SIRK

Styring – Internrevisjon – Risiko – Kontroll

Nr 1 2017

IIA Norge

REDAKTØRENS SPALTE

ELLEN BRATAAS

I Mediakomiteen er vi alltid spent på om vi klarer å få nok stoff til det neste nummeret av SIRK. I de første komitemøtene drodler vi, tenker høyt og diskuterer hvilke temaer som er aktuelle, hvilke personer/organisasjoner som kan mene noe om enkelte temaer, hva nettverkene kan bidra med osv. Mot slutten av perioden er det et kaos av armer og bein i form av purring på artikler, overskridelser av deadline, kvalitetssikring, korrekturlesing, valg av bilder og ikke minst; hva må ut-oppgaven. Både ved utgivelsen av forrige nummer og i denne utgaven har vi satt rekord i antall sider, noe som medfører at enkelte artikler må spares til neste nummer. Dette er et fantastisk «luksusproblem» som bare bekrefter at fagområdene som er omfattet i SIRK, har mange innfallsvinkler og gir rom for et utall interessante artikler. Det beviser også at vi har mange engasjerte skribenter og bidragsytere som gjerne tar tastaturet fatt og deler av egne erfaringer.

I dette nummeret av SIRK kan vi by på mye interessant lesning og påfyll til inspirasjon. Om jeg kort skal oppsummere den røde tråden i dette nummeret, må det være at det slettes ikke er noen. SIRK og foreningen er ikke lenger spisset kun mot internrevisjonsfaget, men inkluderer risiko, compliance og andre nettverk og fagområder som naturlig hører sammen og som glir over i hverandres fagfelt. For å overføre Ronald Reagans kjente sitat «Tear down this wall!» til våre fagområder, kan man si at koordinering og samhandling mellom funksjoner vil være avgjørende for god og effektiv virksomhetsstyring i en verden som endrer seg raskt.

I tiden som kommer vil automatisering og kunstig intelligens påvirke hvordan vi jobber med fagområdene, samtidig som ulike forretningsområder integreres. Hvordan utfordrer dette dagens forretningsmodeller? Hva får dette å si for internrevisjonsprofesjonen? Hvilke kunnskaper må de som jobber med risikostyring, compliance og internrevisjon tilegne seg? Hvordan jobbe smartere og mer effektivt? Det finnes ingen fasitsvar på alle disse spørsmålene, men flere av artiklene i denne utgaven setter søkelys på fremtiden og gir deg «food for thought» du kan bruke late sommerdager til å fundere mer over.

Redaksjonen ønsker alle en solfylt vår og en riktig god sommer!

INGUNN VALVATNE
PRESIDENT
IIA NORGE

IIA SOM GLOBAL ORGANISASJON

Flere har kanskje lagt merke til at NIRF navnet er skiftet ut med IIA Norge. En av begrunnelsene var å synliggjøre det globale nettverket vi er en del av, med over 200.000 medlemmer globalt. IIAs øverste organ, Global Council, møtes årlig for å diskutere strategi og felles anliggender for de ulike filialene i IIA. Årets møte ble avholdt i Roma i februar med deltakelse fra over 80 land. Internasjonalt arbeid med sikte på konsensus krever gode forandringsprosesser og nysgjerrighet på hverandres kultur, og årets møte hadde fokus på strategien for perioden 2019–23.

IIAs overordnede visjon ligger fast. IIA skal fortsatt sørge for kunnskapsformidling og tilby veiledning av høy kvalitet til medlemmene. Kunnskapsformidling, samarbeid og god profesjonsutøvelse skal bidra til at vi får den aksepten vi har fortjent som profesjon.

Så langt er det lett å være enig. I diskusjonen om en strategi, som på en god måte skal sette oss i stand til å realisere en ambisiøs visjon, fremholdt mange lands organisasjoner at det er behov for endringer. Flere organisasjoner hevdet at de har behov for mer støtte i arbeidet med å skape økt aksept for internrevisjonens rolle blant brukerne; myndigheter, styrer etc. Kommunikasjonsverktøy for å demonstrere «added value» ble etterspurt. Selv tenker jeg dette er en krevende utfordring å løse globalt. Kommunikasjon handler jo nettopp om å kjenne sine brukere og om å forstå konteksten vi virker i. Vi må utveksle erfaringer lokalt.

Revisjon har tradisjonelt vært en tilbakeskuende aktivitet; hva gikk galt og hvordan kan vi hindre gjentakelse. I en omskiftelig verden blir erfaringene mindre verdt som læringselementer, endrede rammebetingelser roper på nye løsninger. Digitalisering og endring i bransjestrukturer er stikkord. Mange var nettopp opptatt av internrevisjonens evne til å tilpasse seg skiftende utfordringer og hvordan IIA kan sette sine medlemmer i stand til å speile organisasjonenes raske utvikling og innovasjon.

IIAs medlemsmasse er mangfoldig, og behovene er ulike mellom de ulike land. Noen filialer kritiserte IIA for å ha for lite oppmerksomhet mot de små organisasjonenes utfordringer, særlig fordi så stor del av virksomheten er basert på frivillig arbeid.
Mange av utfordringene er lett gjenkjennbare, og vi må fortsatt arbeide systematisk for å etablere en rød tråd fra den globale IIA til vår egen hjemmebase. Men når det gjelder dugnadsånd er vi privilegerte i IIA Norge. Frivillige komiteer og nettverk utgjør en effektiv førstelinje i IIA Norge. Det nedlegges et imponerende arbeid for å støtte våre medlemmer. Årets andre SIRK nummer er ett av mange konkrete eksempler, spekket med artikler som retter søkelyset bredt, men mest framover. Enig eller uenig i innhold, slik meningsutveksling er viktig for å gi oss en felles plattform som gruppe. Risikonettverket har nettopp lansert IIAs veileder for risikostyring, et annet viktig bidrag i arbeidet med å sette internrevisjonens rolle inn i en utvidet kontekst.

Vi er også konferansekomiteen en takk skyldig. De har i år utarbeidet et interessant program for IIA Norges årskonferanse. Programmet har så langt medført rekord i antall påmeldte. Her inngår flere viktige tema fra IIAs liste over utfordringer; hvordan kan internrevisjonen bli en bedre støtte for sine brukere? Hvilke endringer vil påvirke vår profesjon i årene framover? Vårens konferanse byr også på en unik anledning til å diskutere fremtidige utfordringer med likesinnede. Og til kollegial hygge.

God lesning. Og sees vi på Fornebu?

MEDIEKOMITEEN

Ellen Brataas
Generalsekretær
IIA Norge

Reidar Døli
Internrevisor,
Oslo Børs VPS

Martin Stevens
Internrevisor,
Gjensidige Forsikring

Esa Leporanta
Systems Audit Manager,
Nets Norway Branch

Magnus Digernes
Director
KPMG AS

Neste utgivelse er desember 2017

Årsabonnement: Kr. 150
Annonsepriser:
Kr. 5.000 for en helside
Kr. 3.000 for en halvside
Kr. 6.500 for baksiden
(mva. tilkommer)

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

Grafisk produksjon:
Merkur Grafisk AS

Forsidebilde:
Foto: corgarashu/shutterstock.com

www.pwc.no/karriere

Er du analytisk, engasjert og kreativ?

pwc

Ta gjerne kontakt for en uformell samtale

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

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

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

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

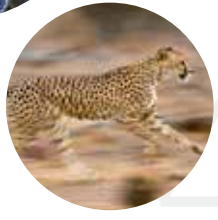
INNHOLD

RISIKOSTYRING

COMPLIANCE

VIRKSOMHETSSTYRING

18



50

24

6

20

INTERNREVISJON

FASTE SPALTER

Veileder for risiko-styringsfunksjonen

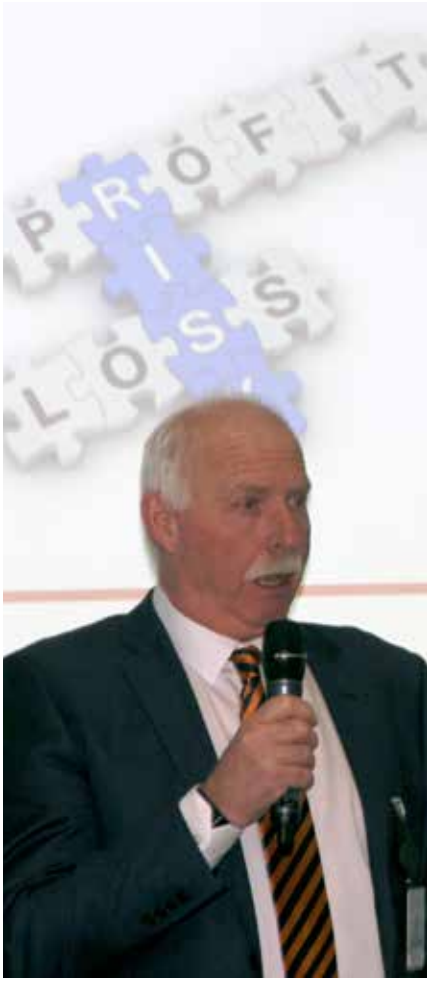
Av
OLE MARTIN KJØRSTAD
Nettverk risikostyring
IIA Norge

Som et utgangspunkt for de som skal etablere en risikostyringsfunksjon, eller evaluere egen virksomhets arbeid med risikostyring, har Nettverk risikostyring i IIA Norge laget en kortfattet og enkel veileder. Veilederen fokuserer på overordnet – eller helhetlig – risikostyring, gjerne kalt ERM (Enterprise Risk Management). Tanken er at den skal være egnet for styremedlemmer og ledere, like mye som for risikostyringsansvarlige.

Noen utfordringer alle i arbeidsgruppen på et tidlig tidspunkt kjente seg igjen i, var at det ofte vies for lite tid til å reflektere rundt hvordan risikostyringsarbeidet organiseres; man hopper gjerne rett til metodikken for oppstrømsrisikoanalyser og -rapportering. Dersom det skal legges til rette for et effektivt og verdiskapende arbeid med risikostyring, må man sørge for at funksjonen som får ansvaret har forutsetningene som trengs for å lykkes. Dette omfatter blant annet kompetanse og ressurser internt i funksjonen, men minst like viktig er grensesnittet mot styret, ledelsen og den øvrige organisasjonen.

Målet ble derfor å lage en kort veileder, som fokuserer på nettopp disse utfordringene. Veilederen skulle beskrive beste praksis for risikostyringsfunksjonen, uavhengig av bransje, kompleksitet og størrelse på virksomheten. Det er lagt vekt på grunnleggende prinsipper som er gyldige uavhengig av virksomhetens art. Metodikk for hvordan man skal innrette arbeidet med å identifisere, evaluere og følge opp risiko, er ikke beskrevet. Dette tar allerede mange gode og langt mer utfyllende rammeverk for seg. Anvendt metodikk vil dessuten fortone seg forskjellig i ulike bransjer og virksomheter.

Veilederen er delt inn i fire hoveddeler. Innledningen definerer kort hva som menes med helhetlig risikostyring. Det gis



også beskrivelse av forholdet mellom risikostyring, internkontroll og virksomhetsstyring. Del to tar for seg prinsipper som er viktige å huske i arbeidet med risikostyring. Hovedfokuset er lagt på ansvar, oppgaver og kommunikasjon. Deretter følger del tre, som omhandler organisering av risikostyringsarbeidet, med fokus på grensesnittet mot styret, ledelsen og øvrige funksjoner. I den fjerde og avsluttende delen, er det henvist til relevante rammeverk og standarder for risikostyring som er relevant for oppbygning av risikostyringsarbeidet. Veilederen er for øvrig også oversatt til engelsk.

Nettverk risikostyring i IIA Norge vil jobbe videre med veilederen og relatert materiale. Innspill til senere versjoner er derfor svært velkomne. Vi oppfordrer alle som har innspill og ideer til å ta kontakt på risikostyring@iia.no.

> Dersom det skal legges til rette for et effektivt og verdiskapende arbeid med risikostyring, må man sørge for at funksjonen som får ansvaret har forutsetningene som trengs for å lykkes.

Informasjon og kommunikasjon – forutsetninger for god risikostyring

Av
HELGE BENUM
Seniorkonsulent
Transcendent Group

IIA Norge utga nylig sin «Veileder for Risikostyringsfunksjonen». Om helhetlig risikostyring sier veilederen, som for øvrig er vel verdt å lese, blant annet: «Kort sagt handler risikostyring om å fremskaffe et best mulig beslutningsgrunnlag og å legge til rette for effektiv gjennomføring og oppfølging av beslutninger». Denne artikkelen skal handle om nettopp beslutninger og betydningen av kommunikasjon for å sikre at beslutningene blir gode.

Hvis et tre faller i skogen og ingen hører det, lager det da en lyd? Eller hvis hver tiende faktura betales to ganger men ingen i ledelsen vet det, har det da noen konsekvens? Spørsmålene er analogier, men mens det første legger opp til undring rundt fysiske objekters eksistens i seg selv, er svaret på det andre tilsynelatende enkelt nok. Ingen som driver kommersiell virksomhet ønsker vel å betale ut mer enn de må?!

Men hva om kostnaden for å utbedre feilen er høyere enn verdien av feilbetalingene? Hva om det å betale ut dobbelt har andre negative effekter for virksomheten? Hvor mye bør virksomheten investere i å redusere antall feilutbetalinger? Hva er riktig kontrollnivå? Disse spørsmålene bringer oss tilbake til viktigheten av kommunikasjon. For at virksomheten i det hele tatt skal kunne ta tak i problemet må de som har beslutningsmyndighet og som kontrollerer ressursene aller først få informasjon om at problemet finnes. Dernest kan de innhente mer informasjon for å skaffe seg et bredest mulig beslutningsgrunnlag.

Som oftest er det ikke beslutningstakerne selv som skal utbedre problemet, og for at det skal skje en endring, må informasjonen om beslutningen flyte nedover eller sidelengs i organisasjonen til den havner hos en utfører. For å sikre at endringen har forventet effekt, må deretter informasjon om effekten kommuniseres tilbake til beslutningstakerne.

Eksemplet over dreier seg om driftsrelaterte feil, men er bare en av mange mulige illustrasjoner. Ta for eksempel innkjøpsavdelingen som fanger opp at det er stor økning i etterspørselen etter enkelte innsatsfaktorer, eller at nye aktører er aktive på markedet. Dette kan være viktig informasjon for beslutningstakere som skal ta strategiske valg for virksomheten. Eller for å snu på det. Styrets og toppledelsens beslutninger om å endre strategien eller virksomhetens risikoappetitt får ikke effekt ved at de blir uttalt, men når resten av organisasjonen faktisk har endret adferd og prioriteringer. I kjernen av dette ligger kommunikasjon (og enda mer kommunikasjon).

Så hvordan kan en virksomhet lykkes med dette? Det handler om å utforme prosesser og systemer som kan fange opp informasjon, og som sikrer at denne flyter i riktig retning til rett tid. Minst like viktig er det imidlertid at virksomheten etablerer (og vedlikeholder) en kultur hvor det oppfordres til at feil blir vist fram og løst, som belønner de som fanger opp og videreformidler viktig informasjon og som skaper ledere som forstår at endring først skjer når de ansatte endrer adferd.

Som veilederen fra IIA slår fast, er det å ta risiko en naturlig del av å drive enhver virksomhet. En helhetlig og gjennomtenkt risikostyring er derfor et viktig kriterium for å lykkes, og her gir veilederen en god redegjørelse for «beste praksis». Når det kommer til den praktiske implementeringen vil vi hevde at den viktigste suksessfaktoren er å erkjenne at alle virksomheter er unike og å skreddersy løsninger som tar hensyn til egenart og som integreres med eksisterende styringssystemer.

Artikkelen er tidligere utgitt i et nyhetsbrev utsendt av Transcendent Group http://www.transcendentgroup.com/no

Måling av modenhet for helhetlig risikostyring – et forslag til enkel modell

Av
AYSE NORDAL
Fagansvarlig –risikostyring, Undervisningsbygg Oslo KF
MSC, BSC METU, Licentiat NHH
Sertifisert -Akkreditert Risk Manager QMCE
Medlem av styret i Nettverk Risikostyring i IIA Norge

OG

OLE MARTIN KJØRSTAD
Spesialrådgiver i internrevisjonen, Norges Bank
Siviløkonom, MSc in Business & Economics
Medlem av styret i Nettverk Risikostyring i IIA Norge

1.Hva og hvorfor

«Risikomodenhet» er en målestokk, et redskap som viser i hvilken grad en virksomhet har implementert helhetlig risikostyring i samsvar med gjeldende beste praksis.

En vurdering av risikomodenhet gir virksomheten muligheter for å:

- Gjennomføre en helhetlig vurdering av sin *tilstand* mot gjeldende beste praksis
- Skaffe seg en oversikt over *forbedringsområder og muligheter* for å oppnå et bedre nivå i forhold til modenhetsskala
- Planlegge *konkrete tiltak* for forbedringer.

Hensikten med denne artikkelen er å:

- gi en kort oppsummering av de eksisterende tilnærminger og løsninger på området
- peke på forbedringspotensialet og muligheter for videreutvikling
- presentere vårt forslag til en enkel modell, som vurderer risikomodenhet i en virksomhet med utgangspunkt i fem dimensjoner og målsettinger – se tabell 1.

2. Eksisterende tilnærminger og løsninger

Det finnes en omfattende litteratur som utgjør det teoretiske fundamentet for risikomodenhet. Fleste konsulentselskaper tilbyr ulike målestokker, som enten rangerer hele virksomheten eller de viktigste aktivitetene etter modenhetsnivå. [1,2,3). Høringsutgavene av det nye COSO-rammeverket og IS0-31000 benytter begrepet «risikomodenhet» selv om disse dokumentene ikke inneholder en definisjon eller en nærmere beskrivelse av begrepet.

De fleste modenhetsmodellene som er i bruk i dag bygger på grunnprinsippene av Capability Maturity Model som ble utviklet av Software Engineering Institute (SEI) i Carnegie Mellon Universitetet i 1993.[4,5] Denne modellen var laget for software -programvareutviklerne, og ikke var direkte relevant for *risikomodenhet*. Tanken om gradvis progresjon i en virksomhet utgjorde likevel et viktig utgangspunkt og en inspirasjon for flere faggrener og startet en diskusjon om egenskaper

Tabell 1 Dimensjoner og modenhetsmålsetninger

Dimensjoner	Modenhetsmålsetninger
Risikostyring, strategi og beslutningsprosesser	Alle beslutninger (strategiske, taktiske og operasjonelle) bygger på en dokumentert vurdering av risiko og muligheter.
Kommunikasjon, informasjon og rapportering	Virksomheten sørger for løpende kommunikasjon og rapportering av relevant informasjon med hensiktsmessig frekvens.
Organisering, myndighet og relasjoner	Virksomheten har en hensiktsmessig organisering og ressursallokering til risikostyringsarbeidet.
IT-verktøy og analyse	Risikostyringen bygger på beste tilgjengelige informasjon og er tilpasset virksomhetens behov.
Rammeverk og prosesser	Virksomheten har implementert et effektivt og egnet rammeverk for risikostyring.

som kunne knyttes til ulike utviklingsfaser i en virksomhet. En av de tidligste eksemplene på bruk av modenhetsbegrepet i risikostyringssammenheng finner vi i de velkjente arbeidene av David A. Hillson [6]. Hillson diskuterer 4 modenhetsnivåer i 4 egenskapsdimensjoner. Disse vises i tabell 2.

Etter Hillson kom det mange varianter av både modenhetsklassifikasjoner -og indikatorer som kan benyttes til å måle modenhetsnivå. Tendensen er en stor økning i antall variabler og dimensjoner som er ment å måle modenhet. Det beste eksempelet for dette er den risikomodenhetsmodell som de fleste har kjennskap til, dvs. RIMS sin (The Risk Management Society) Risk Maturity Model som ble laget i 2006 av Steven Minsky. De viktigste styrker som denne modellen har er at den gir bedriftene mulighet for å måle sine tilstander on- line [7] og at den er forenelig med ISO 31000, OCEG Red Book, BS31100, Solvency II, COSO, Ferma. Modellen definerer 5 modenhetsnivåer som ligner de som finnes i «Capability Maturity Modellen». Disse er:

- Ad-hoc
- Innledende/første
- Repeterbar
- Styrt
- Ledende.

Ulempen er at klassifiseringen av en virksomhet under en modenhetskategori gjøres gjennom tilstandsmåling mot 7 egenskaper, 25 kompetansedrivere og 68 beredskapsindikatorer, og dette kan virke veldig detaljert.

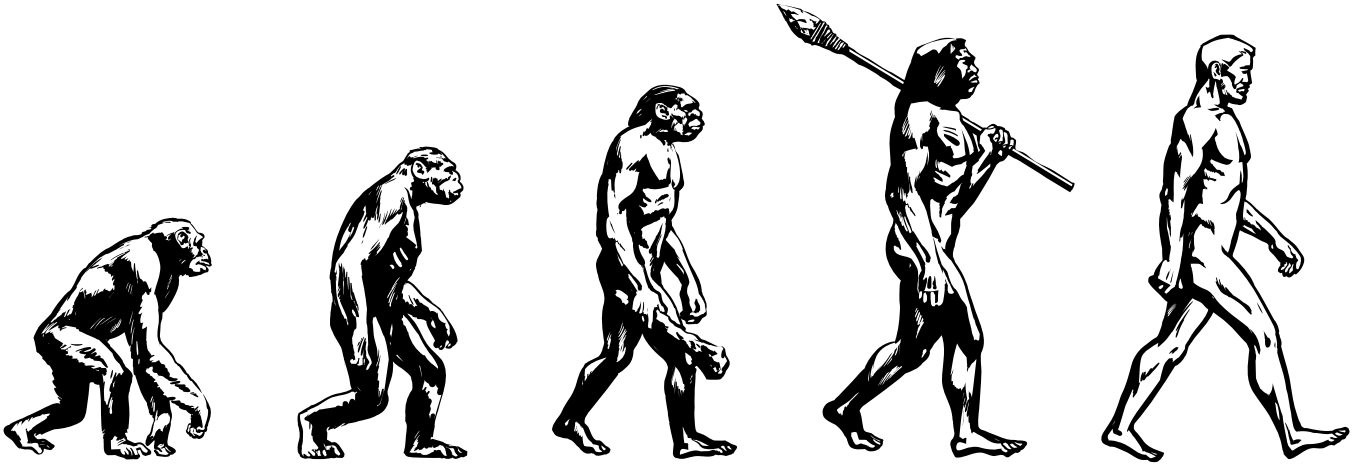
Tabell 2 Modenhet/egenskaper etter Hillson

Modenhet/egenskaper	Kultur	Prosess	Erfaring	Bruk
Naiv				
Nybegynner				
Normalisert				
Naturlig				

3. Forbedringspotensial og muligheter for videreutvikling

Følgende svakheter ved dagens modeller gir rom for videreutvikling:

a. *Modenhetsnivået kan være svært forskjellig innenfor virksomhetens ulike områder,* og dette avhenger av mer enn prosessen eiet av selve risikostyringsfunksjonen. Et godt samspill og en god risikokultur i organisasjonen er blant annet avgjørende dersom man skal kunne gå fra analyse og handlingsplaner, til realisering av utviklingsarbeid.
b. En utfordring med måten flere tradisjonelt har målt modenhet, *er at det gjøres i form av trappetrinn der det forutsettes at man har oppfylt ett nivå, før man kan nå det neste.* Samtidig kan det være egenskaper i de ulike nivåene som ikke nødvendigvis er avhengig av de foregående. Å lage en modell som måler en virksomhets risikomodenhet langs én lineær akse er derfor ikke bare vanskelig, men også upresist.
c. Med få unntak *forutsetter eksisterende modenhetsmodeller stadig progresjon til høyere modenhetsnivåer.* Erfaringen av mange virksomheter er slik at utviklingen av risikostyringsarbeidet kan stoppe eller stagnere. [8] Modenhetsmodeller bruker lite oppmerksomhet på faktorer som stopper eller reverserer utviklingen.
d. Med få unntak fokuserer dagens studier og modeller på «egenskapene» til virksomhetene som befinner seg i ulike modenhetsnivåer, og «variabler» som måler risikomodenhet. *Kilder som fokuserer på hva en organisasjon tjener på å evaluere sitt modenhetsnivå og å benchmarke det mot beste praksis er mindre i antall.* Et hederlig unntak er Mark Farrell og Ronan Gallagher, som presenterer empirisk støtte til sammenhengen mellom høyere modenhetsnivå og større selskapsverdi/ bunnlinje [9]. De har studert selskaper som har benchmarket seg mot RIMS sin Risk Maturity Model og konkluderer, på basis av en analyse av data i perioden 2006-2011, at organisasjoner som kan klassifisere seg som «moden» i forhold til det ovennevnte benchmark har 25 % høyere selskapsverdi enn de andre.
e. En målestokk får bedre annerkjennelse hvis den er universell. *Fravær av en enhetlig, felles og anerkjent metode for å måle modenhetsnivåer* reduserer virksomhetenes motivasjon til å vurdere sine utviklingsnivåer.



f. *I de fleste virksomheter er ambisjonene knyttet til risikomodenhet ikke en del av den strategiske diskusjonen på styre/ledelsesnivå.* Det å vurdere risikomodenhet krever bred innsikt i virksomheten og bør være en del av virksomhetsstyringen.

g. *Eksisterende modeller tar ikke hensyn til at kravene til risikostyring kan betone seg svært annerledes i ulike virksomheter.* For eksempel vil behovet for robuste IT-systemer være større i en desentral virksomhet med høy transaksjonshyppighet, enn i en lokal virksomhet med få transaksjoner. Videre blir kulturdimensjonen ofte glemt. Modenhet vurdert i en trappetrinnsmodell gir heller ikke et godt eller nøyaktig bilde av hvor virksomheten har sitt største utviklingspotensial. Skal man for eksempel ta steget fra ad-hoc, til løpende identifikasjon av risiko, kan dette betone seg svært forskjellig avhengig av virksomhetens art.

Konklusjon

Vi trekker følgende konklusjon fra ovennevnte svakheter: Dersom vi mener at beste praksis for risikostyring i stor grad vil måtte utføres på forskjellig vis, kan vi heller ikke måle modenhet langs én lineær skala med generiske kriterier på tvers av fagfelt, bransje og virksomhet.

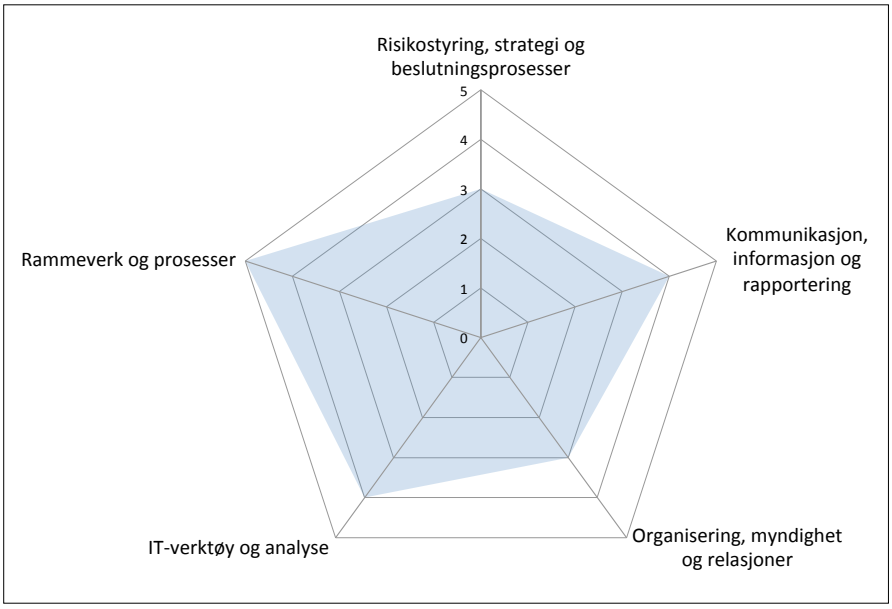
4. Enkel modell for evaluering av risikomodenhet

Som nevnt innledningsvis, presenterer vi her et forslag til en enkel evalueringsmodell for å vurdere en virksomhets risikomodenhet. Modellen baserer seg på dimensjonene og målsetningene beskrevet i tabell 1. Kriteriene som er lagt til grunn, er et forsøk på å peke på egenskaper som lett kan observeres. Dermed skal det være enklere å sette et mål for modenheten i virksomheten. På samme tid skal det gjøre det enklere å identifisere potensielle utviklings- og forbedringsområder.

Modellen følger heller ikke en trappetrinnskala, der de ulike nivåene er beskrevet med et sett kriterier som må anses oppfylt før neste nivå kan nås. I forslaget i tabell 3 er det lagt opp til en systematikk som måler modenhet separat innenfor hver dimensjon, og antallet kriterier som oppfylles dikterer modenhetsnivået i den respektive dimensjonen.

Tabell 3 Scoring basert på kriterier

Modenhetsnivå	Kriterier
5	Virksomheten oppfyller alle 10 kriterier
4	Virksomheten oppfyller 8 eller fler kriterier
3	Virksomheten oppfyller 6 eller fler kriterier
2	Virksomheten oppfyller 4 eller fler kriterier
1	Virksomheten oppfyller 2 eller fler kriterier



Figur 1 - Eksempel på fremvisning av resultat av modenhetsvurdering

Dette blir aldri en eksakt vitenskap, og de ulike kriteriene må leses og vurderes i konteksten av den virksomheten som vurderingen gjøres for. Videre er modellen heller ikke et ferdig kvalitetssikret arbeid. Forhåpentligvis kan den imidlertid danne et utgangspunkt for videre arbeid og dialog rundt hva som kjennetegner risikomodenhet.

Vi mener at resultatet av evalueringen egner seg til en oversiktlig presentasjon - se eksempel i figur 1. Ut fra denne grafiske fremstillingen ser man raskt der skoen trykker og der innsatsen bør legges inn for å forbedre systemet for helhetlig risikostyring.

Vi håper at denne modellen kan testes ut i praksis og vi setter pris på en tilbakemelding om erfaringer og eventuelle innspill til forbedring av kriterier, ris og ros. Send email med kommentarer til risikostyring@iia.no

Kilder:

[1] Iron Mountain, PwC Release, Information Maturity Index, 2014
[2] E&Y, Turning Risk Into results, How Leading Companies Use Risk management to Fuel Better Performance, 2013 p:5
[3] KPMG, Linking Risk Management to Business Strategy, Processes, Operations and Reporting, Financial Management Institute of Canada, February 2010, p:12
[4] M.C. Paulk, B. Curtis, M.B. Chrissis, and C.V. Weber, "Capability Maturity Model, Version 1.1," IEEE Software, Vol. 10, No. 4, July 1993, pp. 18-27
[5] M.C. Paulk, C.V. Weber, B. Curtis, and M.B. Chrissis, The Capability Maturity Model: Guidelines for Improving the Software Process, Addison-Wesley, Boston, 1995
[6] David Hillson, Towards a Risk Maturity Model, International Journal of Project and Business Risk Management I (spring) 35-45.
[7] http://riskmaturitymodel.org/rims-risk-maturity-model-rmm-for-erm/
[8] PwC, How ERM programs evolve, How to Achieve Excellent Enterprise Risk Management Series, Article 3 June 2015
[9] Mark Farrell, Ronan Gallagher « The Valuation Implications of Enterprise Risk Management Maturity, Journal of Risk and Insurance, 10. March 2014.

Tabell 3 FORSLAG TIL MODELL FOR EVALUERING AV RISIKOMODENHET

	Modenhetskriterier	
Risikostyring, strategi og beslutningsprosesser	Alle beslutninger (strategiske, taktiske og operasjonelle) bygger på en dokumentert vurdering av risiko og muligheter	Virksomhetens risikoappetitt er tydelig definert og kvantifisert innenfor relevante dimensjoner, som omfatter både finansiell- og operasjonell usikkerhet.
		Det foreligger dokumentasjon på at beslutninger fattes innenfor rammene av besluttet risiko-appetitt.
		Arbeidet med strategi- og handlingsplaner omfatter risikoanalyser som tar hensyn til usikkerhet i både intern- og ekstern kontekst.
		Risiko-/usikkerhetsvurderinger benyttes som grunnlag i forbindelse med ressursallokering og budsjettering.
		Leder for risikostyring blir invitert og involvert i relevante beslutningsfora.
		Måloppnåelse måles på et vis som gjør det mulig å se grad av måloppnåelse opp mot grad av risiko i virksomheten.
		Usikkerhetsvurderinger er en faktor i forbindelse med ressursallokering. Forventet kost/nytte av tiltak og utviklingsarbeid kvantifiseres og vurderes opp mot kvantifisert risiko.
		Risikovurderinger er en integrert del av strategiske beslutningsprosesser.
		Beslutningsdokumenter inneholder en eksplisitt vurdering av risiko og muligheter.
		Rapportering av måloppnåelse under- og etter implementering av tiltak og utviklingsarbeid gjøres på en måte som kan vurderes opp mot innledende forutgående risikovurderinger.

	Modenhetskriterier	
Kommunikasjon, informasjon og rapportering	Virksomheten sørger for løpende kommunikasjon og rapportering av relevant informasjon med hensiktsmessig frekvens	Virksomheten har en plan og policy for kommunikasjon med eksterne interessenter.
		Leder for risikostyring har tilgang til ekstern rapportering vedrørende forskriftsmessige og forvaltningsmessige krav.
		Det er etablert interne kommunikasjonsmekanismer som sikrer informasjon til alle relevante medarbeidere om prinsipper, rammeverk og prosesser som ligger til grunn for risikostyringen.
		Ledere og beslutningstagere har løpende tilgang til oppdatert informasjon om risiko, herunder status for tiltak og utviklingsarbeid, gjennom rapportering og løpende kommunikasjon.
		Det er etablert prosesser for kvalitetssikring av risikorapportering for å sikre sannferdig, relevant, nøyaktig og tilgjengelig rapportering. Kvalitetssikringsregimet omfatter også lederes rapportering.
		Det vedlikeholdes en dokumentert og tilgjengelig oversikt over risiko-, tiltaks- og prosesseiere i virksomheten.
		Det er etablert informasjonskanaler, -fora og -mekanismer som legger til rette for formidling av informasjon om risiko fra alle stabs- og linjeenheter.
		Det er utarbeidet prosesser og retningslinjer for å ivareta etiske retningslinjer, konfidensialitet og integritet i forbindelse med intern og ekstern kommunikasjon.
		Det er tilrettelagt for transparens og bransjesamarbeid i forbindelse med risiko knyttet til IT-sikkerhet og økonomisk kriminalitet.
		Leder for risikostyring rapporterer periodisk direkte til styret og har en direkte rapporteringskanal ved behov.

	Modenhetskriterier	
Organisering, myndighet og relasjoner	Virksomheten har en hensikts-messig organisering og ressursal-lokering til risikostyringsarbeidet	Virksomhetens ledelse sørger for hensiktsmessig organisering av risikostyringsfunksjonen og støtter opp om funksjonens arbeid. Rollen og ansvaret for risikostyring er tydelig forankret hos øverste leder for virksomhetens respektive områder.
		Risikostyringsfunksjonen har et mandat som er forankret i- og støtter opp om virksomhetens strategi.
		Leder for risikostyring er del av- eller rapporterer direkte til toppledelsen.
		Risikostyringsfunksjonen har nødvendige ressurser til å gjennomføre sitt arbeid. Funksjonens organisering og ressurser står i forhold til virksomhetens størrelse og kompleksitet.
		Virksomhetens har utviklet en risikokultur og felles terminologi knyttet til risikostyringsarbeidet.
		Leder for risikostyring har nødvendige fullmakter og autoritet til å kunne fylle sin rolle.
		Stillingsinstruksen til leder for risikostyring beskriver krav til ytelsesindikatorer, kompetanse og integritet.
		Leder for risikostyring pålegges ikke oppgaver som er til hinder for utøvelsen av en effektiv risikostyringsfunksjon.
		Leder for risikostyring har etablert gode relasjoner i organisasjonen. Det er etablert hensiktsmessige samarbeidsfora som sikrer effektiv samhandling mellom ulike forsvarslinjer og funksjoner.
		Leder for risikostyring kan ikke ansettes eller avskjediges uten styrets samtykke.

	Modenhetskriterier	
IT-verktøy og analyse	Risikostyringen bygger på beste tilgjengelige informasjon og er tilpasset virksomhetens behov	Virksomheten har hensiktsmessige verktøy for fasilitering og dokumentasjon av risikostyrings-arbeidet. Systemer og verktøy omfatter identifisering og analyse av risiko samt oppfølging av tiltak og utviklingsarbeid.
		Brukere av relevante IT-verktøy forstår forutsetningene, begrensningene og mulighetene i verktøyene.
		Beslutningstagere blir informert om mulige begrensninger ved benyttede modeller og systemer.
		Verktøy og modellbruk i virksomheten er ikke fragmentert og gir muligheter for å sammenligne målinger på tvers av virksomheten – modeller og verktøy bygger på sammenlignbare parametere.
		Risikoanalyser kan etterprøves og tilfredsstiller kravene til fullstendighet, sporbarhet og sann-ferdighet
		Benyttede systemer kan tilpasses til å lage rapporter som kreves av relevante myndigheter og eksterne interessenter (HMS, finans etc.)
		Benyttede systemer er egnet til å håndtere sensitive data i tråd med gjeldende krav.
		Virksomheten har tilgang til løpende overvåking av kvantifiserbare risikoparametere.
		Virksomheten har hensiktsmessige kanaler og verktøy for rapportering av hendelser.
		Det er gjort kartlegging av IT-applikasjoner som benyttes, grensesnittet mellom disse og kritikalitet for den operative virksomheten.

	Modenhetskriterier	
Rammeverk og prosesser	Virksomheten har implementert et effektivt og egnet rammeverk for risikostyring	Risikostyringsrammeverket har mekanismer som tar hensyn til kunnskap om virksomhetens interne og eksterne kontekst.
		Metode og rammeverk bygger på et tydelig mandat og en klar risikostyringspolitikk, med avklart ansvars- og ressursdeling.
		Risikostyring integreres i- og tilpasses virksomhetens prosesser; både forretningsmessige og administrative. Ingen områder, nivåer eller prosesser utelates ved utforming av risikostyrings-rammeverket.
		Rammeverket blir jevnlig vurdert og er gjenstand for kontinuerlig forbedringsarbeid.
		Risikostyring er en involverende prosess, som muliggjør impuls og tilbakemeldinger på tvers i organisasjonen.
		Risikostyring er en iterativ prosess der endringer i omgivelser, organisasjon, systemer og strukturer påvirker prosessen.
		Det er definert og synliggjort koblinger mellom beregnet risiko og måling av verdiskapning i virksomheten.
		Evalueringsmodeller for sannsynlighet og konsekvens, skalaer og vurderingskriterier er definert som del av rammeverket og vurderes jevnlig.
		Rammeverket inkluderer systematikk i prioritering og oppfølging av tiltak og utviklingsarbeid.
		Rammeverket inkluderer periodisk evaluering av effektivitet og kost-nytte av alle vesentlige prosesser, kontroller og tiltak.

Wells Fargo-skandalen rir videre

SIRK nr. 2/2016 hadde et innlegg om Wells Fargo hvor de ansatte opprettet cirka 2 millioner konti uten å innhente kundenes samtykke med hensikt å innfri bankens salgsmål. Som en konsekvens av dette måtte bankens administrerende direktør trekke seg fra stillingen sin og Wells Fargo fikk en skikkelig omdømmeknekk.

Ny informasjon om Wells Fargo-skandalen

Siden den forrige artikkelen har det kommet frem ny informasjon som oppsummeres kort nedenfor:

Nytt salgsbonussystem

Allerede i oktober 2016 ble bankens eksisterende bonussystem, som var basert på antall solgte produkter, erstattet med et nytt system, hvor kvaliteten på kundeservice skulle danne grunnlaget for fremtidige bonusutbetalinger. Det ble fortalt til markedet at ledelsen med jevne mellomrom skulle gjennomgå effekten av det nye bonussystemet og følge opp at det fungerer som forutsatt. I tillegg ble det sagt at ledelsen har etablert et kontrollsystem som skulle luke vekk dårlig oppførsel (les fiktiv oppnåelse av mål).

Annen tvilsom praksis

I februar 2017 varslet Prudential, et amerikansk livsforsikringsselskap med 49 000 ansatte, at de vurderte å søke erstatning fra Wells Fargo for salg av livsforsikring med lav utbetalingssum, altså forsikringer som var lite gunstig for kunden men ga banken en provisjonsinntekt. Samtidig ble det igangsatt en intern granskning i Wells Fargo når det ble kjent at kunder av Wells Fargo hadde blitt belastet for gebyr for å låse inn en fastrente. Det som utløste denne granskingen var at Wells Fargo selv bevisst hadde utsatt opprettelsen av kundenes boliglån for å kunne innkassere et slikt tilleggsgebyr.

Kompensasjon til kunder

I mars 2017 ble det fortalt i nyhetene at et søksmål fra kunder hadde blitt forlikt med en utbetaling på USD 110 millioner. Denne utbetalingen skulle delvis være en erstatning for feil gebyrbelastning og delvis en kompensasjon for dårlig adferd fra banken. For Wells Fargo var dette uansett en ekstra utbetaling på toppen av en bot fra myndighetene på USD 185 millioner.

Tidligere ledere får svi

I april 2017 besluttet styret i Wells Fargo at den tidligere administrerende direktøren skulle tilbakebetale ytterligere USD 28 millioner i lønn og at lederen for privatmarkedet skulle miste sine opsjonsrettigheter til en verdi på USD 47 millioner. Summen av tapte godtgjørelser utgjør dermed totalt USD 69 millioner for bankens tidligere toppleder og USD 67 millioner for lederen av privatmarkedet.

> «De ansatte ble presset til å selge sine kunder uønskede eller unyttige produkter»

Å trekke lærdom - internt i banken

I april 2017 publiserte Wells Fargo sin egen granskningsrapport i saken, som hadde blitt gjennomført av uavhengige styremedlemmer. Hensikten med granskningen var å finne årsak til den ureglementerte adferden i banken for å hindre fremtidig gjentagelse. Det er ofte lærerikt å øke vår egen kunnskap om et tema gjennom å lære av andres feil. Derfor gjengis rapportens oppsummering, som tar for seg alle ledd i bankens organisasjon, dvs. mellomledere, topplederen og 2. og 3. linjeforsvaret, her i sin helhet etter en oversettelse:

Hovedårsaken til den dårlige kundehåndteringen var en forvrengt salgskultur og resultatstyring som i kombinasjon med en aggressiv salgsledelse presset de ansatte til å selge sine kunder uønskede eller unyttige produkter. I noen tilfeller ble det også åpnet bankkontoer uten kundens godkjennelse. Wells Fargo sin desentraliserte organisasjonsstruktur ga for mye frihet til toppledelsen i privatmarkedet, som ikke ville forandre salgsmodellen eller ikke engang erkjenne at den var hovedårsaken til problemstillingen. Ledelsen i privatmarkedet var imot denne tilnærmingen og hindret innsyn og ettersyn fra utenforstående. Når ledelsen i privatmarkedet ble tvunget til å rapportere om saken, ble problemets omfang og alvorlighetsgrad bagatellisert.

Den tidligere administrerende direktøren, som stolte på den årelange strategien med salg gjennom flere kanaler samt gode tilfredshetsmålinger fra kunder og ansatte, kom for sent i gang med å granske eller utfordre den eksisterende salgspraksisen i privatmarkedet. Han forsto ikke rekkevidden av problemet og omdømmerisikoen dette medførte for banken.

Kontrollfunksjoner på konsernnivå ble holdt tilbake av den desentraliserte organisasjonsstrukturen. Det var en del av kulturen at forretningsområdene sto sterkt og skulle behandles med respekt. I tillegg ble problemene håndtert enkeltvis og ledelsen fanget ikke opp at det var en sammenheng mellom de ulike utfordringene. Dette førte til at ledelsen gikk glipp av flere muligheter til å analysere, vurdere og eskalere de svakheter som fantes i salgsprosessen.

Svakhetene i salgsprosessen ble først løftet opp til styret som en vesentlig risiko i 2014. Tidlig i 2015 bekreftet toppledelsen at for-

bedringstiltak var iverksatt. I løpet av 2015 og 2016 behandlet styret saken regelmessig, men internrapporteringen ga ikke et riktig bilde av problemets omfang. Styret ble først orientert om dette etter at 5.300 ansatte var blitt sparket for dårlig kundehåndtering, og det ble redegjort for et forlik mellom tilsynsmyndighetene og banken i september 2016.

Hvis vi med stillinger i 2. og 3. linjeforsvaret skal kun lære oss en ting av denne rapporten, så er det å se kritisk på sammenheng og helheten i risikobildet - og fra et ståsted med høy faglig integritet der vi tør å si ifra.

Å trekke lærdom - internt i tilsynet

I midten av april 2017 publiserte den amerikanske banktilsynsmyndigheten OCC sin oppsummering av deres interne granskingsrapport. Hensikten med denne granskningen var å finne svar på hvorfor tilsynet med en stab på 60-70 mennesker dedikert til oppfølging av Wells Fargo ikke hadde tidligere aksjonert mot banken. Hovedkonklusjonen i rapporten ble at tilsynsarbeidet deres var hverken hensikts- eller tidsmessig og staben overså flere signaler på svakhetene som førte til opprettelsen av falske kontoer.

I tillegg viser OCC-rapporten informasjon som kan tolkes slik at styret ikke var fullt så ukjent med det som skjedde i Wells Fargo i forhold til det som fremkom i styrets egen rapport. Ifølge OCC hadde styret helt siden 2005 mottatt regelmessige rapporter, som synliggjorde at de fleste varslinger og oppsigelser av ansatte gjaldt overtredelser av salgspolicyen.

OCC hadde på sin side heller ikke undersøkt varslene nærmere når varsellampene blinket. For eksempel rapporterte banken allerede i år 2010 700 tilfeller om resultatfiksing på salg, men lederen for privatmarkedet bagatelliserte problemet i samtaler med tilsynets medarbeidere. Lederen forklarte at det høye antallet klager skyldtes at Wells Fargo hadde en (sunn) kultur der medarbeidere ble oppmuntret til å klage og at alle tilfeller ble gransket og løst tilfredsstillende.

Det hører med til historien at lederen for tilsynsenheten, som hadde ansvaret for tilsyn av Wells Fargo i OCC, har nå også fratrådt sin stilling.

OCC-tilsynsrapporten gir en sterk påminnelse om at det straffer seg i lengden ikke å ta interne varslinger på alvor.

Avslutningsvis

Til slutt er det verdt å merke seg at selv om skandalen medførte til en verdifall på 20% i bankens aksjer, så er verdien av bankens aksjer i dag på samme nivået som de var før skandalen inntraff. Dette kan indikere at dårlig kundeomdømme ikke varer så lenge i aksjonærenes kollektiv hukommelse, såfremt ledelsen har iverksatt korrektive tiltak.

Martin Stevens

Unngå sjakk matt i risikostyringen

Av
MAGNUS DIGERNES,
KPMG, Director Risk Consulting, hobbysjakkspiller og leder av Nittedal Sjakklubb

INNLEDNING

Magnus Carlsens bragder på sjakkbrettet har ført til mange diskusjoner om sjakk er noe annet eller mer enn et brettspill. Idrett eller sport er ofte nevnt, noen ønsker å se på sjakk som vitenskap, mens andre er mer opptatt av det kunstneriske og skjønnheten i et velspilt sjakkparti. Jeg mener et viktigere spørsmål er om vi kan lære noe av å spille sjakk, eller er det rent tidsfordriv og underholdning? En tidligere verdensmester i sjakk uttalte at «sjakk er kunsten å analysere», men jeg vil legge til at det også er kunsten i å ta de beste beslutningene, nettopp slik som risikostyring i stor grad handler om å legge til rette for gode beslutninger. Gjennom denne artikkelen ønsker jeg å vise at sjakk er mer enn et enkelt brettspill, og at vi også innen risikostyring har noe å lære av sjakken.

Hvor viktig er sjakkpartiet – risikoappetitt

Sjakkspillere har ulik risikoappetitt uttrykt gjennom ulike spillestiler og angrepsvilje. Magnus Carlsen er unik i å finne de beste trekkene og spille med lav risiko. Han gjør sjelden trekk som ikke er de beste fordi han regner med at motstanderen ikke vil finne det beste motsvaret. Samtidig kan risikoappetitt endre seg ved endrede forutsetninger eller endringer i målsettinger. En anonym hobbysjakkspiller merket nylig at sin egen risikoappetitt endret seg i løpet av et sjakkparti i en lag-kamp[1]. Dette partiet var det eneste som var igjen, og laget lå under 2-1 som betydde at den anonyme hobbysjakkspilleren måtte vinne for at vi skulle få uavgjort. Motstanderen hadde over 200 ratingpoeng mer, og hobbysjakkspilleren hadde bestemt seg på forhånd for å ikke ta for stor risiko. Men med resultatene på de andre bordene så han seg nødt til å spille med høyere risiko. Han hadde mulighet for remis ved evigsjakk, men valgte å spille på vinst. Og tapte noen få trekk senere.

For en virksomhet definerer risikoappetitt hvor mye risiko man er villig til å ta for å nå sine mål. En virksomhet kan beslutte å etablere seg i land med svakt styresett på grunn av tidligere erfaringer og med tro på at de kan håndtere korrupsjon på en god måte. På den andre siden vil virksomheter med lav risikoappetitt og liten tro på at de kan håndtere utfordringer knyttet til korrupsjon ikke ta risikoen ved å etablere seg i de samme landene.

Vurdere mulige trekk - analysere og vurdere risiko

Som sjakktrener for barn er noe av det første vi lærer bort at barna skal sitte på hendene til de har sett på brettet flere ganger. Barna er som regel veldig ivrige og noen ganger er det en konkurranse i gjøre det raskeste trekket. Dette medfører ofte at brikker blir satt direkte i slag eller at skole-matten inntreffer etter få trekk. Tilsvarende kan risikoanalyser uten tilstrekkelig dybde og/eller uten å vurdere flere ulike effekter medføre at feil beslutninger tas[2].

For å gjøre gode risikoanalyser er det ulike metoder som kan benyttes. De enkelte metodene bør tilpasses hva slags risiko som skal analyseres og vurderes. En måte å kategorisere risiko som krever ulik tilnærming er å dele de inn i kontrollerbare (eller taktiske) risikoer, strategiske risikoer og eksterne risikoer[3].

Liten tue kan velte stort lass– kontrollerbare risikoer

I Magnus Carlsens VM-match mot Anand i Sotsji 2014 var det et avgjørende øyeblikk som oppsto i det 6. partiet. Matchen var på det tidspunktet 2,5 – 2,5 og en seier til en av de to ville vippe matchen i en avgjørende retning. Etter Magnus sitt 26. trekk oppsto følgende situasjon;

Magnus, som hvit, har nettopp spilt kongen til d2. Dette var en stor tabbe, noe Magnus innså rett etter trekket var gjennomført. Anand så derimot ikke at det var en tabbe, spilte a4, tapte hele partiet og senere hele matchen (hvis du vet hva Anand burde ha spilt i diagrammet så kan du sende svaret til magnus.digernes@kpmg.no).

[1] I en lag-kamp spilles det ett parti pr. spiller, men summen av de individuelle poengene avgjør hvem som vinner lagkampen
[2] «World-class risk management» Norman Marks, 2015
[3] «Managing risk: A new framework» Harvard business review, June 2012. Robert S. Kaplan and Anette Mikes
[4] Bl.a.; CFO executive board; audit director roundtable research, 2009.

Kontrollerbare risikoer handler om risikoer som ofte bør minimeres eller elimineres. Generelt er det ingen gevinst ved å ta disse risikoene. Internrevisjoner har som regel fokus på disse risikoene i form av uønskede hendelser som kan oppstå i ulike prosesser, og om det er tilstrekkelig kontrolltiltak på plass. Hvis man i risikostyringen fokuserer på disse risikoene, eller bruker den samme fremgangsmåten på alle typer risikoer, vil det bli utfordrende å håndtere de viktigste risikoene; de strategiske.

Målet er å sette sjakk matt - Strategisk risiko

Selv om de kontrollerbare risikoene kan ha en vesentlig effekt på virksomheten, ref. Magnus sin tabbe i partiet mot Anand, så er det som regel de strategiske risikoene som er de viktigste for virksomhetene. Flere undersøkelser viser at det er de strategiske risikoene som kan være mest vesentlige for virksomheter.[4]

For nybegynnere i sjakk dreier det meste seg om å lære å tenke to-tre trekk fremover og å unngå å tape materiell (eller brikker). Jo bedre man blir, desto mindre tid behøver man å bruke på å unngå typiske tabbetrekk. Fokuset flyttes til de langsiktige planene som skal danne grunnlaget for det endelige målet om å sette sjakkmatt. I de langsiktige planene er det viktig å sette delmål som for eksempel å få en springer til et sentralt felt på brettet. For å få gjennomført planen må hele tiden risiko vurderes som f.eks. om det er nødvendig å legge inn et trekk for å stoppe motstanderens plan. På samme måte bør virksomheter vurdere risiko opp mot strategiske målsetninger. Risikostyring handler jo tross alt om å håndtere usikkerhet relatert til måloppnåelse. Når virksomheter rapporterer på måloppnåelse for inneværende kvartal, bør det også inneholde informasjon om hvor sannsynlig det er at de langsiktige strategiske målene nås og hvilke usikkerhetsmomenter (risikoer) som påvirker måloppnåelsen.

Rammene rundt - ekstern risiko

Eksterne risikoer kan deles inn i ulike typer[5]; naturkatastrofer eller økonomiske sjokk med umiddelbar virkning, f.eks. vulkanutbrudd på Island, geopolitiske eller miljømessige endringer med langsiktige virkninger som f.eks. global oppvarming, og endringer i konkurransesituasjonen som f.eks. Amazons inntog i bokhandelen.

Noen av teknikkene for å analysere risikoer, spesielt eksterne, kan være stress-testing og scenarioanalyser. Scenarioanalyser ble utviklet rundt 2. verdenskrig av Alan Turing som spilte sjakk med kolleger i pausene, og syslet med tanken om å lage en sjakkmaskin.[6] Han skjønte at det ikke ville nytte å programmere datamaskinen til å regne alle mulige sjakktrekk. Planen til Turing var derfor å få maskinen til å lære av sine tidligere spill, en ide som ble realisert mange år etter Turings død gjennom Monte Carlo-simuleringer der datamaskinen på noen sekunder spiller hundretusentalls partier mot seg selv fra den aktuelle stillingen før den velger det trekket som gir best uttelling statistisk. Brukt på den riktige måten er Monte Carlo-simuleringer i dag et enkelt og raskt hjelpemiddel for å øke virksomhetens forståelse av risiko.

Et sjakkprogram kan enkelt gi råd om trekk som ikke er enkelt å oppdage for mennesker, og med stadig nye tekniske hjelpemidler er det vanskelig å forhindre de som ønsker å jukse i sjakk. En av de største skandalene innen sjakken var da det franske landslaget ble tatt for juks i sjakk-OL i 2010 (ja, det er egne OL for sjakk). En av de franske sjakkspillerne fikk hjelp gjennom en medhjelper som satt hjemme og fulgte med direkte over internett og analyserte partiet. Han sendte en kodet SMS til laglederen for eksempel «63-68» som en del av et telefonnummer. Laglederen fant så plassen sin i OL-hallen hvor han gikk til bord nr. 63 og så til bord nummer 68. Dette ble tolket som at sjakkspilleren skulle flytte brikken på f3 til f8. Den franske sjakkspilleren vant de fleste partiene og ble også tildelt en pengepremie på 5000 Euro. Jukset ble oppdaget av visepresidenten i det franske sjakkforbundet som fikk en feilsendt sms hvor det sto «fort deg, send flere trekk».

OPPSUMMERT

Den beste og mest effektive måten å forbedre seg i sjakk er å analysere partiet i etterkant, gjerne sammen med motstanderen eller sammen med en trener. I denne evalueringen er det viktig å få en forståelse for de beslutninger som ble tatt. Spørsmål en trener kan stille for å få denne forståelsen er om tilstrekkelige analyser ble utført, var det trekk som man ikke tenkte på eller overså, og hva var den langsiktige, strategiske planen. I likhet med en sjakktrener som gir råd om hvordan sjakkspilleren kan forbedre sitt spill, bør også virksomheter ha funksjoner som ivaretar en tilsvarende trenerrolle og som kan stille spørsmål om grunnlaget for større og mindre beslutninger er tilstrekkelig.

Sjakk er et spill hvor situasjonen endrer seg for hvert trekk; taktiske risikoer oppstår og strategiske planer må endres. Dette fordrer at en sjakkspiller gjør tilstrekkelige risikoanalyser før beslutningen om et trekk tas. På samme måte kan virksomheter lære hvordan gode risikoanalyser bidrar til at bedre beslutninger tas. For egen del spiller jeg gjerne sjakk for underholdningen og spenningen, men jeg oppfordrer også andre til å spille sjakk for å bli bedre på risikostyring.

[5] *«Managing risk: A new framework» Harvard business review, June 2012. Robert S. Kaplan and Anette Mikes*

[6] *«Sjakken eller livet» Cappelen Damm, 2016. Atle Grønn.*

Ville du kjøpt en bolig i Afrika eller Sør-Amerika usett?

Skrevet av:
SPESIALRÅDGIVER LENE EIA BOLLESTAD OG PARTNER/ADVOKAT NICOLAI SKRIDSHOL
Advokatfirmaet Steenstrup Stordrange DA

Nei, de fleste ville sannsynligvis ikke kjøpt en bolig usett - hverken i Afrika, Asia, Sør-Amerika eller andre markeder for øvrig. Folk flest ville nok gjennomført en rekke undersøkelser (due diligence) før kjøp, for eksempel lese prospektet nøye, undersøke markedet og ikke minst; dra på visning. Due diligence, både finansiell og juridisk, er også en naturlig del av M&A-transaksjoner i det kommersielle næringsliv. På lik linje med at de fleste av oss drar på visning før kjøp av en bolig, er det naturlig å finne tilsvarende «on site» due diligence-praksis ved kjøp av selskaper i høyrisiko-markeder, men er det egentlig slik? Og hva er utviklingen innen transaksjonsmarkedet?

Korrupsjonsrisiko i internasjonale transaksjoner er i aller høyeste grad reell på lik linje med annen type risiko. Slik risiko kan blant annet være relatert til prosesser for fremforhandling av kjøpskontrakter, fremskaffelse av lisenser/konsesjoner, valg av joint venture-partner, finansieringspartner, långiver og/eller garantist, eller kanalisering av pengestrømmer til skatteparadiser. Korrupsjonsrisikoen kan også typisk være høy ved bruk av agenter, bidrag til politiske personer/partier/organer eller ved svak internkontroll innen for eksempel økonomi- og anskaffelsesfunksjoner, for å nevne noen.

I næringslivet har dokumentgjennomgang og analyser av finansielle regnskap, kontrakter og annen tilgjengelig dokumentasjon gjennom due diligence-prosesser lenge vært vanlig praksis i transaksjonssammenheng; typisk ved bruk av datarom. Men i motsetning til mange andre typer risiko er korrupsjonsrisiko vanskelig å undersøke, avdekke og forebygge gjennom kun en ren dokumentgjennomgang. Er det derfor slik at potensiell korrupsjonsrisiko i M&A-prosesser ofte blir forbigått? Satt på spissen, kan vi sammenlikne denne «datarom due diligence»-praksisen med kun å lese gjennom prospektet?

Konsekvenser ved å bli rammet av en korrupsjonssak kan være både rettslige og økonomiske, slik som bøter eller kostnader

ved å utbedre følgene av korrupsjonshandlingen(e). Andre konsekvenser kan også være av forretningsmessig betydning, som for eksempel omdømmetap, utestengelse fra offentlige anskaffelsesprosesser, eller tap av lisenser/tillatelser.

Disse virkningene kan i ytterste konsekvens ikke bare påvirke oppkjøpmålets verdi og virksomhet, men også kjøpers. Ved mangel på tilstrekkelig due diligence «on site» før closing (lukking av oppkjøpsavtalen), som kan innebære samtaler med lokalt management som CEO, CFO eller andre relevante ansatte, leverandører, revisor, m.fl., vil kjøper kunne bli stilt i strafferettslig ansvar og måtte ta konsekvensene av det. Konsekvensene av strafferettslig ansvar kan være flere, eksempelvis direkte for oppkjøpsmålet eller kjøper av oppkjøpsmålet eller indirekte overfor aksjonær i oppkjøpsmålet. I tillegg vil dette kunne resultere i sivilrettslige konsekvenser, som for eksempel

heving av avtaler og erstatningsansvar. Alt beror på omstendighetene.

Både norsk og internasjonal korrupsjonslovgiving, som eksempelvis UK Bribery Act og FCPA, er global i utstrekning og kan etter omstendighetene ramme selv «uskyldige» norske investorer. I tillegg øker stadig fokuset på og bevisstheten om de alvorlige skadevirkningene korrupsjon har på samfunnet, selskaper og personer. Dette betyr ikke at man skal unngå å investere i høyrisikoland, men det betyr at omfanget av forebyggende arbeid, gjennom for eksempel gjennomføring av anti-korrupsjons due diligence, må være i tråd med risikoen man står overfor. Relevant forebyggende arbeid kan også være en formildende faktor dersom man skulle bli involvert i korrupsjon.

> «Dette betyr ikke at man skal unngå å investere i høyrisikoland, men det betyr at omfanget av forebyggende arbeid, gjennom for eksempel gjennomføring av anti-korrupsjons due diligence, må være i tråd med risikoen man står overfor.»

Selskapsgjennomgang eller «due diligence» (ofte forkortet til «dd») er kort fortalt en systematisk gjennomgang/under-

søkelse av et selskap, ofte i forbindelse med fusjoner eller oppkjøp. Oppdragsgiver er ofte kjøper, og formålet er å gi et bedre beslutningsgrunnlag gjennom å identifisere risiko relatert til oppkjøpsobjektet som kan ha en betydning for transaksjonen, for eksempel prisingen og/eller avtaleutformingen. En due diligence kan omfatte flere delområder, for eksempel finansiell, rettslig, tekniske forhold og anti-korrupsjon.

Formålet med en anti-korrupsjons due diligence er alltid å tilføre merverdi til oppdragsgiver gjennom å sørge for et bedre grunnlag for investeringsbeslutning og muliggjøre bedre tilpasninger i transaksjonsfasen. Formålet vil aldri være å stoppe gjennomføring av transaksjoner, men derimot å gjennomføre dem på best mulig og forsvarlig måte.

For kjøper vil gjennomføringen av en slik «on site» due diligence kunne gi verdifull informasjon og kunnskap om utsatte risikoområder, blant annet om oppkjøpmålets selskapsledelse, agenter, leverandører, problemområder i inntektsstrømmer, hvilke ansatte man ønsker å ta med seg videre, hvilke kontrakter eller lisenser/tillatelser det er knyttet risiko til. Dette er informasjon som vil kunne nyttiggjøres i forhandlinger om blant annet kjøpspris, finansieringsstruktur, garantiklausuler og oppgjørstidspunkt.

For selger vil informasjon om forbedringsområder som bør håndteres forut for et salg kunne bidra til å øke selskapets verdi og gi en kjøpspris langt over forventet.

De siste årene har det skjedd en utvikling innen anti-korrupsjonsarbeid og forventninger til slikt arbeid – også i transaksjonssammenheng. Lovverk og retningslinjer som stiller krav til selskapers anti-korrupsjonsarbeid i forbindelse med transaksjoner, for eksempel Foreign Corrupt Practices Act (FCPA), UK Bribery Act (UKBA) samt norsk korrupsjonslovgivning, håndheves stadig strengere, og stadig flere selskaper og enkeltpersoner straffeforfølges. I tillegg stiller regnskapsloven krav til at et utvalg av selskaper må redegjøre for blant annet hva som gjøres for å integrere bekjempelse av korrupsjon i forretningsstrategier, i daglig drift og i forholdet til interessenter.

I sum har ovennevnte forhold bidratt til et økt fokus på anti-korrupsjon og compliance i mange selskaper og et syn på forebyggende arbeid som verdi-

Har du forberedt din virksomhet på

I mai 2018 får vi en ny personvernlovgivning. Det nye regelverket stiller nye og strengere krav til bruken av personopplysninger fra europeiske borgere – uavhengig av om virksomheten som behandler personopplysningene er lokalisert i Norge, EU/EØS – eller utenfor EU/EØS.

Av
BJØRN OFSTAD
Director i Deloitte Advokatfirma

Bakgrunn

Nye overskrifter om personvern og personopplysninger dukker opp nesten daglig. Datatilsynet varsler tilsyn mot matvaregiganters apper, kommunene får gebyrer for feil håndtering av deres innbyggeres personopplysninger, helseforetak varsler at sensitive data er på avveie, Facebook vil ha tilgang til våre kontoopplysninger og automatiske strømmålere sporer når vi er hjemme og når vi har besøk.

Samtidig viser undersøkelse fra USA at Mac-brukere må betale mer for reiser kjøpt per internett enn PC-brukere da de legger til grunn at Mac-brukere har sterkere økonomi enn PC-brukere.

Den økte oppmerksomheten fører til at også «mannen i gata» er mer oppmerksom på hvordan virksomheter bruker våre persondata. Dagens personvernlovgivning ble implementert så sent som 2001 og har allerede «gått ut på dato» på grunn av den rivende utviklingen som muliggjør bruk av persondata.

Hva blir nytt?

Hva kan vi så vente oss fra den nye personvernlovgivningen, eller General Data Protection Regulation (GDPR)?

Norge har lagt seg på en stram tilnærming hva angår implementering av dagens personverndirektiv. Møter man dagens krav fullt ut, vil ikke den nye personvernlovgivningen by på store overraskelser. Det er likevel så mange endringer i vente at de aller fleste norske virksomhetene må gå igjennom praksis og rutiner på nytt.

Først og fremst vil den nye loven gi økt ansvar til virksomheter som behandler personopplysninger. Det stilles flere og klarere krav til å dokumentere virksomhetens behandling av personopplysninger og, ikke minst, dokumentere etterlevelse av personvernprinsippene (accountability). Videre blir prinsippet «privacy by design» (innebygget personvern) knesatt i det nye regelverket. I dette ligger at behandlingsansvarlig, eller virksomheten, blir pålagt å implementere tekniske og organisatoriske tiltak designet for å

> «Lovverk og retningslinjer som stiller krav til selskapers anti-korrupsjonsarbeid i forbindelse med transaksjoner, for eksempel Foreign Corrupt Practices Act (FCPA), UK Bribery Act (UKBA) samt norsk korrupsjonslovgivning, håndheves stadig strengere, og stadig flere selskaper og enkeltpersoner straffeforfølges.»

skapende og nødvendig ved gjennomføringen av transaksjoner. Flere og flere norske investorer erkjenner i økende grad at anti-korrupsjons due diligence er en nødvendig investering for å redusere risiko i transaksjoner, forhandle pris og av verdimessig betydning for en eventuell senere exit fra selskapet. Dette er i tråd med den utviklingen vi ser i mange internasjonale markeder og bransjer.

Avslutningsvis kan vi konstatere at vi optimalt sett ikke ville kjøpt hverken en bolig eller et selskap i Afrika, Sør-Amerika eller andre høyrisiko-markeder usett. Både der og ved investeringer i verden for øvrig, forventes det at due diligence-prosessene er risikobaserte og korrelert med den risikoen transaksjonen innebærer.

Allerede nå ser vi at mange selskaper foretar handlinger som viser at gjennomføring av «on site» anti-korrupsjons due diligence betraktes som en investering fremfor en kostnad. For mange representerer også økt kunnskap om oppkjøpsmålet et sterkt forhandlingskort og tilretteleggerforbedreinvesteringsbeslutninger.

Artikkelen tar utgangspunkt i et nyhetsbrev til klienter utgitt av Advokatfirmaet Steenstrup Stordrange.

ny personvernlov?

møte personvernprinsipper. For å få til dette må virksomhetens tekniske innretninger programmeres slik at bare helt nødvendige data for hvert enkelt formål behandles.

Utvidede informasjonsrettigheter til den registrerte om hva personopplysningene blir brukt til, sammen med strengere krav til sletting, endrer måten virksomheter jobber på. Den nye forordningen stiller også strengere krav til hvordan man innhenter samtykke til behandling av personopplysninger, og samtykke fra foresatte i forbindelse med opplysninger om mindreårige.

De nye kravene forutsetter at man innfører nye rutiner for hele virksomheten. Behandling av personopplysninger krever dokumentasjon, og rutinene for innsamling og lagring må være på plass. Dette stiller krav til at hele virksomheten må begynne å tenke annerledes i sin behandling av personopplysninger.

I dag er personvernombud en frivillig ordning, men i fremtiden vil langt flere virksomheter måtte utnevne personvernombud. Eksempelvis vil dette gjelde alle offentlige virksomheter. Det samme gjelder selskaper som behandler en stor mengde opplysninger.

Hvordan forberede virksomheten på endringer?

God kontroll

Virksomhetens kunnskap om egen behandling av personopplysninger og dokumenterbar etterlevelse vektlegges i større grad i ny personvernlovgivning. Kunnskap om egen behandling, og dokumentert etterlevelse, er bare mulig med god kontroll over opplysningene. Derfor er det helt nødvendig for virksomheten å ha kontroll på de personopplysninger virksomheten behandler. Virksomheten må vite hvilke opplysninger som behandles, hvor de ligger, formålet med registreringen (behandlingen), juridisk behandlingsgrunnlag og hvem som har tilgang til opplysningene – for å nevne noen forhold.

Gap-analyse

Når virksomheten har oversikt over egen behandling av personopplysninger, må dagens rutiner og praksis avstemmes mot nye krav i personvernlovgivningen.

Prioriter

Mange av prinsippene i ny personvernlovgivning finner du igjen i dagens lovverk. Møter du dagens krav, har du et godt utgangspunkt. Implementeringskravene i ny personvernlovgivning går imidlertid lengre enn kravene i dagens lovgivning, og mai 2018 er ikke langt unna.

Etterlevelse av personvernregelverket er et konkurransefortrinn

Møter din virksomhet juridiske og tekniske krav i personvernlovgivningen, har dere en sikrere og mer gjennomtenkt behandling av personopplysninger. Da bygger dere også tillit hos deres kunder.

Etterlevelse av personvernregelverket skaper verdi, og reduserer risikoen for avvik og funn ved tilsyn. Dette vil bidra til å sikre virksomhetens omdømme.

Etterlevelse av personvernregelverket skal ikke være en byrde, men et konkurransefortrinn som skal bidra til å se muligheter!

Morgendagens vinnere sørger for godt personvern.

Kravene til Personvernombud- kan rollen ivaretas av en compliance funksjon?

Ny personvernforordning fra EU[1] trer i kraft 25. mai 2018. Fra dette tidspunkt pålegges flere norske virksomheter å ha et Personvernombud (PVO)[2], som skal bidra til å sikre at personopplysninger behandles på betryggende måte. Kravene i forordningen til ombudet er på flere punkter sammenfallende med krav som stilles til Compliance Officer og/eller en compliance funksjon. Compliance Nettverket i IIA Norge ønsket derfor å se nærmere på kravene, samt diskutere om rollen kan ivaretas av en compliance funksjon under medlemsmøtet «Compliance & Kaffe» 8. mars.

Av
IZABELLA SALICATH
OG ANN CHRISTIN FLATLAND

Kari Laumann fra Datatilsynet gikk gjennom kravene til personvernombudet i EU forordningen[3]. Laumann startet med å peke på de viktigste endringene, samt hvilke virksomheter som må ha et ombud. Hun la hovedvekten på kravene til private virksomheter og hvilke vurderingstema virksomhetene må ha fokus på når virksomheten vurderer om ombudsordningen er obligatorisk[4].

Deretter gikk Laumann gjennom hvordan ombudet bør utpekes, samt dets oppgaver og stilling. Både behandlingsansvarlige og databehandlere som faller inn under kravene har i utgangspunktet plikt til å oppnevne PVO. Selv om virksomheten ikke har en direkte plikt, kan PVO oppnevnes på frivillig basis. Norske myndigheter kan pålegge andre virksomheter enn de som faller inn under forordningen å oppnevne en PVO.

Når det gjelder ombudets stilling, nevnte Laumann blant annet at PVO må involveres, skal få ressurser og tilgang, skal ha mulighet til å opprettholde sakkunnskap, skal ikke motta instrukser eller straffes og skal rapportere til høyeste ledelsesnivå. I tillegg må PVO ikke ha andre oppgaver som fører til interessekonflikt, herunder kan PVO ikke ha stilling som innebærer at ombudet skal bestemme formålet og metode for behandling av personopplysninger.

Avslutningsvis ønsket Laumann blant annet å fremheve følgende:

«Personvernombudsordningen er styrket i det nye regelverket fra EU. Det at mange norske virksomheter vil ha et personvernombud kan gjøre en stor forskjell for personvernet. Vi i Datatilsynet ser at det å ha en dedikert ressursperson med kompetanse og fokus på personvern i en virksomhet fører til sterkere regeletterlevelse og bedre behandling av personopplysninger.»

Ann Christin Flatland, leder av Nettverk Compliance, pekte i sitt foredrag på likhetstrekk mellom en compliance funksjon og PVO rollen, samt noen utfordringer dersom PVO rollen legges i en compliance funksjon. Sammenligningen tar utgangspunkt i Veiledning for compliancefunksjonen, utarbeidet av Nettverk Compliance[5]. Felles for begge roller er at de:

- kan ikke pålegges å komme frem til et bestemt resultat

Kari Laumann fra Datatilsynet, foto: Privat

- har en risikotilnærming ved utføring av oppgaver
- må ha tilgang til relevant informasjon og ressurser
- må håndtere compliance avvik
- skal overvåke etterlevelse
- bør sørge for dokumentasjon av compliance
- er et kontaktpunkt ved tilsynsbesøk[6]
- må oppfylle krav til faglige kvalifikasjoner[7]

Forordningens krav til PVO innebærer at vedkommende må ha spisskompetanse innenfor personvern og muligens gå noe mer i dybden med hensyn til rådgivning og oppfølging av personvernrelaterte avvik enn en generell compliance kontroll funksjon organisert i andre linje[8] normalt vil gå. Flatland konkluderte imidlertid

[1] *General Data Protection Regulation (GDPR)*
[2] *Eng. Data Protection Officer (DPO)*
[3] *Artikkel 37-39.*
[4] *Se veiledning fra artikkel 29-gruppen.*
[5] *Kan lastes ned fra iia.no: http://iia.no/om-iian-orge/compliance/#veileder-for-compliance*
[6] *Compliance funksjonen kan være et kontaktpunkt, men dette gjelder ikke nødvendigvis alle funksjoner og for alle former for tilsynsbesøk.*
[7] *Compliance funksjonen må som oftest oppfylle generelle kompetansekrav, mens en PVO må ha spisskompetanse innen personvern.*
[8] *Om trelinje modellen, se Veileder for compliance funksjonen punkt 2.1, som kan lastes ned fra IIA Norges hjemmeside.*

Figur 1 Analogisk anvendelse av «revisjonsviften»

med at PVO rollen kan ivaretas av en compliance funksjon, dersom det tas nødvendige forholdsregler under organisering av funksjonen og gjennomføring av arbeidet, slik at funksjonen ikke kontrollerer eget arbeid. Som illustrasjon viste hun til revisjonsviften som kan benyttes analogisk for en compliance kontroll funksjon. Konklusjonen understøttes av det danske Justitsministeriet som under et stormøte om den nye forordningen 9. februar 2017 uttaler at PVO *«Kan være organisationens compliance officer».*

Under diskusjon og spørsmålsrunde kom det frem at kravene til en PVO er tydeligere enn etter gjeldende regler, men at det fortsatt er rom for fortolkning. Det ble vist til IAPP Privacy Advisor «What skills should your DPO absolutely have?», som blant annet fremhever at PVO bør ha juridisk kompetanse, ha kulturell forståelse, ha leder egenskaper og erfaring med styresaker, kunne formidle reglene på en enkel måte, samt ha IT, internrevisjon og risiko kompetanse. I tillegg må vedkommende forstå bransjen virksomheten opererer i. Dette taler for at rollen ivaretas av et team. På spørsmål om Datatilsynet vil akseptere dette, svarte Kari Laumann at dette vil være opp til virksomhetene, men at det må utpekes et formelt kontaktpunkt som er ansvarlig ihht. forordningen.

Izabella Salicath, Chief Compliance Officer i GIEK ivaretar rollen som personvernombud etter dagens regelverk. Hun sier følgende om betydningen av ny GDPR og arbeidet som PVO fremover:

«Det virker som om GDPR virkelig har satt fokus på personvern, og med fokuset kommer også større forståelse av viktigheten av å arbeide med personvern. Ledere etterspør mer informasjon om både regelverket og PVO-rollen. I så måte gir også tonen fra toppen en større legitimitet for PVO-rollen i organisasjonen. Det er selvfølgelig utfordrende å arbeide med GDPR, men også spennende, og ikke minst viktig. Personvern er tross alt en grunnleggende rettighet som virkelig er blitt satt på agendaen.»

Kilder

Forordningen (engelsk): http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

Datatilsynet: https://www.datatilsynet.no/Personvernombud/hva-betyr-nytt-lovverk-for-ombudene/

Presentasjonen tok utgangspunkt i høringsversjon av Veiledning og FAQ fra EU Working Party (WP) 29: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_annex_en_40856.pdf

Endelig veiledning fra WP 29, se: https://www.datatilsynet.dk/fileadmin/user_upload/wp243_dpo.pdf

Veileder for compliance funksjonen: http://iia.no/om-iian-orge/compliance/#veileder-for-compliance

Stormøde om databeskyttelsesforordningen 9. februar 2017: https://erhvervsstyrelsen.dk/sites/default/files/media/praesentation_fra_stormoede_om_databeskyttelsesforordningen.pdf

IAPP Privacy Advisor, 24. januar 2017: «What skills should your DPO absolutely have?»: https://iapp.org/news/a/what-skills-should-your-dpo-absolutely-have/

Nettverk Compliance i IIA Norge inviterer til en uformell møteplass hvor aktuelle temaer innen compliance tas opp.

Etter foredrag som varer ca. 1 ½ time, er ordet fritt for erfaringsutveksling og diskusjon.

Vi avslutter med mingling og sosialt samvær.

Vedlikeholdspoeng (CPE) Møtet gir 2 CPE-poeng for CIA, CCSA, CGAP, CFSA, CRMA og Diplomert Intern Revisor.

COMPLIANCE & KAFFE SEMINARER AVHOLDT VÅREN 2017

25.01.17: Compliance rollen - Hva fungerer og hva fungerer ikke?

08.03.17: Kravene til PVO- kan rollen ivaretas av en compliance funksjon

03.05.17: Hva er et godt compliance program? – En studie av antikorrupsjons-arbeidet i norske multi-nasjonale virksomheter

Har du ønsker for høstens program? Send en e-mail til post@iia.no og merk den med «Compliance»

Hva lærte du av å delta på ekstern kvalitetskontroll?

Lever virksomheter opp til IIA standardene? IIA Norge har de siste månedene gjennomført en rekke eksterne kvalitetskontroller.

Et team bestående av 3 personer gjør et målrettet dykk inn i de enkelte virksomheters internrevisjoner, for å kartlegge i hvor stor grad IIA standardene etterleves.

Generalsekretær Ellen Brataas leder alle disse kvalitetskontrollene på vegne av IIA Norge, men det resterende teamet varierer og består av medlemmer med relevant faglig bakgrunn og erfaring hentet fra IIA Norges egen medlemsskare. Vi har snakket med tre medlemmer som har bidratt inn i ulike kvalitetskontroller de siste par årene, for å høre om deres erfaringer.

Av
MARIT TRODAL,
Prosjektleder i IIA Norge

Izabella Salicath, GIEK

Kan du si noe kort om deg selv og hva du jobber med?

Jeg er utdannet jurist og ansatt i GIEK, hvor jeg har ansvar for virksomhetsstyring og compliance. Herunder ligger også ansvar for outsourcet internrevisjon. Jeg holder tak i vår årlige Enterprise Risk Management prosess, og koordinerer årsplanen for internrevisjonen.

Hva var motivasjonen din for å delta på ekstern kvalitetskontroll?

Det er skikkelig gøy! Da jeg jobbet i KMPG var jeg med på to eksternkontroller og i fjor deltok jeg på en eksternkontroll i regi av IIA Norge. Vi gjorde en vurdering av etterlevelse av IIA standarder hos Statoil.

Var det krevende å sette seg inn i den virksomheten som dere gjennomførte ekstern kvalitetskontroll hos?

Det er komplekst og krevende å sette seg inn i risikobildet til en virksomhet og ha en formening om internrevisjonen er rigget riktig for oppgavene. Det er mye jobb, men faglig utfordrende og givende. Hele prosessen går veldig raskt, og man må ta av seg sin vanlige hatt og sette seg raskt inn i en annen virksomhet.

Var det noen utfordringer for deg ved å delta på oppdraget ved siden av din egen jobb?

Overhodet ikke. Jeg har en veldig fleksibel arbeidsgiver og kan styre min egen tid ganske godt. Men oppdraget jeg deltok på i regi av IIA Norge kom i tillegg til vanlig jobb og innebar en del timer på kvelder for å lese rapporter osv. Men det var verdt det.

Hva lærte du?

Det er nyttig å se hvordan andre opererer og viktig for å øke min egen kompetanse. Vi har hatt mange faglig gode diskusjoner rundt metodikken i internrevisjon.

Opplever du at disse erfaringene kommer til nytte i egen virksomhet?

Jeg har blitt enda tydeligere på behovet for gode revisjonskriterier. Hvis alle parter er enige om disse kriteriene unngår man en del diskusjon rundt konklusjoner.

Espen Andersen, Helse Sør-Øst

Kan du si noe kort om deg selv og hva du jobber med?

Jeg er utdannet siviløkonom, og har i tillegg fullført Executive Master-program innen finansiering og investering og internrevisjon. Den 1. november 2016

begynte jeg i min stilling som direktør for konsernrevisjonen i Helse Sør-Øst.

Hva var motivasjonen din for å delta på ekstern kvalitetskontroll?
Var vel litt todelt. Det viktigste er muligheten til å lære noe mer selv og få inntrykk av hvordan andre internrevisjoner jobber. Man er jo stadig på jakt etter muligheter til å utvikle seg. Den andre motivasjonen er mer idealistisk; Vi er en liten profesjon så det er viktig å bidra inn med relevant kompetanse der det er aktuelt. Evalueringen jeg deltok på var av Forsvarsdepartementet, og i og med at jeg har erfaring fra denne sektoren følte jeg at jeg hadde noe å bidra med.

Var det krevende å sette seg inn i den virksomheten som dere gjennomførte ekstern kvalitetskontroll hos?
Jeg synes ikke det var vanskelig å sette seg inn i forsvarssektoren, siden jeg har jobbet med den tidligere. Men det var krevende å sette seg inn i alle plandokumentene, siden arbeidet i Forsvarsdepartementets internrevisjon omfatter mange ulike organisasjoner.

Var det noen utfordringer for deg ved å delta på oppdraget ved siden av din egen jobb?
Å finne tid i hverdagen, mellom det som skjer i egen virksomhet og planlagte møter. Men jeg synes vi fikk det til å fungere godt. Det var en godt komprimert prosess med tre deltakere i teamet. Samtidig var det jo ingen reisevei for meg. Forsvarsdepartementet holder til rett oppi gata her i Kvadraturen.

Hva lærte du?
Jeg synes det var særlig nyttig å høre hvordan interessentene i en annen sektor tenker. Man har egne referanser i egen sektor og egne erfaringer. Å høre hvordan ledere tenker rundt internrevisjonen og hvilke forventninger de har til hva internrevisjonen skal bidra med var interessant. Her er det jo store forvaltningsorganisasjoner som bruker internrevisjonen i sin styringsdialog.

Opplever du at disse erfaringene kommer til nytte i egen virksomhet?
Jeg tar vel ikke med meg noe helt konkret, men det handler mer om perspektiver på utøvelse av internrevisjon og hva som tilfører verdi. Det kan være vanskelig for interessenter å sette ord på hva de ønsker med en internrevisjon, så det var nyttig med noen refleksjoner rundt internrevisjon fra en annen organisasjon i en fase der vi arbeider med egen utvikling.

Mads G. Kristensen, Norges Bank

Kan du si noe kort om deg selv og hva du jobber med?
Bakgrunnen min er sammensatt med utdannelse som siviløkonom og statsautorisert revisor. I nyere tid har jeg også tatt sertifiseringen CIA. Til daglig er jeg nestleder i internrevisjonen i Norges Bank, hvor jeg jobber med operasjonell revisjon inn mot alle virksomhetsområdene, både sentralbankspesifikke så vel som kapitalforvaltning. Norges Bank har en vesentlig kapitalforvaltningsvirksomhet som forvalter av statens pensjonsfond utland og valutareservene.

Hva var motivasjonen din for å delta på ekstern kvalitetskontroll?
Muligheten til å se hvordan andre strukturer sitt arbeid er noe som interesserer meg. Man kan få ideer fra hvordan andre har løst oppgavene som følger av en internrevisjonsfunksjon og diskutere forskjellige løsninger med andre i teamet.

Var det krevende å sette seg inn i den virksomheten som dere gjennomførte ekstern kvalitetskontroll hos?
Jeg opplevde det som greit å sette meg inn i den virksomheten. Teamet fikk god informasjon om aktivitetene, organiseringen og metodikken til de selskapene som var gjenstand for kontrollen allerede ved oppstart. Dette mener jeg fungerte bra.

Var det noen utfordringer for deg ved å delta på oppdraget ved siden av din egen jobb?
Den største utfordringen for meg er som for mange andre å finne tid i en ellers travel hverdag. Foruten det er min oppfatning at det har vært givende.

Hva lærte du?
Noe av det viktigste jeg tok med meg var bekreftelsen på at alle organisasjoner er forskjellige, med forskjellige behov samt at det er mange veier som fører til mål.

Opplever du at disse erfaringene kommer til nytte i egen virksomhet?
De erfaringene jeg fikk var primært knyttet til praksis hos andre. Jeg tok med meg kunnskap om hvordan andre har løst oppgavene, noe som har bidratt til å øke forståelsen min for kobling mellom organisasjon og praksis.

HVA ER EN EKSTERN KVALITETSKONTROLL?

I henhold til IIA standard 1312 er det påkrevd å gjennomføre en ekstern evaluering minst en gang hvert femte år.

Denne må utføres av en kvalifisert, uavhengig person eller et evalueringsteam utenfor organisasjonen.

Kan gjennomføres som en fullstendig ekstern evaluering hvor evalueringsteamet er ansvarlig for alt i prosessen, eller i form av egenevaluering gjennomført av virksomhetens eget team med påfølgende uavhengig ekstern validering.

Kan også omfatte operative eller strategiske kommentarer, samt observasjoner rundt beste praksis.

Prosessen dekker intervju med interessenter, gjennomgang av dokumenter og rapportering tilbake til virksomheten.

Toppledelsens forventninger

– Internrevisjon og merverdi med utgangspunkt i spesialisthelsetjenesten

Av
SISSEL MARGRETHE KORSHAVN OG TONE OPDAHL MO

Sissel Margrethe Korshavn, spesialrådgiver/ internrevisor ved konsernrevisjonen i Helse Sør-Øst RHF. Sykepleier, Cand. mag i statsvitenskap, Executive master of management og diplomert internrevisor.

Tone Opdahl Mo, internrevisor/ass. leder ved internrevisjonen i Helse Midt-Norge RHF. Dr. polit i sosiologi og diplomert internrevisor.

Internrevisjon i offentlig sektor har fått økt oppmerksomhet de siste årene, blant annet gjennom Finansdepartementets initiativ for økt bruk av internrevisjon i staten (FIN 2014 og 2015). Hvilke erfaringer har så offentlige virksomheter som allerede har en internrevisjon? Artikkelen presenterer resultater fra en intervjuundersøkelse fra 2016 som etterspurte synspunktene til ledere på toppnivå i spesialisthelsetjenesten. Vårt mål med undersøkelsen var å identifisere hva som skal til for at internrevisjonen skal tilføre merverdi og bli oppfattet som en kompetent, konstruktiv og relevant samarbeidspartner for styre og administrasjon i helseforetakene.

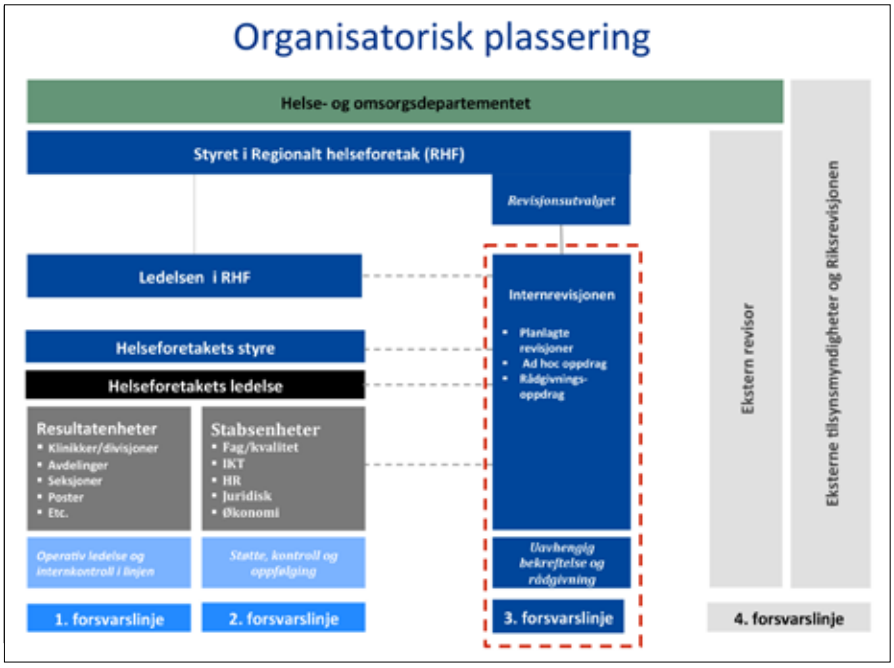
Ifølge internasjonale standarder som angir grunnleggende prinsipper for internrevisjon i offentlig sektor, kan internrevisjonen styrke tilliten til publikum ved å påpeke manglende samsvar mellom vedtatte mål og standarder og prinsipper for god virksomhetsstyring (ISSAI 100 2013). En forutsetning for at internrevisjonen skal kunne oppfylle slike forventninger er at det er et visst samsvar mellom de forventningene som stilles til funksjonen og i hvilken grad disse blir oppfylt. Vi har undersøkt hvilke synspunkter erfarne toppledere i helsesektoren har på internrevisjonen, hva som har betydning for om internrevisjonen tilfører merverdi, og hvilken rolle de beskriver for en fremtidsrettet internrevisjon i helsesektoren.

FORSKNING OM MERVERDI

Fra compliance-revisjon til «value-added role»

Forskning om internrevisjon belyser hvordan internrevisjon som funksjon har endret seg over tid. Utviklingen har gått fra tradisjonell etterlevelsesrevisjon hvor uavhengighet er sentral, til en mer «value-added role» hvor rådgivning, fokus på forbedring og samarbeid med ledelse har større betydning. Selve det å arbeide med en større innretning mot forbedring og samarbeid, med et utgangspunkt i risiko, karakteriseres av enkelte forskere som å jobbe merverdi-rettet (Mihret og Woldeyohannis 2008). De beskrevne endringene påvirker forholdet mellom ledelse og internrevisjon og gjør internrevisjonens objektivitet og uavhengighet til et viktig tema. Endringene har også ført til et behov for å få ny kunnskap om hva som ligger i internrevisjonens merverdi. For at internrevisjonen skal lykkes må den og dens interessenter ha relativt lik forståelse av hva som gir merverdi, slik at tjenesten brukes, og at anbefalinger og råd følges (Sarens og DeBeelde 2006).

Forskning som prøver å identifisere internrevisjonens merverdi er flertydig og preget av mange små studier med begrenset generaliserbarhet. En større studie av 13 500 internrevisorer fra 107 land viste at følgende forhold har positiv innvirkning på merverdi: At internrevisjonen er objektiv og uavhengig, at den etterlever IIAs standarder, og at internrevisjonen bidrar til evaluering og forbedring av internkontroll- og risikostyringssystemer. De understreker spesielt betydningen av relasjonen med revisjonsutvalget, og objektivitet og uav-



Figur 1 Internrevisjonens plassering i de regionale helseforetak

hengighet som sikrer troverdighet og status (D'Onza, Selim et al 2015).

Et annet perspektiv er at internrevisjonen har en «merverditilnærming» ved å bidra til en mer effektiv internkontroll-

> «Utviklingen har gått fra tradisjonell etterlevelses-revisjon hvor uavhengighet er sentral, til en mer «value-added role» hvor rådgivning, fokus på forbedring og samarbeid med ledelse har større betydning».

struktur, som igjen kan føre til et bedre grunnlag for endring og utvikling (Bou-Raad 2000, 182).

Ulike interessenter – ulike ønsker

Ulike nivåer i organisasjonen har ulike forventninger til internrevisjonen. Ifølge Drent (2002) vil revisjonsutvalget tradisjonelt ha uavhengig, objektiv bekreftelse på internkontrollen, for å oppfylle styrets krav til virksomhetsstyring og sikre etterlevelse av lover og regler. Linjeledelsen ønsker hjelp til å identifisere risiko og forbedre internkontrolltiltak, og råd som ikke griper for langt inn i virksomheten, for å få hjelp til å forbedre operasjonell effektivitet. Toppledelsen vil ha bekreftelse på at aktiviteter som er iverksatt for å oppnå mål, virker som forutsatt. Ifølge Sarens og DeBeelde (2006) ønsker ledelsen en støttende funksjon som kan bidra til å kompensere for redusert kontroll som følge av en stadig økende organisatorisk kompleksitet.

Objektivitet og uavhengighet

Objektivitet og uavhengighet har vært mye diskutert og forsket på i sammenheng med utviklingen av internrevisjonens rolle (Stewart og Subramaniam 2010). Christopher et al (2009) undersøkte i hvilken grad relasjonen med ledelsen utfordrer internrevisjonens uavhengighet. De fant at input fra toppledelsen er viktig for å bidra til å utvikle gode revisjonsplaner, men at involvering fra ledelsen i planlegging av revisjoner kunne ha negativ innflytelse på uavhengigheten til internrevisjonen. Det var viktig at slike innspill ikke oppfattes som et krav.

Drent (2002) pekte på at en vanlig oppfatning i ledelsen er at internrevisjonen arbeider for dem, og at rapportering til revisjonsutvalget ses som en formalitet for å møte krav til virksomhetsstyringen. Ledelsen kan få den oppfatning at internrevisjonen er dårlige lagspillere når de insisterer på å opprettholde sin uavhengighet. Internrevisjonens utfordring er å tilføre ledelsen merverdi uten å bli dens «tjener».

Internrevisjon i spesialisthelsetjenesten

- *Staten overtok eieransvaret for spesialisthelsetjenesten fra fylkeskommunene i 2002 og etablerte en foretaksstruktur med fem regionale helseforetak (RHF). I 2007 ble Helse Sør og Helse Øst slått sammen til Helse Sør-Øst, og i dag er det fire RHF i Norge. De eies av staten og har ansvaret for spesialisthelsetjenesten i regionen.*
- *Under hvert RHF er det helseforetak (HF), som varierer i størrelse fra under tusen ansatte og til over 20 000 ansatte. HFene har egne styrer og er selvstendige juridiske enheter.*
- *Lovgivningen stiller omfattende krav til de regionale helseforetakenes tilsyn, internkontroll og virksomhetsstyring. I 2005 påla departementet RHFene i foretaksmøte å etablere en internrevisjon i hver av de fire helseregionene, og etablere revisjonsutvalg nedsatt av medlemmer av styret i RHF. Ordningen med internrevisjon på RHF-nivå ble lovfestet i Helseforetaksloven § 37a med virkning fra 1. januar 2013.*
- *Internrevisjonene er organisert direkte under styret i RHF og rapporterer funksjonelt til styret og administrativt til administrerende direktør.*
- *Helseforetakene er eneste statlige særlovsselskap som i lovs form er pålagt å etablere en internrevisjonsfunksjon (Finansdepartementet 2014).*

Gjennomføring av undersøkelsen

- Datainnsamlingen ble gjennomført ved hjelp av telefonintervjuer i mars-april 2016.
- Intervjuundersøkelsen omfattet administrerende direktør, styreleder og medlemmer av revisjonsutvalg i RHF, samt administrerende direktører og styreledere på helseforetaksnivå i alle fire helseregioner.
- Utvalget omfatter 19 personer. De har og har hatt følgende 24 posisjoner i helsesektoren innenfor de siste to år: Styre og revisjonsutvalg RHF (7), toppledelse RHF (5), styreleder HF (7) og AD HF (5). Alle fire helseregionene er representert i utvalget. Informantene har omfattende erfaring fra ulike lederposisjoner i helsesektoren, og omtrent halvparten har også tidligere erfaring med internrevisjon fra andre bransjer eller stillinger.
- Intervjuene ble gjennomført med utgangspunkt i en semi-strukturert intervjuguide. Temaene tok utgangspunkt i standardene for internrevisjon og relevant litteratur om internrevisjonens oppgaver og ansvarsområder. Den etterspurte synspunkter på ulike sider av internrevisjonens arbeid og kontakt med styre, revisjonsutvalg og ledelse, kommunikasjon og rapportering av funn, prosessen for utvelgelse av revisjonstemaer, samt synspunkter på internrevisjonens bidrag til arbeidet med internkontroll, risikostyring og virksomhetsstyring.
- Artikkelen tar utgangspunkt i oppgave skrevet av forfatterne til Mastermodul ved BI, Internrevisjon: Virksomhetsstyring, risikostyring og intern styring og kontroll.

Reding et al (2013) peker på at rådgivningsoppdrag med sitt fremtidsrettede blikk har et større potensial for å tilføre verdi til organisasjonens systemer for internkontroll i et langsiktig perspektiv, i forhold til tradisjonelle bekreftelsesoppdrag som i større grad beskriver forhold som har skjedd i fortiden.

Ammar (2015) gjennomgikk forskning om internrevisjonens uavhengighet, og pekte på den iboende spenningen som ligger i å skulle revidere virksomheters internkontroll og samtidig bidra med rådgivning og støtte til ledelsen. Gjennomgangen viste at denne spenningen er erkjent, men ikke beskrives som bare negativ, og at rådgivning som aktivitet synes å bidra med merverdi til organisasjonen og derfor oppleves som ønskelig. Andelen rådgivningsoppdrag synes også å være økende.

Hvilken kompetanse vektlegger ledere av internrevisjoner?

Med utgangspunkt i at det stilles nye krav både til kompetanse og hvordan internrevisjonen arbeider, ble det gjennomført en undersøkelse blant 1196 internrevisjonsledere i 63 land (EY 2015). Respondentene anga de kompetanseområder de så som viktigst, og der behovet for forbedring var størst. Kunnskap om virksomheten, internkontroll, operasjonelle revisjoner og analytiske evner ble nevnt som de viktigste kompetanseområdene. Behovet for forbedring var størst innenfor områdene kunnskap om virksomheten, teknologi, prosessforbedring og dataanalyse. Respondentene la moderat vekt på betydningen av muntlig og skriftlig kommunikasjon, og rådgivning og endringsledelse ble vurdert som minst viktig. Når det gjelder rådgivning var det heller ingen som mente at det var behov for forbedring.

FUNN FRA UNDERSØKELSEN

Informantene er i hovedsak positive til internrevisjon som virkemiddel og mener at det er et nyttig verktøy for å bedre intern styring og kontroll. De knytter begrepet merverdi i særlig grad til prosesser som fremmer forbedring i organisasjonen. De kommer med mange felles synspunkter på internrevisjonens rolle i organisasjonen, og gir på flere områder en relativt lik beskrivelse av hva de ønsker seg.

Relevante og aktuelle revisjoner

For å tilføre merverdi må revisjonene være relatert til strategisk viktige mål og ta utgangspunkt i områder med høy risiko, og være relevante for det som helseforetakene opplever har størst betydning. De må reflektere sentrale utfordringer i intern styring og kontroll, og ta utgangspunkt i vurdering av risiko, ha fokus på sentrale temaer innen internkontroll, og bidra til god virksomhetsstyring. En informant fra

> «Det viktigste er at internrevisjonen settes i sammenheng med andre aktiviteter og at man understøtter hvordan det jobbes mot strategisk viktige mål. Hvis internrevisjonen gjør ting de selv er opptatt av uten å tenke på relevansen for virksomhetene blir man jo ikke viktig».
>
> *Uttalelse fra en administrerende direktør i et regionalt helseforetak.*

et revisjonsutvalg sier det slik: *«Det må jo henge godt sammen med oppdraget vårt. Og innenfor oppdraget må man velge der det er størst risiko eller det som har størst betydning, eller der hvor feil og mangler har de største konsekvensene.»* En administrerende direktør (AD) peker på spørsmål de gjerne vil ha svar på: *«Den løpende kvalitetssikringen av virksomhetsstyringen – er den i orden? Driver man rasjonelt, og holder man på med de riktige tingene?»* Flere informanter påpeker at utgangspunktet for revisjoner ofte vil være der man tror det kan være

fare for svikt: «*Man velger jo ikke et revisjonsområde der alt er på stell… Det ville jo vært kjekt og hyggelig, men ikke så nyttig...*» Informantene peker på at det de siste ti årene har vært jobbet systematisk for å få kontroll på økonomi og administrative støttefunksjoner, og at dette nå oppfattes som et område med rimelig grad av kontroll. De største utfordringene er knyttet til kvalitet i pasientbehandling. I tillegg blir også IKT nevnt av flere som et særlig risikoområde.

Revisjonene bør ha relevans for det som helseforetakene driver med. En AD i et regionalt helseforetak (RHF) sier det slik: «*Det viktigste er at internrevisjonen settes i sammenheng med andre aktiviteter i RHF/Helseforetak (HF) og at man understøtter hvordan det jobbes mot strategisk viktige mål. Hvis internrevisjonen gjør ting de selv er opptatt av uten å tenke på relevansen for virksomhetene blir man jo ikke viktig*». For å sikre relevans er kontakt med helseforetakene i prosessen rundt planlegging av revisjoner viktig.

Involvering for å komme frem til områder for revisjon

Det er en utbredt oppfatning at HF-nivået bør komme med innspill til revisjonstemaer. Dette begrunnes med nærheten til den operative virksomheten. Intervjuene viser imidlertid at informantene på dette nivået i varierende grad har erfart å bli involvert i arbeidet med revisjonsplanen. Flere gir uttrykk for at det kunne vært ønskelig å bli spurt, og enkelte sier også at de kanskje kunne vært mer aktive selv med hensyn til å komme med innspill.

På RHF-nivå beskrives noen steder nær dialog mellom internrevisjonen og administrerende direktør, og i noen tilfeller også med ledergruppen på RHF, om aktuelle temaer for revisjon. Dialogen er ikke like tett i alle regioner. Der hvor dialogen karakteriseres som god og etablert beskrives også et strukturert og godt samarbeid i forbindelse med utviklingen av revisjonsplanen. Et styremedlem påpeker et dilemma knyttet til prosessen med å komme frem til hva som skal revideres: «*Det er et prinsipielt spørsmål hvem som skal vedta hva som skal revideres. Så lenge man skal være mest mulig uavhengig av administrasjonen, skal administrasjonen ha noen formening om hva som skal revideres? Administrasjonen kan la være å foreslå områder der man ikke vil bli sett etter i kortene*». Det er en bevissthet om at administrasjonen ikke skal påvirke revisjonene i for stor grad, men samtidig understrekes betydningen av at kjennskapen til virksomheten er et viktig utgangspunkt for å vurdere hvilke områder og temaer som er viktige å revidere.

Spennvidde i syn på rollen

Flere beskriver internrevisjonen som et kontrollorgan som skal påse at styrets vedtak blir fulgt opp, og bidra med informasjon om driften er under kontroll. Andre er mer opptatt av at internrevisjonen skal bidra til læring, og ønsker ikke at kontrollaspektet skal være fremtredende. Flere vektlegger at internrevisjonen, gjennom å fange opp sentrale risikoer, kan forhindre feil og være en «*vaktbikkje*». Et medlem av revisjonsutvalget beskriver internrevisjonen som «*bindeledd mellom revisjonsutvalg, ekstern revisjon og styre, i tillegg til å være en støttefunksjon – en kompetanseinstitusjon som helseforetakene kan bruke i forhold til risikostyring og intern styring og kontroll.*» Denne informanten legger i likhet med flere andre vekt på at internrevisjonen skal være en støtte, ikke bare for styret, men også for administrasjonen.

> «Suksesskriteriet er å selge seg inn som endringsagent for forbedring, noen jeg som styreleder syntes er en åpenbar partner.»
>
> *Uttalelse fra en styreleder i et helseforetak.*

Internrevisjon som katalysator for forbedring

Informantene er opptatt av at internrevisjonens arbeid skal være et utgangspunkt for utvikling av organisasjonen. En AD på et HF uttrykker seg slik: «*Internrevisjonen blir oppfattet som vellykket og nyttig – av de fleste. Det er nok fordi de tonet ned kontrollørrollen og tonet opp forbedringsrollen*». Internrevisjonen må være på tilbudssiden og aktivt kommunisere målet om forbedring. En styreleder på HF-nivå sier det slik: «*Suksesskriteriet er å selge seg inn som endringsagent for forbedring, noen jeg som styreleder syntes er en åpenbar partner.*» En AD fra HF beskriver sin oppfatning på en måte som reflekterer det mange av informantene gir uttrykk for: «*Man må jakte på forbedringsperspektivet og ikke feil som er funnet. Jeg tror at dialogen mellom de som er revidert bidrar til forbedring. Dette sammen med styringsdialog skaper erkjennelse og et rom for endring, mer enn store rapporter. Det skaper ledere som har eierskap til problem-*

stillingene.» En gjennomgående oppfatning er at internrevisjonen har en viktig rolle i å gi et grunnlag for forbedring i virksomheten. Informantene understreker videre at noe av det viktigste ved revisjoner er grunnlaget det gir for arbeidet som gjøres i etterkant, der ansvaret for implementering av forbedringsarbeidet ligger i linjen.

Involvering og kommunikasjon

Merverdi skapes når revisjonene gjennomføres som en prosess preget av dialog og involvering, både i den forberedende fasen, underveis i revisjonen og i forbindelse med verifikasjon og ferdigstillelse av rapporter. En AD uttrykker seg slik: *«Det er dialogen som gjør at man får en bedre måte å jobbe på og det er den som bidrar til motivasjon for forbedringsarbeid. Internrevisjonen bør være tydeligere på hva som er viktige funn, og de bør våge å gå i dialog om dette».* Fra en av informantene i et revisjonsutvalg presiseres det at forankringen på toppen i HF-et er helt sentral i dette arbeidet: En styreleder ved et HF peker på betydningen av kommunikasjon: *«Når vi snakker om forbedringsarbeid er det mye snakk om kulturarbeid. Tør man å være trygg på at internrevisjonen gjør dette for at vi skal bli bedre? Vi har alle vår dedikerte rolle i organisasjonen, og man må huske på at man ikke bedre enn de andre. Det handler om pedagogikken i gjennomføringen, og også litt ydmykhet.»* En AD ved et HF mener at kommunikasjonen må skje i et forbedringsperspektiv og at internrevisjonen ved å *«velge ut temaer som oppleves som relevante og kommuniseres på en måte som skaper engasjement og forbedring»* bidrar til å styrke arbeidet med forbedring i etterkant av revisjonene.

Ønske om rådgivning

Informantene ønsker seg en internrevisjon som i større grad enn i dag bidrar med rådgivning. En AD på HF sier det slik: *«Internrevisjonen har mye kunnskap om hva som er god virksomhetsstyring og risikostyring, og det hadde vært nyttig å dra dem inn tidligere for å få råd om hvordan man skal øke bevisstheten rundt dette. Men det kan være at det kommer på siden av mandatet?»* En leder av et revisjonsutvalg er tydelig i sitt ønske om rådgivning: *«Jeg er villig til å strekke rollen med rådgivning og veiledning litt lengre enn det som står skrevet».* En AD på HF ønsker seg *«en internrevisjon som har en proaktiv rådgivningsrolle, men ikke i konkurranse med konsulentselskap.»* Det understrekes at dette kan gjøres underveis i løpet av en revisjon og ikke som egne oppdrag.

Noen informanter beskriver rådgivning som lite fremtredende i dag, og et medlem av et revisjonsutvalg har dette synspunktet: *«Sånn som det har vært har ikke internrevisjonen fått den plassen den burde ha. De har kommet med sine rapporter som de har lagt frem, men de har ikke blitt sett på som en kompetansebase man kunne trekke på».*

I en av regionene er rådgiverrollen formalisert, og overordnet ledelse både i styre og i administrasjonen i RHF mener at rådgivning er viktig for at internrevisjonen skal oppleves som en nyttig samarbeidspartner.

Kompetanse, integritet og objektivitet

Internrevisjonens kompetanse ses som en nøkkelfaktor for kvaliteten på revisjonene. I hovedsak formidler informantene at de har godt inntrykk av internrevisjonens kompetanse. En informant fra et revisjonsutvalg peker på at perspektivet på organisasjonen er viktig: *«Det faktum at man har kunnskap om systematikk, kartlegging, faglig ballast, det å se ting fra ulike sider – alt dette tilfører merverdi. Internrevisjonen kan gå dypere inn i ting, de ser ting objektivt og kan se ting fra et annet perspektiv».* Det gis uttrykk for klare forventninger til et høyt kompetansenivå som innebærer både faglig ballast og et nødvendig utenfra-perspektiv.

Flertallet av informantene gir uttrykk for at internrevisjonen oppfattes som objektiv og upartisk, og tillegger dette stor betydning. Et medlem av et revisjonsutvalg sier det slik: *«Det å være blottet for tilhørighet til pasientgrupper eller områder er viktig. Det at revisjonen kommer utenfra gjør at de kan ta med seg flere perspektiver».* En styreleder mener objektivitet er avgjørende for at internrevisjonen skal oppfattes å være troverdig: *«Det er viktig at man ikke blir oppfattet som en representant for et kontroversielt standpunkt, at man har en høy etisk standard og en god metodisk tilnærming.»* En AD i RHF legger vekt på integriteten: *«Internrevisjonen har høy grad av integritet, selv om de har kontorer blant oss. Ingen ville drømme om å hevde at de ikke er nøytrale. Det viktigste for å lykkes er troverdighet. Hadde de ikke vært troverdige hadde det ikke vært noen vits».*

Selv om internrevisjonen av de fleste ses som en objektiv og uavhengig instans er det også informanter som ikke oppfatter det slik. En AD på HF påpeker at internrevisjonen med sitt oppdrag fra styret i regionen slett ikke er objektiv: *«Dere har jo et oppdrag, jeg regner med at internrevisjonen går oppdragsgivers ærend. Da er man ikke objektiv og nøytral».*

Å være en del av samme organisasjon

Internrevisjonen kan bli så opptatt av sin uavhengighet at de inntar en rolle hvor de

oppfattes å være på utsiden. Objektivitet og uavhengighet må derfor balanseres opp mot deltakelse i organisasjonen. En AD på RHF utdyper: *«Å være objektiv og uavhengig er det minste problemet, det ligger til funksjonen. Men det er viktig at ikke internrevisjonen blir mer katolsk enn paven. Hvis man setter seg på siden av organisasjonen blir man fort et hår i suppa».*

Flere mener at internrevisjonen må passe seg for å bli en kultur utenfor organisasjonen. En styreleder ved et HF utrykker det slik: *«Når man kommer inn og skal se på andres oppgaver er det kanskje trygt å ha litt avstand. Men man må akseptere at man er del av samme kultur og at alle har sine roller, og skape relasjoner som gjør at man forstår litt mer, at man opptrer på en måte som gjør at folk tør å åpne seg og fortelle hvordan situasjonen egentlig er og hvilke dilemmaer man står overfor».* En AD fra HF mener holdningen internrevisjonen inntar er avgjørende: *«Man kan bli så formell og formalistisk at man mister det menneskelige i kommunikasjonen – det som gjør at man får tillit i situasjonen. Man kan godt være uavhengig og objektiv uten at man er distansert. Det er upartiskheten som kommer i veien».* Flere av informantene er opptatt av at det har skjedd en positiv utvikling når det gjelder opplevelsen av at internrevisjonen tilhører samme organisasjon. En informant fra et revisjonsutvalg forteller *«Foretakene setter faktisk pris på at internrevisjonen kommer, de blir etterspurt, og da har man lykkes. De oppleves nå som at vi jobber mot samme mål og at vi er en del av samme organisasjon. Vi skal skape resultater sammen, og det har internrevisjonen lykkes med».*

Kvalitet på rapporter

Informantene er opptatt av kvaliteten på rapportene, og både relevans og en gjenkjennbar virkelighetsbeskrivelse fremheves som viktig. En AD i et RHF uttrykker seg slik: *«Revisjonen må oppleves som relevant, slik at det er mulig å forstå hva som blir sagt, hvis ikke blir det formålsløst. Hvis rapportene ikke beskriver en virkelighet man kjenner seg igjen i, så er ikke rapportene nyttige. Blir rådene for konkrete blir det feil, revisjonen gir jo bare nyanser av en virkelighet, et situasjonsbilde, og er ingen fasit»*

Et gjennomgående synspunkt er at rapportene bør vektlegge både positive og negative forhold. Samtidig sier flere at internrevisjonen ikke må være redd for å si fra når noe ikke er bra: *«Det er ikke hensiktsmessig hvis rapportene blir for pusete, da vil de miste sin autoritative kraft. Det er en hårfin balanse mellom å beskrive gjenkjennbart og påpeke svakheter.»* En annen informant peker på at anbefalingene kan bli litt runde, og man må ikke være så redd for å tråkke noen på foten. Det er viktig at internrevisjonen tar rollen og har troen på egen posisjon og kraft.

Informantene legger vekt på betydningen av tydelig kommunikasjon. *«Det er alltid en utfordring å få frem poengene uten at det drukner i beskrivelser. Noen ganger gjøres det litt for komplisert, og man kan kommunisere funnene kortere. Vi må ikke undervurdere betydningen av enkle budskap.»* Det påpekes også at man ikke må bruke for intern fagterminologi hvis man vil kommunisere godt: *«Ethvert system har sitt menighetsspråk og det er viktig å få rapportene slik at de kan gjenkjennes. Et formelt språk kan virke fremmedgjørende».*

DISKUSJON

Relevans og timing

Undersøkelsen viser at et hovedpoeng for at internrevisjonen skal tilføre merverdi er at revisjonene som gjennomføres er relevante og aktuelle. Finansdepartementets utredning fra 2014 vektlegger at internrevisjon har dreid i retning av mer omfattende analyser og vurderinger av institusjonens aktiviteter og virkemåte på vegne av ledelsen, og en utvikling der internrevisjonen går inn på strategiske områder og har fokus på å bidra til å «gjøre de riktige tingene». (Finansdepartementet 2014). Dette bekreftes av vår undersøkelse, der det tydelig fremgår at internrevisjonens merverdi er knyttet til at revisjonene bidrar til tilfredsstillende måloppnåelse og oppfølging av strategiske mål, og reflekterer de viktigste utfordringene knyttet til intern styring og kontroll. Når revisjonene reflekterer sentrale risikoområder og har relevans for det som pågår i helseforetakene, oppleves de som nyttige, og et bidrag i forbedringsarbeidet. Derfor er også innspill fra helseforetakene til revisjonsplaner viktig. Dette er avgjørende for at revisjonsplanen skal bli relevant, og selv om uavhengigheten kan være en utfordring, er internrevisjonens håndtering og balansering av forholdet til ledelsen viktig. Undersøkelsen viser at hvis ikke revisjonene er aktuelle og relevante for foretakene, hjelper det ikke om de er metodisk godt gjennomført og om rapporter er godt skrevet. Omhandler de ikke vesentlige områder, vil revisjonene ikke tilføre merverdi.

Forbedring versus kontroll

Alle informantene er opptatt av at internrevisjonen skal bidra til forbedring, men har ulike syn på hvordan dette skal oppnås. I tillegg til å fremme forbedring, beskrives internrevisjonen også som et kontrollorgan som skal påse oppfølging av styrets vedtak, fange opp sentrale risikoer og gi informasjon til ledelsen om driften er under kontroll. Andre toner ned kontrollaspektet, og peker på at det viktigste er forbedring og det å oppnå læring på tvers.

> Undersøkelsen viser et spenn i oppfatningene om internrevisjonens roller, men oppfatningene kan karakteriseres mer av «ja takk begge deler» enn «enten-eller». De som peker på behovet for kontroll, er også opptatt av forbedring. De som er opptatt av rådgivning, vil også ha revisjoner.

Undersøkelsen viser et spenn i oppfatningene om internrevisjonens roller, men oppfatningene kan karakteriseres mer av «ja takk begge deler» enn «enten-eller». De som peker på behovet for kontroll, er også opptatt av forbedring. De som er opptatt av rådgivning, vil også ha revisjoner. Forventningen til internrevi-

sjonen er ulik på de ulike nivåene, slik også forskningen viser (Drent 2002). Ulike forventninger til rollen må balanseres med en felles forståelse av hvordan denne funksjonen kan bidra til de ulike nivåene i organisasjonen. Her ligger det også muligheter til videre utvikling av internrevisjonen.

Økt fokus på rådgivning

Informantene har et ønske om at internrevisjonen i større grad enn i dag bidrar med rådgivning. De ser gjerne at internrevisjonen i forbindelse med gjennomføring av revisjoner byr på sine kunnskaper, og også gir råd ut over den revisjon de er inne i. De ser ikke for seg at internrevisjonen skal fungere som konsulenter.

Forskning om internrevisjon legger vekt på rådgivningens potensial for å tilføre merverdi på tross av at det også utfordrer internrevisjonens objektivitet (Reding et al 2013, Ammar 2015).

Utviklingen innen internrevisjonsfaget har problematisert rådgivningsfunksjonen. I de reviderte standardene fra 2015 er det engelske begrepet «*consulting*» endret til «*advice*». Gjennom dette kan man si at konsulentrollen er tonet ned og at det er lagt mer vekt på rådgivning. Det er denne rollen informantene beskriver at de ønsker internrevisjonen skal ta. I forhold til rammene som standardene setter for internrevisjonens uavhengighet og objektivitet, og sett i lys av forskning på området, burde disse ønskene være innenfor det som internrevisjonen kan tilby. Det viktige her er at internrevisjonen ikke skal ha ansvar for tiltak i organisasjonen som den senere må revidere.

Internrevisjonens samarbeidspartnere

Et spørsmål knyttet til internrevisjonens merverdi er hvem som er deres sentrale samarbeidspartnere. Teori om internkontroll viser at styret har ansvar for å bekrefte internkontrollen og AD har ansvar for å iverksette den. I intervjuene kommer det synspunkter på at styrene både på HF og RHF-nivå har en mindre sentral rolle i forhold til internrevisjonen enn administrasjonen har. Selv om revisjonsutvalget er mer involvert enn resten av styret, kan det være et potensial for at styrene i større grad enn i dag kan bruke internrevisjonen aktivt som verktøy for å ivareta sitt ansvar.

Informantene i undersøkelsen vår peker på at administrasjonen er den mest sentrale samarbeidspartneren både i RHF og HF, og uttrykker et ønske om et tett og nært samarbeid. Dette bekreftes også av forskningen (Drent 2002). Denne oppfatningen hos ledelsen kan være utfordrende i forhold til internrevisjonens uavhengighet, men et nært samarbeid med ledelsen er likevel avgjørende for å tilføre merverdi. Det er derfor viktig at internrevisjonen og ledelsen lykkes i å etablere et godt samarbeid, samtidig som internrevisjonen ivaretar sin uavhengige rolle. I motsatt fall kan internrevisjonens integritet svekkes, og den autorative kraften og påvirkningsevne reduseres.

Kommunikasjon og samhandling

Informantene ønsker seg en internrevisjon som kommuniserer godt, er proaktive og byr på seg selv. Dette er avgjørende for eierskapet til revisjonene og for forbedringsarbeidet i etterkant. På HF-nivået legges det vekt på at merverdi særlig skapes i dialogen som skjer underveis i revisjonen, og da særlig i prosessen med verifisering. Dette er like viktig som rapportene og den formelle behandlingen av dem. Internrevisjonen må kommunisere på en måte som ikke skaper distanse, og flere ønsker mindre bruk av intern fagterminologi. I henhold til teori om internkontroll ligger ansvaret for oppfølging av revisjoner til linjeledelsen, og informantene er også svært tydelige på dette ansvaret.

> Det er viktig at internrevisjon er i stand til å sette seg inn i de revidertes posisjon og ta den andres perspektiv. Det er når man opplever å være i samme båt, og når relasjonen er preget av tillit, at det skapes et klima for endring.

Internrevisjonen som del av organisasjonen

Flere informanter forteller at internrevisjonens uavhengighet kan bli en hemsko som skaper barrierer. Det kan oppleves som et «vi og dem». Informantene ser internrevisjonen som objektive og uavhengige, men mener dette må balanseres slik at internrevisjonen ikke inntar en rolle hvor de plasserer seg på utsiden av organisasjonen. Det er viktig å være i stand til å sette seg inn i de revidertes posisjon og ta den andres perspektiv. Det er når man opplever å være i samme båt, og når relasjonen er preget av tillit, at det skapes et

klima for endring. Internrevisjonen må forstå prosessene i organisasjonen og spille på lag med de som skal revideres for å lykkes i å tilføre merverdi. Inntrykket av at informantene ønsker at internrevisjonen er tettere på organisasjonen, styrkes av uttalelser om betydningen av involvering og kommunikasjon, både i planlegging og gjennomføring av revisjoner. Dette støttes av forskning som viser at samhandling med ledelsen er avgjørende for om internrevisjonen tilfører merverdi

Standardene slår fast at internrevisjonen må være objektiv og ha en upartisk innstilling også i utførelsen av sitt arbeid, og ut fra dette er det viktig at internrevisjonen er bevisst sin rolle i organisasjonen. En mer proaktiv rolle for internrevisjonen burde likevel ikke være i strid med standardene.

Kompetansens betydning

Kompetanse trekkes frem som en nøkkelfaktor for merverdi, og i tillegg til å beherske emner relatert til revisjonsmetodikk, trenger internrevisjonen kunnskap som gjør at de forstår virksomheten og relevante fagområder. Vår undersøkelse viser at kommunikasjon, dialog, involvering og organisasjonsforståelse har avgjørende betydning for å tilføre merverdi. Et økt fokus på slike forhold kan forutsette endret behov for kompetanse, og innebærer også utviklingsmuligheter for internrevisjon i fremtiden.

KONKLUSJON

Undersøkelsen viser at for å tilføre merverdi må internrevisjonen:

- Gjennomføre revisjoner som er relatert til strategisk viktige mål og tar utgangspunkt i områder med høy risiko
- Ha gode prosesser og sørge for involvering i arbeidet med å utarbeide revisjonsplan
- Kommunisere godt og involvere organisasjonen for å skape forankring og motivasjon for oppfølging av revisjonenes anbefalinger
- I større grad enn i dag dele kunnskap og ta en aktiv rådgivningsrolle
- Balansere nærhet til og forståelse av virksomheten opp mot objektivitet og uavhengighet.

Gjennom dette kan internrevisjonen være en katalysator for endring, og for at dette skal oppnås er forankring i organisasjonen viktig. Dette synet på internrevisjonen er i tråd med nyere forskning om internrevisjon, som beskriver en utvikling fra tradisjonell etterlevelsesrevisjon til en «value-added role» hvor samarbeid med ledelsen har stor betydning. En slik utvikling stiller krav til omfattende og kanskje endret kompetanse hos internrevisjonen, hvor blant annet kommunikasjon, organisasjonsforståelse og endringskompetanse kan få økt betydning i forhold til i dag.

LITTERATUR

Ammar, S H. 2015. «Critical Analysis of Internal Audit Independence: International Literature». Journal of Research in Business, Economics and Management, Volume 3, Issue 3.

Christopher, J, G Sarens og P Leung. 2009 A critical analysis of the independence of the internal audit function: evidence from Australia. Accounting, Auditing & Accountability Journal vol. 22 no. 2, pp. 200-220

D'Onza, G, G M Selim, R Melville og M Allegrini 2015 "A Study on Internal Auditor Perceptions of the Function Ability to Add Value". International Journal of Auditing 19 pp 182-194

Drent, D. 2002 «The quest for increased relevance», Internal Auditor, vol 59 no 1

EY (2015) Global GRC-undersøkelse. Internt notat.

Finansdepartementet 2014. «Bruk av internrevisjon i staten». Utredning fra en arbeidsgruppe nedsatt av Finansdepartementet, høsten 2013. Rapport avgitt til Finansdepartementet 6. juni 2014

Finansdepartementet 2015 «Internrevisjon i statlige virksomheter». Rundskriv R-117

ISSAI 100 2013 «Fundamental Principlesof Public-Sector Auditing». INTOSAI

Mihret, D G og G Z Woydeyohannis 2008 «Value-added role of internal audit: an Ethiopian case study». Managerial Auditing Journal vol 23 no 6 pp 567-595

Ramamoorthi, S. 2003, «Internal Auditing: History, Evolution and Prospects», The Institute of Internal Auditors Research Foundation, Altamonte Springs, FL.

Reding, K F, P Sobel, U Anderson et al 2013 "Internal Auditing. Assurance and advisory services". Florida, IIA Foundation

Sarens, G og DeBeelde 2006 «The Relationship between Internal Audit and Senior Management: A Qualitative Analysis of Expectations and Perceptions». International Journal of Auditing, 10: pp 219-241

Stewart, J og N Subramaniam 2010 «Internal Audit Independence and Objectivity: Emerging Research Opportunities». Mangagerial Auditing Journal Vol 25 no 4 pp 328-360

Er kultur et tema for internrevisjon?

Av
VERONICA S. KVINGE,
prosjektleder i konsernrevisjonen,
OG
METTE D. STORVESTRE,
konsernrevisjonssjef, i BKK

Er kultur et tema for en internrevisjon? Ja, i aller høyeste grad sier Veronica S. Kvinge og Mette D. Storvestre i BKK. I denne artikkelen peker de på at kultur er et område der en internrevisjon virkelig kan tilføre verdi til organisasjonen. I BKK utfører mange ansatte farlig arbeid, og risikoen må reduseres med sikkerhetstiltak. Etter flere revisjoner på sikkerhetsområdet i BKK, viser funnene at kultur er en av de viktigste rotårsakene til gjentakende positive observasjoner men også til forbedringsområder.

Det er vanligvis ikke mangler i retningslinjer og prosedyrer som er årsak til at ulykker skjer, men kulturen, det som sitter i veggene i BKK. Det lederne gjør, og det de aksepterer at utførende personell gjør, blir praksis. Derfor er det viktig for en internrevisjon å finne rotårsaken til en ulykke, og ikke bare registrere at regler blir brutt.

At kultur er et område som bør revideres får støtte fra flere hold. James C. Paterson[1] legger til grunn at kultur er et område det er viktig at internrevisjonen dekker, men også at det er et komplekst område å forholde seg til. IIA i UK utgav i 2014 en veileder med tittelen «Culture and the role of internal audit – looking below the surface". I introduksjonen til denne veilederen slås det fast at internrevisjonen vil få en stadig viktigere rolle når det gjelder å revidere ulike kulturelle aspekter ved en organisasjon. Også nasjonalt settes kultur på agendaen. NTNU har blant annet utviklet en modell, Pentagonmodellen, for å analysere sikkerhetskultur i et utvidet perspektiv. Det ser dermed ut som det er på tide at internrevisjonsenheter som mener kultur ikke er et relevant tema, begynner å tenke nytt og utvider sin oppdragsportefølje.

[1] *James C. Paterson er tidligere revisjonssjef for Astra Zeneca PLC, forfatter av en rekke bøker og artikler på revisjonsområdet, samt en anerkjent foredragsholder innen internrevisjon.*
[2] *BKK har en nullvisjon, altså en målsetting om å unngå alle personskader.*

Hva er sikkerhetskultur?

Sikkerhetskultur handler om felles verdier og normer om sikkerhet i en virksomhet som får betydning for arbeidspraksisen, altså *hvordan vi gjør det hos oss*. Begrepet dukket opp på 1980-tallet etter storulykker som Challenger og Tsjernobyl, der en dårlig sikkerhetskultur ble trukket frem som en rotårsak til ulykkene.

Den viktigste indikatoren på sikkerhetskultur i organisasjoner er *hvordan ansatte aktivt forholder seg til sikkerhet i det daglige.* En moden kultur kjennetegnes ved at sikkerhet gjennomgående prioriteres i forhold til andre mål helt fra øverste nivå i organisasjonen og ned til utførende personell. Dette innebærer at vi ikke bare sier at vi skal jobbe sikkert, men at vi jobber sikkert.

HMS-arbeidet kan forenklet sies å bestå av mennesker, prosedyrer og utstyr som virker sammen i en helhet. Det krever systematisk arbeid over tid før et sikkert arbeidsmiljø vil være etablert basert på et godt samspill mellom disse tre delene.

Kan man revidere en kultur?

Høsten 2016 reviderte konsernrevisjonen sikkerhetskulturen i BKK Produksjon, et av BKKs datterselskaper. Da vi tok fatt på denne oppgaven, var det første gang vi adresserte deler av en kultur som et revisjonstema, og det var ikke helt åpenbart for oss hvordan vi skulle gripe an arbeidet. Kritiske røster stilte spørsmål ved hvordan vi skulle kunne revidere en kultur, og anførte at det ikke «fantes et revisjonskriterium».

Vi konkluderte med at sikkerhetskulturen måtte sees i sammenheng med konsernets sikkerhetsstyring. Sikkerhetsstyring har vi tolket som *det systematiske arbeidet som har betydning for sikkerhetskulturen,* og det omfatter i vårt tilfelle konsernets rammeverk med styrende dokumentasjon knyttet til personsikkerhet, systemet vi benytter for å rapportere ulykker og nesten ulykker, etablerte prosesser for å analysere rapporterte hendelser, systematisk arbeid for å innarbeide læring fra rapporterte hendelser også videre. En tilfredsstillende sikkerhetsstyring er nødvendig for å oppnå en moden sikkerhetskultur, men sikkerhetskulturen trenger ikke være moden selv om sikkerhetsstyringen er god. Sikkerhetsstyringen i konsernet ble vurdert opp mot gjeldende krav og mot god praksis. For sikkerhetskultur finnes det ikke tilsvarende klart definerte krav, så her ble revisjonskriteriet god praksis.

Metode og rammeverk

Formålet med revisjonsoppdraget var å *vurdere arbeidet med sikkerhetskultur i BKK Produksjon og foreslå tiltak som kan bidra til å nå nullvisjonen*[2]. Oppdraget pågikk over 3 måneder og inkluderte befaring av flere anleggsplasser, gjennomgang av om-

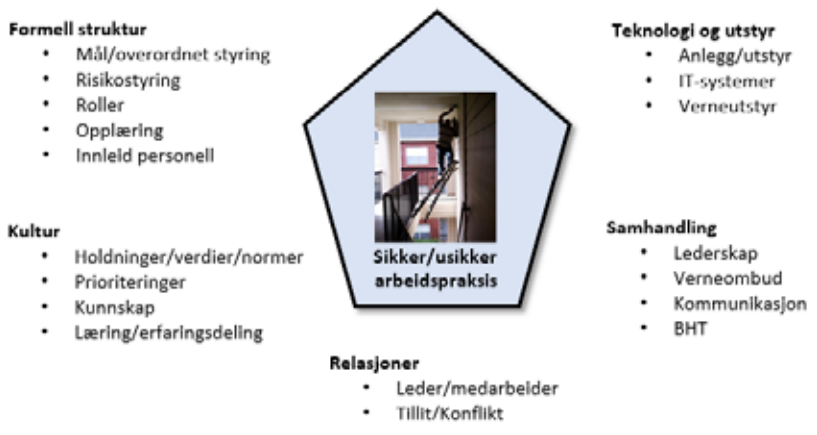
Konsernrevisjonen var i fjor høst på befaring til Kvanndalsvatnet i Eksingedalen. Fra venstre anleggsleder Einar Hovda Nilsen, HMS-rådgiver Stein Edvardsen, verneombud May Irene Langhelle og prosjektleder Bjørnar Rettedal. (Foto: Mette D. Storvestre)

fattende dokumentasjon samt intervju av om lag førti personer. Det ble lagt vekt på å intervjue et stort antall personer i «den skarpe enden», altså personer som faktisk utfører det farlige arbeidet i BKK. Det ble også gjennomført intervju med ledere på alle nivå fra førstelinjeledere på anleggsplassen til konsernsjef, samt med tillitsvalgte, verneombud, kvalitetsleder, bedriftslege, HMS-personell, beredskapsleder og lærlinger. Dette ble gjort for å få et best mulig grunnlag for å kunne vurdere statusen på området.

Vi tok utgangspunkt i James Reasons[3] perspektiv på sikkerhetskultur: *en kultur kan endres over tid ved å påvirke adferd i ønsket retning*[4]. Reason kaller en kultur for sikker arbeidspraksis en *informert kultur.* Han beskriver dette som en kultur der alle forstår og respekterer farene ved arbeidet. De er oppmerksomme på hva som kan gå galt og tar sine forholdsregler for å unngå skader og ulykker. En informert kultur består ifølge Reason av de fire delene *rapporterende, rettferdig, fleksibel og lærende*[5].

Pentagonmodellen, som er utviklet ved NTNU , ble benyttet for å analysere BKKs arbeidspraksis. Den viser sammenhengen mellom relasjoner, samhandling, kultur, formell struktur og teknologi og utstyr. Modellen tar utgangspunkt i at arbeidspraksisen i en bedrift blir påvirket og formet av formelle rammebetingelser som hvordan arbeidet er organisert, ansvaret er fordelt og hvilke regler / prosedyrer som gjelder, og av uformelle rammebetingelser som hvilken kultur som er rådende, hvordan relasjonene mellom grupper som skal samarbeide er og hvordan samhandlingen foregår.

Figur 1: Pentagonmodellen slik den er benyttet i BKK



Noen kjennetegn ved en moden sikkerhetskultur

I en moden sikkerhetskultur går lederne foran som gode eksempler – walk the talk! Det er ikke et effektivitetspress som går på bekostning av sikkerheten, og kommunikasjonen om dette er utvetydig. Dersom det å utføre en jobb sikkert innebærer at den ikke kan gjøres innenfor budsjettert kostnad eller planlagt tidsramme, vil det intuitive valget for både ledere og anleggsarbeidere likevel være å utføre den sikkert. Lederne berømmer medarbeidere som griper inn og stopper farlig arbeid for å iverksette nødvendige tiltak. Lederne er synlige på anleggsplassen, de aksepterer ikke avvik og de griper inn dersom de observerer farlige situasjoner. Å bare rapportere en hendelse men ikke gå i dialog med involvert personell, oppleves som uakseptabelt.

Både ledere og øvrige medarbeidere tror at nullvisjonen kan oppnås. De er klar over farene et arbeid innebærer, og de etablerer nødvendige barrierer for å hindre hendelser. Det er en forbedringsorientert kultur som aktivt innarbeider erfaringer for å lære av tidligere hendelser. Ansatte trives på jobb, de sier fra til hverandre dersom de opplever farlige situasjoner, etterlever etablerte sikkerhetskrav og tar ikke unødvendig risiko.

Ledere og utførende personell har gjennomført nødvendig sikkerhetsopplæring og dilemmatrening, og føler seg trygge i arbeidet. Arbeidsoppgaver planlegges godt, og medarbeidere benytter nødvendig verneutstyr også når de skal utføre mer tilfeldige småjobber. Risikovurderinger og identifisering av nødvendige

[3] *James Reason er professor i psykologi på universitetet i Manchester, og har utgitt en rekke publikasjoner knyttet til temaet sikkerhetskultur.*
[4] *Et annet perspektiv er det fortolkende, der en kultur beskrives og fortolkes, men anses ikke å være påvirkbar.*
[5] *Jf. f eks. «Sikkerhet i organisasjoner» av Trond Kongsvik ved NTNU, 2013, for mer om Reasons perspektiv.*
[6] *Per Morten Schiefloe m.fl., NTNU (2008)*

tiltak gjøres i samarbeid med utførende personell ved milepæler og ved endringer. Det gjøres også i forbindelse med det daglige arbeidet når den enkelte medarbeider ser behov for det. Ledere delegerer ansvar til utførende personell slik at de selv kan beslutte og iverksette nødvendige tiltak på anleggsplassen i et rimelig omfang.

Medarbeidere og ledere rapporterer hendelser for å lære av dem. Alvorlige hendelser følges opp på en konstruktiv måte og i en trygg setting for å lære av det som har skjedd. Det er ingen jakt på syndebukker, og medarbeidere vegrer seg ikke for å rapportere hendelser av frykt for konsekvenser for seg selv eller sine kollegaer. Erfaringsdeling skjer både mellom prosjekt og enheter, og det er lagt til rette slik at det er lett å finne frem erfaringer fra lignende jobber.

Tunnelarbeid kan være risikofylt. Arbeidet må planlegges godt og nødvendige tiltak iverksettes for å unngå ulykker. Her forestår Jan Agnar Trengereid (t.h.) og Arne Langedal tunnelrensking. (Foto: Jarle Hodne)

Beskrivelse av modenhetsnivå

Vi vurderte ulike måter å presentere resultatet av arbeidet på, og landet på at bruk av en modenhetsskala i dette tilfellet la til rette for en konstruktiv dialog om hvordan vi kan oppnå en enda sikrere arbeidspraksis i selskapet. En modenhetsskala ble også benyttet fordi det er vanskelig å gi en sikkerhetskultur en «karakter», samtidig som det vil være grunnlag for å si noe om nivået sammenlignet med beste praksis i bransjen.

Modenhetsmodellen ble benyttet aktivt i kommunikasjonen med revidert enhet. Ledelsen ble oppfordret til selv å vurdere modenhetsnivået på sikkerhetskulturen i selskapet, og det viste seg at denne i stor grad sammenfalt med vår vurdering.

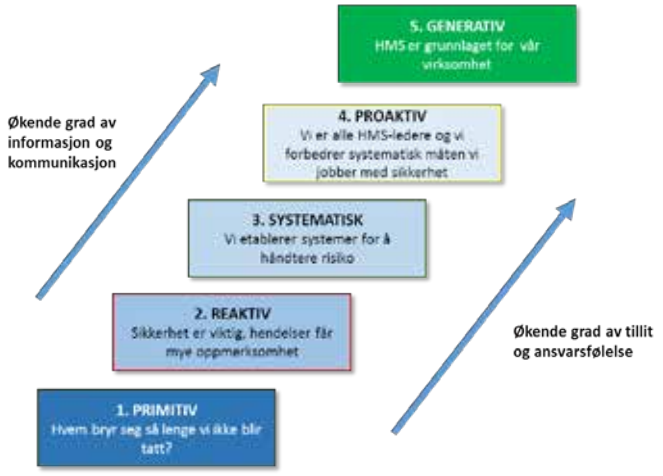
Hva nå?

BKK Produksjon har over flere år arbeidet aktivt med sikkerhetskulturen i selskapet, har HMS-kompetanse og gode rollemodeller. Vi fant en rekke positive trekk ved sikkerhetskulturen i selskapet, men identifiserte også noen forbedringsområder, og det ble avtalt fem tiltak for å oppnå en enda sikrere arbeidspraksis. Sluttrapporten ble godt mottatt, og reviderte enheter er allerede godt i gang med arbeidet med å følge opp tiltakene. Vi legger til grunn at revisjonen har tilført verdi på et svært viktig område – alle skal komme trygt hjem hver dag!

Konsernrevisjonen i BKK har altså etablert en modell for å vurdere sikkerhetskulturen i et selskap, og vi ser ingen grunn til å stoppe der. Arbeidet med å gjennomføre et tilsvarende oppdrag inn mot BKKs entreprenørselskap er allerede godt i gang, og vi har også en ambisjon om å vurdere sikkerhetskulturen i nettselskapet vårt.

Å evaluere en sikkerhetskultur er ikke bare relevant når det gjelder personsikkerhet. Vi leker med tanken om å overføre konseptet til et annet høyaktuelt område, nemlig IKT-området. Også der er det et samspill mellom formelle og uformelle rammebetingelser, og også der står den menneskelige dimensjonen helt sentralt for å kunne oppnå et godt resultat. Stadig flere angrep er rettet mot medarbeidere, for eksempel i form av phishing. Årvåkne medarbeidere med gode grunnholdninger og fokus på informasjonssikkerhet blir stadig viktigere. Dette tilsier at det kan være hensiktsmessig med en gjennomgang av sikkerhetskulturen også på IKT-området.

Figur 2: BKKs modenhetsmodell for sikkerhetskultur – avledet av Hudsons kulturelle stige (2007)



Deloitte.

I takt med tiden

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

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

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

Tredjepartsrapportering – ISAE 3402, SOC1, SOC2 og andre forkortelser

AV
KEVIN F. MCCLOSKEY,
CISA, CIA, CRMA

Kevin har 27 års erfaring med å jobbe med Service Organization Control Reporting, IT-revisjon, internrevisjon, risikostyring og IT-basert internkontroll fra hans tid i Deloitte New York og Oslo.

Outsourcing- en økende trend

Virksomheter er i stadig større grad avhengig av tredjeparter for å levere forretningskritiske tjenester. Det kan gjelde tjenester innen blant annet informasjonsteknologi, finans og regnskap, lønnsprosessering, kundeservice, HR og fondsadministrering- og forvaltning. Outsourcing har gått fra å være et verdibeskyttende tiltak til å bli et verdiskapende tiltak.

Hva er det som driver dette? Enkelt sagt må selskapene akseptere at outsourcing noen ganger er nødvendig for å være konkurransedyktig på global basis, for å vokse i markedet eller for å redusere kostnader og øke kvaliteten. Noen av driverne for outsourcing er:

- Begrenset kapasitet på ledelsesnivå
- Kostnadsoptimalisering
- Informasjonsteknologi
- Ønske om å fokusere på kjernevirksomhet
- Mangel på arbeidskraft eller spisskompetanse
- Ekspertleverandører som leverer høykvalitetstjenester

Illustrasjon: Deloitte

Den økende bruken av outsourcing i dagens marked har gjort selskapene mer avhengig av et komplekst nettverk av tredjepartsleverandører. Fra et risikoperspektiv er det viktig at selskapene selv har oversikt over de risikoene som påvirker dem og forvalter og overvåker disse på en tilfredsstillende måte. Du kan outsource funksjonen, men du kan ikke outsource risikoen og kontrollaspektet.

Hvordan vet virksomheten at outsourcingspartneren har tilfredsstillende internkontroll?

For å sikre at virksomheten har tilfredsstillende internkontroll er det viktig å få innsikt i internkontrollen hos outsourcingspartneren siden de utfører deler av arbeidsprosessene. Som en konsekvens av dette, etterspør ofte virksomheten (og deres finansielle revisor) en bekreftelse på outsourcingspartnerens internkontroll, også kalt tredjepartsrapportering.

Illustrasjon: Deloitte

Tredjepartsrapportering er blitt stadig mer utbredt i markedet siden utstedelse av revisjonserklæring nr. 70 for tjenesteytere (kalt SAS 70) kom i 1992. Som en del av AICPAs (American Institute of Certified Public Accountants) utvikling av Statement of Standards for Attestation Engagements (SSAE) 16, har AICPA etablert Service Organization Control (SOC) rapport rammeverket SOC 1, SOC 2 og SOC 3 som en erstatning for SAS 70 i 2011. Internasjonalt har IAASB (International Auditing and Assurance Standards Board) utgitt en standard, kalt ISAE 3402, og i Norge har Revisorforeningen oversatt standarden til norsk.

De forskjellige rapporttypene har forskjellige formål og bruksområder. For å gi mottaker en bekreftelse på internkontroll relatert til prosessering av finansiell informasjon benyttes SOC1 (SSAE16) eller ISAE 3402 standardene. For å gi mottaker en bekreftelse på internkontroll relatert til ikke-finansiell informasjon benyttes ISAE 3000, SOC 2 og SOC 3-standardene.

Hva er forskjell på ISAE 3402 og SOC1?

Selv om ISAE 3402- og SOC1-standardene er utviklet for det samme formålet, er det noen forskjeller som man bør være oppmerksom på når man vurderer de opp mot hverandre. Noen av forskjellene er:

- SSAE 16 krever at revisor rapporterer etterfølgende betydelige hendelser etter rapporteringsdato, men før avleggelse av rapporten. En etterfølgende betydelig hendelse vil være noe som kan endre ledelsens vurdering etter at revisjonen er avsluttet. ISAE 3402 begrenser typene av påfølgende hendelser som vil bli rapportert i revisjonsrapporten.
- SSAE 16 fastslår at ledelsen anerkjenner og aksepterer ansvaret for å gi revisoren skriftlige representasjoner ved inngåelsen av kontrakt for oppdraget. ISAE 3402 krever ikke denne bekreftelsen.
- SSAE 16 krever at revisor undersøker eventuelle feil som kan være forårsaket av en forsettlig handling av serviceorganisasjonens personell. Standarden krever også at revisor mottar en skriftlig uttalelse fra administrasjonen til serviceorganisasjonen som beskriver eventuelle faktiske, mistenkte eller påståtte forsettlige handlinger som kan påvirke ledelsens beskrivelse av systemet. Selv om begge standarder krever undersøkelse av eventuelle identifiserte avvik, krever ISAE 3402 ikke eksplisitt at revisor får en skriftlig uttalelse.
- ISAE 3402 tillater revisor å konkludere med at et avvik som identifiseres ved testing av kontrollen, kan betraktes som en operativ anomali. En operativ anomali er noe som avviker fra standarden. Dette skyldes at når et utvalg av kontrollene blir testet, er ikke resultatet nødvendigvis representativt for hele populasjonen basert på de utførte stikkprøvene. SSAE 16 krever lik behandling av alle avvik på samme måte, snarere enn å betrakte dem som en anomali.
- SSAE 16 krever at revisjonsrapporten inneholder en erklæring som begrenser bruken av rapporten til ledelsen av serviceorganisasjonen, til kundenes virksomheter og til kundenes revisorer. ISAE 3402 krever at revisjonsrapporten inneholder en uttalelse som indikerer at rapporten er beregnet for serviceorganisasjonen, kundenes virksomheter og kundenes revisorer, men krever ingen uttalelse som begrenser bruken av denne til disse.
- ISAE 3402 krever at revisor samler den aktuelle dokumentasjonen i en engasjementsfil og fullfører sammenstillingen etter at revisjonsrapporten er fullført. SSAE 16 krever også dette tiltaket, men har en 60-dagers tidsfrist etter revisjonsrapportens utgivelsesdato.
- SSAE 16 inneholder visse krav som ikke gjelder for ISAE 3402. Kravene er blant annet:
  - En henvisning til ledelsens vurdering, og en erklæring om at ledelsen er ansvarlig for å identifisere de risikoene som kan forhindre oppnåelsen av kontrollmålene.
  - En erklæring om at undersøkelsen inkluderte vurdering av risikoen for at ledelsens beskrivelse av selskapets organisasjonssystem ikke er riktig presentert, og at kontrollene ikke er hensiktsmessig utformet eller fungerer effektivt for å oppnå kontrollmålene.
  - En erklæring om at et oppdrag av denne typen også inkluderer en evaluering av ledelsens overordnede beskrivelse av selskapets organisasjonssystem og kontrollmålenes egnethet slik de er angitt i beskrivelsen

Illustrasjon: Deloitte

SOC1 og ISAE 3402 vs. SOC2

Som nevnt ovenfor har en SOC 2-rapport fokus på virksomhetens ikke-finansielle kontroller som vedrører sikkerhet, tilgjengelighet, behandlingsintegritet, konfidensialitet og personvern for et system, i motsetning til SOC 1 / SSAE 16 eller ISAE 3402 som fokuserer på de finansielle kontrollene.

Rapporteringsalternativer

Selv om både SSAE 16 og ISAE 3402 er utformet for å oppnå de samme målene med hensyn til rapportering av etablerte, effektivt utformede kontroller for finansiell rapportering, må enkelte tjenesteorganisasjoner rapportere til sine klienter (brukerenheter) etter begge standarder. For de organisasjonene det gjelder tillater den amerikanske standarden at SSAE 16-rapportering kan utføres i samsvar med ISAE 3402-standardene, ofte referert til som en 'kombinert rapport'.

Fordeler med tredjepartsrapportering

Ved å engasjere en uavhengig tredjepart til å foreta en evaluering, blir serviceorganisasjonen kun gjenstand for én revisjon, i motsetning til å måtte gjennomgå mange revisjoner på vegne av flere outsourcingskunder.

Når evalueringen er ferdigstilt distribueres rapporten til virksomhetens kunder, slik at deres revisorer kan bygge på rapporten. Eventuelle funn begrenses eller elimineres med ytterligere revisjonshandlinger. Dette kan bidra til å redusere belastningen på serviceorganisasjonens ressurser og redusere driftskostnader for deres kunder, da kundene ikke lenger trenger å sende revisorer for å revidere serviceorganisasjonens virksomhet.

Blant annet vil rapportene:

- Styrke virksomhetens omdømme
- Bistå med å oppfylle kundenes og deres uavhengige revisorers ansvar
- Dokumentere at kontroller er utarbeidet og implementert i tråd med anerkjente rammeverk for internkontroll (f.eks. COSO, Cobit)
- Sørge for en uavhengig evaluering av kontrollmiljøet basert på en anerkjent standard
- Gi utgiveren en kommersiell fordel ved å skille serviceorganisasjonen fra sine konkurrenter

Illustrasjon: Deloitte

HVORDAN MAN SKAL SCOPE RAPPORTEN

Scoping av en tredjepartsrapport er viktig. Noen av de detaljene man må tenke på når man utvikler en tredjepartsrapport er:

- Hvilke forretningsprosesser bør inkluderes?
- Hvilke enheter er involvert i deling og bruk av systemdata?
- Hvilke enheter er involvert i støtte av systemet?
- Arten og omfanget av bruken av andre tredjepartsleverandører
- Systemdemografi
- Antall ansatte som støtter systemet
- Antall «applikasjoner» inkludert innenfor grensen til «systemet»
- Antall servere og støttet operativsystemplattform
- Antall databaser og støttet database og operativsystemplattform
- Er det noen betydelige endringer i systemet i løpet av de siste 12 månedene eller planlagt for de neste 12 månedene?
- Hvor modent er det interne kontrollmiljøet når det gjelder retningslinjer og prosedyrer?
- Hvor stabilt er det nåværende driftsmiljøet når det gjelder standarder og repeterbare interne kontroller?
- Hva er de primære samsvars- og internkontrollbekymringene til brukerne av systemet?
- Er det andre standarder som brukere vil se demonstrert overholdelse (for eksempel GDPA, ISO, osv.)?
- Hvilken form for rapportering vil tilfredsstille brukerens forventninger?
- Hvilken periode med dekning vil bli forventet? (F.eks. årlig, halvårlig, etc.)
- Når vil brukerne forvente at den første rapporten skal utstedes?

Bruk og misbruk av tredjepartsrapporter

Når man mottar en tredjepartsrapport, enten som bruker av tjenestene som er dekket av rapporten eller som revisor til en klient som bruker en tredjepartsleverandør, må man blant annet være sikker på at:

- Rapportens omfang inkluderer de tjenestene som er brukt av klienten
- Dersom det er en SOC2 rapport, dekker rapporten de Service Principles som du forventer eller trenger å få dekket?
- Rapporteringstypen er tilstrekkelig (Type I – Design og implementering, eller Type II – utvidet til å inkludere operasjonell effektivitet for rapportens periode)
- Omfanget av testingen er tilstrekkelig, sånn at du er sikker på at ditt selskap er inkludert i testpopulasjonen
- Funnene i rapporten er relevante for ditt selskap. Hvis ja, er det gjort noe videre arbeid med funnene?

Dersom man ikke er påpasselig med å lese rapporten nøye og bekrefte at den er relevant for ditt formål, risikerer man å få en 'falsk trygghet' ved å ha mottatt en rapport som egentlig ikke gir deg grunnlag for sikkerheten du trenger. Det er lett å motta en sånn rapport og tro at den løser 'ditt problem' men det er viktig at man kan bekrefte at 'problemet' faktisk er løst. Det kan hende at du må ta et møte eller sende noen spørsmål til selskapet som har gitt ut rapporten for å få en bedre forklaring. Noen ganger kan du til og med påvirke innholdet i fremtidige rapporter.

Utgivelsen av rapporten og fordeler med kompenserende tiltak og følgebrev

Det er flere måter å overlevere en tredjepartsrapport til sluttbrukerne. Den kan sendes over som fil eller papirrapport med en forklarende tekst, det kan holdes et fellesmøte med sluttbrukerne (og revisorene deres) for å diskutere sluttrapporten, eller det kan holdes individuelle møter med sluttbrukerne. Hvis rapporten inneholder funn er det ofte fordelaktig for mottakeren at utgiveren og deres revisor har laget et følgebrev. Følgebrevet forklarer tiltak eller kompenserende revisjonsaktiviteter som har blitt utført for å redusere risiko relatert til funnene og hvordan gjentakelse av funnene skal unngås i framtiden.

Mottakere med avvikende regnskapsår

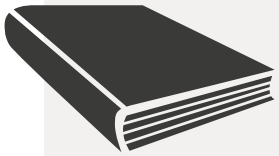
Et problem som skal behandles av utstederen av tredjepartsrapporter, er at kundene kan ha avvikende regnskapsperioder. De fleste kunder vil ha regnskapsperiode frem til 31. desember, men andre kan ha avvikende regnskapsperiode med slutt 31. mai eller en annen dato. Dersom hovedrapportens avvik ikke er for stort, er dette vanligvis ikke noe problem opp til 3 måneder. Et 'bridge letter' utstedt av serviceorganisasjonen kan bekrefte at kontrollbeskrivelsene i rapporten fortsatt er relevante for disse kundene. Dersom avviket fra dekningsperioden er for langt for et 'bridge letter', kan kunden ha sin egen rapport som dekker deres regnskapsår. Et annet alternativ er å vurdere om det er et betydelig antall klienter som krever en rapport rundt en bestemt mellomårstid. Da kan en versjon av rapporten utstedes ved foreløpig testing.

Utvikling framover

Fra 1. mai 2017 vil standardene som er basert på Statements on Standards for Attestation Engagements 16 (SSAE16), som er SOC1, bli erstattet med SSAE 18. SSAE 18 vil ha mer fokus på underleverandører som leverer tjenester til tredjeparten og på andre områder.

Blant annet vil SSAE18 fokusere på følgende:

- Understreke at serviceorganisasjonens beskrivelse av systemet og omfanget av tjenester bør omfatte kontroller utført av ledelsen for å overvåke effektiviteten av kontrollene på underleverandørene sine.
- Introdusere begrepet Complementary Subservice Organization Controls (CSOCs) som representerer kontroller som ledelsen av serviceorganisasjonen forventer vil bli implementert av underleverandørene og er nødvendig for å oppnå kontrollmålene som er angitt i ledelsens beskrivelse av systemet.
- Klargjøre at 'complementary user entity control considerations' bør være begrenset til å omfatte de kontroller og prosedyrer som er relevante for å oppnå kontrollmålene i serviceorganisasjonens rapport.
- Kreve at revisoren vurderer om informasjonen som er overlevert av service organisasjonen er «tilstrekkelig pålitelig» for revisors formål.
- Legge vekt på at revisor vurderer risiko og sannsynlige kilder til feilinformasjon, inkludert det som er relatert til svindel ved planlegging eller i løpet av revisjonen.

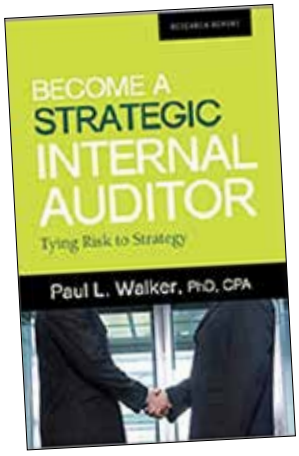


Av
ESA LEPORANTA
Systems Audit Manager,
Nets Norway Branch

Research Report / Book Review

BECOME A STRATEGIC INTERNAL AUDITOR – TYING RISK TO STRATEGY

By Paul L. Walker



In Become a Strategic Internal Auditor, you can learn how leading internal audit functions work with management to play a role in strategic initiatives.

Walker introduces his book by stating that uncertainty is the biggest risk facing the US economy and internal auditors can be a part of the solution for mitigation of this uncertainty by delivering more value-added services to companies. Additionally, he refers to the IIA study[1], which shows that most internal auditors believe strategic business risks are a top priority for both audit committees and executives. Despite acknowledging this fact only 4% of those same auditors say that strategic risks are included in the areas covered by their annual audit.

To demonstrate that there are no explicit limits to what internal audit can do when getting involved in strategy, Walker refers to several Standards and Practice Advisories from the IIA.

For auditors to be «in the same place» as management and the board; the place that adds the most value; Walker has constructed a two-dimensional model with six levels. In the next four chapters, he presents four detailed field research studies to illustrate how auditors, based on their skills, can alter the areas they get involved in and ultimately become Strategic Internal Auditors.

The case studies represent big, well-known multinationals from four different industries. The case studies provide enough practical information to understand how the interviewed CAEs have drawn on their creativity to adapt to their local strategic and risk mindset in order to build a strategy-centered, business-focused, and risk-based audit approach.

In the last chapter, Walker summarizes key lessons from his study. One of the key takeaways is that CAEs should manage the gap between what those at the top think the internal auditors know and what the internal auditors actually know. Another theme that clearly comes through is to engage the business by volunteering for nontraditional audit assignments helping businesses analyze their problems. It is about building relationships and respect, and thus building the internal audit brand. In situations, where the organization does not formally articulate its strategy or its approach to risks, a strategic mindset can still pay off. It is when we have the ability to understand the business and talk about the risks in the business, that's when internal auditors really are respected and valued.

Becoming a Strategic Internal Auditor is a good introduction to how internal auditors can help their organizations both manage their risks and achieve their strategic goals. It analyzes four different cases, which show some of the challenges these organizations initially struggled with. In general, the case studies are the most valuable part of the book reminding us that there is no single correct way to become a Strategic Internal Auditor. It is also a clear advantage that the book can been read at one sitting, making it an easy way to improve your skills and understanding in this strategic area.

1 Defining Our Role in A Changing Landscape; https://na.theiia.org/about-ia/PublicDocuments/2013%20October%20NA%20Pulse%20of%20the%20Profession%20Report.pdf

Tjenesteleverandørers økende behov for attestering

Global konkurranse og globalt kostnadspress har ført til at bedrifter setter ut stadig flere funksjoner til spesialiserte tjenesteleverandører. Dette gjelder også tjenester som ikke er knyttet til kjernevirksomheten. Med dette øker også risikoen.

Av
GUNNAR SOTNAKK
Statsautorisert revisor og Partner KPMG
OG
SANNA SUVANTO
Direktør i Information
Risk Management KPMG

I serviceavtalen er det ofte avtalt at kjøper av tjenestene har anledning til å gjennomføre slike kontroller, men i mange tilfeller blir denne muligheten ikke benyttet.

Økt global konkurranse

Outsourcing er ikke lenger begrenset til rutinemessig kontorstøtte. Det kan være igangsetting, registrering, behandling og rapportering av ulike transaksjoner, noe som kan påvirke organisasjonens regnskaper og sentrale forretningsprosesser direkte. Til syvende og sist er virksomheten selv ansvarlig for sitt eget kontrollmiljø, og dette fører til større etterspørsel etter attestering av kontroller for aktiviteter som utføres av nettopp tredjeparter. Når selskapet selv er ansvarlig for sitt kontrollmiljø, kan det være ønskelig med en sikkerhet for at den delen som er outsourset, også holder den standarden som er ønskelig. I serviceavtalen er det ofte avtalt at kjøper av tjenestene har anledning til å gjennomføre slike kontroller, men i mange tilfeller blir denne muligheten ikke benyttet.

Nye trusler

Outsourcing av en virksomhets informasjon fører til høyere risiko og nye sikkerhetstrusler. Virksomheten kan selv risikere at driften, renommeet og økonomien blir rammet, hvis det oppdages manglende sikkerhet hos eksterne tjenesteleverandører, som igjen fører til brudd på kundenes informasjonssikkerhet. Virksomhetenes risiko øker når eksterne tjenesteleverandører behandler og lagrer kundenes private og/eller konfidensielle informasjon eller utfører transaksjonsbehandling for flere kunder. I de fleste tilfellene er risikoen ved å bruke outsourcing akseptabel, men det finnes nok av eksempler på at outsourcingen ikke har vært noen suksess og at selskapet har måttet ta tilbake de tjenestene som var outsourcet.

Selskaper registrerer mye informasjon om personer og denne informasjonen overlates til andre ved outsourcing, for eksempel dersom lønnstjenester blir outsourcet. Forbrukere selv blir mer og mer opptatt av dette, og ønsker at virksomheter kan klargjøre hvordan deres opplysninger blir brukt. En ny global undersøkelse fra KPMG viser at 75 prosent av de spurte er ukomfortable med at egne opplysninger «blir solgt» til tredjeparter, og mindre enn 10 % sier de har kontroll på hvordan deres opplysninger blir brukt.

En uavhengig gjennomgang av outsourcede kritiske ITfunksjoner og forretningsmessige funksjoner kan hjelpe bedriftene med å identifisere og kontrollere disse risikoene.

Myndighetskrav

Stadig strengere myndighetskrav (f.eks. amerikanske SarbanesOxleyAct) tvinger organisasjoner til å fremskaffe dokumentasjon på at kontrollene deres er effektive. I likhet med håndtering av økt global konkurranse, forutsettes det at virksomhetene har på plass dokumentasjon på at outsourcede ITsystemer og prosesser har de rette kontrollene.

Tjenester på markedet

Det finnes en rekke attesteringstjenester som hjelper organisasjoner med å overholde tredjeparters krav om uavhengige undersøkelser av prosessene, ITmiljøene

og systemene deres og KPMG er blant dem som kan levere disse.

De vanligste attesteringstjenestene omfatter SOC (Service Organization Control) 1 og 2rapporter, som utarbeides i samsvar med henholdsvis ISAE 3402 og ISAE 3000standarden. En slik attestasjon er en bredt anerkjent dokumentasjon på at en tjenesteleverandør har vært gjennom en uavhengig og grundig granskning av sine interne kontroller.

GRUNNLAGET

Grunnlaget for en slik attestasjon er at serviceorganisasjonen har utarbeidet en beskrivelse av sitt system, herunder hvilke kontroller de har etablert og hva som er målene med kontrollene.

Systembeskrivelsen skal gi en dekkende fremstilling slik den er utformet og implementert i perioden under kontroll. Revisor tar utgangspunkt i denne beskrivelsen og gjør handlinger for å få betryggende sikkerhet for at dette er tilfellet. Videre skal revisor også oppnå en betryggende sikkerhet for at kontrollene relatert til kontrollmålene var hensiktsmessig beskrevet for den samme perioden. Basert på sine handlinger avgir revisor en uttalelse i henhold til ISAE 3402 (SOC 1-rapport).

En ISAE 3402-rapport skal være til hjelp for tjenesteleverandørenes kunder og deres revisorer ved regnskapsrevisjon, og dekker tjenester som sannsynligvis er relevante for brukerorganisasjonenes interne kontroll over regnskapsrapportering (ICOFR). Siden ISAE 3402-rapporter ikke er ment å omfatte kontroller som ikke er knyttet til regnskapsrapportering, ble ISAE 3000-rapportering (eller SOC2) utviklet som et alternativ for å hjelpe tjenesteleverandører med å dekke et bredere spekter av spesifikke behov blant brukerne – som å håndtere bekymringer i forbindelse med personvern, konfidensialitet og tilgjengelighet.

Tester som en revisor utfører i en ISAE 3402 revisjon, er svært lik tester av kontroller som en revisor gjør i den finansielle revisjonen. Revisorer bruker ofte å kartlegge prosesser og handlinger og skaffe revisjonsbevis for at en beskrivelse stemmer med de faktiske forholdene, samt at kontroller er implementert. Her bruker revisor revisjonshandlinger som blant annet forespørsler, inspeksjon av dokumentasjon og observasjon. Den store forskjellen sammenlignet med en ISAE 3402-rapport, er at revisor som er engasjert av serviceorganisasjonen kan gjøre testing på vegne av andre revisorer. De revisorene som reviderer selskapene som benytter serviceorganisasjonen kan bygge på rapporten og dermed redusere omfanget av egen testing. Brukere av rapporten kan også være kundene til serviceorganisasjonen, da disse kundene ønsker en rapportering for å sikre seg at tjenestene som leveres er underlagt tilfredsstillende kontroll, men også andre revisorer som reviderer de kundene som benytter serviceorganisasjonen.

> Systembeskrivelsen skal gi en dekkende fremstilling slik den er utformet og implementert i perioden under kontroll. Revisor tar utgangspunkt i denne beskrivelsen og gjør handlinger for å få betryggende sikkerhet for at dette er tilfellet.

Manglende beskrivelser

I enkelte tilfeller ønsker serviceorganisasjonen å engasjere en revisor til å avgi en uttalelse, men så avdekker revisor at det ikke foreligger verken beskrivelse av systemet eller kontrollene. Det vil da ikke være hensiktsmessig å avgi en slik rapport som åpenbart må påpeke svakhetene. Mange serviceorganisasjoner ønsker derfor i forkant å gjennomføre et prosjekt både for å dokumentere sine systemer, men også for å se på om de kontrollene som faktisk er etablerte, er hensiktsmessige for kontrollmålene. Målet med dette er å sikre seg at revisor vil kunne avgi en attestasjon uten anmerkninger. Eksempelvis kan en serviceorganisasjon bruke 2016 til å få på plass kontroller og den nødvendige dokumentasjonen, slik at revisor kan utarbeide en attestasjon for 2017.

Fordeler med SOCrapportering

Både tjenesteleverandører og brukerorganisasjoner oppnår betydelige fordeler med SOCrapportering (Service Organization Control). Brukerorganisasjoner får trygghet for de outsourcede sidene av virksomheten sin, mens tjenesteleverandørene oppnår umiddelbare gevinster:

- Det blir færre avbrudd i forretningsdriften, ettersom det ikke lenger er nødvendig at en rekke brukerorganisasjoner utfører revisjoner
- Det interne kontrollmiljøet styrkes og blir mer finmasket som et resultat av uavhengige undersøkelser i forbindelse med attestering
- Revisjons og kontrollaktiviteter blir mer effektive ved å kombinere leverandører av attesterings og revisjonstjenester
- Et transparent kontrollmiljø skaper tillit i markedet

En slik attestasjon kan benyttes på ulike områder. Det kan være tilfeller der serviceorganisasjonens systemer og kontroller er spesialtilpasset til en kunde og der attestasjonen er tilpasset til disse systemene. Den store majoriteten er likevel relatert til systemer og kontroller som er like for flere brukere. Eksempelvis der serviceorganisasjonen leverer IT-drift, lønnstjenester, regnskapstjenester, varelagertjenester o.l. I disse tilfellene kan revisor lage en felles attestasjon og hver enkelt kunde og kundens revisor slipper å besøke serviceorganisasjonen for en slik gjennomgåelse.

Hvorfor skal internrevisjonen ta i bruk dataanalyse?

Skrevet av:
INGEBORG ORAHAUG
Seniorkonsulent, Uniconsult

PER H. WONGREN
Senior Manager, Risk, EY

CHRISTINE SANDNES
Manager, Risk, EY

Internrevisjonen skal gi objektive og uavhengige bekreftelser og råd til styret og ledelsen om kvaliteten og effektiviteten til organisasjonens prosesser for governance, risikostyring og internkontroll. Dette skal bidra til å forbedre driften i organisasjonen og beskytte dets verdier og omdømme.

En veletablert internrevisjon skal ikke bare evaluere selskapets risiko- og kontrollrammeverk, men bør også bistå organisasjonen med å kvantifisere og vurdere utfordringer knyttet til stadig mer komplekse rammebetingelser, nye forretningsstrategier, teknologiske endringer, nye produkts- og markedssatsninger samt andre strategiske initiativer.

Interessenter legger stadig større vekt på hvordan internrevisjonen kan spille en rolle når det gjelder å vurdere og begrense risikoen i selskapet, samt identifisere og utnytte de muligheter som eksisterer. Det forventes at internrevisjonen i økende grad går fra å være en uavhengig bekreftelsesfunksjon til en sanntidsorientert rådgiver for ledelsen, samtidig som det etterspørres kostnadseffektivisering. Internrevisjonen vil derfor trenge mer effektive ressurser, kompetanse og verktøy for å bidra til at behovene i deres organisasjoner ivaretas. Dataanalyse er en nøkkeldriver og et hjelpemiddel for å imøtekomme organisasjonens fremtidige behov og krav til internrevisjonen, samtidig som det styrker kvaliteten og effektiviteten i gjennomføringen av internrevisjon.

I denne artikkelen tar vi for oss hvorfor dataanalyse vil spille en viktig rolle i fremtidens internrevisjon, hva dataanalyse er, utfordringer og suksessfaktorer ved bruk av dataanalyse, samt hvordan internrevisjonen kan integrere og ta i bruk dataanalyse. Vår tilnærming er forankret i, og bygger på, The Institute of Internal Auditors (IIA) internasjonale standarder for internrevisjon. Artikkelen går ikke i dybden på hvordan ulike dataanalyser kan gjennomføres i praksis, og gir heller ikke en beskrivelse av hvilke ulike analyseverktøy som finnes.

Dataanalyse vil prege fremtiden for selskaper og internrevisjon

«Big Data» er med på å endre måten selskapene driver business på, og internrevisjonen er nødt til å henge med på denne endringen. Vi ser at selskaper utvikler sin tekniske kapasitet for å analysere store mengder informasjon. Innsikten benyttes til å bygge sterkere kundeforhold, nå nye kunder og forbedre bunnlinjen. Internrevisjonen må derfor også omfavne dataanalyse for å holde tritt med selskapets utvikling. Internrevisjonen må videreutvikle sitt arbeid og anvende ny teknologi, i takt med at selskapet og prosesser blir stadig mer digitaliserte. Dette skaper store muligheter, men medfører også større kompleksitet som vil stille nye krav til mer avanserte metoder for å forstå prosesser og transaksjoner.

Dataanalyse må bli en naturlig del av hele internrevisjonens livssyklus; risikovurdering, planlegging, gjennomføring og rapportering. Dette vil ikke bare innebære å ta i bruk nye verktøy og revisjonsteknikker, men også en endring i tenkemåte og tilnærming til problemløsning. Det vil ta tid og kreve investeringer

for å integrere dataanalyse inn i internrevisjonsarbeidet, men resultatene ved å ta i bruk dataanalyse vil gi avkastning. Internrevisjonen vil bringe ny og bedre innsikt som kan hjelpe selskaper til å forbedre sine prosesser og levere bedre produkter og tjenester til kundene.

Reisen med å implementere dataanalyse begynner med en grunnleggende realisering; internrevisjonen må akseptere at de spiller en viktig rolle i å omgjøre data og informasjon til innsikt for styret og ledelsen i selskapet.

Hva dataanalyse er og hvilke fordeler og utfordringer gir det internrevisjonen

Figur: Veien fra data til innsikt, Kilde: EY

Sett fra internrevisjonens ståsted handler dataanalyse om å bearbeide store datamengder for å få innsikt og bedre forretningsforståelse. Kunnskapen som internrevisor tilegner seg brukes også til mer fokusert tilnærming av revisjonen med effektiv og relevant rapportering til styret og ledelsen. Dette kan bidra til å forbedre driften, redusere risikoen og øke verdiskapningen i selskapet.

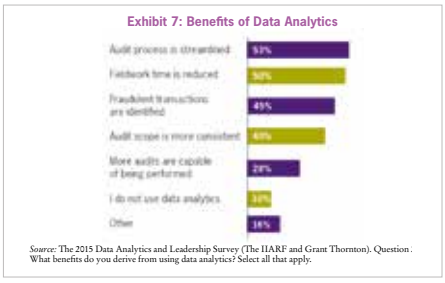
Tradisjonelt har internrevisjonen hatt en hypotesedrevet tilnærming med fokus på hva som kan gå galt, og etter beste evne utført en stikkprøvebasert kontroll. Risikoen med denne tilnærmingen er at stikkprøvene ikke nødvendigvis er representative og at internrevisor dermed kan overse kritisk informasjon, herunder feil/utfordringer og muligheter for forbedring i selskapets styring, prosesser og internkontroll. Ved bruk av dataanalyse kan internrevisjonen undersøke hele populasjonen av data og informasjon. Dette gir internrevisjonen muligheter for å identifisere og fokusere på attributter som tidligere var utenfor rekkevidde, og oppdage mønstre, relasjoner og korrelasjoner som aldri før var synlige. Dette gir et godt grunnlag for å identifisere de reelle problemene gjennom rotårsaksanalyser, og derigjennom presentere innsikt og verdiskapende forbedringstiltak.

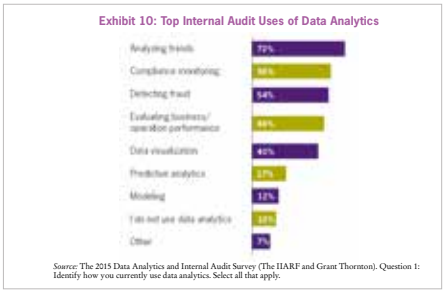
Ved å integrere dataanalyse i revisjonsprosessen kan internrevisjonen oppnå nøyaktige og faktabaserte analyser. Samtidig fører dataanalyse til kostnadsbesparelser siden store deler av revisjonsarbeidet kan utføres i forkant av feltarbeidet, samt at analysene gir god input direkte i revisjonsrapporten. Dataanalyse gjør det også mulig å håndtere et stort transaksjonsvolum og lettere identifisere rotårsakene til observasjoner. På den måten kan internrevisor fremsette kvalifiserte og faktabaserte forbedringstiltak.

Fordelene med dataanalyse kan oppsummeres slik:

- Økt risikodekning da vi kan konkludere på hele populasjonen fremfor et stikkeprøveutvalg som ikke nødvendigvis gir et representativt utvalg.
- Kostnadseffektivitet ved reduksjon av antall revisjonstimer da dataene blir analysert og testet ved hjelp av dataverktøy fremfor manuelt av personell. Det bidrar også på sikt til å redusere tid brukt til utarbeidelse av arbeidsprogrammer, feltarbeid og rapportering.
- Dypere og mer relevant innsyn i selskapets prosesser gjennom å fokusere på nøkkelrisikoene og faktiske problemstillinger som betyr mest for selskapets resultater.
- Økt forståelse av IT-landskapet og -systemer som gir muligheter til å bidra med forbedringsforslag tilknyttet IT.
- Visualisering av preliminære observasjoner som styrker en hypotesetilnærmet revisjon. Internrevisor vil være i stand til å stille de riktige spørsmålene og gjennomføre en bedre rotårsaksanalyse.
- Identifisere og fokusere på attributter som viser mønstre, relasjoner og korrelasjoner som ikke er synlige uten store datamengder og analyser.
- Bidrar til å styrke profesjonell skeptisisme i organisasjonen gjennom mer tilgjengelig informasjon og bedre innsikt i forretningsprosessene.

IIA utførte i samarbeid med Grant Thornton en studie publisert i 2016 rundt bruk av dataanalyse i internrevisjon. To interessante spørsmål som ble stilt var (1) hvilken verdi internrevisjonen mente dataanalyse





ga dem, og (2) hvordan internrevisjonen benyttet dataanalyse i sitt arbeid. Figurene over viser resultatet.

Det er også viktig å nevne at det ikke vil være mulig å bruke datanalyse i alt internrevisjonsarbeid, samt at flere av selskapets prosesser ikke er transaksjonsdrevet og genererer data/informasjon som enkelt kan analyseres. Eksempler på slike oppdrag kan være evaluering av styrets arbeid og evaluering av selskapets strategi- og styringsprosesser.

> Ved å integrere dataanalyse i revisjonsprosessen kan internrevisjonen oppnå nøyaktige og faktabaserte analyser.

Dataanalyse gir internrevisjonen og selskapet en rekke fordeler, men representerer også noen utfordringer. Den første, og mest åpenbare, utfordringen knyttet til dataanalyse er hvordan internrevisor meningsfullt skal bruke all tilgjengelige data for å gi innsikt. Internrevisorene må definere hvilken informasjon de trenger, og hva de planlegger å gjøre med informasjonen. De må forstå forretningsprosessene, risikoene og kontrollmålsettingene for å identifisere de relevante dataene for det aktuelle formålet. Deretter må de sikre tilgang til å eksportere dataen, før risikoeksponeringen i de ulike prosessene presenteres på en hensiktsmessig og pedagogisk måte.

> For å få de riktige svarene, må internrevisor stille de riktige spørsmålene.

For å få de riktige svarene, må internrevisor stille de riktige spørsmålene. Å stille spørsmålene på en riktig måte krever et tydelig definert omfang og et godt samarbeid mellom fagfolkene som skal produsere analysene. Å finne den rette balansen mellom revisjon og dataanalyseferdigheter kan by på utfordringer. Både internrevisorer og analytikere må bringes til bordet. I tillegg er fortløpende kommunikasjon og samspill mellom internrevisjonen og IT kritisk.

Internrevisor må opparbeide en grunnleggende forståelse av sentrale IT-systemer samtidig som de forstår kompleksiteten av spørsmålene de ønsker å besvare. Internrevisor må ikke glemme at analysene har et kostnadsspørsmål. Det tar tid å utvikle robuste og effektive dataanalyser. For å få mest mulig utbytte av analysene må internrevisor kunne gi eksplisitte og klare instruksjoner om hva de ønsker å oppnå. Det er derfor viktig å bygge et sterkt og langsiktig samarbeidsforhold mellom internrevisjonen og IT i organisasjonen.

Det er videre viktig å merke seg at dataanalyser kan ha relativt begrenset bruk og være tidkrevende i oppstarten, da det tar tid å utvikle effektive og målrettede analyser. Utviklingen og forbedringen vil komme etter hvert som internrevisorer og analytiske fagfolk jobber sammen, utvikler datamodeller og bruker dataanalyse i praksis. Det handler om å være tålmodig og akseptere at verden ikke endres over natten.

Når analysene er produsert, har internrevisor et ansvar for å tolke og presentere resultatene. Internrevisor må trekke konklusjoner fra informasjonen og omdanne data til innsikt som kan leveres til styret og ledelsen for bedre beslutningstaking. Dette krever god forståelse av prosessene, risikoene og kontrollmålsettingene innenfor fagområdet som revideres. Analysene fremskaffer bevis og resultater, men internrevisor må forstå hva resultatene betyr, herunder hvordan de kan bidra til å redusere risiko og øke verdiskapningen i selskapet.

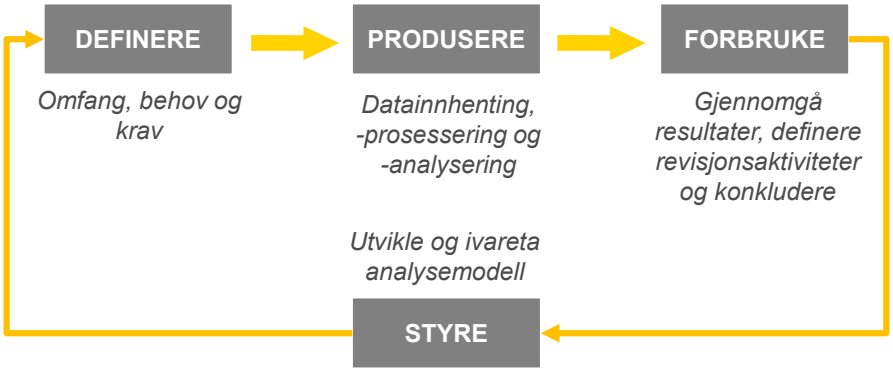
Hvordan internrevisjonen kan integrere og ta i bruk dataanalyse

Implementering og integrering av dataanalyse kan oppfattes som komplisert og omfattende, da databehandling ofte ikke utgjør tradisjonelle aktiviteter i internrevisjonsløpet. Det kreves en viss kunnskap og forståelse for databehandling, og det er viktig ikke å gape over for mye ved oppstart. Vi anbefaler at internrevisjonen starter med dataanalyse innenfor prosesser hvor det er enkelt å fremskaffe data, og opparbeide erfaring med bruk av analyser for deretter å videreutvikle analysemodellen over tid.

For å kunne lykkes med dataanalyser vil vi fremheve følgende suksessfaktorer:

- Kjennskap og kunnskap om selskapets datasystemer og hvordan transaksjoner lagres.
- Tilgang til fullstendig og pålitelig data. Organisasjonen må legge til rette for sporbarhet og datagenerering i sine IT-systemer.
- Tilstrekkelig kompetanse innen databehandling for å kunne anvende den innhentede dataen effektivt og riktig.
- Støtte fra nøkkelinteressenter (eksempelvis IT og ledelsen) i organisasjonen.
- Interaktive analyser gjennom regelmessige møter med internrevisor og IT for å sikre at analytiske fagfolk fokuserer på riktige problemstillinger.
- Tidlig planlegging for å sikre den tiden som trengs for å gjennomføre en dataanalyse. Dette vil ofte kreve endringer i revisjonsplanen og eventuelt forhåndsgodkjenning før dataene kan bli innhentet og behandlet.

Et annet suksesskriterium for å lykkes med dataanalyser er å etablere en dokumentert metode og et rammeverk for dataanalyser. For å implementere dataanalyse bør det først besluttes hvordan internrevisjonen skal arbeide og hvordan dataanalysen skal integreres i revisjonsmetoden. Modellen under viser hvordan arbeidet med dataanalyse kan struktureres i fire steg:



Figur: Modell for arbeid med dataanalyse, Kilde EY

1. **Definere:** I det første steget må revisjonsteamet definere formålet for revisjonsprosjektet med utgangspunkt i omfanget av revisjonen, tidspunktet, teamet og interessentene. Først når revisjonsteamet har fastsatt målsettingene med revisjonen, identifisert vesentlige risikoer og kartlagt hvilke data som skal innhentes, kan dataanalyser tas i bruk for å oppnå disse målene. Her er det kritisk med tydelig definering av informasjonsbehovet, og hvordan informasjonen skal bearbeides når den mottas.

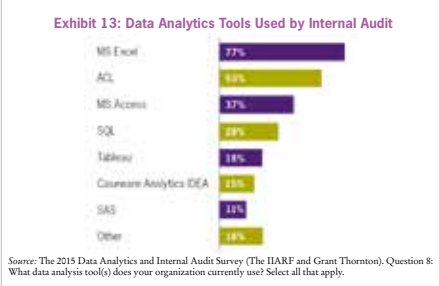
2. **Produsere:** Dette steget innebærer selve produksjonen av analysene. Først må det besluttes hvilke verktøy som skal anvendes for å gjennomføre dataanalysen og visualisere datafunnene. Det finnes ulike verktøy som kan tas i bruk, og valget avhenger av kompleksiteten på analysen og kunnskap om verktøyene. De fleste analysene kan gjøres i MS Excel.
   Deretter gjennomføres dataeksportering og innhenting. All innhentet data bør valideres av prosesseierne før databehandlingen starter. Når det fullstendige og validerte datasettet er tilgjengelig, behandles det av internrevisor og analytiske fagfolk (internrevisor og/eller IT). Utførelsen av dataanalysene er unikt for hvert selskap og krever en viss teknisk kunnskap.

3. **Forbruke:** I det tredje steget konverteres all data til innsikt som er avgjørende for revisjonsrapporten. Gjennom en iterativ prosess med revisjonsteamet utvikles visualiseringer av observasjonene fra dataanalysen. Resultatene av analysen må deretter revideres for å oppnå en dypere forståelse og verifisere foreslåtte hypoteser på en effektiv måte. Analysene kan avdekke et bestemt problem, men oppfølgingsrevisjonen kan avdekke en legitim grunn eller en løsning for analyseresultatet. Det er derfor viktig å verifisere og følge opp analyseresultatene gjennom rotårsaksanalyser før konklusjonen kan utarbeides.
   Revisjonen og oppfølgingen av analysene krever, som tidligere nevnt, god forståelse av prosessene, risikoene og kontrollmålsettingene innenfor fagområdet som revideres. Analysene fremskaffer bevis og resultater, men internrevisor må forstå hva resultatene betyr, herunder hvordan de kan bidra til å redusere risiko og øke verdiskapningen i selskapet. Revisjonsresultatet presenteres i revisjonsrapporten som også bør inkludere analysene for å underbygge konklusjonene og revisjonen.

4. **Styre:** Det siste steget handler om å sørge for at internrevisjonen har de ferdighetene som trengs, at den rette teknologien er på plass, og at de riktige retningslinjene og rollene er definert. Det innebærer styring av kunnskap og ressurser for å sikre at innsikt blir levert til styret og ledelsen i tråd med mandatet. Erfaring er nøkkelen til å lykkes med dataanalyser og integrering av dataanalyse i revisjonsprosessen. Det er derfor viktig å huske at bygging og implementering av en effektiv og robust dataanalyseprosess i internrevisjonen vil ta tid. Det anbefales å begynne i det små og gradvis utvikle en helhetlig dataanalysemodell. Dersom organisasjonen ikke selv besitter nødvendig kompetanse og erfaring kan det være en idé å gjøre strategiske ansettelser av kompetent personell eller innhente bistand fra kompetente tredjeparter.

Verktøy for dataanalyse

Det finnes en rekke verktøy på markedet som kan benyttes til dataanalyse. Noen verktøy som kan nevnes er Tableau, Spotfire, ACL, MS Access, MS Excel, SAS, SQL og IDEA.



Source: The 2015 Data Analytics and Internal Audit Survey (The IIARF and Grant Thornton). Question 8: What data analysis tool(s) does your organization currently use? Select all that apply.

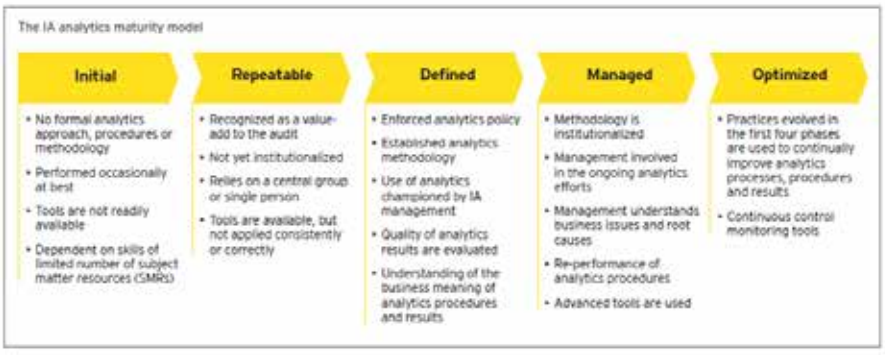
Tidligere nevnte studie rundt bruk av dataanalyse i internrevisjonen, utført av IIA og Grant Thornton, kartla hvilke dataanalyseverktøy internrevisjonen har tatt i bruk. Figuren under viser resultatene.

Studien viser at MS Excel er det mest benyttede analyseverktøyet. Det er ikke overraskende siden MS Excel har en lav brukerterskel og sannsynligvis brukes i stor skala for gjennomføring av revisjoner. Vår anbefaling er å starte med å bruke verktøy som er godt kjent, og heller bruke ressurser på å utvikle en god dataanalyseprosess og -tilnærming. Husk at verktøyet ikke er det viktigste i dataanalyseprosessen, men å definere hvilke resultater som dataanalysen skal gi samt å forstå hvordan analysene skal anvendes for å gi innsikt.

Modenhet på dataanalyse i internrevisjonen

Modenhetsmodellen nedenfor gir en nyttig måte å måle en organisasjons fremgang i bruken av dataanalyse.

Selskaper som ikke har en formell tilnærming og ikke lett tilgjengelige analyseverktøy, er i den grunnleggende fasen. I denne fasen utføres analyser ad-hoc. I neste fase har analysene blitt repeterbare, men ikke formaliserte. Analysene brukes



Figur: Modenhetsmodell for dataanalyse, Kilde EY

ikke konsistent eller korrekt. Selskaper har en tendens til å bevege seg jevnt fra første til andre fase. Den tredje fasen, som kalles definert, har i tillegg en etablert analysemetode, og det er etablert en analysepolicy som etterleves. I den fjerde fasen er datanalysen styrt profesjonelt og brukes aktivt i internrevisjonsarbeidet og av ledelsen i selskapet. Bred kunnskap om datanalyse og bruk av avanserte verktøy står sentralt. Analysemetodikken er institusjonalisert og både internrevisjonen og ledelsen forstår risikoer, utfordringer og rotårsaker i forretningsprosessene. Den siste fasen oppnås når internrevisjonen profesjonelt utfører de foregående fasene, samt driver kontinuerlig forbedring av dataanalyse og har tatt i bruk verktøy for kontinuerlig overvåking i revisjonsprosessene.

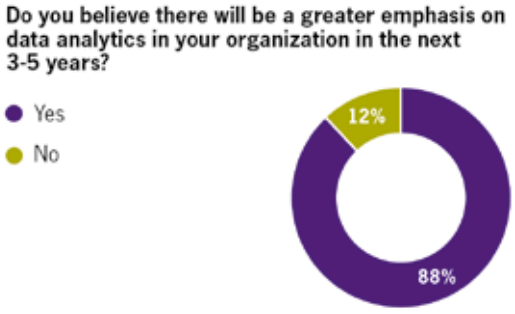
> Dataanalyse er ikke lenger bare «fint å ha», men et «må ha».

Konklusjon: Internrevisjonen må integrere dataanalyse i revisjonsprosessen

Internrevisjonen må integrere dataanalyse i revisjonsprosessen for å holde tritt med selskapets utvikling, men også for å holde tritt med organisasjonens konkurrenter. Dataanalyse er ikke lenger bare «fint å ha», men et «må ha». Internrevisjonen må ha muligheten til å analysere store mengder data generert av organisasjonen for å oppfylle sitt mandat.

Dette underbygges også av studien rundt bruk av dataanalyse i internrevisjonen, utført av IIA og Grant Thornton, hvor hele 88 % av internrevisjonene mener at dataanalyse ville få større fokus de neste 3-5 årene. Figuren under viser resultatene.

Exhibit 19: Future Emphasis on Data Analytics



Source: The 2015 Data Analytics and Internal Audit Survey (The IIARF and Grant Thornton). Question 7: Do you believe there will be a greater emphasis on data analytics in your organization in the next 3-5 years?

Dataanalyse gir internrevisjonen og selskapet fordeler. Hvis riktig utviklet, kan dataanalyse gi forretningsmessig innsikt slik at internrevisjonen kan være en strategisk rådgiver, samtidig som det gir muligheter for kostnadseffektivisering, bedre risikodekning og dypere og mer relevant innsyn i selskapets prosesser.

Hver enkelt internrevisjon må tilpasse strategien og leveransemodellen for dataanalyse slik at den integreres med internrevisjonens visjon, mandat og revisjonsplan. Spørsmålene nedenfor kan hjelpe deg med å finne frem til den beste veien fremover for integrering av dataanalyse:

SPØRSMÅL

1 Hvordan kan du være sikker på at du oppfyller internrevisjonsmandatet på en effektiv måte?
2 Er det en definert styringsmodell og strategi i organisasjonen og i internrevisjonen?
3 I hvilken grad stoler du på informasjon og analyser fra selskapet for å identifisere risiko?
4 Hvilken rolle spiller innovasjon og kontinuerlig forbedring i organisasjonskulturen din?
5 Hvordan oppdaterer du internrevisjonens evner og talent for å holde tritt med utviklingen av data i organisasjonen?
6 Hvordan er dataanalyse integrert i internrevisjonsmetodikken din?
7 Hva er målene og tilhørende fordeler med dataanalyse i internrevisjonen din?
8 Hvilke metoder har du utviklet for å måle fordelene ved bruk av dataanalyse?
9 Hvordan er resultatene av dataanalyse innebygd i revisjonsrapportene?
10 Hvordan klarer du å videreutvikle ferdigheter innen dataanalyse i internrevisjonen?
11 I hvilken grad administrerer du data gjennom revisjonslivssyklusen?

L.I.V.E. THE GLOBAL EXPERIENCE

LEADERSHIP. INNOVATION. VALUE. EFFECTIVENESS.

Join us Down Under in Sydney, Australia for The IIA's International Conference, 23–26 July 2017.

With an innovative program customizable to training needs, this premier event provides an engaging journey, rich with insights for internal auditors at every level.

100+
Speakers From Around the Globe

70+
Sessions in 10 Educational Streams

2,000+
Audit Industry Practitioners and Providers from 100+ Countries

18+
CPE Credit Hours with Pre-conference Sessions

Keynote Speakers:

Jonathan Calvert
Editor, Author, Insight Investigations Team, The Sunday Times

Bend It Like FIFA!

Dee Madigan
Executive Creative Director Campaign Edge

Selling Internal Audit: Is It Really That Hard to Show Our Value?

Register Today!
ic.globaliia.org

THE INSTITUTE OF INTERNAL AUDITORS
INTERNATIONAL CONFERENCE
SYDNEY, AUSTRALIA / 23-26 JULY 2017
SYDNEY2017

2017-0269

Rapid Response

Peter Frost, head of internal audit at Suffolk County Council, is now known as "the man with no plan". He explains how a rolling planning system has transformed the way he and his team identify and prioritise their audits and what winning the Audit & Risk Award for the best public sector team in 2016 means to them.

Article by:
RUTH PRICKETT
Editor of «Audit & Risk" published by IIA UK

Time-consuming research processes, protracted discussions with management and the audit committee and hours wasted putting together an annual audit plan that is out of date almost before it's agreed. Does this sound familiar? Most heads of internal audit will appreciate the frustrations of producing a traditional audit plan, described by Peter Frost, head of internal audit at Suffolk County Council.

Not only was this system becoming increasingly inefficient and unable to keep up with rapid changes to the risks facing the council, but cuts to his budgets and resources meant Frost was finding it ever harder to achieve the number of audits it required. «*For example, if a higher priority unplanned issue arose or there were changes to audit resources, I had to rejig the whole thing,*» he recalls. Not only that, but, during the planning process, he had begun to feel that too often managers were telling him things mainly because they had to think of something to tell the auditors, regardless of their real importance. «*I felt I had a disjointed set of audits on which to base my annual opinion,*» he explains.

This frustration with the planning process, and a crisis of confidence in what it produced, prompted Frost to think again about how he and his team compiled their annual audit plan. Meanwhile, one of the auditors in his team, Christos Constantinou, highlighted an article about the Chartered IIA annual conference, which included the phrase «*auditing at the speed of risk*». The team sat down and discussed their options and what they came up with was radically different.

Frost no longer presents the audit committee with a plan at all. Instead, the audit committee is asked to approve the planning process and Frost merely gives them an overview of the key risks facing the council and potential areas that could get audited at some point in the year, with no guarantees.

«*I'm incredibly lucky that I have an audit committee that really trusts the internal audit team and promotes and supports us internally,*» he says. «*You have to work with the culture of your organisation and Suffolk County Council is generally at the forefront of trying to do things differently, so when we came up with this idea I was encouraged to go away and develop it.*»

The team has incorporated a new risk assessment and planning tool into its existing internal audit software that is used to assess the urgency and importance of new risk areas entered, so the most important can be prioritised without delay.

The changes have not only affected the way the team plans and prioritises audits, they have also affected the way the team works and collaborates at a more fundamental level. Frost has the equivalent of 7.5 full-time team members – about half the number in the team a few years ago. Any of these auditors can identify new risk areas (referred to as «pieces of intelligence») through audit work, discussions with managers, or when they become aware of legislative changes. Furthermore, new risk areas are added to the tool for assessment through Frost's wider corporate role.

Once the intelligence is entered into the system, Frost or his principal auditor will risk assess the intelligence with the member of staff who raised it, meaning that the audit could become the next on the schedule if it's given the highest priority.

Frost explains that the system assesses each new piece of «intelligence» against four criteria: materiality, corporate importance, vulnerability and management concerns. Generally, when auditors become free for the next piece of work, they will be assigned the audit ranked as

the highest priority on the system, although the knowledge, skills and experience of the individual(s) requiring new work is taken into account.

When an audit is allocated, the auditor, after research and discussions with the auditee, will then devise the scope and a programme of work for the audit. This is agreed by the audit manager and, at that time, they also negotiate and agree the number of days it should take. This eliminates the vague guesswork that had previously gone into allocating manhours months in advance.

While this means that auditors no longer know in advance what they will be working on next, each team member knows that they can play a vital part in identifying the next issue to be audited. Consequently, they have developed new analysis skills and the way in which they understand the overall business.

«When I started here in April 2014, I was told I was going to do an audit on waste in January 2015 – but this had first arisen through the annual planning process in November 2013. By the time I did it, I didn't feel it was very useful,» Constantinou says. *«Now this no longer happens. We may have identified a risk very shortly before we audit it, so we know it's important and it's relevant.»*

Since introducing the rolling system, Frost has discussed it with internal auditors at other councils and has been interested by the questions they have asked. *«Some wonder what would happen if all our audits ended up being on one area of the council's work,»* he says. *«I answer that if that happened it would suggest that that area was a particularly high risk so urgently needed attention – although, of course, we would have to assess our priorities here.»*

«I don't have endless resources and it makes sense to look at the highest risks first, but this system also lets me go back to the audit committee if necessary and say 'these things are not being done, because we are focusing on higher risk areas and we can't do both with our current resources',» he adds. So far, both the audit committee and management have been supportive and Frost believes the team has a stronger relationship with senior managers than previously, because everyone can see why an audit needs doing urgently.

«We don't know what the next audit will be – we can see what's at the top of the list now, but it may change. For example, if a situation occurs in adult care, we can swing

into action and do an audit quickly without radically changing any future plans,» Frost explains. *«Early this year we did an audit on a transformational change programme when a risk suddenly emerged. It is unlikely that this would have featured in an annual plan at the start of the year.»*

Some of his peers in other councils have been doubtful that their audit committees would be willing to approve such a vague annual plan, but Frost is quick to allay any impression that he is not playing by the book. *«I've kept the Public Sector Internal Audit Standards (PSIAS) in mind all the way through this process and I've explained to the audit committee how this fits PSIAS requirements and this has been endorsed through an independent external quality assessment against the PSIAS. We also take progress reports to the audit committee throughout the year, have regular liaison meetings with the chair and deputy chair, and summarise everything we've done at the end of the year,»* he explains. *«I'm called the man with no plan, but of course we do have a plan – it's just that it keeps on changing.»*

Giving the team the freedom to focus on high risk audits has also necessitated changes to enable it to work «smarter». This is why Frost's other big innovation was to develop a way of making assurance mapping work at the council across the three lines of defence. He realised that internal audit needed a much clearer understanding of all the main available external sources of assurance and of evaluating their reliability. Making better use of assurance from bodies such as Ofsted and The Care Quality Commission would mean that auditors could focus on those areas that genuinely lacked assurance.

«When assurance frameworks were first mooted, I thought they were a good idea, but the way it was suggested that we should do them wouldn't have worked for us here,» Frost says. *«The concept was good, though, so we worked hard to develop our own assurance mapping framework style. We've picked out eight key areas that we will map, which will enable me to give a more robust annual audit opinion. And there are others carried out that further support the opinion, including corporate governance.»*

The eight key areas are: financial governance; risk management; information governance; performance and data quality; contract management, commissioning and procurement; people management; asset management; and programme and project management. In future, this assurance mapping process will be rolled out to specific services provided by the council – for example, care, transport and waste management.

His team hopes to finish the bulk of this phase of assurance mapping work by the end of the year and this will lay foundations for simpler re-assessments each year. Any gaps they identify in the process sometimes become new pieces of intelligence to enter into the risk assessment system and may generate separate audits.

«Mapping our assurance sources means that we can find out very quickly whether we can get assurance in a given area or whether no such assurance exists. If there is no assurance then it's no point us telling the auditee what they already know, but we can put it on the radar and take the issue to the audit committee,» Frost says.

At a time when resources are tight and risks constantly evolve, innovations that allow stretched teams to do fewer audits with less waste, while producing more meaningful results and a better level of assurance are gold dust. *«A few years ago our team was double the size and I think I can now give a more robust opinion to the audit committee at the end of the year than I could ever do in the past,»* Frost says. *«One good thing about having a small team is that we are a close-knit group and everyone talks to each other, so we all know what is going on.»*

His team's efforts paid off when it won the 2016 Audit & Risk Award for the best public-sector team – while Christos Constantinou was highly commended as the best newcomer. *«We don't know how our work environment will change or who we will be working with in future, but winning the award has given us confidence that we are doing the right thing and clear evidence that others think so too,»* Frost says.

The manager's view

"Audit Services has invested time in looking at the way it operates and how it is perceived within the organisation. This has resulted in the planning and audit practice being developed which ensures the council receives the maximum benefits from the limited resources available.

The flexible planning process means that Audit Services is much more reactive to, and attuned with, the changing environment in which the council operates. It enables greater efficiency and productivity and the resulting audits are now much more meaningful.

The approach to assurance mapping used by Suffolk Audit Services takes into account, and eradicates, the constraint on resources usually spent through the more traditional approach, while promoting a culture of control and risk ownership within the directorates through embedding the three lines of defence model.

As an officer with many areas of responsibility (some of which have been mapped using this approach), I can testify to its usefulness at providing an overview/snapshot of the area, allowing management to understand how we can obtain assurance on the key risks and compliance requirements, and where there are gaps that need attention."

Chris Bally, assistant
chief executive,
Suffolk County Council

NY I INTERNREVISJONEN

Vi ønsker å bli bedre kjent med nye fjes innen internrevisjonen og denne gangen tok vi en prat med Olav T. Hoslemo, som jobber i den maritime gruppen Wilh. Wilhelmsen, ute på Lysaker.

Hva er din bakgrunn?
Jeg er utdannet siviløkonomi fra Universitetet i Agder, som innbefatter en bachelor i revisjon. Jeg begynte som trainee i PwC i 2012, og fikk prøve meg på både consulting og revisjon. Revisjon likte jeg godt og etter hvert tok jeg en Master-grad i revisjon og regnskap ved BI for å bli statsautorisert revisor.

Hvor lenge har du jobbet i internrevisjonen?
Jeg begynte i en 50/50 stilling som controller/internrevisor hos Wilhelmsen den 1. november 2016, så jeg er veldig ny. Jeg er den eneste med «internrevisor» i tittelen, men vi trekker på controllere når vi gjennomfører revisjoner. Det er mao. ikke en rendyrket internrevisjonsfunksjon. Wilhelmsen er til stede i 74 land gjennom ca. 400 kontorer. Vi driver med en rekke internkontroller og bygger ikke opp revisjoner etter IIA standarder.

Hva var det som gjorde at du valgte å gå videre til internrevisjon?
Det var en interessant vei videre, etter å ha jobbet med ekstern revisjon i noen år. Jeg synes det er interessant å komme inn i en stor, internasjonal virksomhet som Wilhelmsen. Stillingen her er veldig variert og det trives jeg med.

Hvilke type revisjoner gjennomfører du?
Primært fokus har vært rettet mot regnskapsrevisjon og substans, samt gjennomgang av selskapenes internkontroll og at de etterlever Wilhelmsens policies. Fokuset er rettet mot det finansielle området og compliance.

Hva opplever du som givende / krevende?
Vi har hatt mye fokus på controlling i den fasen virksomheten er i nå. Wilhelmsen er inne i en stor omstillingsfase. Det å være en sparringspartner er veldig artig. Å bidra til en konstruktiv dialog rundt forbedringer, muligheter og merverdi. Det som kan være krevende er at selskapene kan gå i forsvar når internrevisjonen kommer på besøk.

Er du medlem i IIA?
Nei, men må vel bli det etter hvert.

Hvordan går det med omstillingen i norsk økonomi?

INTERVJU MED
RUNE FOSHAUG
avdelingsdirektør for forskning, innovasjon og digitalisering, NHO

«Nå kommer vinteren», sa sentralbanksjef Øystein Olsen i sin årstale i 2016. Etter en lang opptur med høye oljepriser og høy aktivitet hadde det snudd. Nå kommer en mer krevende årstid fremover og norsk økonomi trenger flere ben å stå på. Det er på tide å omstille seg, var budskapet.

Av
MARIT TRODAL
Prosjektleder IIA Norge

IIA Norge ønsket å ta tempen på omstillingsarbeidet i norske virksomheter og tok en prat med Rune Foshaug, avdelingsdirektør for forskning, innovasjon og digitalisering i NHO.

Hvordan opplever dere i NHO at norske virksomheter jobber med omstilling?
Det er et stort sprik blant norske virksomheter og de som typisk ligger langt fremme er eksportsektoren og næringer der konkurransetrykket er stort. Industrivirksomheter er jo langt fremme på robotisering av produksjonsprosesser. Tjenestesektoren er derimot veldig arbeidsintensiv, og her kan det være mer krevende å gjennomføre omstillinger. Store deler av offentlig sektor leverer jo tjenester, men også her vil endringer fremtvinge seg mer og mer. Ta for eksempel utviklingen av tjenesteroboter til private hjem og velferdsteknologi, som gjør at eldre kan bo lengre hjemme. Når det gjelder risiko ved bruk av ny teknologi, så er alltid effektiv samhandling mellom menneske og teknologi sentralt for å lykkes med omstilling.

Kan du utdype dette risikobildet?
Populært har vi det jeg liker å kalle 'Nike-effekten,' som handler om raskere , sterkere, høyere. Mye innenfor IKT og datateknologi handler om større data- og regnekapasitet. Den andre retningen er kunstig intelligens og deep learning (se faktaboks), som har det tilleggsmomentet at det er selvlærende systemer.

Med 'Nike-effekten' kan man redusere transaksjonskostnader, hvilket vil si at alle mellomledd befinner seg i en utsatt posisjon. Aktører som i dag er tiltrodde tredjeparter vil bli utfordret. Bankene er et eksempel. Blockchain er den «hypen» alle nå snakker om som utfordrer dette. Parallelt ser vi at teknologien har potensialet til å erstatte den kognitive arbeidsinnsatsen. Teknologien kan løfte oss og gi oss en enorm kapasitet, slik Watson-datamaskinen til IBM illustrerer. Men teknologi må implementeres samtidig som arbeidsprosesser endres, for å få en verdiskapende effekt i virksomhetene. Dette er et risikoområde som man må være opp-

OVERSIKT FNS BÆREKRAFTSMÅL

Kilde: http://www.fn.no/Tema/FNs-baerekraftsmaal/Dette-er-FNs-baerekraftsmaal

merksom på. Bruk av teknologi gir gjerne en bunnlinjeeffekt ved å ta ned kostnader, men kan også bidra til å skape topplinjeeffekt ved å skape nye inntektsmodeller. Men det blir gjerne mer fokus på bunnlinjen.

Blockchain gjør at mellomledd er mer og mer utsatt. Men hvem er det som verifiserer hvis vi tenker oss denne teknologien brukt i en leverandørkjede med flere aktører?

Det er jo kun et system, så 'crap in – crap out.' Man må ha tillitsbaserte mekanismer også i slike systemer, for eksempel for å sikre at en diamantleverandør har riktig kvalitet på varene. Forskjellen ligger mer i selve overføringen av verdiene fra en person/gruppe til en annen hvor tilliten er bygd inn i teknologien. Dette vil føre til store endringer fremover.

Er det noen bransjer som utmerker seg som mer innovative i å ta i bruk ny teknologi?

Norge har alltid vært gode på de områdene vi har hatt naturgitte fortrinn på, for eksempel innenfor energi. Leverandørindustrien innenfor olje og gass er et eksempel. Anvendelser der sensorteknologi og analyse av big data brukes vil vokse, blant annet ser vi det innenfor havbruk og fiskeoppdrett, hvor man har utviklet havmerder som er teknologisk veldig avanserte. Velferdsteknologi og helse er også spennende. Vi har en befolkning som raskt tar i bruk ny teknologi, og kombinert med mange gode helseregistre i Norge har vi potensiale for å skape nye næringer her også.

Norge har alltid vært gode på de områdene vi har hatt naturgitte fortrinn på, for eksempel innenfor energi. Leverandørindustrien innenfor olje og gass er et eksempel.

Det ligger også enorme muligheter i å levere på FNs bærekraftsmål (se faktaboks). Verden har behov for gode helsetjenester, ren mat, ren energi osv. Norge er godt posisjonert, men i tillegg til våre naturgitte fortrinn må vi være i teknologifronten. En satsing på de såkalte muliggjørende teknologier som informasjonsteknologi og bioteknologi er sentralt.

Kan du si noe mer spesifikt rundt muliggjørende teknologier?

Vi må skape tjenester og produkter på toppen av de muliggjørende teknologiene. I tillegg til å selge laksen, kan vi også selge teknologien som benyttes i havmerdene. Da har vi skapt en ytterligere topplinjeeffekt. Dette er også noe av essensen i Industri 4.0 (se faktaboks). Når vi automatiserer arbeidsprosesser kan vi produsere billigere her i Norge til tross for høyt lønnsnivå. Industriproduksjon kan hentes hjem til Norge, noe vi ser skjer nå. Dette gir også en tettere kobling mellom design, produksjon, salg og utvikling av teknologi.

Til slutt – hva tenker du er en internrevisors rolle inn i dette bildet?

Internrevisoren må jo kunne analysere data i en virksomhet og bidra til å nyansere forbedrings-potensialet. Det er mange mulige fallgruver og risiko knyttet til teknologi. Den største utfordringen med endring er i grensesnittet menneske og teknologi. Men også informasjonssikkerhet vil være meget sentralt fremover. Jo mer teknologien i og rundt oss, jo viktigere blir IKT-sikkerhet. Vi må endre og kontinuerlig forbedre arbeidsprosesser, og her trenger man ressurspersoner som ser hvordan teknologi bidrar til å styrke disse prosessene.

HVA ER INDUSTRI 4.0?

Begrepet industri 4.0 beskriver den fjerde industrielle revolusjonen, en utvikling der internett smelter sammen med produksjon og produkter. Mange har vel allerede hørt om «the internet of things» hvor f.eks. mobilen kommuniserer med kjøleskapet eller sentralvarmen.

Hvis man overfører dette prinsippet til industriell produksjon, så betyr det at maskiner ikke lenger bare prosesserer produktet, men at produktet selv kommuniserer med maskinene for å gi dem instrukser. På denne måten vil fremtidens maskiner organisere seg selv, leverandørkjeder vil sette seg selv sammen, bestillinger fra kunder vil bli direkte konvertert til fabrikasjonsinstrukser.

Fremtidens fabrikker eller produksjonslokaler vil være så fleksible at hvert enkelt produkt kan skreddersys etter kundenes behov, uten at det koster mer enn storskala produksjon.
Kilde: www.innovasjonsbloggen.com

HVA ER DEEP LEARNING?

Dyp Læring (eng. 'Deep Learning') er en fellesbetegnelse på nyere metoder innen maskinlæring der man tar i bruk nevrale nettverk på nye måter og i flere nivåer enn tidligere. De siste årene har dyp læring oppnådd oppsiktsvekkende resultater innen bl.a. bildegjenkjenning, talegjenkjenning, mm., samt mer generelt på kategorisering av umerkede data.

Kilde: http://www.kodemaker.no/deeplearning/

Etterlevelse av mål og prinsipper for virksomhetsstyring

INTERVJU MED
TORE VEGARD HANSEN-STAVNHEIM
SKATTEDIREKTORATET

Av
MARTIN STEVENS
Gjensidige Forsikring

Martin: Jeg var tilstede på et ledernettverksmøte i slutten av november i fjor hvor du, Tore Vegard, holdt en presentasjon om hvordan dere i Skattedirektoratet har organisert deres arbeid for å sikre etterlevelse av mål og prinsipper for virksomhetsstyring i Skatteetaten. Jeg tenker at deres praktiske tilnærming til virksomhetsstyring fortjener å få en omtale i SIRK. Teori er en ting, men det er den praktiske gjennomføringen som skiller en virksomhet fra en annen.

Men først Tore Vegard litt om din bakgrunn og stilling.

Tore Vegard: Jeg er utdannet siviløkonom fra Handelshøyskolen BI og har hovedfag i sosiologi fra Universitetet i Oslo. Jeg har snart 20 års erfaring med virksomhetsstyring fra statsforvaltningen. I Skattedirektoratet har vi en liten sentral enhet som heter Virksomhetsstaben som er ansvarlig for Skatteetatens virksomhetsstyring og har ansvaret for styring av etatens økonomi.

Martin: Deres virksomhetsstyring tar utgangspunkt i mål- og resultatstyring som hovedprinsipp, men anvender også balansert målstyring. Kan du fortelle om hvilke perspektiver eller fagområder dere har valgt for styring av Skatteetaten?

Tore Vegard: Vi har valgt 7 fagområder - MRS (mål- og resultatstyring), økonomistyring, kompetanse- og ressursstyring, kvalitetsstyring, styring av informasjonssikkerhet, informasjonstyring og HMS.

Martin: Hvordan ble balansert målstyring mottatt i organisasjonen? Opplevde dere motstand?

Tore Vegard: I begynnelsen var vi veldig forsiktige med å bruke begrepet balansert målstyring. Vi gikk skrittvis frem både ved bruk av ord og uttrykk, og ved involvering og aktivisering av styringsmiljøet i etaten i implementeringen. Selve «gjennombruddet» skjedde ved innføringen av et IT-verktøy i målstyringen; organisasjonen ble kjent med alle sentrale begrep i målstyring ved utvikling av styringskort og ved etableringen av en styrt prosess for rapportering og oppfølging. Kompetanseheving og klargjøring av roller knyttet til rapportering på mål har fått en stor plass i utviklingen av styringssystemet. Styringsparametere ble ikke lenger mål i seg selv, men utgjorde snarere et faktabasert grunnlag for å kunne vurdere målene.

> Styringsparametere ble ikke lenger mål i seg selv, men utgjorde snarere et faktabasert grunnlag for å kunne vurdere målene.

Martin: Ofte blir virksomhetsstyring beskrevet som en statisk tilstand i et policydokument, men jeg forstår at hos dere tar virksomhetsstyring utgangspunktet i normative krav og en egen modenhetsmodell som dere bruker for å vurdere etterlevelse av mål og prinsipper for virksomhetsstyring. Hvordan måler dere rent praktisk om etatens metoder for virksomhetsstyring har blitt bedre?

Tore Vegard: Det viktigste er at etaten erkjenner at styringen er noe som kan og bør utvikle seg til det bedre over tid ved bruk av mest mulig objektive og observerbare kriterier. For å realisere dette måtte vi først definere og deretter måle utviklingen. Etterlevelse av prinsippene for virksomhetsstyring vil styrke etatens beslutningsgrunnlag og vår evne til å prioritere mest mulig riktig ved gjennomføring av vårt samfunnsoppdrag. Etterlevelsen av prinsippene handler om eierskap til og modenhet i de prosesser og rutiner som er tilrettelagt. For å kunne se at virksomhetsstyringen etterleves må etaten kunne dokumentere endringer. Skatteetatens modenhet for virksomhetsstyring må derfor måles og rapporteres for å identifisere områder som virksomheten bør forbedre seg på. De utvalgte områdene innenfor virksomhetsstyring har hver sin modenhetsmatrise med kriterier fordelt på fem ulike modenhetsnivå. Dette krever at arbeidet blir tilstrekkelig forankret i aktuelle fagmiljøer for å øke vår treffsikkerhet i valg av kriterier. For strenge kriterier vil kunne bidra til at mange ikke når opp i evalueringen med tilhørende negative motivasjonseffekter. For lite ambisiøse kriterier vil derimot ikke bidra til nødvendig læring for å kunne bli bedre.

Martin: Kan du fortelle oss hvordan dere har definert prinsippene for virksomhetsstyring?

> Etterlevelse av prinsippene for virksomhetsstyring styrker beslutningsgrunnlaget og vår evne til å prioritere mest mulig riktig ved gjennomføring av vårt samfunnsoppdrag.

Tore Vegard: Med utgangspunkt i krav fra Økonomireglementet med tilhørende bestemmelser har vi definert 9 prinsipper for virksomhetsstyring:

1. Overordnet nivå skal fastsette mål og resultatkrav for neste nivå, mens valg av virkemidler i stor grad overlates til neste nivå (intensjonsprinsippet)
2. Det skal være sammenheng mellom mål, prioriteringer og ressursbruk
3. Strategiene skal følges opp gjennom mål- og resultatstyringen
4. Det skal gjennomføres vurdering og håndtering av risiko mot mål som ledelsen har fastsatt
5. Ledere på alle nivå skal legge til rette for å oppfylle virksomhetens etiske ansvar
6. Ledere skal stille tydelige krav til interne og eksterne leveranser
7. Kontroll- og forbedringsaktiviteter skal dokumenteres
8. Styrende dokumenter skal være sporbare og tilgjengelige for alle som har behov for disse
9. Rapportert informasjon skal være basert på riktig registrering til bruk for styring og forbedring

I tillegg skal ledere stille seg følgende kontrollspørsmål:

- Har du god kontroll på egen oppgaveportefølje?
- Har du hånden på rattet med hensyn til oppfyllelse av krav og forventninger gitt i retningslinjer for virksomhetsstyring?

Martin: Kan du forklare hvordan Skatteetaten arbeider med virksomhetsstyring på et overordnet nivå?

Tore Vegard: La meg bruke illustrasjonen i figur 1. Skattedirektoratet har valgt å ha mål- og resultatstyring som hovedprinsipp for etatens virksomhetsstyring. Balansert målstyring er primært en metodikk for å realisere virksomhetsstrategien.

Som du ser i bildet, mener vi i Skattedirektoratet at virksomhetsstyring er en kontinuerlig prosess med logiske delprosesser, der den ene delprosessen delvis parallelt påvirker utviklingen i neste. Skatteetatens omgivelser endrer seg hele tiden. For å håndtere slike skiftende forutsetninger er det viktig å utvikle strategier som sikrer at Skatteetaten leverer på samfunnsoppdraget sitt også i framtiden. Balansert målstyring vil som metode langt på vei sikre at vi operasjonaliserer etatens definerte strategier i strategiske mål, styringsparametere og tiltak. På etatsnivå vil etatens styringskort reflektere virksomhetsstrategien med underliggende områdestrategier for IT, HR, kommunikasjon og anskaffelser.

I neste steg, skal Skatteetatens virksomhetsstrategi understøttes av budsjettprosessen og av kompetanse- og ressursstyringen. Styringskort må avstemmes på underliggende nivå, både i forhold til virksomhetsstrategien og i forhold til avhengigheter mellom enheter på samme nivå.

Ledelsen ønsker at virksomhetsstyringen er en integrert del av etatens styring og ledelse. Etterlevelsen av dette måles gjennom modenhetsevalueringen en gang i året. Modenhetsevalueringer skal bidra til å identifisere tiltak for å forbedre virksomhetsstyringen hvilket igjen skal øke vår organisatoriske læring og gi forbedret kontroll av virksomhetsstyringen.

> Innholdet i årlige resultatavtaler med ledere på ulike nivåer utgjør en sentral del av styringskortet, og er ment å skape forpliktelse rundt viktige mål og resultatkrav i tråd med intensjonsprinsippet.

Innholdet i årlige resultatavtaler med ledere på ulike nivåer utgjør en sentral del av styringskortet, og er ment å skape forpliktelse rundt viktige mål og resultatkrav i tråd med intensjonsprinsippet.

Oppfølging og kontroll skjer gjennom løpende økonomistyring, resultatrapportering og styringsdialog, og gjennom kvalitets- og sikkerhetsstyring som for eksempel stikkprøvekontroller, sikkerhetsvurderinger, helsesjekker av sentrale produksjonsprosesser med avvikshåndtering i kvalitetssystemet, samt ved vurdering av IT-modenhet og ikke minst gjennom revisjoner utført av internrevisjonen.

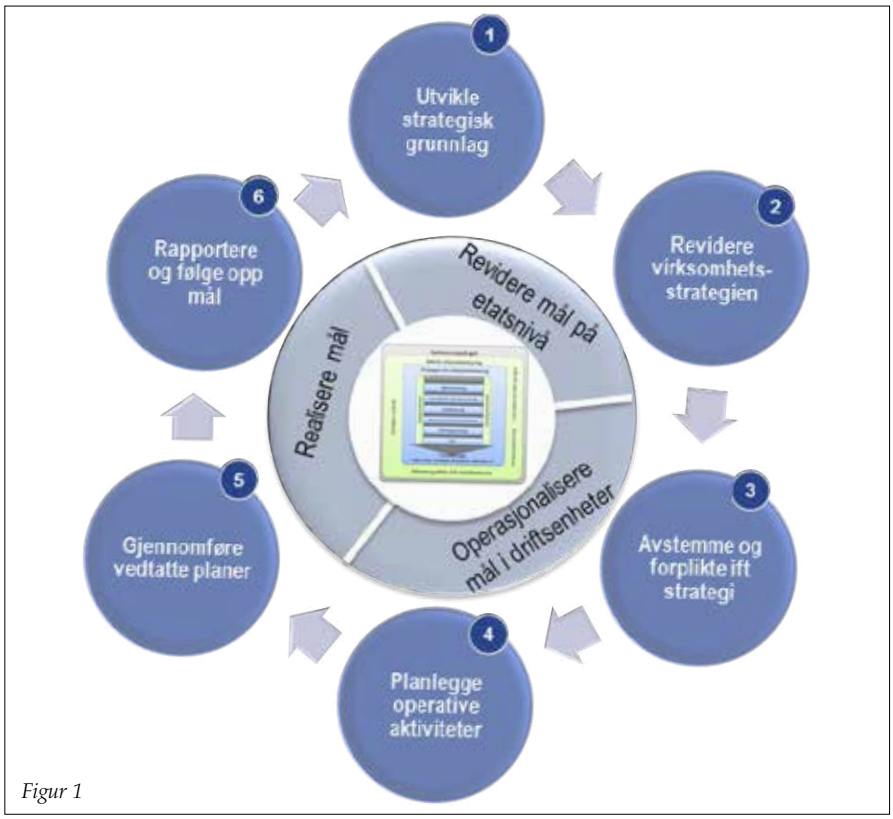
Martin: Hvordan unngår dere at stabsfunksjonene ender opp med å bli ansvarlige for virksomhetsstyringen?

Tore Vegard: Ledere har et selvstendig ansvar for å kvalitetssikre virksomhetsstyringen i sine enheter, samt å følge opp og kontinuerlig forbedre etatens virksomhetsstyring. Videre skal ledere beskrive, styre og kontrollere leveransekvaliteten. De skal legge til rette for håndtering av usikkerhet og risiko, og støtte opp under styring og måloppnåelse for Skatteetaten. Virksomhetsstaben skal fungere som fasilitator, som oppdaterer retningslinjene for virksomhetsstyring sammen med andre fagmiljøer, definerer begrepene og utarbeider hjelpeverktøy for overordnet rapportering som muliggjør sammenligning mellom ulike virksomhetsområder.

> Ledere har et selvstendig ansvar for å kvalitetssikre virksomhetsstyringen i sine enheter, samt å følge opp og kontinuerlig forbedre etatens virksomhetsstyring.

Martin: Tilbakerapportering om status på virksomhetsstyring er basert på egenvurderinger. Hvordan kontrollerer dere riktigheten av rapporteringen?

Tore Vegard: Så lenge det dreier seg om egenevalueringer, vil det alltid være en risiko for vurderingsfeil slik det forsåvidt er i all rapportering i styringssammenheng. Noen ganger kan det være behov for å krisemaksimere og enkelte ganger vil man vise glansbilder. Slik egenevaluering skal imidlertid ikke sees som formelle revisjoner av virksomhetsstyringen, men snarere et hjelpemiddel for kontinuerlig å forbedre virksomhetsstyringen. Målingen av modenhet skal skje ut fra sentralt fastsatte kriterier for å sikre mer likeartet tilnærming i organisasjonen. I tillegg skal sammenstillingen av resultater fra egenevalueringen stresstestes og kalibreres gjennom workshop som fasiliteres av fagpersoner med nødvendig opplæring. Når evalueringen er endelig, vil lokal ledelse ha en faktabasert status på modenhet for de ulike fagområdene, som kan brukes som utgangspunkt for å identifisere forbedringstiltak. De viktigste forbedringstiltakene følges videre opp i kvartalsrapporteringen og i resultatavtaleprosessen.



Figur 1

Martin: Kan du si noe om hvilke refleksjoner dere har gjort ved sammenligning av virksomhetsområder? Er det områder eller kriterier som stikker ut eller som har eventuelt blitt bra håndtert? Bistår Virksomhetsstaben med målrettet innsats på de svakeste områdene?

Tore Vegard: Vi opplever at gjennomgangen av evalueringer lokalt i seg selv gir oppmerksomhet på mulige forbedringsområder og samtidig motiverer mange til å implementere selvstendige forbedringer. I enkelte tilfeller har pilen imidlertid pekt tilbake til øverste ledelsen i direktoratet for nødvendig handling. Ved å adressere dette har Virksomhetsstaben fått god støtte til å gjennomføre initiativ som har forbedret situasjonen betydelig.

Martin: Jeg takker for ditt innspill i hvordan virksomhetsstyring kan gjennomføres og utvikles videre ved bruk av en modenhetsmodell. Jeg har bare et spørsmål til slutt: Hva skal dere gjøre den dagen virksomhetsstyringen fungerer optimalt i alle enheter i hele Skatteetaten?

Tore Vegard: Jeg tror neppe det vil skje i min levetid! Virksomhetsstyring er et område som er i stadig endring, og det vil alltid være behov for å forbedre virksomhetsstyringen for å løfte Skatteetaten videre i sin streben etter å løse samfunnsoppdraget på en best mulig måte.

OP Gruppens nye strategi – Hvem får rett?

Av
ESA LEPORANTA
Systems Audit manager,
Nets Branch Norway

OP Gruppen er Finlands største finansgruppe[1], som ble grunnlagt 1902. Gruppen består av cirka 180 selvstendige andelsbanker samt gruppens sentrale andelslag og deres datterselskaper. Banken, som opererer kun i Finland, ble kåret til verdens 8. sterkeste bank andre år på rad av Bloomberg Markets[2] i 2015. Et slik resultat gjør det interessant å følge med hvilke strategiske valg banken tar fremover.

En finsk forsker, Mikko Riikkinen, som skriver en doktoravhandling om finansteknologi[3], forteller at bankenes strategier i Finland tydelig har gått i hver sin retning i løpet av de to siste årene[4], i motsetning til situasjonen for 10 år siden. OP Gruppen er en av de bankene som har tatt et noe utradisjonelt valg.

Selv om OP Gruppen har mer enn fordoblet resultatet sitt før skatt på siste tiåret, og har også ifølge konkurrentene lykkes bra med sin strategi, er ledelsen i OP Gruppen ikke tilfreds. Bankens ledelse, med generaldirektør Reijo Karhinen i spissen, vurderer at de tradisjonelle banktjenestene kan endre seg mer i løpet av de neste fem årene enn de har endret seg i løpet av de siste 50 årene. For å forberede seg til denne endringen, som har blitt fremskyndet av det reviderte betalingstjenestedirektivet (PSD2), er det skissert at OP Gruppen skal etablere flere nye forretningsområder for å selge nye tjenester innen transport, helse- og velferd, elektronisk handel og sikkerhet. Satsningen innen helse- og velferdssektoren har fått en del publisitet i finsk media, og ifølge planene skal OP Gruppen eie 5 sykehus og 13 helsestasjoner innen 2019, en i hver fylke - unntatt på Åland. Hvis kravet til driftskonsesjon for apotekvirksomhet fjernes, kan distribusjon av medikamenter bli det neste strategiske valget[5].

OP Gruppens nye strategi får støtte av et dansk konsulentselskap, Norfico, som mener at fremtidige aktører i fintechbransjen vil tenke innbetalinger fra kunder som en del av deres samlede forretningsmodell, og vil tjene penger gjennom å forenkle kundens hverdag med andre tjenester enn med betalingstjenester[6].

Dette står i sterk kontrakt til Handelsbankens strategi, som har blitt kjent for å følge sin egen vei[7] i alle år. Ifølge Bloomberg er Handelsbanken faktisk den eneste europeiske banken som var blant verdens 20 sterkeste banker i perioden 2011 – 2015. Handelsbankens ledelse[8] har gitt uttrykk for i det siste at de vil være åpent konservative i sine strategivalg og konsentrere seg om tradisjonelle banktjenester. I motsetning til OP Gruppen, mener ledelsen i Handelsbanken videre at de har råd til å gjøre noen feil. Tiden vil vise om Handelsbankens strategi er god nok –og hvem som får rett.

[1] *Nordens største økonomiske tidskrift, Talouselämä 21/2016, s. 34*
[2] *www.bloomberg.com/news/articles/2015-07-29/hang-seng-repeats-as-world-s-strongest-bank*
[3] *Finansteknologi - Et samlebegrep for ny teknologi innen finansielle tjenester (fintech)*
[4] *http://www.is.fi/taloussanomat/porssiuutiset/art-2000005101933.html*
[5] *Talouselämä 3/2017, s. 46-49.*
[6] *http://finans.borsen.dk/artikel/1/342575/nyt_betalingsregime_fra_eu_truer_banker_-_og_giver_dem_gyldne_muligheder.html?hl=YToxOntpOjA7czo3OiJOb-3JmaWNvIjt9*
[7] *Niels Kroner, A Blueprint for Better Banking, Harriman House Ltd, Hampshire, 2011*
[8] *_http://www.kymensanomat.fi/Online/2017/04/06/Handelsbanken%20pit%C3%A4%C3%A4%20kiinni%20konttoreista%2C%20kun%20muut%20lopettavat%20niit%C3%A4%3A%20%E2%80%9DJos%20olisimme%20ravintola%2C%20tarjoilisimme%20p%C3%B6ytiin%2C%20emmek%C3%A4%20pikaruokaa%E2%80%9D/2017522105285/4*

Korrupsjon i FN – hvordan øvrige organisasjoner kan lære av FNs erfaringer

AV
PERNILLE STORDRANGE,
MANAGER KPMG GRANSKING OG COMPLIANCE

Pernille jobbet tidligere i FNs Investigations Division i New York og gransket blant annet korrupsjonssaken som involverte den tidligere presidenten for Generalforsamlingen i FN.

I oktober 2015 ble den tidligere presidenten for FNs generalforsamling tiltalt i USA for korrupsjon, skatteunndragelse og hvitvasking. Saken skapte stor medieoppmerksomhet og ble gjenstand for grundige granskinger internt i FN. Granskingen avdekket en rekke svakheter i FNs interne kontrollsystem som både FN og andre virksomheter kan lære av.

I tiden før og under hans presidentskap for generalforsamlingens 68. sesjon i 2013/14 mottok John Ashe mer enn 800 000 dollar i bestikkelser fra en kinesisk eiendomsutvikler og hans medhjelpere. Som en motytelse brukte Ashe posisjonen sin til å tilrettelegge for eiendomsutviklerens ønskede utbyggingsprosjekter; blant annet introduserte han et offisielt FN-dokument hvor han promoterte byggingen av et FN-konferansesenter i Macau, Kina, med den korrupsjonstiltalte eiendomsutvikleren som foreslått utbygger.

I forkant av- og i løpet av sitt presidentskap bedro også Ashe 13 medlemsstater for mer enn 2,7 millioner dollar - ved å søke og motta pengestøtte til arrangementer i regi av presidentens kontor. Medlemsstatene overførte imidlertid midlene til Ashes private bankkonto – i god tro om at kontoen var en offisiell FN-konto.

FN initierte granskinger mot en rekke ansatte som var mistenkt for å ha en rolle i korrupsjonen og bedrageriet mot medlemsstatene, og gjennom intervjuer med sentrale personer fikk vi god innsikt i hvordan skandalen kunne skje og hvorfor ingen FN-ansatte forhindret det.

Forklaringsfaktorer - motivasjon, handlingsrom og mulighet til å rasjonalisere uetiske handlinger

Ved å lese tiltalen mot Ashe og vitnesbyrdene til én av de dømte i saken, var det lett å forstå drivkraften til Ashe – grådighet; Ashe skal angivelig ha beriket seg med Rolex-klokker, dyre biler og basketballbane utenfor huset sitt for pengene han mottok. FNs interne gransking avdekket imidlertid at øvrige ansatte var drevet av lojalitet og et ønske om å oppnå politisk kapital i FN-systemet, og dermed strakk seg langt i å være behjelpelig overfor Ashe eller andre høytstående i hans krets, eller valgte å ikke involvere seg når tvilsomme etiske situasjoner oppsto.

Granskingen avdekket videre at det i mangel av preventive kontrollmekanismer oppsto smutthull som Ashe og enkelte av hans medarbeidere kunne utnytte. Én av de ansatte på presidentens kontor hadde god kjennskap til FNs interne forbud mot å motta gaver i embets medfør. Hun var imidlertid også klar over at hun ikke var underlagt FNs regler og retningslinjer, all den tid hun jobbet på konsulentkontrakt med presidenten direkte og således ikke var FN-ansatt, og hadde derfor få kvaler med å motta utilbørlige fordeler fra utenforstående tredjeparter.

Andre ansatte var ikke klar over hvilke interne bestemmelser som regulerer handlingsrommet til FN-ansatte – eller brukte denne forklaringen for å rasjonalisere handlinger som strider imot FNs regler og retningslinjer. Enkelte ansatte hadde ikke gjennomført FNs obligatoriske etikk- og integritetskurs; andre var tildelt oppgaver som innebar økonomisk beslutningstaking uten tilstrekkelig opplæring og kursing i FNs finansielle regelverk og rutiner.

Bakenforliggende årsaker

Avvikene FN-granskingene avdekket skyldtes i all hovedsak to bakenforliggende forhold:

- For det første har presidentens rolle over tid utviklet

seg fra å være symbolsk til å bli mer operasjonell; generalforsamlingen har utvidet presidentens mandat og myndighet som har medført økt risiko for maktmisbruk og misligheter;
- For det andre sitter hver president og hans kabinett i kun ett år, hvilket medfører lav grad av institusjonell hukommelse på presidentens kontor og dermed lav kunnskap om gjeldende regler og retningslinjer.

Disse forholdene kan virke unike for FN, men tilsvarende forhold vil kunne oppstå i eksempelvis selskaper med høy vekst eller høy turnover. Likeledes kan anbefalingene til fremtidige tiltak i FN stå som eksempler til etterfølgelse for andre.

Risikoreduserende tiltak

For å forhindre tilsvarende hendelser som FN erfarte er det viktig å adressere og redusere årsakene til problemet: motivasjonen, handlingsrommet og muligheten til å rasjonalisere uetiske handlinger og misligheter. Dette gjøres ved hjelp av tre kategorier av tiltak: ved å etablere et godt kontrollmiljø, samt innføre preventive-, og avdekkende- tiltak.

Oppskriften på et godt kontrollmiljø inneholder i all hovedsak tre sentrale elementer:

- Nedfelte etiske retningslinjer som regulerer de ansattes handlingsrom
- Tydelig tone fra toppledelsen om hva som er akseptabel og ikke-akseptabel adferd
- Rolle- og ansvarsfordeling som reduserer enkeltansattes myndighet til å ensidig fatte beslutninger på vegne av selskapet.

Dette må suppleres med forebyggende tiltak som reduserer risikoen for illojale ansatte og tredjeparter:
- Robuste ansettelsesrutiner;
- Kartlegging av ansattes potensielle interessekonflikter;
- Grundig evaluering og håndtering av tredjeparter og risikoen for at de kan påføre organisasjonen omdømmeskade;
- Kurs og opplæring.

Til tross for godt kontrollmiljø og preventive tiltak vil utro tjenere som regel finne smutthull for å begå misligheter. Da er det viktig å ha gode mekanismer på plass for å avdekke uønskede hendelser på et tidlig tidspunkt. Dette innebærer:
- Anonyme varslingsordninger;
- Kontrollaktiviteter som internrevisjon og monitoreringsaktiviteter.

Bred implementering

Den interne granskingen i FN viste at mange av de ovennevnte tiltakene allerede var på plass i organisasjonen, men på grunn av FNs størrelse varierer både kultur, etterlevelse og håndheving på tvers av avdelinger og kontorer. Funnene fra granskingen demonstrerte derfor behovet for å sørge for god implementering i alle ledd av organisasjon.

FN har tatt lærdom av korrupsjonen som rammet organisasjonen og har innført flere forsterkede kontrolltiltak i kjølvannet av skandalen. Forhåpentligvis kan også andre organisasjoner og selskaper lære noe av FNs erfaring.

Det var en gang...

SIRK har, som profesjonen internrevisjon, endret seg over tid, og da kan det være interessant og artig å ta en titt i bakspeilet for å se hvor vi har vært. IIA i Norge har en historie som går tilbake til 1951, men det første medlemsblad ble utgitt i 1993. Bladet het Internrevisoren frem til 2011, da det skiftet navn til SIRK.

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

For 20 år siden – Behov for et felles løft

Internrevisjonskonferansen i mai 1997 (det er alltid i mai, ikke sant?) hadde satt temaet «Internrevisors profil og image» på dagsordenen. Med dette som bakteppe utmanet den nyvalgte presidenten i NIRF, Hans Martin Vikdal i sitt «Ord fra Presidenten» oss med dette budskapet.

«Vår evne til å formulere klare budskap fra eget fagområde kommer til kort. Så også vår evne til å kommunisere til omverdenen det formål internrevisjonen har og den verdi internrevisor kan ha i privat næringsliv og offentlig virksomhet. Våre kunder, så vel som omverdenen generelt, synes å ha begrenset kunnskap om internrevisjon og stiller ofte med feil forventninger til, og misoppfatninger om internrevisor.»

Det hadde vært ønskelig å kunne konkludere på at slik var det den gang men ikke nå lenger, men jeg tror ikke vi er der ennå. Det er skjedd mye positivt i de seneste årene med anerkjennelse av internrevisjonens rolle innenfor god virksomhetsstyring både innenfor finansvirksomhet og det offentlige, men allikevel må vi erkjenne at det finnes mange som ikke har fått med seg at det er forskjell mellom intern og ekstern revisjon og mellom internkontroll og internrevisjon. Det er viktig at foreningen jobber på sin side med å markedsføre profesjonen, men ikke minst at vi tar vår del av ansvaret internt i bedriften for, som Vikdal uttrykte det i 1997; *«På samme måte som NIRF har et behov for å kommunisere profesjonens rolle til sentrale målgrupper utenfor bedriftene, må hver enkelt internrevisor gjøre der samme overfor målgrupper innenfor bedriften. Med utgangspunkt i den enkelte bedrifts mål og strategier, må vi kunne vise til og tydeliggjøre hvordan internrevisjonen bidrar til realisering og måloppfyllelse.»*

> «Meget bra foredrag. Det er hyggelig at revisor for en gangs skyld får et overblikk over emnet «før» i stedet for «etterpå».

For 40 år siden – Norsk Bankrevisorforenings landskonferanse

IIA Norge avvikler i disse dager sin årskonferanse for 2017. Av den grunn kan det være passende å ta en titt på programmet til landskonferansen i 1977. Hadde man vært internrevisor i en bank da kunne man ha gledet seg til en konferanse som strakk seg over fire dager og som ble avholdt på Røros og Kongsberg. Det står ikke forklart hvordan den ble avviklet på to steder, men jeg regner med at det ble avholdt på to forskjellige tidspunkter og ikke parallelt eller med felles avmarsj fra Røros til Kongsberg.

Hadde du kunnet skru tilbake klokka 40 år kunne du har gledet deg til følgende program:

1. dag
- Bankdemokratiseringen av underdirektør Per Melsom i Finansdepartementet

2. dag
- Kasseterminaler fra A til Å inklusivt med gruppeoppgaver

3. dag
- Kontantautomater
- Nye forskrifter for revisjon i forretningsbanker
- Hva kan vi som revisorer lære av de senere års misligheter i bank?
- Aktuelle spørsmål om bankgarantier med gruppeoppgaver

4. dag
- Ny lov om aksjeselskaper

Interessant nok gjengis også i bladet en persons anonyme evaluering av konferansen der toppkaraktér gis delt til *«bankgarantier med gruppeoppgaver»* og til *«kontantautomater»* og til den siste medfølger følgende kommentar: *«Meget bra foredrag. Det er hyggelig at revisor for en gangs skyld får et overblikk over emnet «før» i stedet for «etterpå».*

Martin Stevens

ECIIA Conference 21./22.09.2017
from insight to influence

Last Chance to register for ECIIA Conference

The Preliminary Program is available now!

We are pleased to announce that a preliminary program is available now on our Website: **www.eciiabasel2017.eu**

Find out more about what else will be expected in Basel.

We have the honor to welcome two new Keynote Speakers from the Financial Sector and a sweet taste from the Chocolate Industry.

Why to come to Basel? Did you know that Basel offers a lot to explore?
Join one of the numorous Guided Tours in and around Basel:
Tour of the old town
City Hall
St. Alban Tal - Little Venice of Basel
Modern Architecture - Masterpieces in the Centre
Augusta Raurica

Nysgjerrig på hva som rører seg innen

GOVERNANCE, RISIKO OG COMPLIANCE?

Her er noen smakebiter fra agendaen til vårt heldagsseminar den 19. oktober:

- Hva kjennetegner good governance i dag?
- Hvilke faktorer påvirker virksomhetens tilnærming til risiko?
- Schibsted: Hvordan gjøre trusler om til muligheter?
- 'Det kunne ikke skje oss.' Hvordan selvtilfredshet kan være et hinder i arbeid med risikostyring
- Three lines of defence – klart skille eller integrert samarbeid?
- Dong Energy: Supply chain due diligence and the green transformation
- Hva kreves for å lykkes i den digitale økonomien?

med mer...

Påmelding via www.iia.no/aktiviteter

Generalsekretæren informerer

AV ELLEN BRATAAS

OM FORENINGEN – ORGANISERING OG NAVN

Som en forlengelse av styrets revitalisering av foreningens visjon og strategi for neste periode, vurderer vi om det er behov for å gjøre om på selve organisasjonsstrukturen og om vi formelt skal gå under navnet Norges Interne Revisorers Forening eller IIA Norge. Begge deler er prinsippsaker som formelt må besluttes av generalforsamlingen. Det har historisk sett ikke vært mange medlemmer til stede på foreningens generalforsamlinger, selv om vi har forsøkt oss på flere former og tidspunkter. Vi ønsker å høre medlemmenes synspunkter på organisering og navnendring og oppfordrer alle til å engasjere seg i diskusjonen **tirsdag 13. juni fra klokken 16.00 – 17.00.** I etterkant av generalforsamlingen inviterer vi til sommerfest med god mat og drikke på takterrassen i PwC-bygget i Bjørvika.

VI GRATULERER FØLGENDE MEDLEMMER

Diplomert Intern Revisor (Dipl IR)

Christian Andreas Bremnes, DNB Bank ASA
Håvard F. Brændmo, DNB Bank ASA
May Britt Hamnes Grønningen, Oslo kommune
Thérèse S. Hodges, Arbeids- og velferdsdirektoratet
Sissel M. Korshavn, Helse Sør-Øst RHF
Liv Tveiten Lüdemann, Helse Sør-Øst RHF
Sissel Mellgren Mangersnes, Forsvarssjefens Internrevisjon
Tone Opdahl Mo, Helse Midt-Norge RHF
Randi Fløystrand Moland, KPMG AS
Anders Ledsaak Nordlund, Helse Sør-Øst RHF
Sasila Sithamparanathan, Oslo kommune
Arne Solhusløkk, ROM Eiendom AS
Lise Berit Sørum, Riksrevisjonen
Per Henry Wongren, Ernst & Young AS

Certified Internal Auditor (CIA)

Erik Vatn, Statoil ASA

COMPLIANCE

Veileder for Compliancefunksjonen som ble lansert i 2015 er allerede trykket opp i nytt opplag på 1 000 nye eksemplarer. Denne veilederen er også oversatt til engelsk i vår, så spre gjerne det gode budskap videre til engelskspråklige kollegaer og bekjente.

Compliance har også fått sin egen hjemmeside, www.iia.no/compliance og sitt eget kontaktpunkt, post@compliance.no.

AKADEMIA

På tampen av fjoråret inviterte NIRF/IIA Norge seg rundt til et utvalg høgskoler og universiteter med det formål å promotere internrevisjon, risikostyring og compliance som fag på flere studier enn bare de økonomiske. Det er viktig at fremtidens ledere har tilstrekkelig innsikt i risikostyring og internkontroll som en integrert del av ledelsesfaget. Vi har til nå hatt møter med Høyskolen i Oslo og Akershus, Høyskolen i Trondheim og Handelshøyskolen i Bergen. Flere spennende tanker ligger på bordet; alt fra bidrag til formidling av forskning til opprettelse av programmer med formell studiekompetanse. Fortsettelse følger i neste nummer.

KONFERANSER VERDT Å MERKE SEG

IIA Norges årlige konferanse, 29. og 30. mai 2017, Fornebu, Bærum
IIAs International Conference, 23. – 26. juli 2017, Sydney, Australia
ECIIA Conference, 21. og 22. september 2017, Basel, Sveits

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

RISIKOSTYRING

I mars inviterte Nettverk Risikostyring til lansering av *Veileder for Risikostyringsfunksjonen* med hundre spente tilhørere til stede. Veilederen beskriver risikostyringsfunksjonens hensikt, ansvar og oppgaver, samt forutsetninger og suksesskriterier på tvers av bransjer. Prinsippene i veilederen kan også være nyttige for virksomheter som mangler en egen Risk Manager, men som ivaretar lignende arbeidsoppgaver under en annen stillingsbetegnelse. Veilederen er også oversatt til engelsk.

Spørsmål et styre bør stille for å forstå hvordan en virksomhet styrer sine risikoer er et hjelpemiddel for styrer og andre kontrollfunksjoner utarbeidet av Nettverk Risikostyring. Denne korte veiledningen er også oversatt til engelsk.

Nettverk Risikostyring er i promoteringsmodus og er invitert inn til flere fora utenfor foreningen for å presentere veilederen. Alt fra advokater til styremedlemmer har uttrykt interesse for veiledningen.

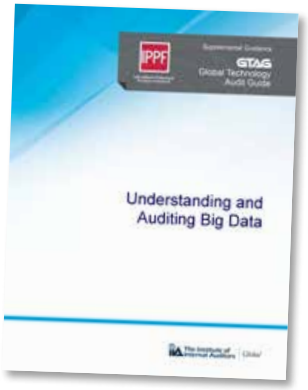
Risikostyring har fått sin egen hjemmeside, www.iia.no/risikostyring hvor oppdatert og relevant informasjon om risikostyring samles. Her finner du en oversikt over publikasjoner, aktiviteter og på sikt også forskjellige verktøy til hjelp i arbeidet med risikostyring. Det er også opprettet en egen mailadresse i tilknytning til risikostyring, post@risikostyring.no.

ANBEFALING TIL EIERSTYRING OG SELSKAPSLEDELSE

NIRF/IIA Norge ble i vår invitert inn på styremøte i NUES. Der redegjorde vi for våre betraktninger rundt internrevisjon i en god governance-struktur og vårt syn på hvordan NIRF/IIA Norge kan bidra inn med sin fagkompetanse på best mulig måte i prosessen med oppdatering av ny anbefaling. I etterkant av møtet har vår Fagkomite for Internrevisjon fått i mandat fra styret å gå igjennom dagens anbefaling og vurdere innspill i forkant av en ny høringsrunde.

The Institute of Internal Auditors | Global

NEW GTAG: UNDERSTANDING AND AUDITING BIG DATA



Big data can provide organization opportunities to innovate and expand their market share by developing new products or making better decisions. Big data enable the consolidation and consumption of large volumes of structured and unstructured data, unique analytics techniques, and the delivery of reports would take days or weeks to prepare without big data.

The participation of internal audit during the planning and implementation of the big data program is important because IA can provide advisory and assurance services to help the organization address risks, and design plans to implement the necessary controls to ensure the success of the big data program. Internal audit also helps by educating the board on the reach and impact of big data, and the importance of executive support to implement and sustain a big data program that supports strategic objectives.

This GTAG provides an overview of big data concepts to help internal auditors identify the different components of a big data program, including strategic objectives, success criteria, governance and operational processes, technology, tools, and other resource; and understand how to align internal audit activities in support of the organization's big data initiatives. In addition, this guidance includes a framework of key risks, challenges, and examples of controls that should be considered when planning big data audits.

Download: https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Understanding-and-Auditing-Big-Data.aspx

IIA GLOBAL SMARTBRIEF

In 2015, The IIA launched IIA Global SmartBrief a monthly e-mail newsletter that summarizes market news and issues affecting internal auditors from leading global news sources. This is a free subscription service available to all members. For subscription, go to:
https://www.smartbrief.com/signupSystem/subscribe.action?pageSequence=1&briefName=iia_global

MODEL INTERNAL AUDIT ACTIVITY CHARTER

This new Supplemental Recommended Guidance is designed to illustrate common practices typically set out in an internal audit activity charter. It has been drafted in a generic manner and may not reflect all legal or regulatory requirements that exist in the reader's jurisdiction. Additionally, stakeholder expectations may influence the inclusion or deletion of certain practices.

The Model Internal Audit Activity Charter acts as a guide to assist with conforming to IIA Standard 1000: Purpose, Authority, and Responsibility and IIA Standard 1010: Recognizing Mandatory Guidance in the Internal Audit Charter. Download the IA Charter: http://iia.no/wp-content/uploads/2017/04/2017-SG-Model-Internal-Audit-Activity-Charter.pdf

Final words

Long before the «Internet of Things» Soviet agents in Moscow got the latest word on sensitive U.S. embassy documents even before U.S. officials had read them. This is what happened!

The Internet of Things (IoT) is expanding rapidly, and may comprise 18 billion connected devices by 2022. Privacy and security concerns are ever increasing as a result of the growing significance of IoT to businesses, government, and critical infrastructure. Likewise, the commoditisation of IoT components leads to significant security challenges and creates the potential vulnerability to new types of attack.

Even if the idea of turning our smart TVs against us sounds scary, Russian spies found as far back as the early 1980's a way to extract information from electronic devices by using magnets. According to a report from the US NSA in 2012, Russian spies developed bugs that were implanted into typewriters and transmitted the information at the same time as it was being typed.

The bugs were initially discovered in 1983 and could be used in nearly any electronic device. This kind of technology required a massive and modern infrastructure serviced by many people, and as a result of this, the NSA initiated its own counterintelligence operation called Project Gunman. The target of this operation was to analyse every piece of equipment inside the US Embassy in Moscow and replace any bugged devices with new ones without alerting the Russians.

After a lengthy and cumbersome project, using x-rays to examine the devices, the analysts finally found an anomaly on the IBM Selectric typewriter's power switch. The implant used magnetometers to recognize which keys were pressed and transmitted that information with the help of radio frequencies to nearby receivers, allowing information to be shared in real-time.

The Gunman project had a major impact on the intelligence community as a whole. When the Gunman story broke in the press, the U.S. State Department was forced to take security more seriously. The Bureau of Diplomatic Security of the U.S. State Department and its Diplomatic Security Service were officially established on 4 November 1985. The importance of the new organization was indicated by its head being made an assistant secretary of state in the US[1].

[1] *https://www.nsa.gov/about/cryptologic-heritage/historical-figures-publications/publications/assets/files/gunman-project/Learning_From_the_Enemy_The_GUNMAN_Project.pdf*

Returadresse
IIA Norge
Postboks 1417 Vika
0115 Oslo

Verdiskapende Internrevisjon

I BDO er vi opptatt av å kombinere internrevisjonserfaring med spesialistkompetanse innen de fagfeltene som preger risikobildet norske virksomheter står overfor i 2017. Gjennom tverrfaglige team bidrar vi til en løsningsorientert internrevisjon, med fokus på det som virkelig betyr noe for virksomheten. Vi gir alltid våre kunder tilgang på spisskompetansen som behøves for å løse nettopp deres problemstillinger. Slik bidrar vi til å skape merverdi og trygge, gode løsninger for deg.

INTERNREVISJON	
Etablering av internrevisjonsfunksjoner	• Risikostyring og internkontroll • IT-risikotjenester • BDO CERT • Personvern • Sikkerhet og beredskap • Compliance og gransking • Økonomistyring • Strategi og utvikling • Transaksjonsrådgivning • Utredning og analyse
Ivaretakelse av internrevisjons-funksjoner (outsourcing)	
Samarbeidsavtaler (co-sourcing)	
Spesialisttjenester og gjennomføring av enkeltprosjekter	
Kvalitetsgjennomganger (Quality Assurance Review)	

KONTAKT OSS

Karl-Ludvig Mauland
Partner - Rådgivning
karl-ludvig.mauland@bdo.no, +47 902 40 488

Anette Aaser-Stene
Senior Manager - Rådgivning
anette.aaser-stene@bdo.no, +47 970 79 235

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