etablering av risikoutvalg.

Formålet med veiledningen er å belyse mulige konsekvenser av ny lovgivning, med fokus på etablering av risikoutvalg i tillegg til revisjonsutvalg. Dokumentet gir råd om hvordan revisjons- og risikoutvalg kan understøtte selskapsstyret, samt få bistand fra risk management og internrevisjon. Krav til etablering av risikoutvalg må ses på som en direkte følge av finanskrisen. Evalueringer som er gjennomført etter finanskrisen viser at en forklaring til at det gikk galt var blant annet svakhet i risikostyring og at styret ikke fikk presentert en helhetlig oversikt over virksomhetens risikoer. Ett annet forhold som har blitt trukket frem var at flere selskaper hadde etablert en unødig komplisert organisering, med utydelige roller og ansvar.

Bente Sverdrup, revisjonsdirektør i Gjensidige var medlem i arbeidsutvalget og sier om publikasjonen; "Arbeidet med denne veiledningen viser hvor viktig det er å sørge for at risk management og internrevisjonen bidrar med helhetsbilde i sin rapportering. Dette for å hjelpe styret med dets ansvar for å sikre at virksomheten har oversikt over de vesentligste risikoene og at det er etablert tiltak som skal sikre effektiv styring og kontroll. En må også huske på at krav til risikoutvalg har sitt utspring innen store internasjonale finanskonsern, hvor evalueringer etter finanskrisen viser at de før var organisert på en uhensiktsmessig måte. 2. og 3. linjen evnet ikke i tilstrekkelig grad å bistå med helhetsbildet på risikosituasjonen. Utfordringen med etablering av eget risikoutvalg er at det er stor grad av overlapp av oppgaver mellom risikoutvalg og revisjonsutvalg. Det betyr mer byråkrati og behov for koordinering og kan fremstå unødvendig og faktisk lite hensiktsmessig i mindre virksomheter eller mindre komplekse virksomheter. Kontrollfunksjonene skal utfordre at 1. linjen overskuer egne risikoer og at nødvendige tiltak blir iverksatt, det er her 2. og 3. linjen kan tilføre verdi».

White Paper from IIA Netherlands: Combining Internal Audit and Second Line of Defense Functions?

There are many different views across companies and industries on the benefits, feasibility and acceptability of combining risk, compliance and assurance functions. Management Boards, Supervisory Boards (in particular the Audit Committee) and other governing bodies want to know if such combinations are possible, and under which circumstances, based on which basic conditions and facilitated by which safeguards. The key question is if the Internal Audit Function can work independently and objectively if support is provided on areas relating to risk management, compliance and internal controls.

In order to answer these questions and provide clear direction to the stakeholders involved, a task force of IIA Netherlands conducted research and held roundtable sessions. This white paper provides an overview of existing global standards and good practices and considers the different stakeholder perspectives.

Tips: Du kan laste ned standardene og alle veiledninger ved å logge deg på medlemssiden.

Upcoming Guidance

Enhancing Integrated Reporting – Internal Audit Value Proposition
A European task force was initiated in April 2014 by IIA UK & Ireland, IIA Spain, IIA Netherlands, IIA France and IIA Norway, to clarify the impact of Integrated Reporting (<IR>) on internal audit activity. The task force propositions are not mandatory. They are based on the International Professional Practices Framework (IPPF) of The IIA and a literature review on <IR>. Each section of the <IR> framework has been reviewed to:

- highlight the IIRC recommendations;
- identify potential challenges to and enablers for the implementation of these recommendations;
- clarify the underlying governance, risk and control issues;
- discuss internal audit¡¦s assurance and advisory role;
- share good practices. For example, regarding coordination with other functions.

Eli Moe-Helgesen (PwC) has been IIA Norway's voice in the group. The proposition is expected to be released by year end 2014.

Audit Channel.tv
I tråd med mottoet "Fremskritt gjennom deling av kunnskap" har IIA laget en videoside som publiserer videosnutter fra hele verden med relevant innhold for internrevisorer og andre. Såkalte "videokanaler" fokuserer på områder som misligheter, compliance, goveranance, risk, etikk og mye mer. Gå til - www.auditchannel.tv og vurder innholdet selv.

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

Sertifiseringshjørnet

Certified Internal Auditor (CIA)
Minner om at fra 1. juli 2013 skal CIA-kandidater bestå tre, ikke fire, eksamener som tidligere. CIA del 1 består av 125 spørsmål, mens del 2 og 3 er på 100 spørsmål hver. Hvilke områder som testes på den enkelte eksamen, finner du en detaljert oversikt over på www.globaliia.org. Kravet til to års praksis er ikke endret. Selv om du ikke har tilstrekkelig praksis, kan du avlegge eksamene og får automatisk tildelt CIA-tittelen hvis du oppfyller kravet til praksis innen fire år. Du avlegger eksamen hos et test-senter i Oslo, eller andre deler av verden, når det passer din kalender best.

Certification in Risk Management Assurance (CRMA)
Det er nå muligheter for å avlegge CRMA-eksamen som består av 100 mulitiple-choice spørsmål fra følgende områder:
Domain I: Organizational governance related to risk management (25-30 %)
Domain II: Principles of risk management processes (25-30 %)
Domain III: Assurance role of the Internal Auditor (20-25 %)
Domain IV: Consulting role of the Internal Auditor (20-25 %)

I tillegg må du også ha bestått del 1 av CIA eksamen og kravet til praksis for å oppnå tittelen CRMA.
Les mer på www.gobaliia.org.

Årlig innrapportering av CPE-poeng
Fra og med 2013 skal alle som innehar en global sertifisering, selv rapportere poengene direkte inn i IIAs CCMS-system. Poeng for 2014 må rapporteres innen 31.12.2014. Det holder å rapportere at man har nok poeng, så man trenger ikke føre opp alle kurs eller poenggivende aktiviteter. Dokumentasjonen skal ikke sendes inn til IIA, men må tas vare på som bevis dersom du blir trukket ut for tilfeldig kontroll fra IIA. NIRF har besluttet å dekke innrapporteringsgebyret fra IIA for alle sine medlemmer. Medlemmer velger derfor skjemaet «FORM-FEE WAIVED» for å unngå gebyr.

Denne prosedyren gjelder dessverre ikke for Diplomert Intern Revisor. Dere må derfor som tidligere år rapportere denne direkte til NIRF på post@iia.no.

NEWS: Qualification in Internal Audit Leadership (QIAL)
Today, growth and change in the internal auditing field is demanding a new type of leader — one who drives a high performing audit team while delivering value by consistently addressing stakeholder needs, top-down risks, and expectations of an evolving marketplace. The IIA has developed the Qualification in Internal Audit Leadership™ (QIAL™) to support you on this journey to be the next generation of visionaries for the profession. So whether you're an aspiring leader or an audit executive, the QIAL is the right qualification for the next stage in your career progression.

Find the QIAL Pathway that meets your level of experience below:

Elgibility Requirements		CIA	Experience	Other Elgibility	QIAL Pathway
Aspiring Leader	a	Yes	Five years' internal audit or related area		Program Pathway 1
New Leader	b	No	15 year's general management including three as audit executive	Now working as an audit executive	
	c	Yes	10 years' general management including three as audit executive	Now working as an audit executive	
Experienced Leader	d	No	15 years' general management including three as audit executive	Audit executive for three of last five years	Program Pathway 2
	e	Yes	10 years' general management including three as audit executive	Audit executive for three of last five years	

QIAL Method and Steps to Achievement
As a QIAL candidate, you'll work with an assigned panel of accomplished senior audit executives to give you highly focused feedback and coaching. You'll make a presentation based upon case information or your own experiences. The knowledge and skills you develop are directly linked to The IIA's latest Competency Framework. Although in-person sessions are beneficial, if schedules don't permit, web-based meetings are available.

Activities by Program Pathway	Program Pathway 1	Program Pathway 2
Case study 1	✔	Portefolio of Professional Experience
Case study 2	✔	
Case study 3	✔	
20-minute Presentation	✔	✔
90-minute Panel Interview	✔	✔
Post-qualifying	Continuing Professional Development	Continuing Professional Development

Methodology Description

QIAL Methodology	Description	Time
Three Case Studies	Candidates critically analyze an extensive set of complex information and produce a written response providing penetrating insights for a senior-level audience.	3 – 4 hours per case study
Portfolio of Professional Experience	Experienced AEs may opt to replace the three case- study exams and document their own professional experience with supporting evidence.	
Presentation	Candidates present to a senior-level panel on a set topic followed by a question and answer session.	20 minutes
Interview	A panel interview draws upon personal and professional experience.	90 minutes

QIAL Investment

	Member	Nonmember
Application	US$250	US$300
Case Study (or experience portfolio) unit 1	US$450	US$600
Case Study (or experience portfolio) unit 2	US$450	US$600
Case Study (or experience portfolio) unit 3	US$450	US$600
Presentation	US$950	US$1,150
Interview	US$1,450	US$1,750

Access CCMS to begin the application process or contact QIAL@theiia.org for more information.

INTERVJUTEKNIKK

Hvordan bli bedre til å intervjue? Hva som skal til for å beherske intervjusituasjonen, forberede og ta kontroll over intervjuet? Hvordan best få tak i relevant informasjon på en effektiv og formålstjenlig måte? 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, hvordan en stiller de gode enkeltspørsmålene, hvordan en hindrer avsporinger og hvordan en bestemmer mål og strategi for intervjuet.

Brynjulf Handgaard er programutvikler i NRK og forfatter av boken «Intervjuteknikk for journalister». Brynjulf har ved flere tidligere anledninger holdt kurset for NIRF og med gode skussmål.

Når: 10. og 11. februar 2015

Sted: Oslo

Pris: Medlemmer: kr 6 900, ikke-medlemmer: kr. 7 500

CPE: 14 for CIA, CCSA, CGAP, CFSA og Dipl. IR.

CIA EXAMINATION PREPARATION COURSE

The CIA designation is the only globally accepted certification for internal auditors and remains the standard by which individuals demonstrate their competency and professionalism in the internal auditing field. NIRF offers courses for candidates who want to achieve the CIA designation. The CIA exam consists of three parts, with one exam for each part. The exams are computer based multiple choice tests. Note: you don`t have to take the exam in any given order. In our experience, part three is the most challenging part of the exam, hence the offer of this course. However, if you are a native Norwegian speaker, you may benefit from attending these courses this fall in preparation for parts 1 and 2: Introduksjon til internrevisjon og Praktisk internrevisjon.

CIA preparation course part 3 will be of four days duration. The course will be held in Norwegian or in English if required by participants. This is also an opportunity to form study groups. It is recommended that you already got the study material for the CIA exams.

We got highly qualified members as instructors. In addition to a CIA designation, they got in-depth knowledge of the different parts of the CIA that they will be teaching.
Anders Blix, CIA, CISA, MBA from NHH. Anders has 14 years of experience as an internal auditor and IT auditor, and has been with EVRY since 2002.
Kent M. E. Kvalvik, CIA, CRMA, CGEIT, CRISC, Dipl. I.R. Kent is partner and head of Risk & Advisory Services at RSM.

Date: 10th - 13th of February, 2015

Place: Oslo, Norway

Price: NOK 9 800 for members and NOK 10 900 for non-members, IIA members from the Baltic region NOK 7 200

CPE: 24 for CIA, CRMA, CCSA, CGAP, CFSA and Dipl. IR.

WRITING REPORTS THAT GET READ

A lot of hard work goes into writing a report, but it does not always have the impact we would like. How do you make your voice heard? This one-day workshop will take you through the basics of writing for a professional audience. The workshop takes participants systematically through the most problematic areas of writing, with a focus on audience, core argument and structure. The workshop also covers developing good writing habits as well as giving and receiving feedback. Workshop objective is to increase participants' understanding of what professional writing is all about, how they can get more out of the writing process, and how they can most effectively reach their audience. The presentation will be held in English, but participants may bring Norwegian texts, and discussion can take place in either English or Norwegian.

Facilitator Lynn P. Nygaard has led writing workshops for academics and researchers for more than ten years, and works daily with researchers in the institute sector as an advisor. She has also published a practical guide for writing to make sense and be heard.

Date: 24th of February

Place: Oslo

Price: Members NOK 3 500, non-members NOK 3 800

CPE: 7 for CIA, CRMA, CCSA, CGAP, CFSA and Dipl. IR.

INTRODUKSJON TIL INTERNREVISJON

Kurset er en innføring i internrevisors roller og ansvar, begrepsavklaringer og definisjoner, samt hvilke etiske regler og hvilke krav som ligger i internrevisjonens standarder. Det vil gi deltagerne de nødvendige grunnkunnskaper i internrevisjon da det spesielt tar for seg de obligatoriske delene av det internasjonale rammeverket for profesjonell utøvelse av internrevisjon (IPPF). Kurset er nødvendig basiskunnskaper for kurset Praktisk internrevisjon som avholdes hver høst. Kurset passer for personer som er nye i internrevisjon, samt internrevisorer som ønsker oppfriskning av rammeverket.

Presenteres av Karl-Ludvig Mauland, partner i BDO og Hilde Tanggaard, rådgiver i NIRF.

Når: 24. mars 2015

Sted: Oslo

Pris: Medlemmer kr 3 500, ikke-medlemmer kr 3 800

CPE: 8 for CIA, CCSA, CGAP, CFSA, CRMA og Dip. IR.

NORGES INTERNE REVISORERS FORENING

www.iia.no

COSOS RAMMEVERK FOR INTERNKONTROLL

Internkontroll hjelper virksomheter med å oppnå viktige målsettinger, opprettholde og forbedre presentasjoner. COSOs *Internkontroll - et integrert rammeverk* 2013 gjør organisasjoner i stand til å utvikle målrettede og kostnadseffektive systemer for internkontroll, for å kunne tilpasse seg endringer i forretningsmiljø og rammebetingelser, redusere risikoer til akseptable nivåer og støtte opp under en hensiktsmessig beslutnings- og styringsprosess.

I kurset presenteres helheten i rammeverket, dets oppbygging, hva som er nytt i forhold til 1992-versjonen, nyhetene prinsipper og fokuspunkter, rammeverkets Illustrative Tools med de praktiske hjelpemidlene Templates og Scenarios, og hvordan rammeverket og de praktiske hjelpemidlene kan være til nytte for internrevisorer.

Presenteres av Tor Solbjørg, leder av internrevisjonen i Helse-Nord RHF og Karl-Ludvig Mauland, partner i BDO.

Når: 6. mai 2015

Sted: Oslo

Pris: Medlemmer kr 3 500, ikke-medlemmer kr 3 800

CPE: 8 for CIA, CCSA, CGAP, CFSA, CRMA og Dipl. IR.

KVALITET - MED HOVEDFOKUS PÅ EKSTERNE GJENNOMGANGER

Et program for kvalitetssikring og forbedring gjør det mulig å vurdere om internrevisjonen er i overensstemmelse med definisjon av internrevisjon, standardene og de etiske reglene. Samtidig skal programmet gjøre det mulig å vurdere effektiviteten og hensiktsmessigheten av internrevisjonen og identifisere muligheter for forbedring. Hva ligger egentlig i dette og hvilke krav setter standardene til kvalitet? Hva bør internrevisjonen ha fokus på og hvordan forbereder den seg til en ekstern evaluering? Disse sentrale spørsmålene skal vi belyse gjennom forelesninger, erfaringsdeling og diskusjoner.

Kurset tar utgangspunkt i kvalitetsmanualen fra IIA Quality Assessment Manual for the Internal Audit Activity, 7th edition. Vi har tilpasset gjennomgangen til norske forhold, samt at vi har utviklet egne verktøy. Det er ingen «one size fits all» så vi vil formidle hvordan du best kan anvende verktøykassen i din virksomhet. NIRF har utført ekstern evalueringer siden 2009 og vil i kurset trekke på tidligere erfaringer og generelle observasjoner.

Forelesere: Ellen Brataas, CIA, CRMA, CISA, generalsekretær i NIRF og Hilde Tanggaard, Dipl. IR, rådgiver i NIRF.

Når: 17. mars

Sted: Oslo

Pris: Medlemmer kr 4 400, ikke-medlemmer 4 700. Inkludert i kursavgiften er IIA Quality Assessment Manual 7th edition.

CPE: 7 for CIA, CRMA, CCSA, CGAP, CFSA og Dipl. IR.

IIA Norway is delighted to have James Paterson return to Norway, this time to deliver courses on ***Lean Auditing*** and ***Assurance mapping***. James delivers training on this topic for the IIA UK and works as a consultant in this field. If attending both courses you will qualify for a discount of NOK 600 off the total fee. Price for one day: Members NOK 3 500, Non-members: NOK 3 800.

LEAN AUDITING – DRIVING VALUE AND PRODUCTIVITY IN AUDIT

This course addresses two key questions 1) how to define value added from internal audit and what does delivering the maximum value add look like from audit, and 2) how to drive efficiency and productivity in audit, beyond simple benchmarking of efficiency right back to first principles.

Upon completion of the lean auditing workshop you will be able to apply lean tools and techniques to make your internal audit efforts more streamlined, develop greater insights into the key stakeholders of audit, have a clearer sense of how lean your audit function is compared to others, and develop a practical, step-by-step route map of the key areas to focus on to add value and improve efficiency.

Presented by James Paterson, who has specialist skills in this field and real life experience applying lean to the internal audit team at AstraZeneca. James has written a book on lean auditing that will be published just ahead of the workshop and this workshop gives us a great opportunity to hear the latest about progressive audit practices from leaning audit functions.

Time: Monday 2nd of February

Place: Oslo

CPE: 8 Continuing Professional Education points for CIA, CRMA, CCSA, CGAP, CFSA and Dipl. IR.

RISK ASSURANCE MAPPING

Risk assurance maps and Risk assurance frameworks are a vital tool for a modern progressive internal audit function. A robust assurance map or risk assurance framework can give greater confidence to stakeholders that key risks and objectives are being properly managed, help to clarify how the risk assurance jigsaw is joined up – or not, act as a tool to enhance the quality of risk assessments by the wider organisation, act as an important accountability framework to confirm and clarify how key business objectives and key business risks are being managed, and provide stakeholders with a clearer sense of the best way to allocate the resources of internal audit. Upon completion of the assurance mapping workshop you will be able to deliver assurance in a timely and cost effective way, with clear benefits for key stakeholders, save time and effort in terms of delivering assurance maps with internal resources, recognize the key components of an effective assurance map, assess your current efforts and plans to deliver an assurance map so that you can avoid the common pitfalls and difficulties, build a realistic business case for an assurance map, including likely 'quick wins', and prioritise your current efforts and understand future opportunities, including assurance scorecards and synergy opportunities.

Time: Tuesday 3rd of February

Place: Oslo

CPE: 8 Continuing Professional Education points for CIA, CRMA, CCSA, CGAP, CFSA and Dipl. IR.

På tampen

Det hadde seg slik at vi var to som dro på ferie til det sydlige Frankrike, nærmere bestemt Lyon. Reisen var godt forberedt og planlagt som seg hør og bør når revisorer drar på tur. Planen var, siden vi befant oss midt i vin- og matdistriktet, at vi virkelig skulle slå på stortromma og bestille bord på en Michelin-restaurant. Bestillingen ble selvfølgelig ordnet i god tid. Vi hadde litt vanskeligheter med å finne et egnet sted siden vår ferie var lagt til en tid der de fleste franskmenn inklusive de fleste kokker, også var dratt på ferie.

Vi fant imidlertid frem til en restaurant som vi etter nøye vurderinger mente skulle holde mål. Den hadde én stjerne. Menyen som var bestilt på forhånd inneholdt hele syv retter. Vinpakke var også forhåndsbestilt. Vi hadde der valget mellom en pakke på tre, fire eller fem viner. Vurderingen var at tre var litt snaut, mens fem var for råflott, så vi falt ned på fire viner.

Vi dro på oss våre beste antrekk og stilte presis til avtalt tid. Vi ble vist til et nydelig bord. Restauranten lå solvendt, med flott utsikt over byen og vi hadde bord ute på terrassen. Det svermet rundt oss av kelnere og vinkelnere og vi bestilte først en *kir royal* som vi mente var på sin plass, omgivelsene tatt i betraktning. Denne bestillingen klarte restauranten imidlertid å kludre til, men vi fikk noe som lignet, og gjorde ikke noe nummer av det.

Før vi visste ordet av det stod første rett på bordet med en passende vin til. Det fulgte deretter på med *Médaillon de homard, Loup de mer grillé, Filet de canard* med flere bitte små hvileretter innimellom før vi var over på det søte med *Petite gourmandise*. Vi var så interessert i det vi fikk servert at mobilen ble sneket frem for en liten snapp hver gang det kom en ny rett på bordet.

Vi koste oss og snakket og smattet og drakk og glemte nesten å følge med på antallet retter. Plutselig sto siste dessert på bordet med dessertvin til. Vi fortærte også dette før vi begynte å telle opp hva vi hadde fått i oss. Vi repeterte de viner vi hadde satt til livs, og var kjapt helt enige om at vi kun hadde fått servert tre viner. Dette kunne kontrolleres mot den dokumentasjon som befant seg på mobilen. Vi var likevel så fornøyde med måltidet og opplevelsen at vi ikke så på dette som noe problem.

I mellomtiden hadde det brutt ut et forferdelig tordenvær med dertil hørende styrtregn som skylte innover terrassen. Måltidet var på dette tidspunktet nærmest avsluttet og vi fant da at vi ville vende nesen hjem mot hotellet. Pengehåndteringen ble ivaretatt av en ung dame som var plassert i hjørnet av restauranten, rett ved utgangen.

Denne damen presenterte oss for regningen, som naturligvis ble nøye kontrollert. Til vår store overraskelse hadde vi blitt fakturert for en vinpakke med fire viner! Nå hadde vi nok kunnet godta den prisforskjellen det ene glasset representerte uten at det hadde tatt fra oss nattesøvnen, men vi kunne simpelthen ikke unngå å påpeke feilen. Damen lot oss forstå at hun måtte ta kontakt med den aktuelle vinkelneren, som straks ble kalt bort til kassen.

Lyon Basilique de Fourvière. Foto: Redaksjonen

Heldigvis var alle i denne restauranten i stand til å forstå vår engelsk, og vi forklarte glippen på nytt til den unge vinkelneren. Vårt budskap var at her er det begått ikke mindre enn tre feil. For det første hadde vi fått feil vordrink. Dernest hadde vi ikke fått servert hele den vinpakken vi hadde bestilt. Til slutt var vi blitt fakturert for den vinen vi ikke hadde mottatt. Det ble også lagt til noe fra vår side om at dette var en lite anbefalelsesverdig opplevelse fra en restaurant av denne kaliber, mens vi forsøkte å la det skinne gjennom at vi var svært erfarne Michelin-travere.

Vinkelneren ble gjennom vår redegjørelse først lysegrønn i ansiktet. Så ble han helt stum. Så ble han enda grønnere. Vi forsto raskt at dette var en svært ubehagelig opplevelse for ham. Han var nok livredd for at vi skulle rapportere til hovmesteren eller enda verre, at vi skulle offentliggjøre skandalen gjennom Trip Advisor.

Når personalet fikk summet seg ble vi presentert for en korrigert regning og en paraply etter at vi høflig hadde avslått tilbudet om gratis champagne. Vinkelneren pustet lettet ut, og følte seg nok helt sikkert skjerpet og gjennomrevidert for en stund. Mette og tilfredse bega vi oss ut i regnet.

Returadresse: NIRF, Postboks 1417 Vika, 0115 Oslo

www.pwc.no

Styring og kontroll skaper verdier

pwc

Kontaktpersoner

Eli Moe-Helgesen
Tlf: 952 60 113
eli.moe-helgesen@no.pwc.com

Petra Liset
Tlf: 952 60 152
petra.liset@no.pwc.com

Jonas Gaudernack
Tlf: 952 60 769
jonas.gaudernack@no.pwc.com

Bedre styring og kontroll er fellesnevnere for våre bidrag til økt verdiskaping. Det bygger og sikrer tilliten til din virksomhet, det legger grunnlaget for at dere satser riktig og det reduserer risikoen for negative hendelser.

Store bedrifter har gjerne komplekse utfordringer og muligheter, hvor løsningene krever tverrfaglig samarbeid.

La oss snakkes om hva våre revisorer, rådgivere, advokater og regnskapsspesialister kan gjøre sammen med deg for å forbedre din bedrift!

ISSN 1892-9370