SIRK

Styring – Internrevisjon – Risiko – Kontroll

IIA Norge

Er julenissen en privacy risk?

Finner du løsningen på julekryssordet?

Treffpunkt GRC 2019

Hva er jomfru-revisjon?

REDAKTØRENS SPALTE

ELLEN BRATAAS

Til deg som hadde håpet på en pause fra GDPR denne julen, kanskje sittende foran peisen med et knitrende nytt nummer av SIRK i fanget - du slipper ikke helt unna!

Personvernforordningens mange fasetter fanges opp i flere artikler også denne gang, deriblant har NAV gjort en revisjon av knyttet til implementeringen av GDPR. Og har du forresten tenkt over hva som befinner seg i motsatt enda på GDPR-skalaen, i en helt GDPR-fri sone? Artikkelen «Smil – du er blitt identifisert!» gir et innblikk i bruk av overvåkningsteknologi og hvilke muligheter som åpner seg når personvernet blir underordnet. Grøss & gru!

Om du har behov for en mer triviell inngang til julen dette året, kan vi anbefale å bla frem til side 15 hvor Mediekomiteen for første gang lanserer et julekryssord. Vi håper på et skred av tilsendte løsningsforslag og lover premie til alle som klarer å løse foreningens «jomfrukryss». Vi har også latt oss inspirere av kreative medlemmer og laget en kollasj av nye revisjonsuttrykk som har dukket opp denne høsten. Hvorvidt de nye ordene blir å finne i revisjonsvokabularet i fremtiden er uvisst, men du finner de oppsummert og forklart «På tampen» bakerst i SIRK.

Spill som metode er et annen kreativ måte som Forsvarets forskningsinstitutt (FFI) i en årrekke har benyttet for å bidra til gode beslutninger og effektiv ressursbruk. Spilleksperten i FFI deler sine erfaringer fra 22 år med spill og beskriver hvordan denne metoden brukes for å studere effekten av ulike beslutninger for en gitt problemstilling. Spill kan brukes enten til å skape ny eller samle eksisterende kunnskap. Spill kan brukes kreativt for utfordre tanker om fremtiden, eller brukes analytisk for å støtte struktur- og organisasjonsutvikling, og spill kan være et bra virkemiddel i undervisning.

Vår oppfordring til alle for det kommende året er: Spill i vei og la kreativiteten blomstre! Vi skal i alle fall gjøre vårt beste – inspirert av det som skjer på tvers av internrevisjoner, compliance- og risikofunksjoner både her i Norge og internasjonalt. Vi gleder oss til 2019 og alt vi skal få til sammen med dere!

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

SIRK ønsker sine lesere en riktig god jul!

STYRELEDER HAR ORDET

METTE STORVESTRE
STYRELEDER
IIA NORGE

Det stunder mot jul og mange av SIRKs lesere bruker kanskje en stille stund til å se tilbake på et år med både opp og nedturer, gleder og utfordringer.

En definitiv opptur i år var årskonferansen i Bergen. Rekordstort oppmøte gjorde dette til det konferansen skal være - et attraktivt møtested for de som arbeider med internrevisjon, internkontroll, risiko og compliance. At det i tillegg var varmerekord og sprakende grønn forsommer i Bergen under festspillene gjorde dette også til en minneverdig opplevelse. Foredragene viste bred faglig kvalitet. Det var mye nytt som ga bekreftelse på at vi arbeider i en profesjon i fremgang og utvikling. Årskonferansen gir rammer og innhold som viser retning, inspirerer oss og gir substans i de utfordringer vi står overfor.

En styrke som IIA Norge har er det store engasjementet blant medlemmene og all frivillig innsats som gjøres i nettverk og komiteer. Det nye styret trådte sammen i august og vi har hittil invitert fire av nettverkene for å høre om arbeidet deres. Vi er imponert over det dere får til og heier på dere. Vi ser at det er muligheter for gruppene å lære av hverandre på tvers. Sekretariatet skal legge til rette for at gode maler og arbeidsformer kan deles. Vi oppfordrer også nettverkene å benytte anledningen til å fremsnakke andre nettverks arrangementer slik at medlemmene blir oppdatert på det rike tilbudet til faglig og sosial utveksling som finnes i IIA Norge.

Noe som i utgangspunktet kan ses på som en nedtur er at Master of Management programmet på BI Internrevisjon: governance, risikostyring og intern styring og kontroll ikke avholdes i år. Grunnet nedgang i antall deltagere i år valgte BI å avlyse kurset. Pr. nå ser IIA Norge på dette som en mulighet til å få opp et nytt oppdatert kurstilbud som appellerer til både våre medlemmer og andre som er interessert i virksomhetsstyring som fag. BI gjennomfører fokusgrupper med tidligere studenter for å evaluere hva studentene har vært fornøyd med av kurset og forslag til forbedringer. IIA Norge skal gi innspill til faglig innhold og oppbygging av programmodulene. Dette er et godt utgangspunkt for å få opp et nytt revitalisert program som leder frem til tittelen diplomert internrevisor høsten 2019. Vi holder dere som er interessert i kompetansebygging løpende oppdatert på videre utvikling.

Det foregående styret har gitt oss et godt grunnlag som vi bygger videre på. I styrets strategiarbeid bygger vi på de tre målene fra IIA globalt: styrke profesjonen, bygge kompetente ledere og medarbeidere og sikre at forretningsmodellen bærer seg. Ambisjonen er enkel - Vi skal være en forening som har et så attraktivt tilbud til våre medlemmer at de vil være med videre og stadig nye kommer til. Og selv om ambisjonen er enkel, så er det hardt arbeid å nå den. I desembermøtet diskuterer vi hvordan sekretariatet kan få spissede strategier slik at de kan lage konkrete handlingsplaner som gjør at vi når dette målet. Det betyr at vi lager delstrategier innen produkt- og marked, kommunikasjon, medlemmer og partnerskap. Styret har også vedtatt en governance struktur som skal ligge til grunn for arbeidet i foreningen. Dere finner nye etiske retningslinjer, styreinstruks og instruks for generalsekretæren på nettsidene.

God lesning av juleutgaven av SIRK. På vegne av hele styret ønsker jeg dere en god jul og et fredfylt nytt år.

MEDIEKOMITEEN

Ellen Brataas
Generalsekretær
IIA Norge

Reidar Døli
Komiteens leder
Internrevisor,
Oslo Børs VPS

Martin Stevens
Internrevisor,
Gjensidige Forsikring

Ola Otterdal
Seniorrådgiver
Forsvarsdepartementet

Esa Leporanta
Senior Risk Manager, DNB Bank ASA

Hilde Tanggaard
Manager, KPMG AS

Marit Trodal
Prosjektleder, IIA Norge

Neste utgivelse er mai 2019

Årsabonnement: Kr. 150

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

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

Grafisk produksjon:
Merkur Grafisk AS

Trykksak
2041 0672

Forsidebilde:
Foto: corgarashu/shutterstock.com

INNHOLD

RISIKOSTYRING

COMPLIANCE

VIRKSOMHETSSTYRING

KONTROLL OG SIKKERHET

16

34

52

Julekryssord

15

12

INTERNREVISJON

FASTE SPALTER

Preparing Internal Audit for an External Quality Assessment (EQA)

BY JAMES C PATERSON
Director, Risk & Assurance Insights Ltd.

Over the past few years I have worked as an External Quality Assessor, helping Internal Audit teams to meet their obligations to have an EQA at least every 5 years. In addition, I have helped several Heads of Internal Audit to prepare for an up-coming External Quality Assessment, often with important and unexpected results and benefits. Clearly each IA team is different and some are very well prepared for an EQA, but here are some of the key themes that I have picked up:

1) Make sure key documents have been updated for the latest IIA International professional practices framework

It is a requirement of the new IIA standards to ensure that IA team charters etc. are in line with the requirements of the new standards and most readers will be aware that these have been updated in 2017, covering, for example, that: 1) IA teams should be aligned with the strategies, objectives and risks of the organisation, 2) IA teams should operate in an insightful, forward looking and proactive manner and 3) IA teams should coordinate with other assurance providers and consider relying on their work (using a systematic basis of determining this).

2) Ensure you have done an assessment of the strengths and improvement needs of your IA team, within all levels of the IA team (managers and staff)

Especially for larger internal audit teams, it is not unusual for an HIA or IA management team to have one impression of key strengths and improvement areas against the IIA standards, but find that the auditors «on the coal face» have another view about, for example, skills and training plans, the quality of audit planning process (even if they are not involved in it!), the quality of assignment planning, the usefulness of supporting tools (e.g. data analytics) and the quality of the audit software that they use (often less positive than the IA management team). Readers are encouraged to ensure there is an IA team discussion about the IIA standards and IA team strengths and improvement areas, to avoid vital information that is known to team members, but perhaps not to the IA management team, being missed until the EQA starts.

3) Be clear about the EQA scope and process and ensure you will get credit and acknowledgement for known issues and current improvement plans

Sometimes EQA assessors are keen to have as broad a remit as is possible, interviewing large numbers of senior managers across the organisation; and whilst this can have benefits, some HIAs have spoken of concerns about «fishing trips» and EQAs based on stakeholder opinions. Some have even reported the EQA as a precursor to the outsourcing of the IA function (which may of course be merited, it is hard to generalise). Hopefully this is not a serious risk for most IA teams, but some sensible conversations and appropriate due diligence about this potential risk are worth bearing in mind.

In addition, readers will appreciate that there is nothing worse than reading a final draft EQA report and finding known issues and improvement areas reported back as if they are «fresh» findings. Ensure any EQA process explicitly includes a clear step that involves getting the IA team perspective on key issues, and what it is already working on, and understand how this will be reported in the final EQA report.

4) Ensure there is clarity about how the EQA will distinguish between judgements against the IIA standards and judgments against «best practice».

For several clients, I have seen EQA reports that list improvement actions against best practice as if they were basic IIA requirements. This can give the impression that the IA team is much further back than it actually is. Therefore, it is important to clarify with any proposed EQA assessor how they will distinguish between basic compliance points and improvement areas towards best practice. Also, make sure that if something is being cited as best practice it is clear how many IA functions have actually implemented it, and their circumstances. For example, I have seen EQA recommendations suggesting the implementation of practices for audit teams that have under 10 staff, which when challenged, have turned out to be more suited and more common in audit teams of 25+ auditors.

5) Look at IIA guidance on common EQA findings.

These may vary from country to country, but some of the most common findings I have seen are:

- The need to strengthen stakeholder management (both senior executive and audit committee / board)
- The need to have a plan that is truly aligned to strategies, objectives and risks (all too often the plan is based on a process/ unit based audit universe and retrofitted

to the organisation´s strategy, objectives and key risks)
- The need to do audit work in the context of the overall assurance picture - which can be evidenced by having an assurance map and a clear sense of measuring the assurances from both line management and 2nd line functions (a big topic in its own right).
- The need to be very proactive about audit team skills and capabilities and ensuring these match the needs of the audit plan (linked to key risks etc.).

6) Remember an EQA can give you significant benefits, but only if you trust the EQA assessor.

Despite the risks outlined above, I am personally a strong believer in the benefits that can flow from having the right EQA. It can sometimes bring prominence to gaps that have concerned the audit team, but have been rather stuck - for example by helping to remove «no go» zones in the audit planning process, or by encouraging a stronger flow of experienced staff into the audit team, or more support for the use of guest auditors and guest advisors.

All this highlights the need to choose your EQA assessor carefully, so that you can be confident it will have a positive impact, not just on the internal audit team, but on some related organisational governance, risk and compliance activities. And - speaking of a pet hate - make sure your assessor does not take pride in raising minor housekeeping points in relation to audit files, unless there is a clear impact on important audit conclusions!

7) Engage with key decision makers and manage their expectations

Audit Committees and Senior Managers may play a key role in selecting an EQA provider and considering their feedback. Make sure they are fully onboard with the considerations discussed in this note.

In conclusion, I hope this short overview explains some of the key opportunities and threats of an EQA and encourages readers to ensure they properly prepare their IA team for an EQA and choose their EQA assessor carefully.

IIA Norge og NUES

AV INGUNN VALVATNE
Styreleder, IIA Norge, 2015-2018

Ett av IIA Norges fire strategiske mål for inneværende perioden er «å befeste og videreutvikle internrevisjonens rolle som styre- og lederstøtte.» Dette kommer ikke av seg selv, og derfor må påvirkningsarbeid være en av flere viktige roller som IIA Norge har. NUES, Norsk Utvalg for eierstyring og selskapsledelse utgir den norske anbefalingen om eierstyring og selskapsledelse. Organisasjonen når, gjennom sin brede medlemsmasse, fram til mange og er en viktig aktør også for IIA Norge. Vi mener internrevisjon har en naturlig og selvfølgelig plass i anbefaling om god eierstyring og selskapsledelse. Dessverre har vi så langt ikke nådd fram med våre synspunkter. Men vi gir oss ikke.

NUES anbefaling fra 2014 spesifiserer at styret har ansvar for årlige gjennomgang av risikoområder og internkontrollsystemer. I omtalen av internrevisjonen begrenser anbefalingen seg imidlertid til å slå fast hvordan styret kan ivareta sitt påseansvar i eventuelt fravær av internrevisjon. IIA Norge mener dette er et for lavt ambisjonsnivå og at NUES anbefaling bør gjenspeile krav som stilles til virksomheter i store og viktige sektorer i Norge.

Vi har også sett utenfor Norges grenser. I vår dialog med NUES har vi vist til OECDs rapport fra 2014 som slår fast at norske kravene om internrevisjon har en svakere forankring enn i land det er naturlig å sammenligne seg med; *«The absence of an internal auditor in 90% of listed Norwegian companies is also unusual in comparison to most developed markets».*

I våre daglige roller er vi som internrevisorer vant til å fremholde uavhengighet som ett av våre viktigste særtrekk. Det er gjennom vår objektivitet og uavhengighet fra resten av organisasjonen at vi tilfører verdi. For å bevare tillit må vi alltid være satt opp til å bidra med et perspektiv som er upåvirket av ledelsenes interesser. Det er et bærende prinsipp at internrevisjonen aldri kan ha ansvaret for verken utforming eller iverksettelse av internkontrollen i et selskap.

Men uavhengighet er et spørsmål om ståsted og synsvinkel. Fra eiers ståsted vil internrevisjonen være en vesentlig del av internkontrollen. En godt fungerende internrevisjon er et viktig ledd i styrets ansvar for styring og kontroll og øker eiers sikkerhet for god styring.

Betydningen av velfungerende eierstyring og selskapsledelse er aktualisert gjennom at flere norske virksomheter har vært funnet skyldige i korrupsjonssaker. I noen av tilfellene har internrevisjonen hatt en sentral rolle i å avdekke og håndtere korrupsjonssaker.

IIA Norge mener at NUES anbefaling som et minimum må slå fast at styrer bør vurdere å etablere en internrevisjon. Viktige vurderingskriterier vil være omfang, kompleksitet og type virksomhet. Slik kan NUES anbefaling bli et enda mer relevant verktøy for styrenes utøvelse av sitt ansvar. Og slik kan internrevisjonen få en forankring i selskapsstyringen for øvrig.

Det er skuffende at NUES ikke har tatt hensyn til våre innspill i denne omgang. NUES vil fortsatt være en viktig organisasjon i arbeidet med å bringe Norge opp til en standard vi kan være stolte av også i internasjonal sammenheng. Det kommer en ny dag og nye anledninger og IIA Norge vil fortsette med å komme også i årene fremover med innspill til forbedring av NUES anbefalingen.

Mislighetsområdet – en bekymring for internrevisor?

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

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

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

AV HEGE SKJELBRED-ERIKSEN
Nestleder, internrevisjonen Norconsult AS

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

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

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

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

Vurdering av risiko for misligheter

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

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

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

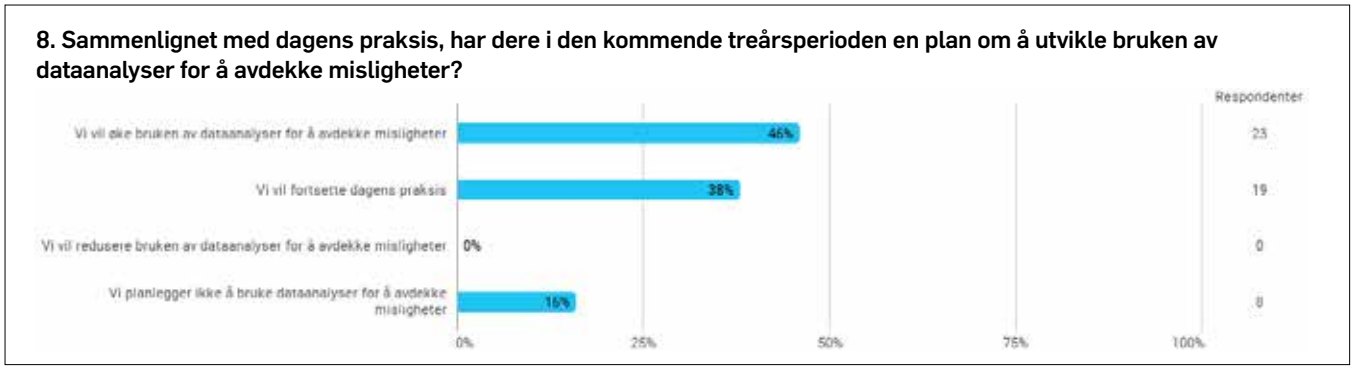
Teknologibasert revisjon (figur 1)

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

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

Risikovurdering av mislighetsrisiko i revisjonsoppdrag (figur 2)

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



Figur 1

Figur 2

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

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

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

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

Avdekking av misligheter (figur 3)

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

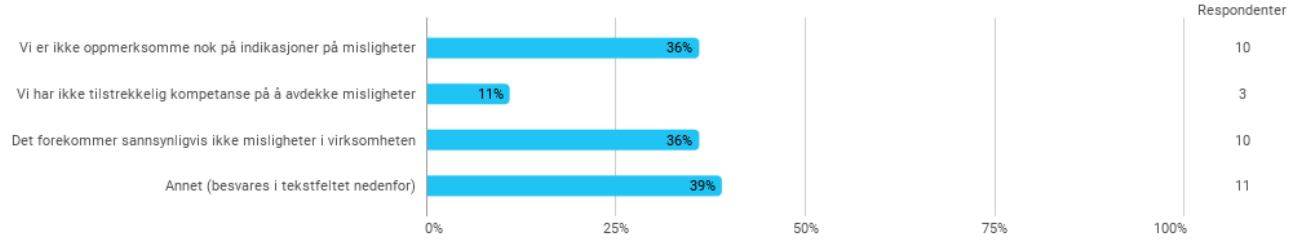
Det er interessant at hele 36% av respondentene som ikke hadde avdekket misligheter oppga at det sannsynligvis ikke forekommer misligheter i virksomheten. Eksperter på avdekking av misligheter anslår at kostnader knyttet til misligheter beløper seg til om lag 5 % av virksomheters omsetning globalt. Det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

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

Rapportering til toppledelse og styret

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

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



Figur 3

E-læringskurs i internrevisjon

IIA Norge har i løpet av 2018 utviklet et introduksjonskurs til internrevisjon.

Gjennom dette e-læringskurset får deltagerne en innføring i rollen og det faglige rammeverket til internrevisjonen, samt en forklaring av begreper som er viktige å forstå for en blivende internrevisor. Målet er å gi deltakere en grunnleggende innføring som de kan bygge videre på gjennom deltakelse i mer praktisk rettede kurs og seminarer.

Kurset er beregnet på nyutdannede, personer som er nye i internrevisjonen, internrevisorer som ønsker en oppfriskning av det faglige rammeverket, eller andre som ønsker mer informasjon om hvilken nytteverdi internrevisjonen kan bidra med.

Hva er prisen?
Kr 2900 for medlemmer av IIA Norge
Kr 3500 for ikke-medlemmer
Kvantumsrabatt for virksomheter som kjøper flere tilganger til kurset. Send forespørsel til post@iia.no

Kursoppbygging:

Leksjon 1: Internrevisjonens rolle i virksomheten
Leksjon 2: Dette er internrevisjon
Leksjon 3: Governance og risikostyring
Leksjon 4: Internkontroll
Leksjon 5: Det internasjonale rammeverket – IPPF
Leksjon 6: Det internasjonale rammeverket – standardene
Leksjon 7: Egenskapsstandardene
Leksjon 8: Utøvelsesstandardene

Hver leksjon er 8-15 minutter og etterfølges av en kort quiz.

Når alle leksjonene er gjennomgått og quizen er gjennomført vil du motta et kursbevis.

Screenshot fra E-læringsprogram

Transocean-saken:

Internrevisjonen tar på seg et evalueringssoppdrag for ledelsen

I en presentasjon for ledernettverket i IIA Norge fortalte Stokka og Lillestøl Melaa om et evalueringsoppdrag knyttet til Transocean-sakene som internrevisjonen i Skattedirektoratet hadde fått ansvaret for. Flere internrevisorer kan være interessert i å høre om oppdraget og deres erfaringer i saken

AV MARTIN STEVENS
Internrevisor, Gjensidige Forsikring

Saken var utgangspunkt for mange avisoppslag, her Teis og Marie med en samling av disse.

Hva gikk oppdraget deres i hovedsak ut på?

- Transocean-saken var en straffesak mot to Transocean-selskaper og deres tre rådgivere. Saken har blitt kalt «Norgeshistoriens største skattestraffesak» og pågikk fra 2004 til 2017.
- Tiltalen hadde 5 tiltaleposter med et skattefundament på 11,3 milliarder og resulterte i flere sivile og strafferettslige rettsaker
- Skatteetaten fikk medhold i en del av de sivilrettslige sakene, og ble i liten grad idømt å betale saksomkostninger, hvilket viser at det var stor grad av tvil knyttet til de juridiske fortolkningene.
- I straffesaken ble samtlige tiltalte frikjent med begrunnelsen at det ikke var unndratt skatt.
- Saken har fått mye oppmerksomhet i media og spesielt i Dagens Næringsliv.
- Riksadvokaten har foretatt en offentlig evaluering av Økokrims håndtering av Transocean-saken.

I ettertid ønsket skattedirektøren en uavhengig evaluering av Skatteetatens forvaltningsmessige håndtering av saken og henvendte seg til sin internrevisjon. Oppdraget skulle imidlertid ikke innebære en vurdering av de skattemessige vedtakene i sakskomplekset. Videre bestemte skattedirektøren at internrevisjonens evaluering skulle offentliggjøres.

Hvorfor henvendte skattedirektøren seg til internrevisjon i stedet for et advokatfirma eller en ekstern konsulent?

Vi tror at ledelsen i etaten over tid har opparbeidet stor tillit til internrevisjonen som en kompetent enhet med stor integritet.Vi har ansatte med høy kompetanse og stor personlig integritet. Vi har også tilgang til ekstern bistand på områder hvor vi selv mangler spisskompetanse, og internrevisjonen signaliserte tidlig til skattedirektøren at det var behov for tung ekstern juridisk bistand i denne saken. Denne tilnærmingen var også viktig for å sikre nødvendig distanse og uavhengighet til etatens juridiske miljø.

Hvilke faktorer veide tyngst for internrevisjonen i beslutningen deres om å ta på seg dette oppdraget?

Internrevisjonen så på dette som en stor utfordring.Vi var ydmyke til oppgaven, og samtidig så vi det som en stor anerkjennelse for arbeidet vårt at vi fikk denne henvendelsen. Håndtering av store komplekse skattesaker ligger i kjernen av Skatteetatens oppgaver, og dette har gjennom mange år vært en av de viktigste skattesakene etaten har jobbet med. For

at internrevisjonen skal bli sett på som en viktig bidragsyter må den også være aktuell og relevant for ledelsen og jobbe med de saker ledelsen er opptatt av.

Hvor mange internrevisorer har dere i Skatteetaten og hvor mange av dere skulle arbeide med dette prosjektet? Hadde dette oppdraget noen konsekvenser for allerede planlagte revisjoner?

Vi er 6 ansatte i Internrevisjonen i Skatteetaten. To av disse har jobbet med Transocean oppdraget i ett år. Disse to har også fått noe støtte fra andre kollegaer i internrevisjon. Konsekvensen av at internrevisjonen tok på seg dette oppdraget ble at andre revisjoner måtte nedprioriteres. Internrevisjonen i Skatteetaten planlegger for 18 måneder om gangen, men planen vår er dynamisk slik at nye mer aktuelle oppdrag vil kunne erstatte allerede planlagte oppdrag.

Identifiserte dere noen hull i deres kompetanse? Hvordan løste dere dette?

For å løse oppdraget var det nødvendig med tung kompetanse særlig knyttet til forvaltningsloven, men også skattefaglig kompetanse. Internrevisjonen hadde ikke tilstrekkelig kompetanse innen dette området, og vi knyttet oss derfor til advokatfirmaet Grette. Med dette tiltaket kunne vi også forsterke evalueringens objektivitet og uavhengighet.

Hvordan samlet dere revisjonsbevis ved gjennomføringen av oppdraget? Skjedde dette hovedsakelig gjennom intervjuer? Hvis det var tilfelle, ble intervjuene gjennomført på alle organisasjonsnivåer eller bare blant ledelsen?

Internrevisjonen samlet revisjonsbevis gjennom intervjuer og gruppesamtaler. Vi snakket både med saksbehandlere og ledere i Skatteetaten, advokater på begge sider i saken og med Økokrim. Vi gikk også gjennom en betydelig mengde dokumenter, inkludert lovdata, tidligere dommer og vedtak fattet av Skatteetaten.

Hvordan ble dere møtt av egen organisasjon – forsterket det en oppfatning om internrevisjon som «politi»?

Internrevisjonen i Skatteetaten ble startet opp i 1999. Vårt fokus har hele tiden vært å være en støttespiller for organisasjonen. Både observasjoner og anbefalinger er grundig kvalitetssikret av aktuelle parter. Vi spiller på lag og er løsningsorienterte. Internrevisjonen i Skatteetaten blir derfor ikke sett på som «politi».

Tok det lang tid å ferdiggjøre prosessen fra revisjonens utkast til en endelig omforent revisjonsrapport?

Det følger av IIAs etiske retningslinjer at internrevisjonen skal være objektiv, ha

Foto: Shutterstock

integritet og inneha nødvendig kompetanse. Dette er ord med et viktig innhold som vi har hatt med oss gjennom hele oppdraget. Det følger av dette at vi ønsket å levere en faktisk riktig rapport, så fakta ble grundig sjekket ut. Det at rapporten var bestemt offentliggjort bidro også til sterkt fokus på kvalitet, balanse i fremstillingene og faktasjekk. Rapportutkastet ble sendt på høring i flere omganger. Flere aktører, både interne og eksterne, fikk tilsendt deler av rapporten til gjennomgang og kommentarer. Vi mener at det var nødvendig å bruke tid på denne kvalitetssikringen i en så viktig sak. Vurdering av komplekse juridiske problemstillinger og nyanser bidro også til at arbeidet tok tid.

Kan dere fortelle hva som var hovedkonklusjon i deres rapport?

Hovedformålet med evalueringen var å vurdere hvorvidt den forvaltningsmessige håndteringen av saken, sett i lys av samarbeid med politi/påtalemyndighet i en parallell straffesak, har vært i samsvar med god forvaltningsskikk. I tillegg skulle evalueringen gi svar på om Skatteetatens interne håndtering av Transocean-saken var hensiktsmessig og tilstrekkelig.

Hovedkonklusjoner i rapporten var at:

1) skattesakene ble godt opplyst, og at skattyter ble gitt adgang til kontradiksjon. Skattevedtakene er omfattende, begrunnet og skattyters anførsler ble behandlet i vedtakene. Gjennomgangen viser også at Skatteetatens arbeid ble kvalitetssikret ved at det ble benyttet flere saksbehandlere samt at ledere, Skattedirektoratets spesialutreder, nemndsenheter i tillegg til at eksterne eksperter, Finansdepartementet og Regjeringsadvokaten ble involvert. Etter vår vurdering har ligningsvedtakene vært forvaltningsmessig forsvarlig behandlet.

I tillegg viser undersøkelsen forhold som Skatteetaten kan ta læring av. Undersøkelsen har vist at behandlingen av innsynsbegjæringer ikke oppfylte kravene til hurtig behandling; dette gjelder spesielt klagebehandlingen. Skatteetaten må også i større grad sikre etterlevelse av rutinene for involvering av etatsledelsen i prinsipielle saker. Beslutninger om å fremme, og eventuelt å anke krav om erstatning i forbindelse med straffesaker bør forankres i rutiner som sikrer og dokumenterer saksbehandlingen.

2) det generelt ikke er grunn til å kritisere Skatteetatens samarbeid med Økokrim under etterforskningen og i forbindelse med tiltaler og iretteføringen av straffesaken. Slik samarbeid er forutsatt i lovgivningen og akseptert av domstolene. Motsatt av hva Riksadvokat-utvalget konkluderer med, finner internrevisjonen det også akseptabelt at saksbehandlere som har deltatt i ligningsbehandlingen bistår politi og påtalemyndighet i straffesaker.

Samtidig har undersøkelsen vist at det er forhold tilknyttet til samarbeidet mellom Skatteetaten og Økokrim i Transocean-saken som Skatteetaten kan ta læring av. Dette er særlig knyttet til rettsregler som regulerer forhold av betydning for etatssamarbeid.

Evalueringen er offentlig og de som ønsker mer informasjon om saken vil finne evalueringsrapporten her:

https://www.skatteetaten.no/globalassets/om-skatteetaten/analyse-og-rapporter/rapporter/evaluering-av-skatteetatens-handtering-av-transocean-saken.pdf

Hvilken respons fikk deres rapport – både internt og eksternt?

Rapporten har blitt presentert i flere ulike interne fora, samt for Finansdepartementet og ledernettverket for IIA Norge. Evalueringen ble anerkjent som et kvalitativt godt arbeid.

Har rapporten deres blitt omtalt i media?

Rapporten ble publisert på Skatteetatens nettsider 23. mai i år. Det ble en del medieomtale om saken da rapporten ble publisert, blant annet gjennom en kronikk fra skattedirektøren, leder i DN og avisintervjuer.

Hadde dere vurdert å gjennomføre et lignende oppdrag i fremtiden? Ble deres forventninger til å ha et slikt oppdrag innfridd? Ville dere anbefale andre internrevisorer å ta på seg et slikt oppdrag?

Ja, det vil vi. Det er en stor anerkjennelse av internrevisjonen å få ansvar for å evaluere en slik stor og samfunnsviktig sak. Det aktuelle fagområdet er i kjerne av vår virksomhet, og etaten har jobbet med denne saken fra 2004 til den ble avsluttet i 2017. For at internrevisjonen skal bli sett på som en verdiskapende funksjon er det helt avgjørende at vi er opptatt av og kan levere på de saker som toppledelsen retter sin oppmerksomhet mot.

Julekryssord

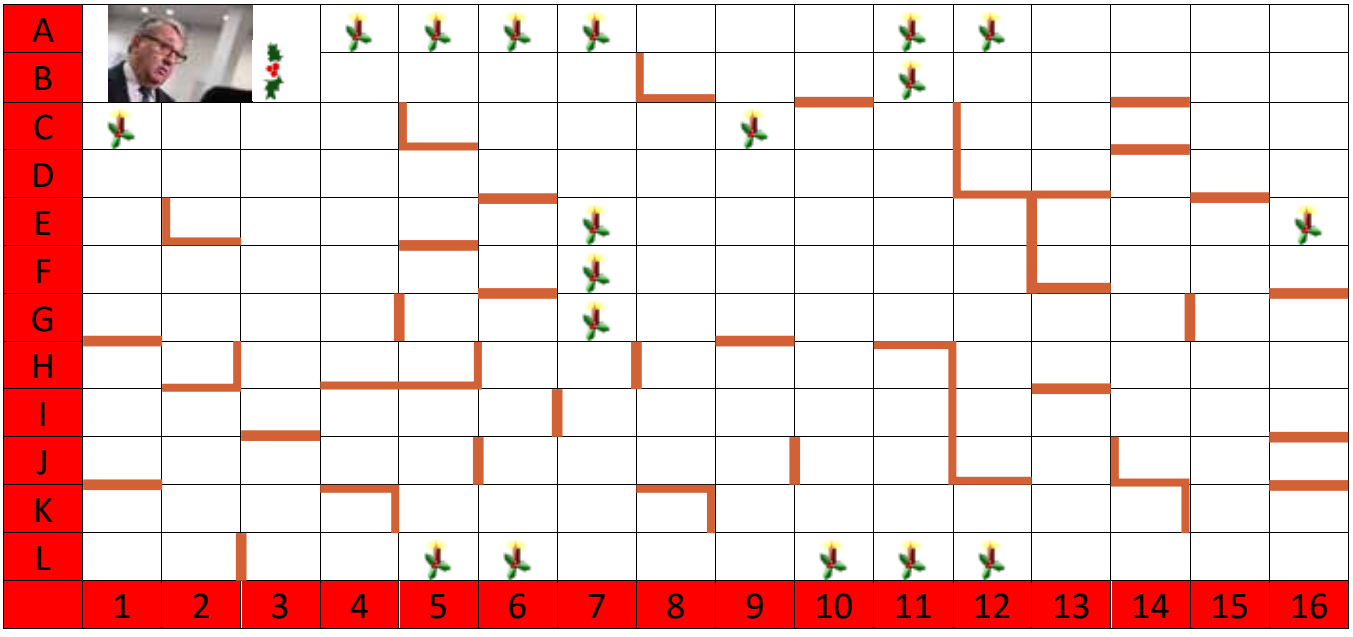
Løsning sendes til: post@iia.no
Premie til ALLE!

VANNRETT

1D	MANNEN PÅ BILDET
1E	PREPOSISJON
1F	TYSK KVINNENAVN
1G	EN LOV
1H	AMERIKANSK SELSKAP
1I	KONFERANSEBY
1J	PUNKT
1K	BEDEHUS
1L	SKLI
2C	STANDARD
2E	MAJONESRETT
3H	POPULÆRT PRODUKT
3L	SELSKAP
4B	KONGENAVN
5C	BLOMST
5G	IDRETTSLAG
5K	ALKOHOLHOLDIG DRIKK
6H	SELSKAPSFORM
6J	BETALINGSMIDDEL
7I	VALGSPRÅK
7L	COCKTAIL
8A	REGEL
8B	KVINNEORGANISASJON
8E	HILSEN
8F	SANG
8G	RAPPORT
8H	BY OG MODELL
9K	KJEKKAS
10C	AVIS
10J	SELSKAPSFORM
12B	MENGDE
12C	BÅTROM
12D	RISIKOTYPE
12H	KONFLIKT
12I	STYRELEDER, FORNAVN
12J	ORDNE
13A	KJERNE
13E	STORFERASE
13F	BIBELSK KVINNE
13L	POPULÆR PRODUSENT
14J	LAND, FØRSTE DEL, SE 6G
15G	MODERNE
15K	ARTIKKEL

LODDRETT

1D	MARITIMT UTTRYKK
1H	VALUTA
1K	YTRET
2C	ORGANISASJON
2F	TANKE
2I	MANNLIG LEDER AV NETTVERK
3C	LØYPE
3J	IDRETTSORGANISASJON
4B	RAMMEVERK
4I	NORSK ELEKTROFIRMA
4K	NORGE
5B	POLITISK PARTI
5D	AMERIKANSK MOTEDESIGNER
5F	STED I TELEMARK
5I	FORHENVÆRENDE
6B	SKJELDNE MINERALER
6E	IKKE AKTUELT
6G	LAND, ANDRE DEL, SE J14
7B	TILLATELSE
7H	BABYTRØST
8A	BAKKE
8C	POPULÆR DAME
8K	ARTIKKEL
9A	UTROP
9D	GRENSEELV
9H	KVINNEGRUPPE
10A	BILMERKE
10C	POLITIKER
11C	OMSTRIDT LEDER
11H	POPULÆR DRIKK
12B	KRINGKASTNINGSSELSKAP
12E	TEDDYBJØRN
12K	NORGE
13A	ÅR
13E	STANDARD
13G	TO LIKE
13I	KJEDELIG
14A	HELLIG
14C	STØRRELSE
14D	GENERALSEKRETÆR
14K	DIALEKTORD
15A	LÆRESETNING
15E	GJEST I LUKKET SELSKAP
16A	HEVER
16G	BITTERHET
16J	GRESK GUDINNE



LØSNING:

15H	13C	3D		8F	10A	12G	2J		15K	6B		2L	4G	15G	3C	6C		15A	13K	11J	7K	2E	5E	5F	

2H	6J	15C	3G	8K	13G	10I	8D	5K	8G

Foto: Shutterstock

Nettverksmøte - en kulinarisk opplevelse

AV REIDAR DØLI
Leder, Mediakomiteen i IIA Norge
Internrevisor, Oslo Børs VPS

Når jeg hører ordet *kulinarisk* så går tankene i retning av mat som er tilberedt med stor omhu og som smaker utsøkt. Det var nettopp den følelsen jeg fikk da jeg deltok på Ledernettverket for finans i IIA Norge sin høstkonferanse den 6. november, men der var mat erstattet av faglig input.

Invitasjonen til konferansen gikk ut til en engere krets siden nettverket er forbeholdt ansatte ledere av internrevisjonsavdelinger. Det opptar kun ledere fra virksomheter innen finanssektoren som er underlagt tilsyn i Norge. Dette snevrer inn medlemsgrunnlaget til ca 25 og det var 20 representanter som møttes rundt årets konferansebord.

For å ta litt historie så har nettverket sitt utspring i det som het Revisjonssjefkretsen, eller bare Kretsen. Det var opprinnelig en svært så mannsdominert forening, og jeg er blitt fortalt at det helt til langt ut på åttitallet nærmest var utenkelig at det skulle tas opp kvinnelige medlemmer. Det var bare lederens sekretær som fikk være med på middagene. Den

situasjonen har heldigvis endret seg, selv om den forsamlingen som inntok sine seter rundt konferansebordet i Bjørvika hadde en klar overvekt av menn. Foredragsholderne, eller servitørene som vi kaller de her, var til alt hell 50/50 kvinner og menn, så et stykke på vei er vi kommet.

Menyen besto først av et svært så inspirerende innlegg om det makrobildet som omgir oss. Dette ble servert av Thomas Eitzen. Han er Head of Credit Strategy i SEB – Markets. Han konkluderte med at vi har vært med på en flott reise fra år 2010 og at festen vil vare helt til inntjeningen blir dårligere, la oss si om et par tre år. Til tross for at det har vært mye geopolitisk støy de siste årene med Krim, Brexit, Trump, Nord Korea og det som verre er, er det beroligende å se at verdens innkjøpere sier at det fortsatt går helt ok og at de ikke har mistet lysten til å investere. Reguleringen som er kommet etter kriseåret 2008 har imidlertid ført med seg at vi er blitt flokkdyr, alle tenker likt og alle har fått mindre risikokapital. Det er veldig få motsykliske investorer. Resultatet er at samfunnet har fått en større buffer, mens bankene og livselskapene er de som blir sittende med risikoen. Hans spådom var at neste finanskrise blir en likviditetskrise.

Annen forrett fulgte i form av et innlegg med nytt fra Finanstilsynet. Irene Støback Johansen og May Camilla Bruun-Kullum, begge fra seksjon for banktilsyn, krydret vår tilværelse med nytt om krisehåndteringsdirektivet og hvitvaskingsregelverket. Sistnevnte kom som ny lov og forskrift fra 15. oktober. Viktig å merke seg var, også her, at det tydeliggjør en risikobasert tilnærming. Det ble nevnt og vi ble skremt med at spesialtilsyn på AML/CFT vil bli mer vanlig nå heretter. De refererte til at det nettopp var gjennomført AML tilsyn. Det nedslående resultatet etter et slik tilsyn i en bank nordpå flimret på skjermen i bakgrunnen og satte en ekstra piff på smaken. Krisehåndteringsdirektivet trer i kraft her i Norge fra 1. januar 2019.

> Som første hovedrett fikk vi servert en god porsjon GDPR.

Som første hovedrett fikk vi servert en god porsjon GDPR. Dette bidraget kom fra Personvernombud i DNB Fred Richard Elsheim og Lillian Engebø. Sistnevnte fra Konsernrevisjonen i DNB. Mange har kanskje fått den følelsen at GDPR etter hvert kan sammenlignes med å sette til livs en kraftig og seig biff, men det var ikke tilfellet med dette innlegget. Elsheims utgangspunkt var en saying fra noen år tilbake om at «det ikke er noen mulighet for å beskytte persondata lenger». Dette var etter at block chain, cyber crime, skytjenester, Big data, AI, maskinlæring etc hadde gjort sitt inntog. GDPR er intet mindre enn en krigserklæring fra EU mot at personvernet skal være umulig å oppfylle. Fascinerende var også utsagnet «Persondata er kundenes gull; vi skal tilby det beste hvelvet». De som ikke fremstår som tillitvekkende får en stor kundeulempe. En utfordring mange sliter med er legacy systemene som gjør det vanskelig å implementere nye regelverk-

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

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

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

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

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

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

Vidar Hansen, Intern revisjonssjef Sparebanken Sør.

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

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

ECIIA 2018

Pumping up your powers i Madrid

AV MARIT TRODAL
Prosjektleder, IIA Norge

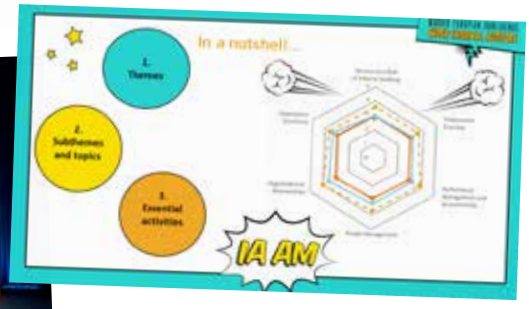
Å bidra til at internrevisorer bygger muskler var ambisjonen til årets ECIIA, som ble organisert av IIA Spania. Programmet var innholdsrikt og bar preg av at internrevisjonen er inne i en brytningstid og at vi må forholde oss til mye – både endringstakten i markeder, teknologi og digitalisering, økonomisk usikkerhet og ikke minst et politisk bakteppe som skaper mye uforutsigbarhet.

Hvordan skal internrevisjonen bli mer proaktiv og mindre reaktiv? Hvordan respondere raskere på endringer i risikobildet? Digitaliseringen av internrevisjonsfunksjoner har nettopp startet.

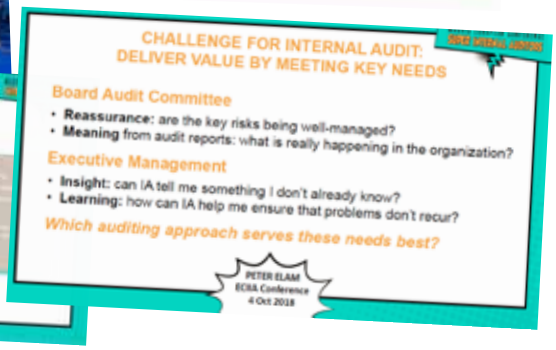
Er internrevisjoner klare til å lede an i den digitale reisen og selv transformere seg til å levere mer omfattende tjenester til virksomhetene de er del av? Kan vi utfordre oss selv og ta i bruk nye verktøy og metoder?

IIA Spania hadde gjort seg stor flid med programmet og hadde invitert en rekke virksomheter til å dele sine erfaringer. Se et knippe inntrykk fra konferansen. Vi i IIA Norge har invitert noen av disse inspirerende foredragsholdere til vår egen årskonferanse i mai 2019. Gled dere!

"In the end Internal Audit will be judged by the things it misses."



"Culture, more than rule books, determines how an organisation behaves." (W. Buffet)



Hva skal til for at internrevisjonen holder tritt med økt digitalisering i virksomhetene?

AV HELENE RAA BAMRUD
Partner og leder,
Deloittes Risk Advisory avdeling, Norge

AV KINE KJÆRNET
Director, Deloittes Risk Advisory avdeling, Norge

Skal internrevisjonen beholde sin posisjon som en strategisk aktør, må funksjonen i tillegg til å revidere være en rådgiver for håndtering av fremtidige risikoer. Internrevisjonen må se fremover, identifisere og vurdere styring og kontroll av aktiviteter som kan representere nye og ukjente risikoer. Denne artikkelen presenterer hovedpunkter fra undersøkelsen *Deloitte Internal Audit Insights 2018*.

«De siste årene har digitalisering og kunstig intelligens preget agendaen i både næringslivet og politikken. Vi kan forvente store og raske endringer i forretningsmodeller og måten vi jobber på. Hvor står internrevisjonen oppi det hele?», spurte SIRKs redaktør i forrige utgave.

Internrevisjonen må holde tritt med utviklingen, for å beholde relevans og innflytelse i organisasjonen. Hvilke aktiviteter og relaterte risikoer representerer muligheter for internrevisjonsfunksjonen til å kunne påvirke positivt og beholde sin posisjon?

En ny rapport fra Deloitte har identifisert 13 områder som internrevisjonen må vektlegge for å følge med i den digitale utviklingen. I denne artikkelen trekker vi frem de viktigste teknologiene og verktøyene for å kunne identifisere risikoen som oppstår som følge av økt digitalisering av virksomhetens prosesser.

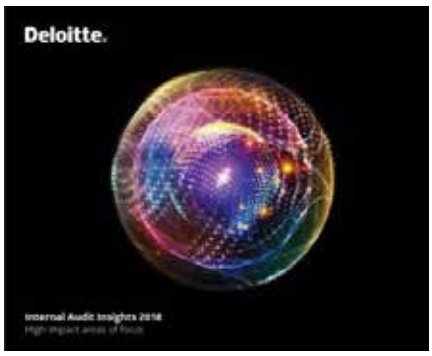
RPA og kognitiv intelligens

Robotisering og prosessautomatisering, eller «robotic process automation» (RPA), er bruken av algoritmer for å utføre regelbaserte oppgaver i et virtuelt miljø, ved å etterlikne brukerhandlinger for å oppnå de samme – eller enda bedre – resultater. RPA griper ofte inn i flere IT-systemer. Disse «digitale medarbeiderne» utfører generelt repetitive og manuelle oppgaver mye bedre enn mennesker.

Når ulike funksjoner i virksomheten innfører «digitale medarbeidere», kognitiv intelligens (KI) og liknende teknologier, bør internrevisjonsfunksjonen bistå med å identifisere og vurdere risikoer som oppstår som følge av disse teknologiene.

Internrevisjonens planer må adressere effekten av RPA og KI på ledelse, organisasjon og prosesser.

Internrevisjonsfunksjonen bør gjennomgå dokumentasjon av testprosedyrer, og eventuell tidligere gjennomførte tester, gjennom å ta stikkprøver av dokumenterte tester, resultater og loggførte hendelser.



Andre muligheter inkluderer å gi råd om risikoreduserende tiltak og automatiseringsstrategier. Internrevisjonsfunksjonen bør også vurdere å bruke RPA selv til å automatisere repetitive kontrolltester, interne rapporteringsoppgaver og oppfølging av funn.

Cyber-sikkerhet

I de senere årene har revisjon av cybersikkerhet ofte dreid seg om etterlevelse av regelverk. Det gjelder områder som personvern (GDPR), IT-sikkerhet og krise-, beredskaps- og kontinuitetsplanlegging, samt ISO 27001. Virksomheter som har vært involvert i høyprofilerte cyber-hendelser i senere tid, har ofte vært i samsvar med gjeldende regelverk og standarder. Den største risikoen ligger som regel ikke her. Den ligger ofte i bruken av skybaserte løsninger, tredjeparts risiko knyttet til arbeid utført av eksterne utviklere, og bruk av applikasjoner som ligger utenfor eget IT-miljø.

Mye av denne aktiviteten får imidlertid verken CIO'ens, CISO'ens eller internrevisjonens oppmerksomhet selv om den som regel utgjør en vesentlig risiko. Utfordringen ligger i å identifisere et bredere spekter av cyber-risikoer før de oppstår. Internrevisjonen som er vant til å levere revisjoner som skal sikre samsvar med forskrifter og standarder, trenger nye metoder og må tenke nytt – og stort;

Vær proaktiv i planleggingen av revisjoner, se utover eksisterende revisjonsplaner for å identifisere nye produkter,

markeder og eksterne parter. Utfordre ledelsens arbeid med å identifisere risikoer, overvåke og styre disse. Ledelsen bør være bevisst på hvordan beslutninger og atferd kan øke eller redusere cyber-risiko. Oppfordre til bruk av simuleringer for å teste virkningen av cyber-hendelser på drift, infrastruktur, data, økonomi og omdømme, og for å kunne måle respons og robusthet – og gjør dette regelmessig.

> Internrevisjonen som er vant til å levere revisjoner som skal sikre samsvar med forskrifter og standarder, trenger nye metoder, verktøy og må tenke nytt – og stort

Personvern og GDPR

EUs generelle databeskyttelsesforordning (GDPR) berører alle virksomheter i Europa som samler inn eller behandler data om enkeltpersoner, samt foretak utenfor Europa med virksomhet i EU. GDPR utvider i stor grad enkeltpersoners mulighet til å bestemme hvilke personlige data som samles inn og hvordan disse dataene behandles. Mens de aller fleste berørte virksomheter har jobbet for å oppfylle disse kravene, er det fremdeles flere som ligger etter på enkelt områder.

Internrevisjonen kan bistå virksomheten med å håndtere den økte risikoen som følge av de nye forskriftene, og med å realisere potensialet for en bedre forståelse og bruk av disse dataene. Virksomheter må etablere tydelige ansvarsområder for data. I tillegg til å utpeke en databehandler, trenger man ansvarlige for å håndtere spesifikke krav, som for eksempel innsynsbegjæringer, respons på brudd, og datalagring.

Ansvar og relaterte prosesser må dokumenteres i et rammeverk som beskriver utførelsen av informasjonsforespørsler, lagring av data og andre prosedyrer. Gitt mandatet til å beholde data bare så lenge som nødvendig, bør man fokusere på dataenes livssyklus og på lagrings- og slettingspolicyer. Ta en risikobasert tilnærming når du planlegger hvordan virksomheten håndterer forespørsler og krav. Forsikre deg om at det gjennomføres en vurdering av personvernkonsekvenser «Data Privacy Impact Assessment» (DPIA) for ethvert nytt initiativ som involverer data om individer. Vær spesielt oppmerksom på dataoverføringer til tredjeparter.

Krise- og beredskapshåndtering

Fagområdet krise og beredskap omhandler styring, struktur, ledelse, beslutningstaking og kommunikasjon for å støtte organisasjonen i å håndtere en krisesituasjon. Det innebærer å kunne fortsette daglig drift, respondere på sikkerhetshendelser, og å komme tilbake etter en katastrofe.

De fleste store virksomheter har grunnleggende krise- og beredskapsplaner på plass, spesielt for IT og verdi- og forsyningskjeden. Vanligvis vil internrevisjonen gå gjennom disse planene med jevne mellomrom, forsikre at de blir etterlevd samt gjennomføre evalueringer etter en hendelse. Arbeidet med å opprettholde daglig drift under en hendelse har imidlertid utvidet seg til også å inkludere eventuelle hendelser som kan gjøre uopprettelig skade på økonomi, drift, cyber-funksjoner, omdømme eller andre viktige eiendeler.

Ansvaret for krisehåndtering ligger hos toppledelsen i virksomheten. En krisehåndteringsplan gir rammer for lederne dersom krisen oppstår. En organisasjon trenger et krisehåndteringsprogram som omfatter styring, prosesser og risiko. Krisehåndteringsrammeverket organiserer eierskap og roller og ansvar for sikkerhet, jus, IT, internrevisjon og andre funksjoner. Prosesser er nødvendige for kriserespons, beslutningstaking, kommunikasjon og beredskapsplaner. Risikoer må identifiseres for å kunne planlegge og respondere på ulike scenarier, samt å trene på og simulere disse scenariene. Sett mål om å bidra med rådgivning innenfor alle disse områdene, prøv å forutse hendelser og beskriv beste praksis. Sørg for at ledelsen trenes jevnlig for å teste og videreutvikle planer og tiltak.

Verktøy og metoder

Den kontinuerlige digitaliseringen av virksomhetene genererer enorme mengder data som dataanalyse kan gjøre om til verdifull informasjon og innsikt. Verktøyene for å analysere og visualisere data er nå mindre kompliserte, rimeligere, mer tilgjengelige og enklere å bruke enn noensinne. I tillegg er virksomhetens interessenters behov for høyere grad av bekreftelse på etterlevelse, innsikt og risikoforventning aldri vært høyere.

På tross av dette har internrevisjonsfunksjonens utvikling knyttet til dataanalyse vært relativt ujevn og langsom. Dataanalyse bør sees på som en integrert del av all planlegging, gjennomføring og rapportering i internrevisjonsfunksjonen, og bør også bli reflektert i metoder og verktøy.

I stedet for å sette faste mål – bruk data under scoping for å kunne fange opp uvanlige mønstre, uventede forhold og endringer i forretningsforhold. Bevis verdien av dataanalyse ved å ta initiativ til pilotprosjekter på områder der data allerede er lett tilgjengelig, hvor suksess er mer eller mindre garantert, og hvor resultatene vil drive verdi – som for eksempel ved å redusere svindel, svinn eller andre retningslinjebrudd.

Konklusjon - bekreft, rådgi og forutse

Å bekrefte vil fremdeles utgjøre kjernevirksomheten til internrevisjonen, men å forutse vesentlige endringer i virksomhetens risikobilde vil kunne bety at internrevisoren kan bli en bedre rådgiver.

Bruk data som grunnlag for råd om fremtidige aktiviteter som kan representere nye og ukjente risiko. Det krever nye rammeverk, nye metoder, og interaksjon med nye interessenter. Tenk nytt og tenk stort for å møte behovet din organisasjon har for fremtidens revisor.

Artikkelen har tatt utgangspunkt i Deloittes rapport Internal Audit Insights 2018, som tar for seg totalt 13 områder som representerer muligheter for internrevisjonsfunksjonen til å holde seg relevant fremover. Se https://www2.deloitte.com/nl/nl/pages/risk/articles/internal-audit-insights-2018.html

Treffpunktet for deg som er interessert i god virksomhetsstyring og aktuelle temaer

13. februar kl. 0830 – 1600

Thon hotell Storo, Oslo

Treffpunkt GRC 2019
Governance / Risk / Compliance

Tema: Strategisk styring og transformasjon

Tid	Hva	Hvem
Kl. 0830	Registrering	
Kl. 0900–0945	**«Mot alle odds»** – et case som synliggjør viktigheten av god governancestruktur og proaktiv risikostyring når det uventede skjer	Gisele Marchand heltids styrearbeidende
Kl. 0945–1030	**Slik avslørte DN manipulasjon** av data hos strømmetjenesten Tidal	Markus Tobiassen journalist Dagens Næringsliv
Kl. 1045–1130	**Risikostyring** og økt rapporteringsmengde – hvordan se skogen for bare trær?	Kristian Andersen The Governance Group
Kl. 1230–1315	**From DONG Energy to Ørsted:** The green transformation and implications for governance, risk and compliance	Thomas Nordestgaard Sørensen Senior Manager Rasmus Peter Brock Danielsen Strategy Project Leader, Corporate Strategy, Ørsted
Kl. 1315–1345	**Avinor: Slik får vi risikostyringen til å fly** Et kulturelt paradigmeskifte	Ingvild Høydalsvik Røsæg Strategisk risikostyring, Konsern økonomi og finans, Avinor
Kl. 1400–1445	**Stormberg: Samfunnsansvar** – fra ord til handling	Steinar J. Olsen Stormberg-gründer
Kl. 1445–1515	**Oslo – miljøhovedstad 2019:** Hvordan påvirke innbyggere til å ta miljøvennlige valg og nå felles klimamål?	Anita Lindahl Trosdahl Prosjektleder Oslo Europeisk miljøhovedstad 2019
Kl. 1515 – 1600	**Tillitsoverskudd eller -underskudd?** Slik revideres virksomhetens omdømmeregnskap	Øystein Bonvik kommunikasjonsrådgiver og fagbokforfatter PR- og kommunikasjonsledelse Handelshøyskolen BI

Se www.iia.no/aktiviteter for mer informasjon og påmelding.

Følg oss på sosiale medier

Risikostyringsfunksjon i vekst og utvikling

AV KENNETH HANSEN
Senior prosjektleder, Konsernrevisjonen, Avinor

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

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

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

Konklusjoner fra spørreundersøkelsen:

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

Flere bruker et rammeverk for helhetlig risikostyring (figur 1)

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

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

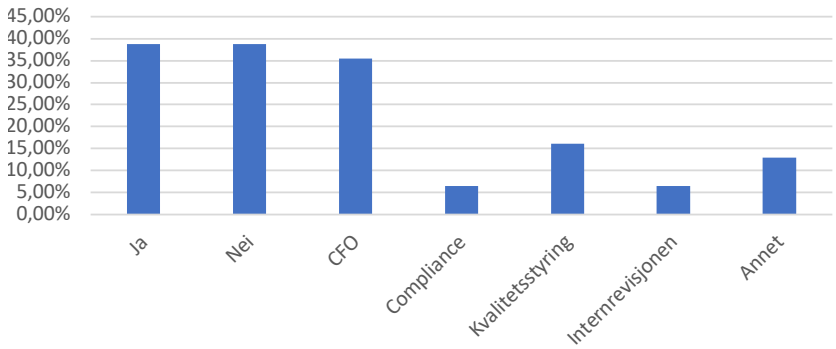
Av figur 2 ser vi at nesten 39 prosent svarer at de har organisert seg slik at risikostyringen ivaretas av en egen CRO-funksjon. Dette er en betydelig økning sammenlignet med en undersøkelse blant nordiske foretak i 2011, hvor 12 prosent svarte at de har en egen CRO-funksjon (Lundqvist, 2014).

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

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

Figur 1

Figur 2



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

I 6,5 % av tilfellene utføres risikostyring av internrevisjon

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

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

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

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

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

Figur 3

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

Hensiktsmessig organisering

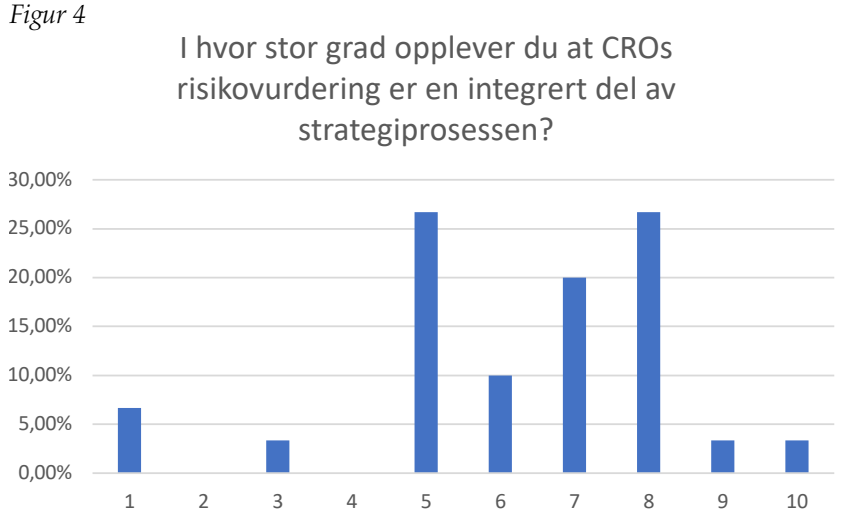
En ting er hvordan risikostyringsfunksjonen formelt er organisert, noe annet om den oppleves som hensiktsmessig av de som jobber med dette. Så hvordan opplever CRO og andre med CRO-lignende funksjon organiseringens hensiktsmessighet? Nærmere 75 prosent av respondentene har svart 7 eller høyere (ut av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

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

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

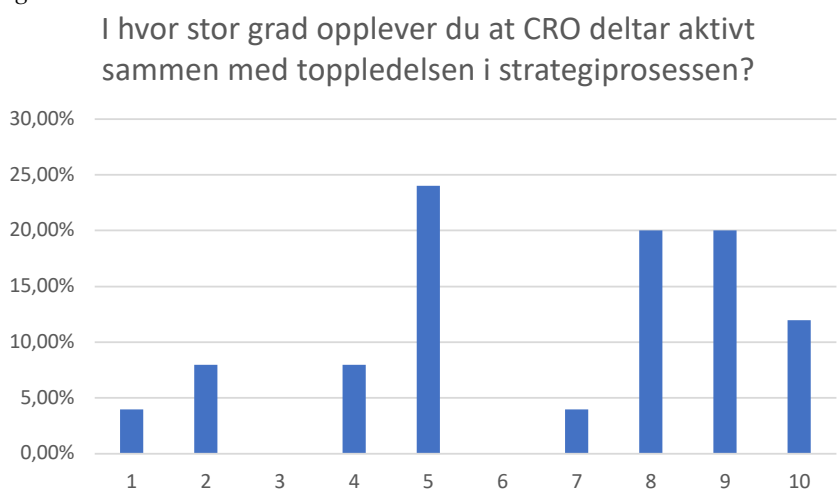
I gjennomsnitt ligger våre svar i figur 4 med feilmargin i et intervall mellom [5,0 – 6,9]. Dette tyder på at risikostyringsfunksjonen er relativt godt involvert i selskapenes strategiprosesser. Bare om lag 10 prosent av respondentene svarer at de i liten grad er en integrert del av strategiprosessen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

Figur 4



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

Figur 5



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

..Men brukes ikke som en aktiv rådgiver i strategiprosessene

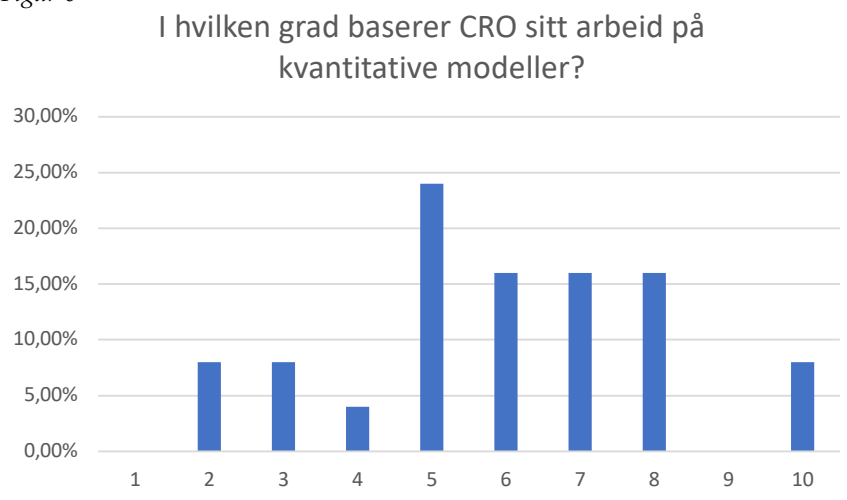
Når vi spør om de opplever at CRO deltar aktivt sammen med toppledelsen i strategiarbeidet ligger gjennomsnittet blant våre respondenter på 5,5 (se figur 5). Dette tyder på at CRO/leder for risikostyringsfunksjonen synes å bli hørt og deltar aktivt i strategiprosessen i større grad enn hva organiseringen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

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

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

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

Figur 6



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

Anbefalinger for videre undersøkelser

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

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

Konklusjon

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

Oppdatert veileder for risikostyringsfunksjonen

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

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

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

In my opinion

Internal Audit by Any Other Name

BLOGG BY MIKE JACKA - OCTOBER 23, 2018

Is "Internal Audit" the right name for what we do?

Actually, before I get started on this one, let me make a confession. I'm not sure where I really stand on this. Part of the reason I am putting this particular blog post together is to help me think it through. So, don't hold me to anything here. Unless you agree with me. Then feel free to give me credit. Unless you really disagree. Then I never really meant it. Unless…well, you see my dilemma.

Why do we continue to call ourselves "Internal Audit"?

Here's the problem. Internal audit means something important to us. We know the history of the profession, the great strides that have been made, and the evolving nature of our work that is all a part of the title "internal audit.". As a profession – as "internal auditors" – we have embraced the need to provide value, to be a partner with the business, and do all we can to help organizations achieve their objectives.

The history and related branding that comes with the name "internal audit" is not trivial and should not be shredded and disposed of like ten-year-old workpapers.

However, no matter how much we try to change perceptions, "internal audit" will continue to mean something else to a significant portion of our customers. The reason it fails with so many is that it emphasizes two important points that, in today's world, our clients don't understand, don't think is all that important, and/or don't want to hear.

Start with the word "internal." We feel it is an important part of our name because it immediately shows that our department is internal to the organization. We proudly point out, just by the use of the word, that we are partners with the business. But that is a concept that few of our customers understand. They don't understand the nuance of our department being internal, and they do not understand the importance of that relationship. (Part of this is all a marketing thing – helping customers understand who we are. I've talked about that before, and will probably talk about it in the future. But now is not the time.)

And then there is that second word – audit. Face it, we even try to shy away from it. That's part of the reason we no longer refer to clients and customers as "auditees". We also speak less and less about doing audit work, instead talking about assurance, advisory, and consulting. Nary an "audit" to be seen. But, as much as we try to skirt around the word, it is right there in our name and even in our job titles. Auditor, junior auditor, auditor-in-charge, audit manager, audit director, Chief Audit Executive – no one, not even the audit department, seems to be able to get over that hurdle.

So, what is the solution?

(Quick story: This reminds of years ago when all the Personnel departments started calling themselves Human Resources. Our little group in Phoenix started thinking about what we might call our department. Someone came up with Human Product Review. We quickly dismissed this when it looked like it meant it was our job to ensure restrooms worked correctly. The discussion died at that point.)

Some departments now call themselves "Audit Services." That's a good start. It emphasizes that there is a broader range of services beyond audit work that our department can provide. Of course, you will note that one of the important hallmarks of our profession – being internal to the organization – disappears with this title. And the biggest stumbling block still exists – continued use of the "A" word.

Further, any group I have worked with who uses the Audit Services sobriquet is still focused on basic audit work. In other words, the focus for people using the name Audit Services still tends to be on doing basic audit work. Few (at least few that I have had experience with) are exploring the wide range of services that internal audit can provide. The new name is

Foto: Shutterstock

promising much more than those departments are delivering. (If you are an exception – if you use Audit Services and you truly offer a wide range of service – I apologize and beg you to share your story.)

And I've seen other names. But I've never really seen one that resonated or revealed an audit department doing much more than it ever had in the past.

So, let me throw out an idea. I've gone back to the mission as spelled out in the IPPF. "To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight." (Let me quickly note that I do not believe the title "Internal Audit" properly reflects that mission. Again, I keep waffling on what the right answer is.)

And, somewhere in that mission I came up with the title "Internal Assurance Services."

I don't know. I don't know if it is better. I don't know if it stinks. I can't tell if I really like it or not. In fact, the more times I read it, the less much I like it. I am firmly convinced the profession needs a rebranding, but is "Internal Assurance Services" the way to go? And does this just represent another conglomeration of words that would mean something to us and nothing to anyone else?

Part of the problem is we can call ourselves anything we want – Internal Audit, Audit Services, Internal Assurance Services, Fred and Ethel's Grand Audit Emporium – and it won't make a hint of difference if the department doesn't embrace change. An Internal Audit department by any other name would smell as sweet, stinky, or ineffective.

But, the act of naming provides power. And it may be time we evoked new powers with a new name.

Again, I apologize because you are literally seeing me think (type) about this one out loud. But I sincerely believe this is important – it is a necessary conversation if we are really going to let internal audit provide the value that is possible.

Let me know your thoughts. Do we need a change? If so, what would that change be? And where do we go from here?

This blog is reprinted with permission from the website of Internal Auditor (IIA online), published by the Institute of Internal Auditors, Inc., www.theiia.org
Denne blogg ble først utgitt på websiden til Internal Auditor:
https://iaonline.theiia.org/blogs/jacka/2018/Pages/Internal-Audit-by-Any-Other-Name.aspx

Grenseløse digitale tjenester – hvordan få kontroll på risikoen?

I denne artikkelen vil jeg først ta for meg en beskrivelse av den nye digitale hverdagen og det endrede risikobildet som er nå vår virkelighet. Dette er et risikobilde som i stor grad påvirkes av økt bruk av tjenesteutsetting og tjenestekjøp. For å møte disse utfordringer er det viktigste å ha forståelse for kompleksiteten i de databehandlingsprosessene man har.

AV HANS CHRISTIAN PRETORIUS
Executive Director, KPMG

Utvikling i digitale tjenester – hva skjer med kontroll?

Digitalisering gjør verden stadig mindre. Teknologi og infrastruktur blir stadig mer sammenflettet og selskaper knyttes tettere sammen gjennom ulike digitale løsninger. Denne utviklingen, som skaper nye mulighetsrom, fører også med seg nye utfordringer for den enkelte organisasjon eller selskap. Den stadig økende bruk av digitale tjenester innebærer blant annet at brukere blir mer mobile og bruken av skybaserte tjenester øker. Denne utviklingen gir fordeler, men fører også til økt kompleksitet ved at data og applikasjoner blir distribuert til flere enheter og lokasjoner, og således øker avhengighet til ulike tredjeparter. Risikoen øker for at feilkilder ikke oppdages hos virksomheten når deres informasjonsverdier strekker seg ut over egen virksomhet. I dette landskapet finnes nye typer risikoer som må tas stilling til. Grenser hviskes ut og avhengigheten av de ulike IKT systemene gjør selskaper sårbare. Hvordan kan vi møte slike utfordringer i en kontrollkontekst?

Metodikk for sikkerhetsstyring og risikovurdering har hvilt på forestillingen om tydelig avgrensning, kontroll og ansvar. Man har hatt som utgangspunkt at ulike risikoer må oversettes til kontrollerbare størrelser, og noen må eie risikoen. Hva om de nye digitale systemene og deres sårbarheter er grenseløse, eller hva om ingen eier dem? Dette kan være sårbarheter som er ukjente av flere årsaker; de kan være ignorert, glemt, aldri tenkt på, umulig å identifisere, feiloppfattet eller underestimert.

Det nye risikobildet

Gjennom de siste årene har flere offentlige og private bedrifter opplevd hendelser hvor man av ulike årsaker har endt opp i en situasjon hvor eksterne aktører har fått tilgang til bedriftssensitiv informasjon. Rotårsaksanalysen har stort sett kommet frem til samme konklusjon ved hendelsene. I mange av tilfellene lå ikke sårbarheten hos organisasjonen selv, men andre steder i verdikjeden og ofte utenfor organisasjonens definerte scope for systemgrenser og risikoanalyser. Sårbarheten som ble utnyttet for å få tilgang til data var ukjent for beslutningstagere og risikoeiere.

> Nye utfordringer hvor de «gamle» definerte systemgrensene ikke lenger eksisterer krever ny tenkning og nye tilnærminger til risiko og sårbarhet.

Akademia har de siste årene fokusert på at man må anerkjenne de nye risikoene gjennom å godta at nåværende risikotilnærminger kan komme til kort. Denne type utfordringer, hvor de «gamle» definerte systemgrensene ikke lenger eksisterer krever ny tenkning og nye tilnærminger til risiko og sårbarhet. Man må rette oppmerksomheten mot komplekse landskap av risiko, som involverer flere systemer som kan generere, overføre og omplassere risiko. Man må åpne for at scenarier griper inn i hverandre – med muligheter for overføring og eskalering. Dette kan defineres som et «sårbarhets- og trussellandskap». Et landskap som involverer flere systemer i samspill. Stadig flere peker nå på perspektiver som kan utfordre dagens risikoerkjennelse. Et sentral spørsmål er hvordan man kan hjelpe risikoanalytikere og beslutningstakere til å se de skjulte, dynamiske truslene og kompleksiteten i dem.

Nyere forskning har sett på denne utfordringen i et samfunnsperspektiv. Man har sett på hvordan man kan sette sammen sektororienterte trusselbilder til større bilder som kan gjenspeile koblinger og avhengigheter mellom sektorer og dermed også få frem underliggende koblinger og sårbarheter. Forskning har vist at denne type komplekse risikobilder på tvers av sektorer ikke normalt fanges opp. Det er derfor et behov for å stille flere spørsmål omkring hvilke uforutsette hen-

delser som kan inntre som følge av dagens tette digitale koblinger.

Så hvordan treffer denne problemstillingen den enkelte organisasjons evne til å kunne oppdage og håndtere egen risiko? Et eksempel er hvordan dataviruset NoPetya medførte at selskapet Mærsk fikk et faktisk tap på mellom 250 og 300 millioner dollar som følge av virusangrepet. Mærsk har tidligere fortalt at skadevaren ble distribuert gjennom en programvare kalt MeDoc, som blir brukt for å levere skattemeldinger i Ukraina. Det er ikke kjent i hvilken grad selskapet faktisk hadde fanget opp avhengigheten mellom et enkelt IT system i Ukraina og selskapets samlede logistikksystem, men eksemplet illustrerer hvilke konsekvenser denne type avhengigheter kan ha.

Tjenesteutsetting og tjenestekjøp

Økt digitalisering utfordrer de tradisjonelle forutsetningene rundt kontroll og ansvar. Digitale tjenester er ikke lenger en plattform som eies og forvaltes av organisasjonen selv. Det er en økende trend at private og offentlige virksomheter velger å tjenesteutsette hele eller deler av sin IKT portefølje. Ifølge Statistisk sentralbyrå (SSB) har andelen norske virksomheter med ti eller flere ansatte som kjøper skytjenester, økt fra 40 til 48 prosent bare fra 2016 til 2017. Tjenesteutsetting, inkludert skytjenester, er av de mest betydningsfulle trendene innen digitaliseringen av samfunnet. Digitalisering er en viktig faktor for at organisasjoner skal sikre nødvendig innovasjon og konkurransekraft. Tjenesteutsetting er også ett av virkemidlene for å holde følge med teknologiutviklingen, men med denne utviklingen kommer også utfordringen knyttet til å ha oversikt over risikoene de allerede komplekse verdikjeder innfører.

En annen trend som øker kompleksiteten ytterligere, er hvordan markedet i større grad tilbyr tjenestekjøp. Tjenester som før ble levert av en intern infrastruktur, blir nå levert som tjenester. Tjenester som gjerne tilbys som virtuelle skytjenester tilgjengeliggjort over internett. Dette gjør at den gamle «systemgrensen» blir visket ut og man får en situasjon hvor man i stor grad arver risiko fra sine ulike partnere og underleverandører. I dette markedet ser man ofte at kontrakter som regulerer ulike IT-tjenestekjøp stiller krav til opptid for å sikre stabile leveranse. Gjennom ulike kontrakter stilles det krav til for eksempel opptid på 99.75%. Kontrakten vil også ofte regulere ulike sanksjoner som inntreffer hvis det kontraktfestede oppetidskravet ikke innfris. Til tross for dette inneholder kontrakten veldig sjelden faktiske krav til hvordan leverandørens infrastruktur skal understøtte oppetidskravet. Dette medfører i ytterste konsekvens at underleverandøren står fritt til å ta så mye risiko de ønsker for å levere på kontraktens oppetidskrav.

> Vil det i dette fremtidige digitale landskapet være mulig å definere en systemgrense? Det korte svaret er nei.

Vil det i dette fremtidige digitale landskapet være mulig å definere en systemgrense? Det korte svaret er nei.

Vil det i dette fremtidige digitale landskapet være mulig å definere en systemgrense? En ramme som historisk sett er brukt for å plassere ansvaret for risikoaksept. Jeg tror at svaret på spørsmålet er nei. Man vil ikke på samme måte som tidligere kunne definere tydelige systemgrenser som definerer både ansvar men også omfanget av risikoaksept. Tidligere har risikometodikk definert løsningen gjennom en grundige verdi- og risikovurderinger, som i sin tur danner grunnlag for å etablere de riktige tiltakene. Utfordringen kommer når man ikke er i stand til å forstå de ulike IKT avhengighetene som visker ut de ulike grensene mellom tjenester og systemer.

Prosesskartlegging

For at risikovurdering faktisk skal kunne vurderes som relevant og korrekt må man evaluere hvordan omfang og scope er definert og hvordan denne prosessen har blitt gjennomført. Det er kritisk at det gjennomføres en god prosess for å identifisere og kartlegge leveranser, verdikjeder, funksjoner og ressurser som kan ha innvirkning på risiko og valg av risikoreduserende tiltak i forbindelse med beskyttelse av virksomhetens IKT-miljø og tjenesteleveransen.

En fremtidig tilnærming av den «grenseløse digitale infrastrukturen» vil kreve en dynamisk tilnærming. Det å kjenne sin egen virksomhet er viktig for å drive effektivt og levere gode tjenester. Dersom virksomheten ikke har identifisert, prioritert og satt fokus på å beskytte sine viktigste prosesser og funksjoner, kan mange av de viktigste verdiene og understøttende ressurser være eksponert for aktører med onde hensikter eller utilsiktede hendelser. Dersom en virksomhet ikke har oversikt over hele verdikjeden for sine viktigste leveranser kan enkelte deler være godt sikret, mens andre vitale deler kan være åpent eksponert og sårbare for tilfeldige og målrettede angrep. I tillegg til sikring av konfidensialitet og integritet, vil det for de fleste virksomheter være like viktig å ivareta behovet for tilgjengelighet av sine kritiske leveranser.

Konklusjon

En fremtidig løpende og dynamisk kartlegging av leveranser og tjenester vil ha som mål at viktige verdikjeder, informasjon og avhengigheter blir kartlagt og prioritert. Kartlegging må også inkludere sikkerhetsdesign, soneinndeling, tilgangsstyring, konfigurasjon, logging og sikkerhetsovervåkning. Det er viktig å hensynta alle komponenter som vil påvirke hvordan risiko kan «bevege» seg mellom ulike digitale løsninger og tjenester. I tillegg må man se på avhengigheter til leveranser og tjenester fra samarbeidspartnere, tjenesteleverandører eller underleverandører.

Kunnskapen om leveranser og verdikjeder må forvaltes dynamisk over tid, noe som kan være krevende i en hektisk hverdag. Men tiden der kunnskap lagres i permer er forbi, og det krever at det fokuseres på digitalisering og automatisering for å sikre et løpende bilde av faktisk risiko.

[1] *Tor Olav Grøtan SINTEF: New Strains of Society: Hidden, Dynamic ad emergent Vulnerabilitie*

Smil – Du har blitt identifisert!

Hvordan er det å leve i en GDPR-fri sone? Les mer om hvordan Kina og enkelte andre land tar i bruk overvåkningsteknologi og hvilke muligheter som åpner seg når personvernet blir underordnet.

AV ESA LEPORANTA
Operational Risk Officer, IT & Security, Group Risk, DNB Bank ASA

AV MARIT TRODAL
Prosjektleder, IIA Norge

I en videregående skole i Hangzhou i Kina gjenkjenner kameraene elevens ansikt og overvåker elevens ansiktsuttrykk og stilling. I denne skolen med tusen elever kan man låne bøker, kjøpe snacks og kontrollere klasserom ved hjelp av ansiktsgjenkjenning. I klasserommene henger et kamera som tar bilder av elever hvert 30. sekund mens undervisningen pågår. Kameraet er koblet til en database som inneholder bilder av alle skolens elever. Kameraet registrerer i tillegg elevens bevegelser og leverer all informasjonen til læreren. Læreren ser alt.

Da systemet ble presentert for allmenheten førte det til opprør i sosiale medier. Skolens rektor forsvarer imidlertid systemet og mener at media ikke har forstått bruksområdet. Ifølge rektoren ønsker skolen å få bedre forståelse av hvordan elevene oppfører seg i skolen og vil benytte systemet for å forbedre kvaliteten i undervisningen. Senere innrømmer skolens assisterende rektor at det også er et poengsystem knyttet til hvordan elever oppfører seg i skolen. Selv om skolen ikke samler bilder av elevene, vil dårlig oppførsel dokumentert via kamera gi effekt på elevens karakterer.

Jianq Qi går i første klasse og sier at han ikke synes systemet i skolen er skremmende. Ifølge Jianq vil kameraene ikke påvirke hans oppførsel; Så lenge jeg oppfører meg som forventet vil det ikke påvirke meg i det hele tatt.[1]

Nye teknologiske løsninger gjør det mulig å overvåke mennesker med en helt ny type presisjon. Ifølge South China Morning Post i Hongkong som rapporterte om dette først, har kineserne tatt i bruk droner med kameraer som er så tilnærmet lik ekte duer at det er nærmest umulig å skille dem fra vanlige fugler. Dronefuglene er nesten lydløse og kan etterligne 90 % av duers bevegelser slik at ekte duer fra tid til annen flyr ved siden av dronedueene. Bruken av droner er konsentrert til Xinjiang, en region hvor den islamske uigur-minoriteten utgjør den største befolkningsgruppen med rundt 11 millioner mennesker. Kina har fått mye kritikk internasjonalt for sin håndtering og påståtte undertrykkelse av uigurene. Det hevdes fra diverse hold at uigurene lever under fullstendig kontroll og overvåkes til enhver tid. Kinesiske myndigheter har i tillegg satt opp såkalte omskoleringsleirer hvor en FN-komité anslår at opptil en million uigurer er internert[2].

Professor Lauri Paltemaa i

Spiondue. For detaljer, se referansen til Daily Mail [3]

Universitet i Åbo tror at styring av mennesker ved overvåking av deres oppførsel kan medføre at mennesker begynner å oppføre seg annerledes. Hvis du en dag ikke får en billett til tunnelbanen etter å ha skrevet en negativ artikkel i sosiale medier, så vil det påvirke hvordan du oppfører deg fremover.[4]

Kineserne har lang erfaring med kontroll, men er dette bare noe som skjer i Kina eller skjer det også i andre steder i verden? Overvåking av mennesker ved bruk av kunstig intelligens kan snart bli tilgjengelig også hos våre naboer i Norden. Ansiktsdekkende slør blir forbudt eller er forbudt i land som Belgia, Frankrike og Østerrike. Ifølge eksperter kan dette delvis knyttes til bruk av ny teknologi. Ansikts¬gjenkjenning blir også en viktig funksjon i nye forbrukerprodukter. Apple iPhone X vil bare åpne seg hvis den gjenkjenner eierens ansikt. Sonys legendariske robothund Aibo gjør et comeback. Nå gjenkjenner den også sin vert.

Ansiktsgjenkjennelsesalgoritmer er allerede flinkere enn vi mennesker. Det russiske systemet FindFace har en treffrate på 99,9 prosent, men den beste applikasjonen er utviklet i Kina. Nylig arresterte kinesiske myndigheter en kriminell på konsert med 50 000 personer til stede. De brukte et ansiktsgjenkjenningssystem.
Det tok også bare 7 minutter å lokalisere og pågripe BBC reporter og Beijing-korrespondent John Sudworth i begynnelsen av 2018. Dette var et planlagt stunt for å illustrere effektivitet i det kinesiske overvåkningssystemet – og demonstrere makten til myndighetene.

Kina hadde ved inngangen

Smart specs

til året mer enn 170 millioner overvåkningskameraer og det er anslått at dette antallet vil tredobles innen 2020. Det gjør Kina til verdens største nettverk av CCTV-kameraer. Ansiktsgjenkjennings-systemer har blitt tatt i bruk flere og flere steder i Kina. De finnes i kjøpesentre, i banker, i automater og til og med i såkalte 'smart specs. 'Smart specs' er briller som gir kinesiske politistyrker mulighet til å identifisere potensielt mistenkte i folkemengder ved bruk av ansiktsgjenkjenning matchet opp mot et dataregister.

Utviklingen går raskt og det siste nye er teknologi som kan gjenkjenne personer basert på kroppsfasong og måten de går på, selv om de har ryggen til kamera og er opptil 50 meter unna kameraet. Denne teknologien er allerede tatt i bruk i Beijing og Shanghai. Tilgangen til persondata gir også myndighetene tilgang til å ekstrahere enormt mye informasjon om personer, med det mål å bidra til at politiet kan utføre sine oppgaver mer effektivt, sikre harmoni og sosial kontroll.

Alle våre Facebook-likes og Google-søk gir et overraskende klart bilde av våre preferanser. Den enorme mengden biometriske data i ansiktet vårt truer med å ta bort all anonymitet og personvern. Slik Google sin tidligere CEO Eric Schmidt en gang spådde, blir identiteten vår den mest verdifulle digitale eiendelen vi har i fremtiden.[5]

1 https://yle.fi/uutiset/3-10296993
2 https://www.bbc.com/news/world-asia-china-45474279
3 https://www.dailymail.co.uk/sciencetech/article-5882159/China-secretly-developing-army-robot-SPY-doves.html
4 https://yle.fi/uutiset/3-10367198

Rap i Kina

Et moderne fenomen i Kina er kinesisk rap og hip hop. I fjor sommer ble det gjennomført en sangkonkurranse, The Rap of China. Konkurransen skapte rundt 2.7 milliarder visninger på online plattformen iQiyi og gjorde en rekke unge deltakere til stjerner i løpet av 12 episoder. Med den enorme popularitet til enkelte av disse stjernene begynte også kommunistpartiet å lytte nærmere til tekstene. Er de vulgære? Bruker de stygge ord? Blir det for mye gangster og lite moral? Man ville ikke ha tekster som kunne inspirere til motstand mot regimet.

Siden han ble utnevnt i 2013 har President Xi Jinping pushet for mer fokus på tradisjonelle konfutsianske verdier og moralske retningslinjer. Som et ledd i prosessen med å nå ut til ungdommen med patriotiske budskap rekrutterte kommunistpartiets ungdomsorganisasjon unge rappere og fikk blant annet lansert låten 'Dette er vår generasjon', hvor rapperne deriblant sang at «jeg hadde aldri forestilt meg for 20 år siden at Hangzhou ville være vertskap for G20…

En av de andre deltakerne fra The Rap of China som fikk stjernestatus var Sun Bayi. Mens hans tidligere låter tok for seg det man kan kalle klassiske temaer innen rap – eksempelvis dyre biler, damer, penger og champagne, fikk singelen "Brilliant China" et mer regimevennlig preg. Sangen åpner med "Alle vet at formålet til det kinesiske kommunistpartiet er å skape glede for sitt folk og storhet for nasjonen." Uvanlig lite gangster for vestlige ører, men Sun Bayi hevder at kinesisk rap ikke skal kopiere vestlig musikk men ha sitt eget unike uttrykk.

Selv-sensur er blitt vanligere etter hvert som myndighetene har slått ned på musikere som ikke bidrar til sosial harmoni. Men det er fortsatt muligheter for dem som er fleksible nok til å tilpasse seg, sier Sun Quan, en rapper som går ved kunstnernavnet Falao. Han rydder i sine egne tekster og tar ut vulgariteter, sikrer at han bruker ordentlig språk samtidig som han forteller historien han ønsker å formidle, hevder han. Utfordringen ligger i å unngå å tråkke over den røde streken….

Kilder:
https://qz.com/1183806/chinese-rappers-fearful-of-authorities-are-cleaning-up-their-lyrics/
https://www.bbc.com/news/blogs-china-blog-41236746
https://edition.cnn.com/2018/03/29/asia/hip-hop-china-intl/index.html

Mørketallsundersøkelsen 2018

For. 11. gang har Næringslivets sikkerhetsråd (NSR) kartlagt sikkerhetstilstanden hos over 1500 virksomheter i privat og offentlig sektor.

Mørketallsundersøkelsen har en sentral plass i organisasjonenes opplysnings- og informasjonsstrategi – og gir et unikt innblikk i norske virksomheters holdninger knyttet til digital sikkerhet, kunnskap, utfordringer, erfaringer, strategier og tiltak knyttet til risikovurdering, forståelse, forebygging og beredskap. Årets Mørketallsundersøkelse bekrefter at visse tiltak fungerer, men at vi fortsatt har behov for arenaer hvor virksomheter kan dele oppdatert kunnskap og erfaringer.

Styringssystemer gir dramatisk bedre deteksjonsevne

6 av 10 virksomheter har et styringssystem eller rammeverk for informasjonssikkerhet, på samme nivå som sist undersøkelse i 2016. Hos virksomheter med over 100 ansatte gjelder dette 8 av 10. Av de som har rammeverk eller styringssystem, opplever 9 av 10 at dette etterleves i virksomheten.

> - Det er altfor mye snakk om uflaks og tilfeldigheter, mener NSR-direktør Jack Fischer Eriksen.

- Den virkelig gode nyheten er at Mørketallsundersøkelsen bekrefter at de som har implementert rammeverk og styringssystemer, og dermed evner å drive et systematisk og forebyggende sikkerhetsarbeid, i mye større grad klarer å identifisere og detektere sårbarheter, trusler og hendelser. Dermed kan de raskere iverksette forebyggende og konsekvensreduserende tiltak, sier Jack Fischer Eriksen, direktør i NSR.

Norsk sikkerhetsnaivitet

Men, Mørketallsundersøkelsen viser også at norske virksomheter har liten oversikt over kostnader og tap som følger i kjølvannet av sikkerhetshendelser. Bare blant de som har deltatt i undersøkelsen, og som klarer å fastslå en kostnad, utgjør dette nesten 30 millioner i 2017. Dette gir et estimat på 1,3 milliarder blant norske virksomheter alene. I tillegg vil tap i form av mistede kontrakter, et svekket omdømme og andre immaterielle skader få en negativ effekt på bunnlinja.

- Norske virksomheters naivitet er fremdeles påfallende stor når det kommer til konsekvensen av å ikke sikre sine verdier og leverandørkjeder. Når samtlige respondenter svarer at de ikke har tapt forretningshemmeligheter gjennom informasjonstyveri og spionasje, kan man jo spørre seg om dette skyldes manglende kunnskap og deteksjonsevne, undrer direktøren.

Mer phishing, hacking og bedrageri

Når det kommer til hendelser de har vært utsatt for, er de vanligste virus og malwareinfeksjoner (21 prosent), phishing eller annen sosial manipulering (18 prosent) og forsøk på datainnbrudd og hacking (13 prosent).

Sammenlignet med 2016 er det en betydelig økning i andelen virksomheter som utsettes for phishing, hacking, DDos-angrep og bedrageri. Det er en vekker at 67 prosent mener sikkerhetshendelsene skyldtes tilfeldigheter eller uflaks. Det gjelder i noe mindre grad de som har et styringssystem. Sistnevnte gruppe mener i større grad at årsaken til hendelsene skyldtes manglende teknisk kompetanse eller utstyr som gjorde dem ute av stand til å forhindre trusselen.

Andre faktorer som oppgis som årsak til sikkerhetsbrudd er menneskelige feil (55 prosent), mangel på sikkerhetsbevissthet hos ansatte (39 prosent) og

Jack Fischer Eriksen

mangel på etterlevelse av prosesser (28 prosent) eller at prosessene i seg selv har vært utilstrekkelige (20 prosent).

4 av 10 oppdager sikkerhetsbrudd ved en tilfeldighet

Antallet virksomheter som oppdager sikkerhetshendelser ved en tilfeldighet er helt oppe på 40 prosent, veldig likt antallet som detekterer hendelser gjennom rutinemessig intern sikkerhetsmonitorering, på 39 prosent. 31 prosent sier at det ble oppdaget som en følge av negative effekter på virksomheten. Og sjokket har nok vært stort for de 5 prosentene som oppdaget hendelser gjennom varsling fra myndigheter eller politi, for ikke å snakke om de 5 prosentene som måtte lese om det i mediene.

- Sikkerheten er i mindre grad overlatt til tilfeldighetene hos de virksomhetene som har styringssystem. 44 prosent av disse oppdaget sikkerhetsbrudd gjennom rutinemessig monitorering, 30 prosent gjennom andre interne kontroller og revisjoner. 37 prosent av dem gjorde tilfeldige oppdagelser, forteller Fischer Eriksen.

- Merkelig nok sier så å si halvparten (49 prosent) at hendelsen ble oppdaget umiddelbart, eller det ble detektert i løpet av få timer (23 prosent). Her er det tydeligvis mye flaks ute og går, med tanke på

Foto: Shutterstock

at 40 prosent sier oppdagelsen var tilfeldig, smiler han.

Tiltakene reflekterer ikke alltid behovene

I 6 av 10 tilfeller har selskapets ledelse blitt involvert dersom virksomheten har blitt utsatt for sikkerhetshendelser, mens styret har blitt varslet og involvert i 3 av 10 tilfeller. Kun 2 av 10 mener det har påført virksomheten økonomiske tap, og under 1 av 10 melder om organisasjonsendringer som følge av sikkerhetsbrudd.

Når det kommer til gjennomføring av tiltak som en konsekvens av sikkerhetshendelser, sier nesten halvparten (47 prosent) at de da har endret retningslinjer og rutiner. 24 prosent har som en følge investert i nytt sikkerhetsutstyr, mens 22 prosent har strammet inn på kontrollen av eksterne leverandører og konsulenter. 20 prosent har investert i utvikling av sikkerhetsprosesser og etablert sikkerhetsmiljø.

- Når 55 prosent sier at hendelser skyldes menneskelige feil, og 39 prosent mener det er resultat av manglende sikkerhetsbevissthet hos ansatte, burde enda flere virksomheter fokusere på ansattes sikkerhetsforståelse og kompetanse, holdningskampanjer og opplæringsprogrammer. Kun 16 prosent sier at den interne opplæringen har blitt forbedret etter en hendelse, og bare 4 prosent har som en konsekvens ansatt flere kompetente mennesker i eget selskap, påpeker Fischer Eriksen.

Fremgang å spore

- Mørketallsundersøkelsen 2018 viser at det å etablere en systematisert og planmessig tilnærming til sikkerhetsarbeidet gjennom styringssystemer og rammeverk har en positiv effekt. Dette er tiltak som gir økt deteksjonsevne, bedre beredskap og forebygging. Kostnaden ved å en slik proaktiv tilnærming til sikkerhet, er mye lavere enn kostnadene og det potensielle skadeomfanget ved en alvorlig hendelse, understreker direktøren.

I Mørketallsundersøkelsen kommer det samtidig tydelig fram at kunnskapen om trusler og risikoområder generelt sett er altfor lav. Norske virksomheter har verken god nok oversikt over sine verdier eller risikoen de er utsatt for, og dermed heller ikke oversikt over skader og kostnader sikkerhetsbrudd og cyberangrep kan påføre dem.

- Kunnskap og innsikt er helt essensielle innsatsfaktorer for å kunne forebygge hendelser og etablere gode og riktige sikkerhetsmekanismer. Da må det investeres– i lederkompetanse, i virksomhetens egen risiko- og sikkerhetskompetanse, og i programmer som øker bevissthet og kunnskap hos de ansatte, avslutter han.

> Sjokket har nok vært stort for de 5 prosentene som oppdaget hendelser gjennom varsling fra myndigheter eller politi, for ikke å snakke om de 5 prosentene som måtte lese om det i mediene

Superforecasting

Hva kan vi lære av Philip Tetlocks bok – Superforecasting – The Art and Science of Prediction?

AV ESA LEPORANTA
Operational Risk Officer, IT & Security, Operational Risk Management, DNB Bank ASA

Risikoanalyser handler om å predikere fremtidige tap. Derfor anses det som viktig å kjenne til hvilke prosessrelaterte utfordringer det finnes når man skal forutsi fremtiden. Studien til den amerikanske forskeren P. E. Tetlock, som gjennomgås i boken *Superforecasting – The Art and Science of Prediction*, har blitt løftet frem som en snarvei til bedre prognoser. En rask undersøkelse på Internett viser at Tetlocks ideer faktisk har gitt inspirasjon til nye tjenester innen algoritmiske prognoser[1].

I prosjektet sitt, Good Judgment Project, rekrutterte Tetlock og hans kollegaer gjennom Internett 2800 frivillige personer som skulle svare på nesten 500 spørsmål. Ved å benytte offentlige nyhets- og informasjonskilder skulle disse menneskene anslå sannsynligheten for at ulike hendelser oppstår over en periode på flere år. Frivillige ble bedt om å bekrefte eller justere sannsynlighetene sine daglig, inntil spørsmålene utløp på en forhåndsbestemt sluttdato. Det som var overraskende at 2 % av disse frivillige, som ble kalt for *superforecastere*, arbeidet 30 % bedre enn alle andre grupper de ble sammenlignet med, inkludert amerikanske etterretningsanalytikere som hadde tilgang til klassifisert informasjon[2].

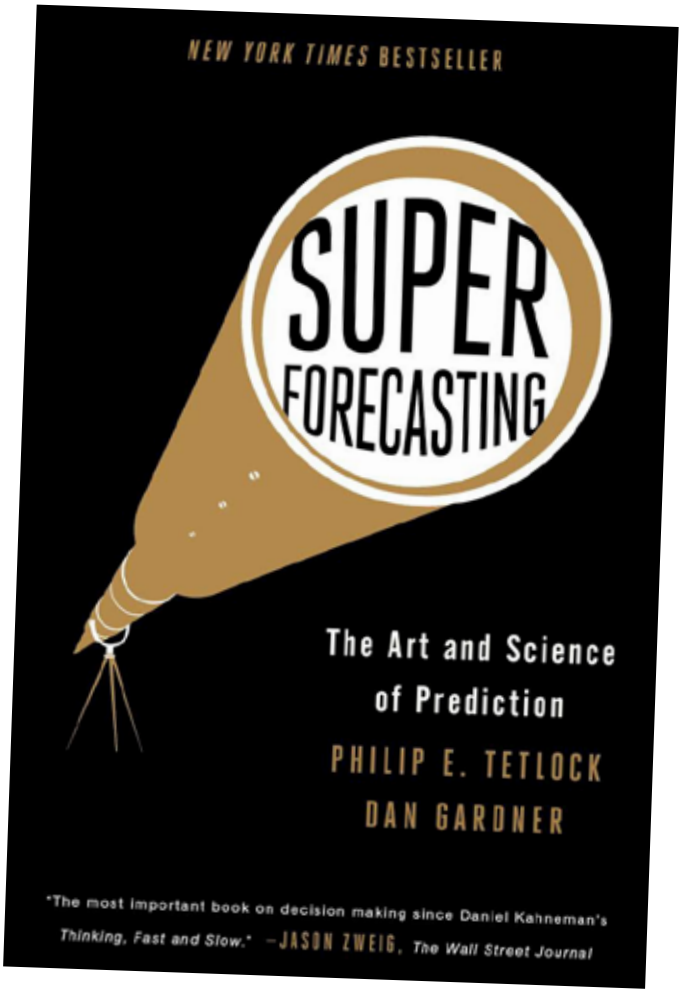
Hovedfunnet i boken er at gjennomsnittekspertens spådommer ofte ikke er bedre enn en tilfeldig gjetning[3]. En av grunnene til dette er at ekspertene ofte overvurderer sine evner. En annen grunn til at vi ofte mislykkes med prognoser er at nesten ingen - inkludert den som presenterer prognosen - har en ide

> Hovedfunnet i boken er at gjennomsnittekspertens spådommer ofte ikke er bedre enn en tilfeldig gjetning.

om hvor ofte det er riktig eller galt det ekspertene gir uttrykk for. Tetlock fant i tillegg ut at de som lykkes bedre med sine prognoser hadde noen bestemte personlige egenskaper; de var mer åpne for å endre sine synspunkter når de fikk presentert ny fakta, men også mer forsiktige og selvkritiske i sine prognoser enn sine mer skråsikre kollegaer[4]. Utover dette var det viktig å ha en god oversikt over sine egne resultater for å vite helt nøyaktig hvor bra man hadde lykkes med sine prognoser. Det var også fordelaktig å dele komplekse spørsmål i flere delspørsmål og skille mellom det som er kjent og ukjent og deretter revurdere sine egne antagelser gjentatte ganger[5]. Ifølge Tetlock var de som var de beste til å forutsi fremtiden ikke genier, men åpne, nysgjerrige mennesker med metodiske vaner, hvilket gir håp for oss alle når det gjelder å kunne forbedre kvaliteten i våre egne prognoser.

I et intervju med journalist Robert Armstrong fra Financial Times[6], ble professor Tetlock i 2016 spurt om hvor optimistisk han var av effekten av sitt arbeid. Tetlock anslo at om ti år vil mellom 10 og 20 prosent av nasjonale etterretningsestimater inneholde et kvantitativt element som baserer seg på nettdugnadsprognoser, hvor et stort antall mennesker utfører en felles oppgave basert på felleskap, medvirkning og selvorganisering. I lys av

[1] *https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance-transformation/us-crunch-time-manual-algorithmic-forecasting-infographic.pdf*
[2] *M.J. Mauboussin & D. Callahan: Credit Suisse - Sharpening Your Forecasting Skills, 28. September 2015*
[3] *https://www.ft.com/content/803a430a-442b-11e6-b22f-79eb4891c97d*
[4] *https://www.svt.se/nyheter/inrikes/forutspa-politik-ett-lockande-men-svarnavigerat-minfalt*
[5] *https://www.nytimes.com/2015/10/18/books/review/mindware-and-superforecasting.html*



dette innspillet er det interessant å lese at prediksjonsevne ifølge Forsvarets forskningsinstitutt (FFI) kan være viktig i forsvarsplanlegging. Slik forskeren Alexander William Beadle[7] i FFI skriver, kan ikke alle ha like rett om hva som skjer i fremtiden. Gitt de store konsekvensene av å ta feil, er det ikke likegyldig hvem beslutningstakere hører på. Utfordringen er at treffsikkerheten til en håndfull personer som har uttalt seg mest om Forsvaret i Norge de siste fem årene imidlertid aldri har blitt målt. Derfor velger vi ofte å høre på løsningen og analysene vi liker best. Ved å måle treffsikkerheten kan vi bli bedre til å avgjøre hvem vi skal høre på. Som et resultat av denne erkjennelsen etablerte FFI et treårig forskningsprosjekt som skal kartlegge det norske forsvars- og sikkerhetspolitiske miljøets evne til å forutsi hendelser. De har en egen webside, som heter https://prediksjonsturnering.ffi.no. Prediksjonsevnen i FFIs turnering måles ved hjelp av en metode, som er en tilpasset versjon av beregningen, som ble benyttet i Tetlocks opprinnelige forskning.

For å hente inspirasjon til slike turneringer, kan fremtidige superforecastere gå gjennom en liste over tips i et vedlegg til boken til Tetlock og Gardner med tittelen Ten Commandments for Aspiring Superforecasters. Faktisk viste resultatene til Tetlock at ved å bruke 60-minutter til en slik opplæring, økte deltakerens nøyaktighet med rundt 10 prosent i løpet av hele det påfølgende året. Innledningsvis kan det tenkes at det ikke er så stor forbedring, men kompensert over tid vil det gi en stor innvirkning for mange organisasjoner.

I dagens samfunn kan det være fristende å tenke at egenskapene til superforecasterne kan automatiseres ved å kode det i algoritmer. Tetlock vurderer dette spørsmålet i boken sin etter å ha diskutert med David Ferrucci, som har utviklet Watson[8]. Ferrucci er enig i at Watson ville ha lite problemer med å svare på et spørsmål som: Hvilke to russiske ledere har byttet jobber de siste fem årene?, men innrømmer at det ville være mye mer krevende å svare på spørsmålet: Vil de samme russiske lederne bytte jobb i de neste fem årene?. Det andre spørsmålet er noe som superforecasterne kan løse ganske enkelt, men så vanskelig at ingen kunstig intelligens på planeten kan håndtere det på en overbevisende måte. Hvorfor er det andre spørsmålet så mye vanskeligere enn det første? For å kunne svare på det andre spørsmålet kreves det at man har etablert en relativt innviklet årsaksmodell av det russiske politiske systemet, de involverte personlighetene og de fremvoksende truslene og mulighetene disse personene sannsynligvis vil møte. Det er ikke nok å skanne en massiv database og triangulere i det mest troverdige svaret[9].

Tetlocks bok viser at gode analytiske vurderinger ikke er avhengige av noen eksterne kompetanseutviklingsprosesser, men av et sett av diskrete ferdigheter og tilnærminger med en klar start og slutt som kan læres og undervises - og enhver virksomhet, som vil forbedre kvaliteten på sine beslutningsprosesser, bør investere i dette gjennom å diskutere og analysere sin treffsikkerhet i virksomhetens nøkkelbeslutninger. Det er ikke lett å lage slike analytiske kraftsentra, men superforecasting og prinsippene rundt det kan være grunnlaget for å hjelpe enkeltpersoner og organisasjoner til å skape mer struktur i hvordan de bruker data for å forutsi fremtiden.

[6] *https://www.ft.com/content/803a430a-442b-11e6-b22f-79eb4891c97d*
[7] *https://forskning.no/krig-og-fred-fremtidsforskning-kronikk/kronikk-er-du-bedre-til-a-forutsi-fremtiden-enn-ekspertene/1161870*
[8] *Watson er et spørsmålssvarende datasystem som er i stand til å svare på spørsmål som stilles i naturlig språk, utviklet i IBMs DeepQA-prosjekt.*
[9] *P.E. Tetlock & D. Gardner: Superforecasting – The Art and Science of Prediction, pp. 21-23*

GDPR – Ready or not, here we come

Ovenstående tittel var også tittel på et innlegg på den nasjonale fagkonferansen i offentlig revisjon, avholdt på Lillestrøm den 23. oktober. Innlegget ble holdt i to-spann av NAVs personvernombud, Anders Holt, og undertegnede. Hensikten var å gi en overordnet status på GDPR og fortelle hva internrevisjonen gjorde våren 2018 for å vurdere hvor langt fra å oppfylle GDPR forordningens krav NAV ville være ved forventet ikrafttredelsesdato ultimo mai 2018.

AV TERJE KLEPP
Revisjonsdirektør, NAV

Det hele starter noen år tilbake. NAV har som mange andre organisasjoner vært underlagt personvernlovgivningen som har eksistert i Norge i en år-rekke. Tidlig i 2016 ble det avdekket at en betrodd medarbeider hadde gjort en rekke uberettigede oppslag i NAVs fagsystemer på personer vedkommende ikke hadde tjenstlig behov for å undersøke. NAV valgte i dette tilfelle å anmelde vedkommende.

På bakgrunn av denne saken valgte Arbeids- og velferdsdirektøren å engasjere et eksternt advokatfirma, som i samarbeid med et revisjonsselskap gjennomførte undersøkelser av blant annet hvordan NAV forholdt seg til regelverket om behandling av personopplysninger. I slutten av oktober 2016 avga disse en omfattende rapport til ledelsen i NAV, som valgte å offentliggjøre hele rapporten.

En av anbefalingene i rapporten var at NAV etablerer et personvernombud. På dette tidspunktet var det kjent hvilke krav som ville komme i GDPR forordningen som var ventet å tre i kraft ca 1,5 år etter at rapporten til NAV ble presentert. Ett av disse kravene var at NAV måtte ansette et personvernombud senest i annet halvår 2018. På bakgrunn av rapportens anbefaling ble arbeidet med å ansette et personvernombud igangsatt, og høsten 2017 hadde NAV ansatt sitt første personvernombud, Anders Holt, som kom fra tilsvarende stilling i Telenor-konsernet.

Internrevisjonen i NAV starter planleggingsarbeidet for kommende kalenderår på høsten. Ett av prosjektene som ble diskutert med ledelsen og vedtatt av Arbeids- og velferdsdirektøren sent i 2017 het; «Implementering av personvernforordningen». Målet for denne revisjonen var å kartlegge hvor langt NAV var kommet med hensyn til implementering av GDPR ved forventet ikrafttredelsesdato 28.05.2018 (denne fristen ble som kjent senere utsatt flere ganger sist til 28.07.2018). Dette revisjonsoppdraget, som vi i kortversjon kalte *«GDPR readiness»*, måtte derfor gjennomføres tidlig i 2018.

Vi startet revisjonsprosjektet vinteren 2018, og i vår oppdragsdefinisjon valgte vi følgende innfallsvinkel; «Internrevisjonen vil i denne revisjonen undersøke om:

- NAV har kartlagt hvilke personopplysninger de har og hvilket formål disse brukes til
- Hjemmel for behandling av personopplysninger er på plass
- Nødvendigheten av personopplysningene er vurdert
- Risikoanalyse for brukers forhold er gjennomført
- Det finnes regler og rutiner for lagring, retting, sletting av personopplysninger
- Det finnes regler og rutiner for innsyn
- Det finnes rutiner for informasjon om rettigheter og plikter til bruker
- Avtaler (eks. databehandleravtaler ol.) er på plass»

Revisjonen ble basert på intervjuer og dokumentgjennomgang, og vi tok sikte på å levere vår revisjonsrapport før sommerferien.

Rapporten ble sendt på høring tidlig i juni, og den endelige revisjonsrapporten ble datert 29. juni 2018. På det tidspunktet var det klart at implementeringstidspunktet for GDPR forordningen hadde blitt utsatt til 6. juli, slik at vår rapport ble sendt til toppledelsen i NAV før reglene trådte i kraft. Fordi Norge fulgte implementeringstidspunktet for EØS land ble ikrafttredelsen ytterligere utsatt til 28. juli, uten at det hadde noen praktisk betydning.

Internrevisjonen hadde en hypotese om at NAV ikke ville klare å oppfylle alle forordningens krav ved implementeringstidspunktet. Denne hypotesen ble da bekreftet gjennom revisjonsarbeidet, og vi trakk følgende hovedkonklusjon i vår rapport: *«Etaten er i gang med forberedelser for å imøtekomme GDPR krav, men arbeidet er ikke helhetlig og systematisk og mye gjenstår. Samtidig er det ikke avsatt nok ressurser til*

arbeidet. Etaten vil ikke etterleve alle sentrale GDPR krav når forordningen trer i kraft.»

Som det fremgår av hovedkonklusjonen hadde NAV iverksatt mye arbeid, og flere av tiltakene ble også nevnt i vår hovedoppsummering hvor vi skrev;

«Følgende er utført:

- Personvernombud er ansatt
- Det er utarbeidet en oversikt over etatens behandlinger av personopplysninger på et overordnet nivå
- Det er gjennomført personvernkonsekvensvurderinger for alle nye systemer, om enn av forskjellig detaljgrad og kvalitet
- Det er laget informasjonspakker for NAV kontaktsenter og NAV kontorene og egen side på Navet (som er NAVs interne intranettside)
- Klageinstansen i Bergen har fått delegert ansvaret for forespørsler om retting og sletting
- Styringsdokumenter for personvern er utarbeidet
- Mal for Databehandleravtaler er oppdatert
- Det er gitt opplæring til flere personer i direktoratet
- Det er opprettet Personvernforum som møteplass og for læring i direktoratet
- Personvernerklæring er publisert på nav.no (NAVs eksterne kilde til informasjon)
- Rutiner for varsling til Datatilsynet og bruker ved brudd på personvernet lages av Sikkerhetsseksjonen og vil være på plass fra 01.08.18

En god del arbeid var altså igangsatt før eller under perioden vi gjennomførte vår revisjon. Imidlertid var det relativt mye arbeid som gjenstod på det tidspunkt vi avga vår revisjonsrapport. De forhold vi valgte å fremheve i vår konklusjon var følgende;

- Vi kommer ikke i mål på alle punkter med implementeringen av GDPR i etaten før fristen 06.07.18
- Prosjekt fase 3 er ennå ikke fullstendig oppbemannet og prosjektet er forsinket
- Det gjenstår å gjøre personvernkonsekvensvurderinger for så å si alle gamle systemer med høy risiko
- Etatens kompetanse på området er mangelfull og det er ikke satt av tilstrekkelige ressurser til arbeidet

Revisjonsrapport - C2018-03

Implementering av personvernforordningen

29. juni 2018

Rapportmottakere:
Yngvar Åsholt, kunnskapsdirektør; Geir Axelsen, økonomi- og styringsdirektør; Anders Holt, Personvernombud; Kjell Hugvik, arbeids- og tjenestedirektør; Torbjørn Larsen, IT-direktør; Kjersti Monland, ytelsesdirektør; Inger-Johanne Stokke, HR-direktør; Hege Turnes, kommunikasjonsdirektør

Kopi:
Sigrun Vågeng, arbeids- og velferdsdirektør

side 1

- Noe testing foregår fortsatt på reelle brukerdata
- Når det gjelder automatisering og sammenstilling av opplysninger på utviklingssiden må GDPR krav ivaretas og det er krevende
- Det er utfordringer med fortolkningen av kravene i det nye regelverket, og dette påvirker spesielt utviklingssiden
- Systematisk opplæringsløp for etaten er ikke på plass
- Etatens arbeid for å imøtekomme GDPR krav er skriftlig dokumentert i varierende grad
- Det synes å mangle en helhetlig koordinering av etatens arbeid, enheter adresserer GDPR separat, noe som ikke er effektivt og innebærer risiko for ulik adressering og tolkning

Ovenstående kan synes som en lang liste med mangler. Det er imidlertid et meget omfattende regelverk som nå er gjeldende. Selv om forordningen ble vedtatt i EU våren 2016, er nok erkjennelsen at de fleste kom sent i gang med arbeidet for å tilpasse seg regelverket, og at det vil være mange andre instanser i Norge som nok opplever å ha mye gjenstående arbeid før alt er på plass, selv mange måneder etter forordningens ikrafttredelse.

Etter at vår rapport ble publisert har NAV satt ekstra ressurser på arbeidet – og også engasjert eksterne konsulenter med spisskompetanse på forordningen. En del av tiltakene vi anbefalte i vår rapport hadde forfall først mot slutten av året. Så selv om det fremdeles er en del gjenstående arbeid når denne artikkelen skrives, vil NAV ved inngangen til 2019 være langt bedre stilt enn da internrevisjonen startet sin gjennomgang av «*GDPR Readiness*».

Enhancing GRC with intelligence

SHAUN REARDON
Senior consultant,
the Transcendent Group

KIM JOHNNY MATHISEN
Branch manager,
the Transcendent Group

Foto: Shutterstock

Shaun's article in SIRK 1/2018 "Why gather intelligence?" illustrated the distinction between intelligence and information and how to deal with the information acquired. This article builds on that introduction and aims to answer the question "How can the use of "intelligence" enhance Governance, Risk and Compliance functions so that the whole benefit is greater than the sum of the parts?

The GRC functions

Are we saying that the Governance, Risk and Compliance functions are not up to the task? Well, each function has immense value when correctly implemented and performed and each should have checks and indicators built-in to signal if anything is not working as intended. They should also allow remediation to take place before bad things happen.

Now, off at a complete tangent. Imagine a person wearing a swimsuit sitting on a motorcycle on a crowded highway and that the person is wearing a helmet. Oil, fuel and tyre pressure are all showing green lights and speed is within the limit. So, the internal rules and expected behaviour are being complied with:

Governance, the person probably considers himself safe.

Risk has been assessed and should he be stopped by the police he will not have broken the law.

Compliance, the person is wearing a helmet and keeping to the speed limit, additionally he has ensured that the motorcycle is in good running order.

So, what's missing? The weather forecast, the state of the motorcycle, the area he is in, the condition of the roads and the accident rate can be considered as intelligence.

Putting them all together gives a totally different perspective. It is useless thinking about all these things when you are lying in your hospital bed. Hindsight is an exact science, intelligence is all about doing informed decisions so that hindsight stays as positive as possible.

The key phrase is "putting them all together…" Analysing and aggregating inputs from different sources can give a completely different perspective and through that the possibility of vastly improved decisions even though each element alone is not telling the whole story.

If we could "glue" together all the small and disparate bits of information from GRC activities then it should be possible to turn hindsight into foresight. If this is expanded further to include all activities within your organization then you must surely be better prepared. For example: Consider a pilot who has an immense array of information coming in from sensors in the engines and avionics. Is this the total picture? What other information might be needed to ensure a safe and successful flight? The cabin crew can

provide Information about the passengers and their disposition which may affect the flight, Information from other aircraft in the vicinity regarding adverse flying conditions may contradict the weather forecast regarding turbulence necessitating a change of altitude. Green lights on the flight deck do not mean that all is well or will continue to be so. The point is that the pilot has to make judgements based on multiple and separate (siloed) information in real time.

For this you do not need a crystal ball or the ability to read the runes. You just need the ability to objectively assess one piece of information in the context of all the other bits of information. Sounds daunting, but hopefully by the end of this piece you will see where we are coming from.

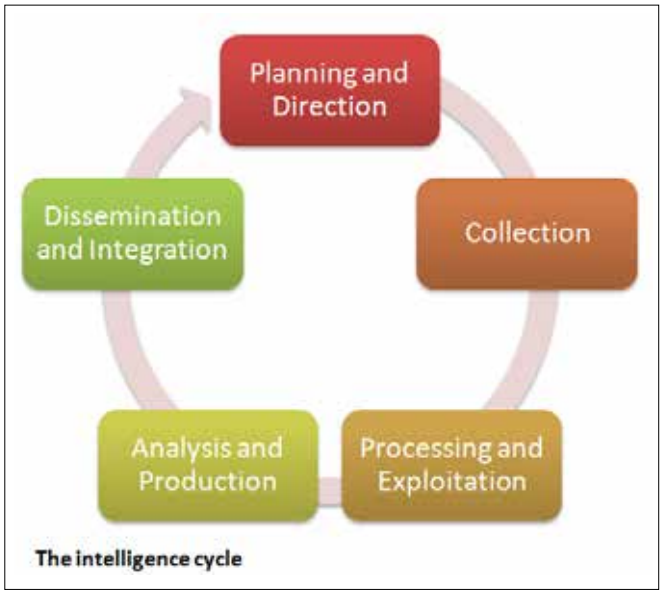
Key concepts

Before we dive in to the detail it is useful just to have an understanding of some key concepts.

Intelligence: This is the product resulting from the collection, evaluation, analysis, integration and interpretation of all available information.

The initial step 'Planning and direction' is key. What are you seeking to achieve, who is directing it and what does success look like?

Sources of Information are virtually unlimited. Open source research, SIEM (Security Information and Event Management), social media, HR records, trade publications, news stories, IT logs, audit results, management reports, trends from threat intelligence, products, people, regulators, exception reporting, vendors… the list goes on. The technical term for sources is "sensors;"



The intelligence cycle

They are collectors, not interpreters of value to you. It is crucial that sensors are assessed to make sure they are applied correctly and collecting data that can be used. At this stage, you define and design your own sensors or adjust the format of the output. We suggest that the best inputs are the raw data not subject to filtering by decision. Filtering may add a degree of bias prior to analysis.

Veracity. Each piece of information is accorded a weight based on the reliability of the source. Is it known, first hand, second hand, rumour or merely an assumption made? Blindly acting on information is a recipe for disaster as in the event of an investigation you would be hard pressed to explain your decisions. Hence ´weighting´ is part of turning information into intelligence.

Legality: The collection and processing of personal data is strictly regulated by the General Data Protection Regulations(GDPR) and its provisions must be strictly adhered to. In a potential event of a data breach you will need to be able to demonstrate to the regulator that you took all necessary technical and organizational steps to prevent it. Some provisions of the GDPR give some leeway in what is collected and why. These include network security and prevention of fraud... Building a suitable intelligence system should support your existing organizational measures and is good evidence to present to the regulator in the event of a breach.

GRC and intelligence - key points

We need to 'glue' our GRC activities together and the following statement summarises our key points:

- Governance is about people
- Risk can be anything
- Compliance is about people
- Intelligence is about everything

Governance is about people

Put simply, governance is about making sure that the organisation (people) follow the direction of management and that important information reaches management and the board. Governance provides the strategy (direction) for the organisation - a place to prosper for people. But there is a problem; governance has a tendency to become rigid and sometimes even a goal in itself. As a consequence, the organization may experience slow decision making, loads of resources

going into meaningless reporting and the feeling of total detachment between C-level and the operational level.

Risk can be anything

To our knowledge it appears organisations attempt to avoid such problems by decentralising decisions whilst trying to understand the overall risk exposure through aggregation of information - from decision makers up to management and board levels. This approach may have a cost, mostly because risk does not come with a clear explanation as to how it should be communicated, and the chances are the C-suite could be looking at something else.

Intelligence indicators from the governance function could be non-conformity reports, results of root cause analysis, staff feedback, whistle blowing submissions, customer complaints etc. No doubt all of these will be considered in due course but here we are talking about immediate action to process and analyse the data in the context of the whole business.

The value of a well conducted risk assessment cannot be overstated and is something that some organisations do well. The downside is that they tend to be ´static points in time´ and focus on controlling risk, based on factors known or anticipated at the time the assessment was conducted. Failure of a control or a "black swan" event leads into incident handling, business continuity management and potentially an investigation.

Sometimes indicators are strewn all across the corporate landscape and it is only when the "I told you so brigade" find them that the pain starts, mainly because they are actually correct. The trick is to collect these little nuggets and constantly compare and contrast them. Each business is different so you have the opportunity to define your own "red flags". One good method is to ask your staff "If you were malicious / dishonest how would you damage or bypass the system? There are no rules or restraints so give free reign to your imagination"

The intelligence system outlined above has five distinct parts which matches quite nicely with the five stages of risk: Identify; Analyse; Evaluate & Rank; Treat and Monitor/ review. Risk underpins almost every activity these days and similar to risk management intelligence allows the determination of probability, but more dynamically. The gathering of intelligence does not require a new system but rather dovetails neatly with your existing framework.

The risk appetite of the organisation may be based on a number of factors such as financial or regulatory but intelligence knows no such bounds. Rather it raises the red flags without taking those pre-set factors into account. Therefore, it supports future decisions not decisions that have already been made.

Compliance is about people

Rules have been set internally or imposed externally as we have seen in the Governance section. Risks have been assessed and treated and now the compliance officer has the responsibility to make sure all is well and that the figurative landmines and tiger traps are avoided. There is an expression used about detecting when things have gone wrong as "indicators of compromise". These indicators could have come from specific events or from an audit but are all post-event. The damage is already done unless you were fortunate enough to nip something in the bud. The question is, was it by luck or judgement? One example might be the exercise of ´management override´. Sometimes this action can be justified but it can an indicator or something more sinister (such as fraud). A questionable action on its own may just mean a disregard for the rules but what about other indicators such as queried expense claims, staff complaints etc. The expression "the signs were there for all to see" offer no comfort when an investigation concludes.

Intelligence is about everything

We see the value of collecting and analysing data from activities that may be siloed for organisational reasons. It may even be that the benefit of such an activity has not been considered. Additionally, opportunities exist to define your own ways of collecting data and to design your own sensors.

Intelligence provides decision support. The techniques described above are "battle tested" throughout the world, affect most people in their daily lives whether they realise it or not, are understandable to most and can be explained in a clear and concise manner.

There is no requirement to initially re-engineer your existing frameworks or to re-train all of your staff. Of course, any necessary organizational learning can be fed back for a policy decision but the day-to-day operation of this system will give "near time" situational awareness in terms of opportunity and threat.

> Governance is about people
>
> Risk can be anything
>
> Compliance is about people
>
> Intelligence is about everything

Det var en gang

FOR 40 ÅR SIDEN – REVISOREN

I Bankrevisoren 3 fra 1978 finner man følgende oppsummering av kjennetegn ved internrevisjonsarbeid under tittelen «Hva er revisjon?!»

«Vi har undersøkt en del revisjonsprogrammer (revisjonshandlinger) og funnet at revisjon er at revisor skal:

1. kontrollere
2. kontrollsummere
3. avstemme
4. sammenligne
5. sammenholde
6. påse
7. følge opp
8. undersøke
9. vurdere
10. utarbeide
11. gjennomgå
12. gjennomlese
13. telle opp

14. sette opp
15. redegjøre for
16. teste
17. sjekke
18. verifisere
19. velge ut
20. ?»

Hvis vi hadde satt opp en tilsvarende liste i dag, ville den blitt veldig annerledes? For egen del må jeg bruke liten tid på punkt 13 i internrevisjonshverdagen! Det jeg derimot savner er «intervjue» – kanskje dette kan erstatte spørsmålstegnet ved pkt. 20?

FOR 20 ÅR SIDEN – «INTERNREVISOR - EN MISVISENDE BETEGNELSE PÅ VÅR PROFESJON?»

På side 28 i denne utgaven av SIRK har vi trykket et innlegg fra USA som tar opp avstanden mellom det vi faktisk gjør og profesjonens betegnelse: Internrevisjon.

Karl H. Sigurdssøn, som i en periode også var sekretær i internrevisor-foreningen, skrev pussig nok om nettopp dette temaet. Han nevner en artikkel av Larry Sawyer i Internal Auditor som foreslår en bedre beskrivelse av henholdsvis internrevisjon og internrevisorer. Sawyer benytter betegnelsene «Performance evaluation» og «performance evaluators». Sigurdssøn legger til:

«Jeg er personlig ikke spesielt fascinert av betegnelsene han bruker, men er helt enig med ham i at det er behov for en klargjøring, både på engelsk og norsk. Det norske begrepet bidrar så visst ikke til forståelsen av hva internrevisorene i dag gjør. Dette er imidlertid ikke noe nytt, begrepet var misvisende den gang undertegnede forrige gang, for 25-30 år siden, var sterkt engasjert i intern revisjon og denne foreningens virksomhet. Jeg lette allerede da etter et mer dekkende begrep, men fant ikke noe bedre.

Utviklingen innen internrevisjonen har imidlertid gjort at betegnelsen har blitt mindre og mindre dekkende for det internrevisjonen i dag representerer. Etter hvert som tiden har gått, har jeg blitt mer og mer i tvil om det å skifte betegnelse er den rette veien å gå. Vi driver revisjon, la oss ikke glemme det. Vi har imidlertid flere verktøy i dag enn tidligere og ofte angriper problemene på en annen måte. Internrevisorene er sterkt opptatt av «internal control». På norsk ofte ufullstendig oversatt til intern kontroll. En mer dekkende oversettelse er etter min mening «styring og intern kontroll». Det er en hovedoppgave for internrevisorene å se etter at bedriftens styringssystemer er adekvate og at virksomhetens retningslinjer etterleves. Det gjelder også lover og retningslinjer gitt av det offentlige. Det siste er nok våre omgivelser klar over, men ikke alltid at vi er sterkt opptatt av styringsproblematikken, altså hvorledes en bedrift overvåker at de mål den har satt seg blir nådd.

Kanskje vil det bidra til en klargjørende utvikling om vi døpte NIRF (Norges Interne Revisorers Forening) om til NISIR – Norsk Institutt for Styring og Intern Revisjon!

Ápropos «internal control» er det interessant å merke seg at våre nærmeste naboer benytter det oversatte begrepet «intern styrning och kontroll».

Martin Stevens

Spill som metode – erfaringer fra forsvarssektoren

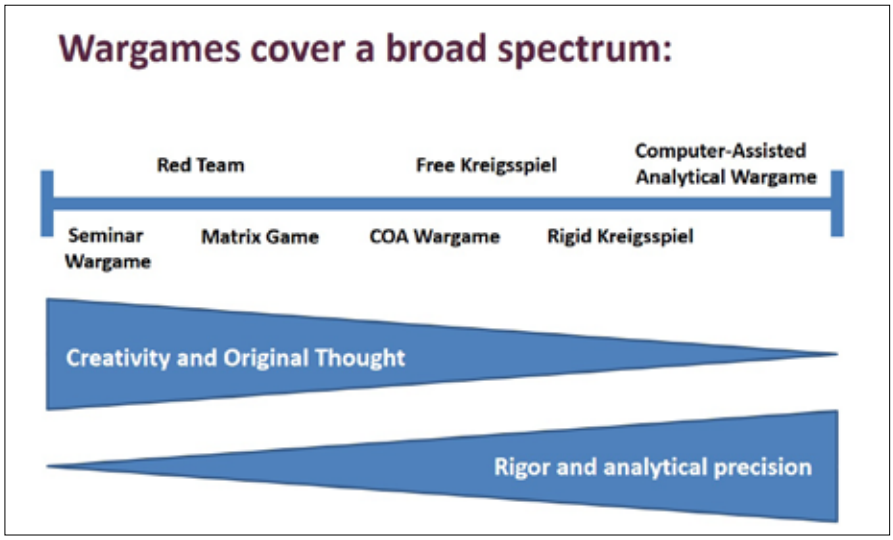
Spill som metode kan brukes til langt mer enn det tradisjonelle krigsspillet man typisk ser for seg. I et spill kan det samles inn data på hvordan aktørene handler og påvirker hverandre. Et utgangspunkt for et spill kan eksempelvis være nye retningslinjer for organisasjonen eller en øvelse av krisehåndtering innenfor sikkerhet. Spill som metode egner seg dermed godt som verktøy også utenfor forsvarssektoren. Forsvarets forskningsinstitutt (FFI) har i en årrekke benyttet spill for å kunne bidra til gode beslutninger og effektiv ressursbruk. FFI deltar også i internasjonale fora der spill diskuteres og er et av landets fremste fagmiljø på dette feltet.

AV HELENE BERG
Forsker, FFI

AV OLA OTTERDAL
Seniorrådgiver,
Forsvarsdepartementet

Bilde fra diskusjonsseminar. Foto: FFI

I denne artikkelen vil vi se spesielt på to spill FFI gjennomførte i 2015 og 2016 på oppdrag fra Forsvarsdepartementet. Begge disse spillene pågikk over flere dager og hadde form som diskusjonsbaserte seminarspill. Nye retningslinjer for investeringer i materiell og i ny bygningsmasse ble testet ut. Dette ga blant annet innsikt i hvor godt retningslinjene bidro til å klargjøre roller, ansvar og myndighet hos sentrale aktører. I tillegg ga spillene mulighet til å se hvordan aktørene opptrådte i ulike situasjoner, samt hvordan deres avgjørelser påvirket gjensidig i ulike situasjoner. Dette ga nyttige innspill til beslutningstakernes videre forbedring av retningslinjene. I denne artikkelen kan



Figur 1: Ulike typer krigsspill

[1] *Figur fra «Wargaming 101 – An introduction to wargaming"», presentasjon gitt av Tom Mouat, Defence Academy of the United Kingdom, under Connections UK 5. September 2017.*

du lese mer om erfaringer fra disse to spillene, bruk av spill som metode generelt og mulighetene for å ta i bruk spill i andre sektorer.

Spill som metode

Ved å sette ordet «spill» i sammenheng med «forsvarssektoren» kan man typisk få assosiasjoner til krigsspill der to motstandere møtes og deres militære kapasiteter flyttes på et kart. Men spill som metode kan benyttes i andre former også. Begrepet «spill» benyttes svært bredt, om aktiviteter i hele spekteret fra enkle diskusjoner (tabletops, seminarspill) til komplekse og tidkrevende datastøttede spill. Disse aktivitetene overlapper også med andre teknikker, som workshops, øvelser, modellering og simulering. Det finnes med andre ord ingen allment omforent definisjon av hva spill er. Likevel er det noen fellestrekk mellom alle aktiviteter vi kan kalle for spill: **Spillere** tar **beslutninger** i en **simulert virkelighet** som beskriver en **felles historie**, og spillerne **deler erfaringer** og identifiserer **læringspunkter for videre arbeid**.

Figur 1 viser ulike spilltyper og anvendelsen av disse. Diskusjonsbaserte spill (til venstre) brukes ofte for å utvikle ny kunnskap, utforske nye problemområder og stimulere til nytenkning. Lenger mot høyre i figuren blir spillene mer komplekse, ofte i form av mer avanserte regelsett, mer komplisert avdømming og en mer realistisk representasjon av den simulerte virkeligheten (for eksempel kart, 3D-modeller eller datamodeller). Robustheten i resultatene fra et spill vil typisk øke jo lenger til høyre i figuren man er.

Slik kan en spilldag se ut

I forsvarssektoren brukes det hvert år over 10 milliarder på investeringer og det er avgjørende at pengene brukes på best mulig måte. FFI gjennomførte i november 2015 et diskusjonsbasert seminarspill med utgangspunkt i opprettelsen av Forsvarsmateriell og behovet det ga for nye og endrede retningslinjer for materiellinvesteringer. I september 2016 ble et tilsvarende spill gjennomført, der tema var retningslinjer for forsvarssektorens investeringsprosess for eiendom, bygg og anlegg (EBA).

ERFARINGER FRA FORSVARSDEPARTEMENTET OG FORSVARSMATERIELL

Morten Ringheim, underdirektør Materiellseksjonen FD III

1. Hvordan opplever du at spill som metode passet til å treffe de aktuelle problemstillingene?
Etter at beslutningen om å etablere etaten Forsvarsmateriell ble tatt i april 2015 var det relativt kort tid til planlegging for etableringen den 1. januar 2016. Det var da viktig å avklare rolle, ansvar og myndighet for den nye etaten i forhold til departementet og Forsvaret. I den forbindelse måtte vi revidere retningslinjer for logistikk og retningslinjer for materiellforvaltning, i tillegg til å utarbeide nye retningslinjer for fremskaffelse av materielle kapasiteter. Etter at vi hadde utarbeidet utkast til nye retningslinjer gjennomførte vi spillet ved FFI der vi fokuserte på roller, ansvar og myndighet mellom de tre aktørene og aktuelle grensesnittutfordringer. Spillet ga oss god innsikt i disse problemstillingene og vi oppdaterte utkastene til retningslinjer og utga disse i forbindelse med etableringen av etaten Forsvarsmateriell.

2. Hva slags effekt eller resultat mener du spillet har gitt?
Spillet ga oss et godt innblikk i samhandlingene mellom etatene og departementet, og de grensesnittutfordringene vil måtte ha spesiell fokus på da vi ferdigstilte retningslinjene. Det ga også muligheten til at aktørene ble bedre kjent med hverandre noe som var med på å bygge tillit og innsikt i hver andres utfordringer.

3. Hvordan ser dere i FD for dere å benytte metoden fremover?
Som resultat av våre gode erfaringer med spillet for å validere utkastene til retningslinjene, valgte departementet å bruke spill som metode i forbindelse med revisjon av retningslinjene for tjenestefeltet eiendom, bygg og anlegg med gode erfaringer. Når vi snart skal gjennomgå de tre retningslinjene på nytt etter at det har gått noen år etter etableringen av Forsvarsmateriell er det sannsynlig at vi vil benytte spill som metode også i denne prosessen.

4. Hvor overførbar mener du spill som metode er til andre statlige virksomheter?
For statlige virksomheter som har utfordringen med roller, ansvar og myndighet, og der grensesnittutfordringer eksisterer, vil spill som metode kunne være et godt virkemiddel til å belyse disse utfordringene.

I begge spillene stod FFI for planlegging, design og analyse. FFI ledet også gjennomføringen av spillene, som blant annet innebar å styre diskusjonene underveis. I begge tilfellene ble det utarbeidet forskjellige case som skulle spilles over flere dager. Casene tjente rollen som spillets scenarioer og var alle fiktive investeringer i materiell eller nye bygg. Hver spillgruppe fikk sitt case og spilte dette i de følgende dagene gjennom hele investeringsløpet – fra idéfase der et nytt behov dukker opp, til materiellet ble tatt i bruk eller bygget sto ferdig. Det ble også utarbeidet hendelser som FFI spilte inn underveis. Dette kunne være alt fra jordskred der et nytt bygg skulle bygges, til manglende ressurser for prosjektleder eller endrede behov i Forsvaret. Sammen dannet casene og hendelsene muligheten til å teste hvorvidt det var uklarheter, uenigheter eller andre mangler i retningslinjene. Formålet var ikke å teste spillerne på hvorvidt de hadde innsikt i styrende dokumenter, retningslinjene og andre relevante dokumenter var dermed tilgjengelige for gruppen slik det ville vært i en normal arbeidssituasjon.

I løpet av spilldagen ble det vekslet mellom arbeid i grupper og i plenum der hver gruppes hovedpunkter ble oppsummert og diskutert. De håndfaste produktene fra spillene var i begge tilfellene presentasjon av hovedfunn på forbedringspunkter for oppdragsgiver samt en FFI-rapport. I tillegg kommer verdien

av å skape en møteplass for diskusjon mellom aktører som arbeider innenfor samme område, men som i tilfellet forsvarssektoren ofte er spredt geografisk til daglig.

Erfaringer

Hovedfordelen med å benytte spill i eksempelvis testing av nye retningslinjer er dynamikken det gir. Til forskjell fra en spørreundersøkelse eller et intervju får oppdragsgiver i et spill muligheten til å være mer utforskende og observere hvordan spillerne påvirker hverandre når ny informasjon eller nye utfordringer blir spilt inn. Videre kan det å samle en spillgruppe med relevante aktører bidra til eierskap og forankring av prosessen når man skal implementere nye retningslinjer.

Det å samle relevante aktører for å spille over flere dager krever ressurser. God planlegging og arbeid med både case og hendelser som skal spilles inn er en avgjørende faktor for å få utbytte av spillet. Her var det FFIs erfaring at et tett samarbeid i forkant med de som arbeidet med problemstillingene til daglig var nødvendig for å sikre at man traff de relevante områdene.

Erfaringene fra arbeidet med både EBA-spillet og Materiellspillet har synliggjort noen forhold det kan være greit å tenke ekstra igjennom om man vurderer å gjennomføre et spill:

- Tydeliggjøre hva man ønsker å få ut av spillet for de som skal designe, planlegge og gjennomføre spillet. Dette inkluderer eventuelle referenter som bør ha innblikk i hva som er relevant informasjon.

- Spill kan være ressurskrevende. I materiellspillet ble det eksempelvis benyttet om lag to månedsverk i forkant av spillet til å utarbeide case og hendelser, og dette var personell som var godt kjente med investeringsprosessen. Det er viktig å definere et klart og tydelig formål og vurdere hva man minimum trenger av ressurser, slik at spillet ikke blir unødvendig omfattende.

- For et vellykket spill må det brukes tid i forkant på å sikre at man treffer relevante problemstillinger gjennom utarbeidelsen av scenario (investeringscasene i tilfellet EBA-spillet og Materiellspillet) og hendelser. Rent konkret kan dette være å ha arbeidsmøter i forkant med eksperter som kjenner prosessen. I EBA-spillet og Materiellspillet innebar dette å ha god dialog både med oppdragsgiver, men også med aktører som gjorde arbeidet til daglig – for å sikre begge perspektivene. Det kan også være en fordel å ha noen eksperter med underveis i spillet.

ERFARINGER FRA FORSVARSDEPARTEMENTET OG FORSVARSMATERIELL

Geir Midtun Hove, seniorrådgiver EBA-seksjonen FD III

1. Hvordan opplever du at spill som metode passet til å treffe de aktuelle problemstillingene?

Spillet ble gjennomført i etterkant av en revisjon av retningslinjene for tjenestefeltet eiendom, bygg og anlegg (EBA) i forsvarssektoren. Retningslinjene regulerer ansvar roller og myndighet, mellom departement, og sektorens ulike etater innenfor EBA-området.

Erfaringer viser at det er utfordringer i grensesnittene mellom aktørene, samt i utøvelsen av rollene som er beskrevet i retningslinjene, som i verste fall kan påvirke fremdrift, kvalitet og kostnader på EBA-området.

Basert på gode forberedelser var det mulig å legge opp spillet slik at disse utfordringene ble synliggjort gjennom praktiske eksempler, der alle aktørene var tilstede samtidig. Synliggjøring av utfordringer og avhengigheter, samt felles refleksjon rundt dette fra alle aktørene, fungerte etter min mening svært godt.

2. Hva slags effekt eller resultat mener du spillet har gitt?

Utfordringene i samhandlingen mellom aktørene ble synliggjort, og noen erfaringer vil danne grunnlag for justeringer i fremtidige retningslinjer. Kanskje like viktig er effekten av at aktørene tilbringer tid sammen, og gjennom spillet blir gitt kunnskap og innsikt i de andre aktørenes utfordringer. Kunnskapen og innsikten, sammen med personlige relasjoner, bidrar til å bygge opp tilliten mellom aktørene.

3. Hvordan ser dere i FD for dere å benytte metoden fremover?

Jeg mener bruk av spill bør være aktuelt i forbindelse med vurderinger av større endringer i roller, ansvar og myndighet mellom etater, mellom departement og etater eller mellom etat og sivile aktører. I tillegg kan det være aktuelt i situasjoner med kritisk manglende tillit mellom ulike aktører.

4. Hvor overførbar mener du spill som metode er til andre statlige virksomheter?

Regulering og utfordringer knyttet til roller, ansvar og myndighet mellom overordnet og underordnet eller mellom sideordnede virksomheter er problemstillinger som i større eller mindre grad er aktuelle i alle sektorer. Jeg mener spill som metode er egnet til å belyse og løse opp i slike utfordringer. Dette krever imidlertid gode forberedelser og kunnskap hos de som fasiliteter spillet. På det området har forsvarssektoren en åpenbar fordel ved å ha et eget forskningsinstitutt med inngående kunnskap om bruk av spillmetodikk, som en av sine etater.

HÅVARD FRIDHEIM (SPILLEKSPERTEN PÅ FFI) DELER SINE ERFARINGER

Foto: FFI

Kan du si litt om din erfaring med bruken av spill som metode og hvordan denne metoden henger sammen med beslektede metoder?

Jeg har 22 års erfaring med spill. Det er en teknikk som kan brukes til ulike formål, men først og fremst spiller man for å studere effekten av ulike beslutninger for en gitt problemstilling. Til syvende og sist er spill et strukturert opplegg for å legge til rette for at folk tar beslutninger – og ser konsekvensene av disse.

Spill kan brukes enten til å skape ny eller samle eksisterende kunnskap. De kan brukes kreativt for utfordre tanker om fremtiden, eller de kan brukes analytisk for å støtte struktur- og organisasjonsutvikling, som eksempelvis i langtidsplanleggingen i forsvarssektoren. Spill kan også bidra til å spre kunnskap (for eksempel om nye retningslinjer), og de kan være et bra virkemiddel i undervisning. Et annet viktig element i spill er underholdning – spill skal ikke bare være nyttig, men også morsomt. Her er det mange mulige overlapp mellom profesjonelle krigsspill i forsvarssektoren og kommersielle spill du kan kjøpe i butikken.

Hvilke miljøer i andre land (for eksempel NATO) samarbeider dere med for å få mest mulig riktig og nyttig bruk av metoden?

Jeg deltar i en System Analysis and Studies Panel (SAS)-gruppe i NATO som ser spesielt på spill i analyseøyemed, såkalt «analytical wargaming». Vi ser på hvordan vi kan designe, planlegge og gjennomføre spill for å kunne få robuste og relevante data. Vi ser også på mulige nye metoder for å samle informasjonen. Mange NATO-land er involvert i denne SAS-gruppen. I tillegg har vi også bilateral informasjonsutveksling og samarbeid med land som Sverige, Storbritannia, Nederland og USA.

Det skjer mye på spillfronten nå, ikke minst i store land som USA og Storbritannia. I USA tok det av rundt 2015, med flere initiativer for å styrke satsingen på krigsspill. I tillegg har det de siste årene kommet en ny konferanseserie med navn «Connections», hvor krigsspill er tema. «Connections» startet i USA, men det er nå egne årlige konferanser i Storbritannia, Nederland, Frankrike og Australia i tillegg. De største av disse konferansene samler drøyt 200 deltakere hver gang.

FFI har skrevet to rapporter om bruken av spill som metode knyttet til testing av retningslinjer – i hvilke andre sammenhenger benyttes metoden i forsvarssektoren?

Ulike former for spill brukes mange steder i Forsvaret, ofte også uten at spillbegrepet brukes. Det er mange eksempler på relativt enkle spill som kjøres som workshops, hvor en gruppe mennesker samles og diskuterer strukturert rundt et scenario. Ellers gjennomføres ulike spill til støtte for alt fra beslutninger på strategisk politisk-militært nivå til planleggingsprosesser på operasjonelt og taktisk nivå. I

Illustrasjonsfoto: Shutterstock

tillegg skjer det mye på sivil side, relatert til samfunnssikkerhetsarbeidet.

Så spill er mye brukt, men det er likevel en kunst å planlegge, designe og gjennomføre spill slik at man når de ønskede målsettingene og får robuste resultater.

Hvordan har bruken av metoden utviklet seg de siste årene?

Matrix gaming er et eksempel på en teknikk som har bredt om seg internasjonalt. Dette er en type diskusjonsbasert spill som tar inn elementer fra tradisjonelle brettspill, for eksempel terningkast og sannsynlighetsvurderinger knyttet til spillernes beslutninger. Spillerne blir i større grad tvunget til å ta beslutninger under press og usikkerhet. Her kan beslutningene også feile, noe som ofte er vanskelig å ta inn i mer tradisjonelle diskusjonsbaserte spill.

Det er også sterkere koblinger mellom profesjonelle spillmiljø og det kommersielle. Det finnes eksempler på folk som har gått fra forsvarssektoren og over til å lage spill for det kommersielle markedet.

Metoden utvikler seg også når det gjelder hvordan man kan samle og bruke informasjonen etter et spill. Det er økende bevissthet rundt metodiske fallgruver ved bruk av spill, i alle faser av planlegging, design, gjennomføring og analyse. Dette er temaer i SAS-gruppen som ble nevnt tidligere.

Har ny teknologi hatt betydning for metodens anvendelighet og i så fall hvordan?

Mange spill er low tech, i den grad at det ikke kreves stort mer enn en scenariobeskrivelse og en gruppe med mennesker for å gjennomføre et enkelt spill. Det er imidlertid mange muligheter for å ta inn mer teknologi, blant annet for å øke realismen og detaljgraden i spillet. Datastøttet simulering kan for eksempel brukes til å presentere scenarioet og representere spillverdenen langt mer realistisk enn å bare ha et kartutsnitt på en vegg. Teknologi kan også gi nye muligheter for å samle inn og prosessere data fra spillerne mer effektivt, i stedet for å skrive tekstreferater.

Hva slags tanker har du om fordeler og ulemper knyttet til «diskusjonsseminar»- formen som FFI benyttet på EBA-spillet og Materiellspillet?

Fordelen er at man får samlet mennesker med ulik erfaring og deretter samlet informasjon fra disse på en systematisk måte. I tillegg er det en styrke med disse spillene at ulike grupper arbeider i parallell med forskjellige caser, men at de fortløpende møtes i plenum og utveksler erfaringer med hverandre. Dette gjør det mulig å avklare usikkerheter og identifisere læringspunkter fortløpende.

Denne formen for spill krever likevel en del ressurser, så det er viktig å få tidlig klarhet i hva formålet med spillet er og hva resultatene skal brukes til. Deretter kan man designe et spill, basert på behov og tilgjengelige ressurser.

En generell utfordring med diskusjonsspill er at man er prisgitt den samlede kompetansen til spillerne som kommer. Du vil alltid ønske å ha mye kompetanse til stede, men du kan heller ikke invitere alle som er relevante – til slutt blir det for mange deltakere. I tillegg kan spillerne ha ulike kognitive føringer og grader av forutinntatthet, både bevisst og ubevisst, som påvirker resultatene. Internasjonalt er det nå økende fokus på hvordan spill kan designes for å motvirke effektene av dette.

ERFARINGER FRA FORSVARSDEPARTEMENTET OG FORSVARSMATERIELL

Jonny Marton Otterlei, sjef Materiellavdelingen Forsvarsmateriell

1. Hvordan opplever du at spill som metode passer til å treffe de aktuelle problemstillingene?

Spill som metode kan være velegnet for å teste ut ulike forhold der det ikke er mulig å gjennomføre dette i virkeligheten og hvor aktørers handlinger kan påvirke utfall og skape usikkerhet om utfall. I forbindelse med etableringen av FMA ble gjennomgangen av retningslinjene benyttet til å sjekke ut om roller, ansvar og myndighet var tilstrekkelig klargjort innen Forsvarsmateriell ble skilt ut av Forsvaret. Spill er imidlertid ikke en universalmetode og det krever meget gode forberedelser av spillstaben for at det skal bli bra. "Spillet" som ble gjennomført var heller ikke et spill i tradisjonell forstand, men en strukturert gjennomgang og diskusjon av ulike case knyttet til foreliggende utkast av retningslinjene.

2. Hva slags effekt eller resultat mener du (Materiellspillet) har gitt?

Jeg mener at spillet bidro til å sjekke ut konsistens og klarhet i retningslinjene i forhold til roller, ansvar og myndighet. Det var også et nyttig verktøy for en "ufarlig" gjennomgang hos en "nøytral" part, i dette tilfelle FFI, som gjorde at aktørene kunne både øke sin innsikt i de reelle konsekvensene av etatsutskillelsen og øke sin forståelse av endringene i roller, ansvar og myndighet. Det var nemlig svært krevende å få ulike aktører til å vurdere konsekvensene av etatsetableringen uten at de var sterkt farget av sitt syn om at dette var en meget dårlig løsning. Jeg mener derfor at spillene også bidro til å skape noe mer trygghet hos ulike aktører på militær side i forhold til etatsutskillelsen.

3. Hvordan mener du metoden bør benyttes fremover i sektoren?

Metoden er spesielt egnet i forbindelse med trening innen krisehåndtering og beredskap og konseptutvikling og støtte til vurderinger av strukturers effektivitet, men kan også være egnet innenfor andre område der det er hensiktsmessig at flere aktører setter seg ned og diskuterer gjennom ulike case og hvor utfall vil kunne variere avhengig av hva en annen part gjør.

4. Hvor overførbar mener du spill som metode er til andre statlige virksomheter?

Jeg tror den er overførbar også til andre sektorer, men det krever uansett gode forberedelser og en "spill-stab" som tilrettelegger. Jeg tror også at den brukes som metode innenfor krisehåndtering, men har ikke bred kjennskap til det. Mulig at FFI har bedre oversikt her eller f. eks. Direktoratet for sivilt beredskap.

Følg oss på sosiale medier

Aktsomhetsvurderinger – hvordan går vi frem?

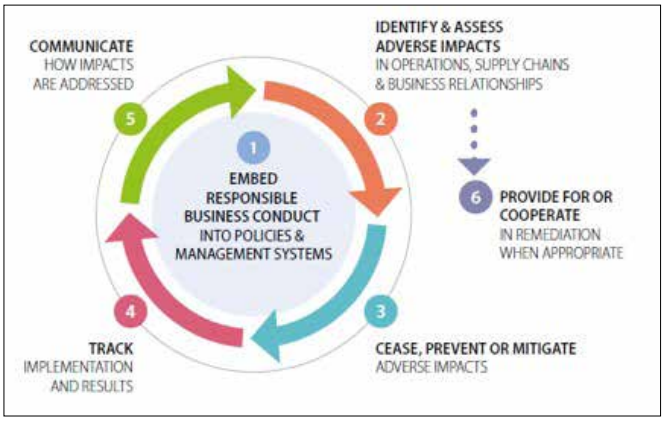
OECD har utarbeidet en veileder for risikobaserte aktsomhetsvurderinger for et ansvarlig næringsliv. Veilederen ble vedtatt på OECDs ministermøte 31. mai[1], og fremmes nå ifølge Norges OECD[2] Kontaktpunkt[3] for ansvarlig næringsliv av de 48 landene som følger investeringserklæringen i OECD. Bente Follestad Bakken og Åse Sand fra Norges OECD Kontaktpunkt, presenterte veilederen på Compliance & Kaffeseminar i de nye lokalene til IIA Norge 14. november.

AV ANN CHRISTIN FLATLAND
Nettverk for Compliance, IIA Norge

Esther Borgen fra KPMG innledet med å peke på tilfeller hvor negativ oppmerksomhet og omdømmetap som virksomhetene kunne unngått dersom de hadde gjennomført gode aktsomhetsvurderinger med påfølgende avhjelpende tiltak - tidlig i prosessen. Hun nevnte videre at compliancefunksjonen ofte kommer for sent inn i due diligence vurderinger og til tider begrenses til å kun være en kontroll- og monitoreringfunksjon etter at avgjørelser er tatt og kontrakter inngått. Da kan det ofte være for sent, fordi saker gjerne oppdages etter lang tid, oftest ved revisjon der man opplever svikt i rutiner eller at en hendelse avdekker behov for tettere oppfølging eller gransking. Ved tidlig involvering, der risikovurdeinger og Integrity Due Diligence (IDD) integreres i virksomheten øvrige beslutningsprosesser, vil compliancefunksjonen ha en mer preventiv rolle med fokus på å iverksette nødvendige tiltak, bygge kompetanse samt sikre at virksomheten har en felles forståelse av virksomhetens risikoappetitt.

Bente Follestad Bakken fra Norges OECD Kontaktpunkt innledet med å påpeke at OECDs retningslinjer er en del av den globale forventning om å drive ansvarlig forretning hvor aktsomhetsvurderinger bidrar til å avdekke den eventuelle negative påvirkningen virksomheten har på mennesker, samfunn og miljø. Retningslinjene skal bidra til at bedriftene bevarer miljøet, respekterer menneskerettighetene, ivaretar arbeidstaker rettigheter og unngår korrupsjon og smøring.

OECDs prosess for aktsomhetsvurderinger går noe lengre enn tradisjonelle compliance tilnærminger og inkluderer hele verdikjeden (inkludert underleverandører og uten avgrensing mht. antall ledd). Vurderingene tar utgangspunkt i virksomhetens interessenter og kartlegging av risiko for at virksomheten kan unngå skade og negativ effekt på mennesker, miljø og samfunn. Målet er å etterleve OECDs retningslinjer og sikre ansvarlighet. Det er med andre ord et



Kilde: Bildet er hentet fra "OECD DUE DILIGENCE GUIDANCE FOR RESPONSIBLE BUSINESS CONDUCT" (side 21)

større fokus på påvirkningen på tredjeparter og ikke virksomheten som sådan.

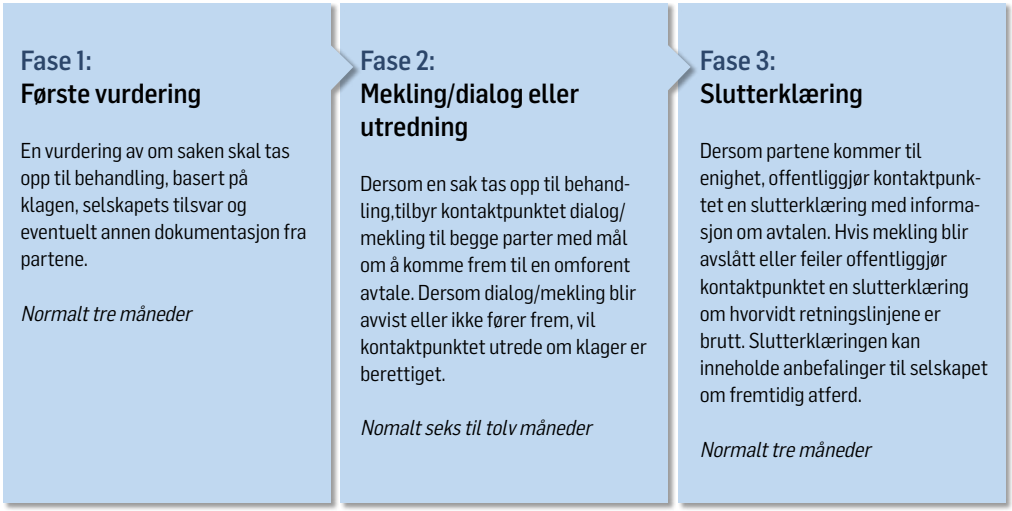
Follestad Bakken forklarte at due diligence prosessen består i å:

1) Forankre ansvarlighet i bedriftens retningslinjer og styringssystemer
2) Identifisere og kartlegge negativ påvirkning i egen virksomhet, leverandørkjede og forretningsforbindelser
3) Stanse, forebygge og avbøte negativ påvirkning
4) Spore implementering og resultater
5) Kommunisere hvordan påvirkningen er håndtert
6) Sørge for eller samarbeide om gjenoppretting der dette er påkrevet.

Det ble anbefalt at virksomheter med sammenfallende interesser slår seg sammen og diskuterer avhjelpende tiltak med samarbeidspartnere og myndigheter i de land de opererer. Dette er blant annet gjort innenfor internasjonal shipping hvor Marit Trodal forteller at man har etablert et maritimt anti-korrupsjonsnettverk (MACN) i kjølvannet av at UK Bribery Act trådde i kraft. Bakgrunnen for dette var å bygge en sterkere allianse av både store og mindre aktører som kunne samarbeide med myndigheter og institusjoner om å forebygge korrupsjon. Videre opplyser hun at Telecom operatører også har etablert et såkalt Joint Audit Cooperation, hvor medlemmer forplikter seg til å gjennomføre revisjoner av felles leverandører og dele resultater i en felles pool, samt samarbeide om forbedringstiltak.

OECD veilederen bygger på det vi ofte kaller «soft law» og forutsetter frivillig bruk og implementering. Brudd på retningslinjene kan derfor ikke håndheves på linje med brudd på lovbestemte rettigheter og plikter. Vi har for eksempel ingen slaveri lovgivning i Norge i dag, slik tilfellet er med blant annet i UK med deres Modern Slavery Act. Markedsføringsloven og hvitvaskingsreglene dekker imidlertid deler av nedslagsfeltet til veilederen og kan håndheves av norske myndigheter og domstoler. Det kan imidlertid tenkes at virksomhetene selv vil kunne påvirke etterlevelse retningslinjene som sådan ved at de i kontrakt med sine leverandører stiller krav om å følge kravene i veiledningen eller forklare hvorfor kravene ikke følges («comply or explain»).

Alle som mener at en bedrift ikke etterlever OECDs retningslinjer for flernasjonale selskaper kan levere en klage til det norske OECD Kontaktpunktet. Kontaktpunktet behandler saker der norske bedrifter er involvert, og saker som oppstår mot norske virksomheter med operasjoner i utlandet. Kontaktpunktet gjør en første vurdering, bidrar til megling/dialog og avgir en eventuell slutterklæring. Saksbehandlingen er beskrevet nærmere i figuren ovenfor.



Kilde: Bildet er hentet fra hjemmesiden til Norges Kontaktpunkt om behandling av enkeltsaker.

Avslutningsvis opplyste Follestad Bakken at Norges OECD Kontaktpunkt holder kurs i ansvarlig næringsliv og aktsomhetsvurderinger. Informasjon om dette finner du på kontaktpunktets hjemmeside[4].

Deltakere på Compliance & Kaffe seminaret hilser veiledningen velkommen og anser dette som et nyttig verktøy i vurdering av leverandører og underleverandører. Noen kunne nok ønske seg at den var enda mer konkret i å skissere konkrete forventninger, men den gir likevel en god retning med hensyn til de viktige vurderingene og beslutningene virksomhetene må ta og da særlig ved samhandling i særlig utsatte områder.

[1] *http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf*

[2] *The Organisation for Economic Co-operation and Development (OECD)*

[3] *Se hjemmeside for Norges Kontaktpunkt hvor det står: Kontaktpunktet skal fremme OECDs retningslinjer for flernasjonale selskaper, og bidra til å håndtere enkeltsaker om etterlevelse av retningslinjene. Alle OECD-land er forpliktet til å etablere en slik ikke-rettslig klageordning. Hvordan kontaktpunktene er organisert, varierer fra land til land.*

[4] *https://www.responsiblebusiness.no/*

GDPR – The way forward to 'business as usual'

Building trust with your business partners and customers

KEVIN F. MCCLOSKEY
Director, Deloitte

BJØRN JONASSEN
Partner, Deloitte Cyber Risk Services, Norway

GDPR and the concept of trust

Most, if not all, EU-based companies have either completed or have extensive GDPR projects under way. Essentially all have business relationships with which they exchange information, some of this classified as personal information. Understanding how this personal information is managed in regards to complying with the GDPR once it is sent to a business partner is probably one of the areas with which companies are most uncomfortable, as they do not have direct control over all of the information once it leaves their hands. Companies need to rely on the systems and processes at these business partners for protecting the information they share with them.

When thinking about GDPR compliance, the concept of 'trust' relates to having confidence in your business partners' ability to meet the requirements of the GDPR such that the information you share with them is 'safe'. At this point in time, establishing a basis for this trust in all of a company's business partners is difficult to do. You may have the proper contracts in place, but is that enough? This is a complex situation with many uncertainties and no one knows yet as to how enforcement of the GDPR will play out in real life. What will non-compliance look like? How seriously will it be taken? How much is non-compliance going to cost you, really? Who will be held responsible? How responsible am I really for the actions taken (or not taken) by my business relationships?

No one has the answers to all of these questions at this point, time will tell. However, we do have some insight as to how the market will react to addressing this issue of 'trust' from a practical perspective. We have been dealing with these types of regulatory issues for a long time and we have seen how things played out in real life before. No matter how uncertain, complex, strict or vague, difficult or seemingly endless some of these new regulations appear, the market always finds a way to work through it and create a new 'business as usual'.

Before we look at some of the tools which can be employed to develop trust, let's start with a quick overview of GDPR, who's affected by it and what's new about it.

GDPR in a nutshell

The General Data Protection Regulation (Regulation (EU) 2016/679) was adopted by the European Union in May, 2016. The new regulation will came into force in every member state in May 25th, 2018

The new regulation harmonizes data protection laws throughout the EU, strengthen individuals' control over the use of their personal data, imposes new obligations to data controllers and introduces significant penalties for non-compliance.

Who is affected?

The main focus of the regulation are all EU-based data controllers and processors, including private and public organizations regardless of size, shape, or color

where personal data is processed in the context of organization's activities (to be interpreted broadly). The regulation will also affect non EU-based data controllers and processors where EU residents' personal data is processed in connection with goods or services offered to them.

What is changed?

The core privacy principles basically remain the same. Personal data must be fairly and lawfully processed, it must be adequate, relevant and not excessive, it must be processed for specific purpose only and must not be kept for longer than necessary. Data subjects must be informed about the processing of their personal data, personal data must be accurate and up to date, it must be kept secure, data subjects must be able to inspect and correct their personal data and personal data must not be transferred to other countries without adequate protection.

Enforcement - Control and supervision

Data Protection Authorities (DPAs) are provided with effective means of enforcement:

- **Complaints** - Data Subjects whose personal data are processed in a way that does not comply with the GDPR have the right to lodge a complaint with a DPA.
- **Investigatory powers** - To investigate a possible violation the DPA may request access to all personal data, other information, data processing equipment and premises necessary for the performance of its tasks.
- **Other enforcement powers** – DPA's can issue warnings and reprimands, or impose a temporary or definitive limitation or ban on processing.

Sanctions - Monetary penalties of non-compliance

The economic repercussions of non-compliance can be massive.

- **Administrative fines** – A DPA can impose significant administrative fines, up to 4% of total global annual turnover of the preceding financial year or 20 M, whichever is higher.
- **Compensation and liability** - Companies are liable to pay compensation to individuals in the event of any unlawful processing of their personal data.
- **Negative publicity** - A publicized privacy breach – real or suspected – may result to damaged reputation, lost revenues, and destruction of shareholder value.

What remains unknown? - The uncertainty of interpreting GDPR requirements

Many details remain unanswered. There is no case law yet.

- **General interpretation** - How to interpret the requirements set forth in the GDPR? For example, what is considered to be "high-risk" or "core activities"?
- **National implementation** - Despite being a regulation, the GDPR allows Member States to legislate numerous data protection matters. Various GDPR articles state that their provisions may be further specified or restricted by Member State law.
- **The role of supervisory authorities** - Will the DPAs emphasize enforcement and sanctions, rather than providing support and guidance?

There are a number of new requirements, including the following examples:

Requirement	Explanation
Accountability	Organization must not only comply with the regulation. It must also be able to demonstrate compliance to supervisory authority and other stakeholders.
Right to erasure	Under certain circumstances, organization must enable data subjects to request the removal of their personal data.
Consent	Consent remains a lawful basis to process personal data, but the definition of consent is much stricter. Consent must be separable from other written agreements, clearly presented, and as easily revoked as given.
Privacy by design	Organization must build privacy directly into technology, systems and practices at the design phase, thereby ensuring the existence of privacy from the outset.
Right to restriction of processing	Data subjects can require the organization to "restrict" processing of their personal data while their complaints are being resolved – or as an alternative to erasure. If restricted, the data can only be stored.
Breach notification	Organizations must report personal data breach to supervisory authority, and in certain cases to the affected individuals, without undue delay, not later than 72 hours after becoming aware of it.
Information notices	Organization must provide information to data subjects about the processing of their data in a concise, transparent, intelligible and "easily accessible" manner.
Data portability	Under certain circumstances, data subjects have the right to transport their personal data from one organization to another. The data must be provided in a structured, "commonly used" and machine-readable format.
Vendor management	The GDPR expands significantly upon the controller's responsibility for processing activities, and sets specific rules for allocating responsibility between the controller and processor.

Haven't we seen this before… do past actions predict future performance?

Those of us that remember the first days of the roll-out of the Sarbanes Oxley requirements (SOX) (hint: it went into effect in 2002) probably have at least a few war stories of some 'interesting' SOX projects. In the past 15 years or so of figuring out how to live with SOX, the market has found a way of 'normalizing' the various requirements. The ways in which SOX is enforced / implemented and how business partners / service providers and customers gain the levels of comfort with each other that they require to fulfill the SOX requirements have become 'business as usual'. There are best practice SOX control databases, FAQs answering the most complex SOX questions, white papers addressing a myriad of issues, international methodologies for implementing the requirements and whole audit methodologies implemented into automated systems for global audit engagement execution. The need to be able to 'trust' your business partners in a SOX world relates to how well you can trust that your financial information is being processed correctly through the processes not happening directly under your control (e.g., due to outsourcing or a shared service center).

Although SOX projects are still among the most complex in regards to obtaining and maintaining compliance and the requirements can still seem excessively strict, companies have found their ways of addressing SOX and have become 'comfortable' with it, in a sense. Auditors who need provide opinions in regards to their clients' SOX adherence as part of their engagements as external financial auditors have also come to terms with their responsibilities and the methods they need to employ to gain the comfort needed to sign off on the SOX opinion. The relationships between companies, their Outsourcing Service Providers (OSPs) and global partnerships can present numerous complexities in regards to SOX scoping and in regards to obtaining assurance as to the effectiveness of the SOX processes and controls in place at each of these. This 'network of controls' is similar to the network of trust relationships which is being forced by GDPR. The SOX network is built around ensuring the reliability of the information being processed through to a company's financial statements while GDPR is focused on the reliability of the processing of personal information in regards to the specific GDPR requirements.

What are our options for building trust?

How will this develop in regards to building trust among those who share personal information with each other? Based on our experience and based on what we have seen in the SOX world, there will be a number of choices available. The possibility for being able to make use of each will depend on the:

- company's budget for compliance (e.g., to purchase third party reports)
- breadth of knowledge of internal resources tasked with performing these (internal audit)
- availability of competent additional capacity in performing (cosourcing agreements)
- ability to obtain relevant information from business partners (through contractual agreements)

A company will have, for the most part, the following methods to obtain assurance in regards to the level of GDPR compliance at their business partners':

- **Self-reporting / Confirmation by the business partner** – As the persons performing the evaluation are the business partner itself, this type of assurance is the least reliable and provides a very low degree of assurance.
- **GDPR Certification** – Some EU countries will be implementing programs for GDPR Certification. This requires the creation of a certification authority to manage the program and issue certifications. In our experience, certification processes similar to, for example an ISO27001 certification, allow for a level of 'freedom' in setting the scoping of certification and in the level of maturity at which the organization wants to be certified. In addition, many of these certifications allow confirmation of compliance on a rolling 3 year cycle, with all areas and controls being tested within a 3 year period. Based on the level of assurance desired, these types of programs may not be sufficient.
- **Review executed by company's own resources** – reviews of business partners performed by company resources with a very good understanding of the interchange of information with the business partners and the company's processes would be a very strong method of obtaining assurance. These types of audits are reliant on the:
  - o competencies of the person(s) performing the reviews
  - o quality and completeness of the methodologies followed
  - o methods used to extract information from the vendor and to test compliance
  - o availability of resources to perform the reviews
  - o cost restrictions

Business partners may also be hesitant or unwilling to open themselves to such audits.

- **Independent attestation** – Companies may choose to issue an independent attestation report, much like the current ISAE3402 reports we see in Norway but based on standards that are more relevant to GDPR. The standards we see being used for these types of GDPR attestations are SOC2 and ISAE3000. We have delivered several SOC2 reports in Norway and see the relevance in relations to GDPR. We have also delivered numerous ISAE3000 reports and can also see how this standard could be used in a GDPR attestation program, but the audience for these reports is generally limited and a SOC2 would be more attractive for a business partner wishing to distribute the report to several partners.
- **A combination of the above** – The best solution, providing the most assurance with a greatly reduced need for performing your own audit procedures - for those who require a lot of ‹security›. Most of the requirements are confirmed through independent certification provided by the Processor but the Control-

ler also performs some control actions to ensure they are covered.

Market trends in Norway – What does recent history say about the way forward?

Over the past years we at Deloitte have been asked to deliver a number of specialized third party assurance reports (e.g., SOC2) for some of our Norwegian customers. These reports focus on a company's controls as they relate to the security, availability, processing integrity, confidentiality, and privacy of a system, as opposed to the ISAE3402 reports we have historically delivered to cover internal controls related to the processing of financial information mostly used for external audit reliance purposes. The interest in these specialized reports has been driven by requests mostly from the non-Norwegian customer base of the service providers. These requests seem to be coming from customers concerned about gaining a high level of assurance as to the maturity of the service provider in respect to their system for providing adequate security, availability, processing integrity, confidentiality, and privacy in the delivery of their services to customers. It is worth noting that these companies being asked to deliver the SOC2 reports were already ISO27001 certified.

With the recent addition of the GDPR requirements to the already long list of areas that companies need to be concerned about, there will be even more focus on gaining assurance that business partners and service providers are able to meet these requirements. If you cannot prove that you can meet the requirements, you may be written-off as an unacceptable risk. Your customers or prospective business partners may choose the next company on the list that can provide them with a satisfactory level of assurance.

How a company chooses to provide assurance, as mentioned before, is dependent on a number of factors. Based on what we see in other countries and how companies react to these needs, one of the most sought after solutions will be the issuance of attestation reports. We can expect that more customers will be putting specific clauses in their requests for proposals and choosing vendors or business partners that can provide the level of assurance provided by these reports. It remains to be seen whether a certification track may also be a possible solution, but we would expect that, as we have seen in other countries, the path to certification would at least be supported by the issuance of attestation reports.

There remain numerous questions as to how this will develop. What role will the local regulators play in this going forward and what position will they take as to attestation versus certification? Will there be any GDPR certification possibilities in Norway or across the EU? How will the methods implemented in other countries affect Norway's chosen preferred method and will Norway have a choice to do anything but follow the pack? In any event, it will be exciting to see how this develops in the coming months and years.

GDPR Self Evaluation

Here are some questions to consider when assessing your own or your business partners' compliance with GDPR. Our practitioners use these questions in assessing overall compliance with GDPR and in determining areas which will require attention.

- Do you have a privacy strategy in place? If so, is the GDPR incorporated in that strategy?
- Do you have a DPO assigned (if mandatory) or a Privacy responsible (if not mandatory) and are relevant roles and responsibilities defined?
- Do you have a privacy framework that includes a privacy policy and additional standards/guidelines?
- Do you have a incident management strategy in place that includes management of data breaches?
- Have you incorporated data privacy clauses (where relevant) in legal agreements with third party service providers or those that data is shared with?
- Do you have processes in place for managing data usage and sharing that includes reviewing and monitoring the sharing of data with both internal (e.g. with other business lines, legal entities, or countries) and external (outside the organisation)?
- Have you evaluated how you will respond to the rights of the data subject? If so, do you have procedures and processes in place to manage them?
- Do you perform any data privacy or GDPR related training and awareness activities?
- Are you aware of the privacy risks related to your data processing? If so, are you performing 'Privacy Impact Assessments' (GDPR: Data Protection Impact Assessment)?
- Do you have requirements concerning excessive processing, data retention, data minimisation, encryption and pseudonymisation when developing new products?
- Is data protection considered in all aspects of the data processing life cycle from the outset till the end (data destruction)?
- Have you established if and when you are a processor and a controller? And also your responsibilities?
- Are you aware of the basis for processing all personal data?
- How do you use consent? To what extent?
- Do you have a record of your processing activities?
- Are you relying on the exemption for unstructured data in the Data Protection Directive (95/46/EC)?
- Are you aware of where you have personal data in the organisation? (E.g. applications, databases, file servers, shared drives etc.)
- Do you process sensitive types of personal data, e.g. special categories of data or data of children?
- Do you have data protection controls in place built into your technology (systems/applications, databases, etc)?

Styret og internrevisjon

Styrets overordnede ansvar for organisasjonens måloppnåelse, risikostyring og etterlevelse av lover og regelverk er omfattende. En dyktig internrevisor er en verdifull bidragsyter og proaktiv rådgiver for styret og toppledelsen ved å gi risikobaserte og objektive bekreftelser, råd og innsikt. På denne måten bidrar internrevisjonen til måloppnåelse og til å fremme og beskytte organisasjonens verdier.

AV DOROTHEE SAUER
Rådgivning BDO

Internrevisjonens formål

Definisjonen av internrevisjon fra IIA er «Internrevisjon er en uavhengig, objektiv bekreftelses- og rådgivningsfunksjon som har til hensikt å tilføre merverdi og forbedre organisasjonens drift.

Den bidrar til at organisasjonen oppnår sine målsettinger ved å benytte en systematisk og strukturert metode for å evaluere og forbedre effektiviteten og hensiktsmessigheten av organisasjonens prosesser for risikostyring, kontroll og governance.»

Internrevisjonen har hele virksomheten som sitt arbeidsfelt, dvs. strategiske- og ledelsesprosesser, kjerne- og støtteprosesser.

Samtidig er internrevisjonens kapasitet begrenset og internrevisjonens ressurser bør benyttes slik at internrevisjonen bidrar til størst mulig merverdi for virksomheten. Dvs. på områder og prosesser som er mest kritisk for virksomhetens omdømme, virksomhetens måloppnåelse og risikostyring.

Hvordan jobber internrevisjonen?

Internrevisjonsfunksjonen og -oppdrag gjennomføres i henhold til anerkjente standarder som IIA-standardene. I tillegg kan andre anerkjente standarder som eksempelvis ISO, COSO eller COBIT være relevante, avhengig av bransje og størrelse av virksomheten og type internrevisjonsprosjekt. Selv om ulike rammebetingelser kan påvirke hvordan internrevisjonen gjennomføres i forskjellige miljøer, er overensstemmelse med relevante standarder avgjørende for å sikre at internrevisjonen ivaretar sitt ansvar.

Kommunikasjon og formidling av resultatene fra internrevisjonen er meget viktig, og må ikke undervurderes. Kommunikasjonen skal i stor grad tilpasses hvilke ønsker og behov styret har, samt hvilket budskap internrevisjonen ønsker å få frem. Presentasjonsformatet bør derfor være spisset for formålet. Internrevisjonen skal også minst en gang i året vurdere og rapportere tidligere observasjoner og anbefalinger til styret, og kommentere hvordan disse er blitt fulgt opp av organisasjonen, herunder hvilke tiltak som er iverksatt i forhold til kravene om god risikostyring og internkontroll.

Rammebetingelsene for dagens virksomheter er i stadig endring.

Det er viktig at internrevisjonsfunksjonen utvikler og tilpasser seg tilsvarende, er framoverskuende og kan levere sine tjenester til nytte for og etter behovet til ledelsen og styret.

Internrevisjonens rolle som del av god virksomhetsstyring

Internrevisjonen er et essensielt element i god virksomhetsstyring.

Avhengig av størrelsen og art av virksomheten, bør det være etablert flere kontrollnivåer i selskapet. Den såkalte «Three lines of defence model» visualiserer dette bra, med internrevisjon som den «3. forsvarslinjen».

Følgende punkter skiller internrevisjon fra 1. og 2. linje, og også fra ekstern revisjon og andre bekreftelsesgivere (eksempelvis tilsynsmyndigheter):

- «Uavhengighet» er et sentralt element for internrevisjonen som skal sikre at funksjonen utøves til størst mulig verdi for virksomheten. Definisjonen til IIA er: *«Uavhengighet innebærer fravær av forhold som truer internrevisjonens evne til å utøve sine internrevisjonsplikter på en upartisk måte.»* Dette oppnås ved direkte rapportering til styret, som gjør at internrevisjonen er uavhengig av den daglige driften og ledelsen.
- Utøvelse av funksjonen og eksterne evalueringer av funksjonen ihht. IIA standarder sikrer kvalitet.
- Internrevisjonen omfatter hele virksomheten og alle typer risikoer som er relevant for virksomheten.

Det er viktig at internrevisjonen bevarer sin uavhengighet. Internrevisjonen gjør evalueringer og kommer med råd og anbefalinger, men kan aldri ta beslutninger eller være operativt ansvarlig for eksempelvis risikostyring eller deler av internkontrollen.

Hvordan kan internrevisjonen organiseres?

En hensiktsmessig organisering av internrevisjonsfunksjonen bør tilpasses organisasjonens størrelse, kompleksitet, modenhet og øvrige funksjoner. Nedenfor er eksempler på alternative organiseringe. Disse er ikke «fastlåst», og kan også slås sammen, f.eks. alternativ 2 og 3.

1. Egen organisatorisk internrevisjonsenhet med fast ansatte internrevisorer
2. Ansatt leder for internrevisjon med team fra egen virksomhet
3. Ansatt leder for internrevisjon som kjøper eksterne tjenester (co-sourcing)med ERM

3.1 Ansatt leder for internrevisjon som har at lite team og i tillegg kjøper eksterne tjenester, f.eks. for tilgang på spesialistkunnskap eller ved ekstra ressursbehov (co-sourcing)

4. Felles internrevisjonsfunksjon på tvers av likartede virksomheter (i praksis bare relevant for statlige virksomheter)
5. Full outsourcing av internrevisjonsfunksjonen

Vurdering av løsning for virksomheten bør diskuteres godt mellom styret, ledelsen (og internrevisjonen). Behovet kan også endres over tid, dvs. at modellvalget bør diskuteres på nytt f.eks. når virksomheten vokser, ekspanderer til utlandet eller ved andre vesentlige endringer.

Hva kjennetegner en effektiv internrevisjon?

Svaret er selvfølgelig individuelt og blant annet avhengig av virksomhetens art, bransje, modenhet, kompetanse og erfaring hos styret og ledelsen. Allikevel, følgende attributter synes avgjørende for at internrevisjonen skal være en nyttig bidragsyter:

- God og regelmessig kommunikasjon mellom internrevisjon, styret og ledelsen. Dette skal blant annet bidra til internrevisors forståelse av virksomhetens mål, muligheter og risikoer. Samtidig økes ledelsens og styrets kunnskap om god virksomhetsstyring.
- Tydelig sammenheng mellom organisasjonens mål, risikoer og revisjonsprosjekter
- Koordinert samarbeid mellom de forskjellige roller innen virksomhetsstyring
- Fleksibilitet; det vil si å ha kompetanse og kapasitet til å kunne bistå ledelsen og styret både proaktivt og ved forespørsel
- Regelmessig oppdatering av risikobildet for virksomheten og sikre at alle «nye» risikoer (for eks. cybersikkerhet) er tilfredsstillende ivaretatt i revisjonsplanen
- Kontinuerlig forbedring, f.eks. ved bruk av nye verktøy for «løpende revisjoner» («ongoing auditing»), og business analytics som del av revisjonsprosjekter og overvåking av trender
- Sikre godt teamwork og tilfredsstillende kompetanse til enhver tid, (stikkord: Continous learning» og diversity») både innenfor internrevisjonen som fag og også spesialistkompetanse f.eks. innen teknologi eller juridisk.

I tillegg til overnevnte, er den personlige kompetansen til en internrevisor avgjørende for suksess, her er et utvalg:

- Vise respekt ovenfor den ekspertisen og jobben som gjøres ved den reviderte enheten, være ydmyk
- Gjøre jobben med høy integritet, være modig og ta opp også ubehagelige ting på en konstruktiv og saklig måte, for organisasjonens og medarbeidernes / ledelsens beste
- Evnen til å bygge tillit og relasjoner, ved å lytte og effektivt kommunisere med alle nivåer i organisasjonen
- God prosjektledelse, herunder levere på tid, involvere rett kompetanse, involvere ledelsen i revidert enhet og levere lettleste rapporter

Hva er styrets oppgaver og ansvar ifm. internrevisjon?

Det er styret som normalt etablerer internrevisjonen og funksjonen rapporterer direkte til styret. I enkelte virksomheter, f.eks. statlige direktorater, der man ikke har et styre, vil det normalt være den øverste lederen, direktøren, som ansetter og er rapporteringsinstans.

Styret fastsetter og godkjenner internrevisjonens formål, fullmakter og ansvarsområder gjennom en instruks. Instruksen er et viktig styringsdokument. Dette sikrer uavhengigheten i revisjonene og sørger for et tydelig mandat.

Leder for internrevisjonen og styret skal ha regelmessig kommunikasjon, og internrevisjonen skal ha direkte og uinnskrenket tilgang til toppledelsen og styret for å sikre uavhengighet av internrevisjon. Ihht. IIA standarden 1110 må «internrevisjonens rapportering og kommunikasjon med toppledelsen og styret inkludere informasjon om:

- Internrevisjonsinstruksen og internrevisjonens uavhengighet
- Internrevisjonsplanen og fremdriften i forhold til planen
- Ressursbehovet
- Resultatet av revisjonsaktivitetene
- Overensstemmelse med de etiske reglene, standardene, og handlingsplaner for å håndtere eventuelle vesentlige uoverensstemmelser.
- Ledelsens håndtering av risiko som etter leder av internrevisjonens vurdering kan være uakseptabelt for organisasjonen.»

Årsplanen for internrevisjonen, inkludert budsjett for ressurser, godkjennes av styret etter gjennomgang med toppledelsen og styret. Lønn for leder fastsettes vanligvis også av styret.

Styret bør også holde seg orientert om programmet for kvalitetssikring og forbedring for internrevisjon. Dette inkluderer krav om ekstern evaluering av internrevisjonsfunksjonen minst hvert femte år.

I de tilfeller der organisasjonen har et revisjonsutvalg skal internrevisjonen rapportere til revisjonsutvalget, i tillegg til styret. Dette følger av blant annet EUs åttende selskapsdirektiv som slår fast at revisjonsutvalget skal «*følge opp effektiviteten og hensiktsmessigheten av selskapets systemer for internkontroll, eventuell internrevisjon og risikostyring [...]*». Revisjonsutvalget vil, som saksforberedende organ for styret, bedømme internrevisjonens kompetanse og engasjement, forslag til planer samt jevnlig gjennomgå internrevisjonens instruks.

Hvilke virksomheter er forpliktet til eller anbefales å ha en internrevisjon?

Enkelte bransjer og næringer har lovkrav om internrevisjon.

For eksempel har visse typer finansforetak under gjeldende regelverk krav om internrevisjon.

For statlige virksomheter[7] gjelder bl.a. Rundskriv 117 fra 2016:

«Kravet om å vurdere bruk av internrevisjon gjelder for alle virksomheter som har samlede utgifter eller samlede inntekter over 300 mill. kroner i henhold til siste publiserte årsrapport.

... Statlige virksomheter kan bruke internrevisjon som en del av virksomhetens system for styring og kontroll, jf. krav til virksomhetenes interne styring i bestemmelser om økonomistyring i staten.» Vurderingskriterier er nevnt i R117 og resultatet skal dokumenteres. Hvis det ikke skal etableres / videreføres en internrevisjon må dette begrunnes. Vurderingen skal gjøres regelmessig, minst hver fjerde år. Resultatet sendes til riksrevisjonen, departementet og DFØ.

For børsnoterte selskaper i Norge er det ikke et direkte krav om internrevisjon. Selskapene må imidlertid forholde seg til «Løpende forpliktelser for børsnoterte selskaper»[8]. Blant annet er det krav om redegjørelse for eierstyring og selskapsledelse ihht. Norsk anbefaling for eierstyring og selskapsledelse (NUES). Her kan en internrevisjon være en god bidragsyter med sine uavhengige bekreftelser og råd ifm. risikostyring, kontroll og governance.

[7] *https://dfo.no/fagomrader/internrevisjon/internrevisjon-i-staten*
[8] *https://www.oslobors.no/Oslo-Boers/Regelverk/Loepende-forpliktelser-for-boersnoterte-selskaper*

Utover lovpålagt internrevisjon er det per i dag stort sett (mellom-)store virksomheter i privat og offentlig sektor, børsnoterte selskaper eller datterselskaper fra internasjonale konserner som har egen internrevisjon eller som kjøper slike tjenester av eksterne aktører. Grunnen til dette er som regel kompleksiteten i driften og styrets behov for å få uavhengige og objektive bekreftelser og råd.

Tre sentrale fordeler som alltid bør oppleves ved en dyktig og moderne internrevisjon

Samtidig ser vi en tydelig trend til å etablere en internrevisjonsenhet også i mindre og mellomstore virksomheter. Årsakene er blant annet økende utfordringer med et mer komplekst risikobilde for mange typer virksomheter.

Hvordan sikre og måle internrevisjonens merverdi og bidrag til virksomhetens måloppnåelse

Det er viktig å synliggjøre, måle og sikre merverdi av Internrevisjon for å sikre at midlene til internrevisjonen er godt anvendt, forventningene er avklart og internrevisjonen har rammebetingelser for å kunne bidra til virksomhetens måloppnåelse.

Men måling av nytte og bidrag til virksomhetens måloppnåelse er ikke alltid rett frem og enkelt. Noen indikatorer kan selvfølgelig enkelt måles, som for eksempel hvor mange prosjekter internrevisjon har gjennomført, og hvor mange funn prosjektene resulterte i.

Dette sier likevel forholdsvis lite om internrevisjonens bidrag til måloppnåelse og til å fremme og beskytte organisasjonens verdier.

Synliggjøring og måling av merverdien ved internrevisjonen må tilpasses den enkelte virksomhet. Den vil blant annet være avhengig av virksomhetens og internrevisjonens størrelse.

En ekstern kvalitetsevaluering, slik det er påkrevd ved standardene, kan være et godt utgangspunkt. Utover (og uavhengig av det) kan en praktisk tilnærming være at internrevisjonen:

- Med jevne mellomrom vurderer direkte og indirekte verdi ved tiltak som er implementert etter et revisjonsprosjekt, f.eks. lavere kostnader, økt måloppnåelse av avdelingen eller prosjektet, mer effektive prosesser, overensstemmelse med relevant lovverk, forbedret omdømme, redusert risiko for misligheter, sikker behandling av personopplysninger, økt kontroll med IT-/Cyberrisiko.
- Etterspør tilbakemelding fra den reviderte enheten om deres opplevde merverdi, hvilke behov de ser for internrevisjonen i fremtiden og muligens forbedringer for internrevisjonen selv.
- Gjennomfører en SWOT analyse av internrevisjonsfunksjonen for å få nyttig innsikt.
- Legger frem resultatene av de tre forrige punkter til ledelsen og styret og diskuterer mulige utfordringer, behov og forbedringspotensialet.

Det bør avtales konkrete tiltak etter gjennomføring av en slik intern evaluering. Det kan også være nyttig å lage en strategisk plan for internrevisjon og senere oppdatere denne, på basis av forventningene og behovene til styret og ledelsen. Den bør helst være kort og presis og definere:

- Visjonen til internrevisjonen og hva den skal bidra med i virksomheten (utover den tekniske definisjonen ihht. instruksen)
- Kritiske suksessfaktorer for internrevisjonen (eksempelvis ifm. kommunikasjon, fokus og prioriteringer, ressurs- og kompetansekrav, og kvalitet av prosjektene)
- Måling av internrevisjonens bidrag og verdi, inkludert konkrete måleparametere, og rapportering til styret.

Styret vil ved dette sikre at midlene til internrevisjonen er godt anvendt, forventningene er avklart og internrevisjonen har rammebetingelsene for å kunne bidra til virksomhetens måloppnåelse.

Hva nå?

Der det allerede er etablert en internrevisjonsfunksjon i virksomheten, bør styret regelmessig vurdere følgende spørsmål:

- Utøver styret (og revisjonsutvalg hvis relevant) sine oppgaver og ansvar ovenfor internrevisjon tilfredsstillende?
- Utøves internrevisjonsfunksjonen i samsvar med standardene til IIA, og når er det neste gang behov for en ekstern evaluering, slik det er påkrevd ved standardene?
- Hvordan er merverdi ved internrevisjon sikret og målt? Hvordan oppleves kommunikasjon med og nytten av internrevisjonen? Er det behov for en vurdering og eventuell forbedring av funksjonen og / eller samarbeidet?

Der det ikke er etablert en internrevisjonsfunksjon i virksomheten, bør styret regelmessig vurdere følgende spørsmål:

- Hva er årsaken til at det ikke (ennå) eksisterer en internrevisjon, og når ble det sist vurdert om en internrevisjon bør etableres?
- Hva kan være gode grunner til å etablere en internrevisjonsenhet i virksomheten, både fra ledelsens og styrets perspektiv?
- Bør det diskuteres på neste styremøte og med ledelsen om kost-nytte effekten ved en internrevisjon kan være positiv?

Tre sentrale fordeler som alltid bør oppleves ved en dyktig og moderne internrevisjon

Internrevisjonen er del av virksomheten og derfor vanligvis mye «tettere på» den daglige driften enn styret. Den har kontakt med mange medarbeidere og kjenner organisasjonen på alle nivåer, ikke bare ledelsen. Gjennom dette kan internrevisjon få nyttig innsikt som ledelsen eller styret ikke nødvendigvis ellers får. I tillegg kan internrevisjonens uavhengighet fra linjen være en døråpner for at medarbeiderne er mer åpne, særlig ved tilfeller av kritikkverdige forhold i ledelsen, misligheter eller andre forhold som det bør varsles om.	Positive effekter av gjennomførte tiltak som følge av en revisjon. Eksempelvis mer effektive prosesser, kostnadsbesparelse, sikring av etterlevelse av lover og regler og godt omdømme. I tillegg er «å ha kontroll» vanligvis i seg selv en merverdi. Det skaper trygghet for (topp-)ledelsen, styret, eierne og omverdenen.	Gjennomføring av internrevisjonsprosjekter og tilhørende diskusjoner med ledelsen og medarbeiderne som er berørt av revisjonen har positive ringvirkninger, utover de konkrete resultatene fra revisjonsprosjektet. De positive effektene er økt kunnskap og et skjerpet fokus på god internkontroll, virksomhets- og risikostyring. Dette kan også være nyttige refleksjoner og en bevisstgjøring av ens bidrag til måloppnåelse for virksomheten, effektivitet i eget ansvarsområde, og om samarbeid med andre deler av organisasjonen fungerer optimalt eller om det er forbedringspotensial.

Santa Claus – a Jolly Old Man or A privacy risk?

A BLOG BY MARIE MURPHY
Marie Murphy is Co-Founder of Fort Privacy (www.fortprivacy.ie) and an expert in Privacy by Design

As the first Christmas post-GDPR approaches here's a pressing question. How well prepared was Santa for the introduction of the new EU General Data Protection Regulation in 2018?

Santa himself is a very private individual and lives a low-key life away from the limelight for 11 months of every year. We know he is married to Mrs Claus. He lives near the North Pole and is a major employer in the region (the elves). We all know he is kind to animals (the reindeer). That is the extent of our knowledge. Clearly Santa understands the value of privacy.

So, let's forget the presents for the moment and take a closer look at Santa's data protection record. How does Santa's North Pole operation match up against data protection principles? How prepared is Santa to meet the rights of data subjects? What safeguards has Santa put in place to cover the global nature of his data processing operations?

Are there privacy risks inherent in Santa's operation? Did he address them in time to continue operating as usual this Christmas?
A Data-Centric Overview of Santa's operation
First, lets examine the data Santa collects about our children:

- **Identity:** Name, age, gender and home address.
- **Geo-location:** Place of sleep on Christmas Eve
- **Behaviour:** Santa maintains a naughty and nice list. He reportedly knows if children have "been good or bad".
- **Living conditions:** Santa knows whether children live in houses or apartments, with and without chimneys.
- **Personal preferences:** He has intimate knowledge of children's wish lists including multiple revisions made from September to December every year. He knows whether children prefer their presents left at the foot of their bed or under the tree.

Combine this with the fact that almost all of Santa's data subjects are under the age of 13 and this is a huge database of information held on children who are afforded special protection under GDPR.

As a data protection practitioner I would be advising Santa to carry out a Data Protection Impact Assessment (DPIA) to identify the risks in his data processing activities. I would be most concerned about the scale of processing and the mass surveillance activities required to maintain that naughty and nice list. I would be checking if all the processing is strictly necessary and I would be asking to see his privacy statement.

Data Protection Risks in Santa's Operations

So without going into a formal DPIA process here are a few possible areas I'd look at in Santa's massive data-heavy operations:

1. **Transparency:** When those letters go up the chimney what does Santa do with the data? Where does he store it? How does he process it? Has anyone ever seen Santa's privacy statement or is that chimney a one-way communication system?

2. **Legal basis:** What is Santa's legal basis? Is it public interest? Does he get the consent of his data subjects? Has he assessed the necessity and proportionality of his processing?
3. **Retention:** How long does Santa retain information? Does he still hold mine? If he does it is clearly long after it is necessary because I haven't received a present in many, many years.
4. **Automated decision making:** How does Santa determine who is on the naughty and nice list? Are machines involved in the process? Do children have recourse to challenge the list?
5. **Accurate and up-to-date:** How does Santa keep track of the ever-changing wish-list contents (I know I can't and I only have a small number of children to track)? How does he record when children are spending Christmas with grandparents or their cousins?
6. **Surveillance:** Santa has a lot of information about children's location on Christmas Eve and at other times. Clearly, he is carrying out some form of surveillance on children if he knows "when they have been good or bad". Has he carried out an impact assessment? Has he put controls in place to address any risks?
7. **Data Transfer outside the EU?** We know Santa lives near the North Pole but not his exact location. Is his operation EU based or does he transfer his massive database outside the EU?

Clearly this is not an exhaustive list. Perhaps other data protection practitioners would like to add to it (but please don't scare the children!).

Have a wonderful Christmas in 2018. I do hope Santa took some good GDPR advice and that everything will go smoothly this year.

Generalsekretæren informerer

AV ELLEN BRATAAS

Det har vært høy aktivitet i alle nettverk og komiteer denne høsten, og spesielt nå på tampen av året. En og annen deltaker benyttet sikkert muligheten til å sanke årets siste vedlikeholdspoeng, men jeg velger å tro at flesteparten kom fordi temaene var interessante. Denne høsten har vi hatt fokus på å skape flere arenaer hvor formålet utelukkende er erfaringsutveksling, diskusjon, nettverk og dypdykk ned i spesifikke temaer. Vi har kopiert modellen fra Compliance & Kaffe og overført denne til rundeborddiskusjoner på risikoområdet og SmartTalk, et konsept som tar for seg mer internrevisjonsspesifikke temaer.

Sekretariatet har en visjon om å videreføre temaene og gjenbruke poengene fra disse diskusjonene inn i en egen podcast for virksomhetsstyring. For at medlemstilbudet skal være tilgjengelig utenfor Oslo, vurderer vi også muligheten for å strømme aktiviteter fra gang til gang. Bruk av video for informasjon om nye veiledninger og bokanmeldelser er andre ideer vi leker med. Vi har denne høsten lansert foreningens første e-læringskurs i introduksjon til internrevisjon som kan gjennomføres når som helst og hvor som helst, enten på pc eller via en app - IIA Academy. Kongstanken er på sikt å kunne tilby en rekke e-læringskurs under fanen «Virksomhetsstyringsskolen». Vi erfarer også at nettsider er ferskvare, og i takt med utvikling av faget og god praksis for oppbygging og layout på nettsider, ser vi at tiden igjen er moden for å justere og optimalisere foreningens nettside. Uansett hvilke strategiske handlinger styret velger å prioritere på årets siste styremøte i desember, blir det garantert en hektisk og morsom vår å se frem til.

VI GRATULERER FØLGENDE MEDLEMMER

Diplomert internrevisor

Sissel Kristiseter, Oslo kommune internrevisjonen
Vivi Haller Grimstad, Utlendingsdirektoratet
Trond Ingebretsen, Oslo politidistrikt
Dag Nenningsland, Norad
Bjørg Beate Kristiansen, Sparebanken Sør
Merete Kroglien, Sparebanken Sør
Håvard Myreng, Skatt Øst
Nitika Dhall, Oslo kommune internrevisjonen
Nahid D. Naroei, Arbeids- og velferdsdirektoratet
Trine Louise Dahlen, Skattedirektoratet
Susanne Øyen, Mattilsynet
Veronica Kvinge, BKK
Anette Karine Dehli, Akershus universitetssykehus

Certified Internal Auditor (CIA)

Blanka Magdolna Balazs, Equinor ASA
Aksana Tikhonova, Kommunal Landspensjonskasse

KONFERANSER VERDT Å MERKE SEG

Nordic Light, 8. – 10. mai 2019, Reykjavik, Island

En konferanse og nettverksplattform spesielt tilrettelagt for internrevisjonsledere i Norden. IIAs globale president, Richard Chambers, COSO Chairman Paul Sobel og IIAs styreleder Naohiro Mouri kommer også. Kommer du?

IIA Norges årlige konferanse, 27.-28. mai 2019, Fornebu

IIA's International Conference, 7. – 10. July 2019, California, USA

NYHETER FRA IIA, ECIIA OG ANDRE PARTNERE SISTE HALVE ÅR:

RISK IN FOCUS 2019: HOT TOPICS FOR INTERNAL AUDITORS

Syv europeiske institutter har gått sammen for finne ut hvilke risikoer de mener er å anse som mest relevante å ivareta på revisjonsplanen for 2019. Risk in focus 2019 var også tema på første SmartTalk i foreningen. Her er de ti største risikoene sett fra et europeisk ståsted, og hvis du ønsker en mer utdyping av den enkelte risiko, kan dette lastes ned fra vår nettside:

1. Cybersecurity: IT governance & third parties
2. Data protection & strategies in a post-GDPR world
3. Digitalisation, automation & AI: technology adoption risks
4. Sustainability: the environment & social ethics
5. Anti-bribery & anti-corruption compliance
6. Communications risk: protecting brand & reputation
7. Workplace culture: discrimination & staff inequality
8. The new era of trade: protectionism & sanctions
9. Risk governance & controls: adapting to change
10. Auditing the right risks: taking a genuine risk-based approach

UTVIKLING AV INTERNREVISJON I OFFENTLIG SEKTOR I NORDEN

I fjor ble det for første gang foretatt en undersøkelse som sammenlignet utviklingen av internrevisjon i offentlig sektor på kommunalt-, fylkes- og statlig nivå i de nordiske landene. Resultatet ble presentert i "Icelandic Review of Politics and Administration" i juni.
Undersøkelsen viser hvor at det er forskjeller mellom landene når det gjelder regulering av internrevisjon, ressurser og organisering. Du kan laste ned hele undersøkelsen på vår hjemmeside.

INTEGRATING A DATA-DRIVEN APPROACH: LEARNING THE BASIC

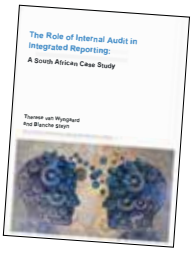
Successful internal audit departments must be able to grow their capabilities to harness those tools and technologies and use the vast amount of data in their organisations to provide greater levels of assurance and value-added services, all the while improving the efficiency with which they do so. Learn the basics of building data analytics into the internal audit methodology. Make the investment and become a leader in your organization and in the profession of internal auditing.

AUDITING THIRD-PARTY RISK MANAGEMENT

This practice guide is a useful tool to become better informed on risks related to third-party provider management. Risks across the full vendor life cycle are considered, including the appropriate sourcing, ongoing management, and termination of vendors. Further exploration into risks resulting from the types of services being provided and the sensitivity of data being shared is covered. Sample audit guidance is offered, making this a robust resource with tangible tools.

THE ROLE OF INTERNAL AUDIT IN INTEGRATED REPORTING: A SOUTH-AFRICAN STUDY

The continuously evolving need for internal audit to move beyond simply focusing on financial statements is being experienced around the globe, as evidenced by the new South African case study released by the Internal Audit Foundation. It highlights the role internal audit can and should play in integrated reporting so that financial, nonfinancial, and sustainability considerations are adequately assessed.



ALIGNING INTERNAL AUDIT ACTIVITIES AND SCOPE TO ORGANIZATIONAL STRATEGY

The current business environment is changing constantly, and many organizations are shifting their strategy to cope with this vibrant environment. How does change impact the internal audit function? At which levels does the organizational strategy impact internal audit's scope and role? These questions are the basis of this research project.

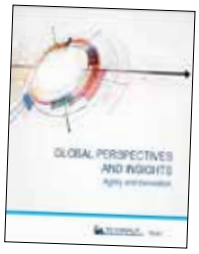
EFFECTIVE WORKPAPERS

Just as good communication is at the core of a quality and successful organization, good documentation can put good communication in a manageable context and render it central to effective policies, procedures, regulations, legal matters, disputes, and audits. Many have heard the phrase, «If it is not in writing, it didn't happen.» This phrase is often used as a method to strive for better, and more complete, documentation. Simply put, it just makes sense to document what is planned, what is done, and what is communicated.

GTAG: AUDITING INSIDER THREAT PROGRAMS

This GTAG helps internal auditors understand insider threats and related risks by providing an overview of common dangers, key risks, and potential impacts. Additionally, the guide defines key terms in the insider threat universe, and presents security frameworks, techniques, considerations, and resources that can help during the planning and execution of audit engagements.

AGILITY AND INNOVATION



Agility and Innovation hits on key areas that are critical for internal audit functions to master — such as strong data management and data analytics — and discusses areas where artificial intelligence and process automation can be leveraged to allow practitioners to spend their time on more value-added activities. To assist internal auditors with getting on the path to agility and innovation, the report concludes with five steps they can take now to put the wheels in motion.

AUDIT COMPETENCIES: UNDERSTANDING AND BUILDING COMPETENCIES FOR SUCCESS

Internal auditing requires a unique set of characteristics and competencies that differentiate the profession from others. Discover the key competencies for the profession of internal auditing and learn how to build competencies for success.

AUDITING STRATEGIC RISKS

The insights on leading practices shared by CAEs are by turns familiar and fascinating when these leaders open up about how their internal audit functions work with management and the board to address three specific areas of strategic risk for their organizations: cybersecurity, IT projects, and capital projects.

UNITED, CONNECTED AND ALIGNED

A new whitepaper from The IIA and the International Federation of Accountants (IFAC) examines the distinct roles of internal audit and the finance function. United, Connect and Aligned draws on the vast experiences of 11 governance experts who offer their insights on how these two vital components drive good governance

IIA POSITION PAPER: WHY CONFORMANCE MATTERS

To best serve the organization and inspire stakeholder confidence, internal audit must operate at the highest level of ethical and professional competencies to ensure consistent and accurate delivery of risk-based and objective assurance, advice and insight. Internal audit is most effective when its resource level, competence, and structure are aligned with organizational strategy, and when it follows the International Professional Practices Framework (IPPF).

IIA POSITION PAPER: STAFFING/RESOURCING CONSIDERATIONS FOR INTERNAL AUDIT ACTIVITY

Knowledgeable and competent resources within internal audit are needed to ensure assurance and advisory work are performed in alignment with the organization's expectations and in conformance with widely accepted principles and standards.

IIA POSITION PAPER: INTERNAL AUDITING'S ROLE IN CORPORATE GOVERNANCE

The word governance has become a staple of the boardroom and C-suite lexicon, but just what governance is can sometimes become muddled. At its core, governance simply is the amalgam of processes and structures designed to help the organization achieve its objectives.

REDUCING ENTERPRISE RISK – PROTECTING YOUR BRAND THROUGH STAKEHOLDER SUPPORT

Today, more than ever, reputation can make or break an organization. As part of the risk management structure of their organizations, internal auditors in environmental, health and safety (EHS) should know what drives negative publicity, how organizations can turn it into positive momentum, and what effects these actions can have on the bottom line. Bringing together both sides or all sides of an issue, even those that are vehemently opposed to one another, can lead to much more effective and long-lasting solutions than fighting it out to see who wins.

Grov REVISJON

DØDSING Jomfru FJERN

Det dukker stadig opp nye ord. Med det mener jeg ikke ord på nye fenomener slik som blokkjede, skytjeneste osv. Nei jeg sikter til velkjente ord og kombinasjoner av ord brukt på en ny måte, à la Nytt på Nytt på NRK.

Noen ganger treffer de nye ordene midt på spikeren. Andre ganger må de ledsages av en forklaring. Jeg hørte for eksempel nylig 'jomfrurevisjon' fra vår hjemlige fagarena. Ordet fanget umiddelbart min interesse og måtte raskt googles. Først på listen kom «Hjelp til årsoppgjøret? BDO Regnskap har kompetansen». Det var m.a.o ikke mye hjelp å få derfra, så jeg måtte prøve meg på en egen fortolkning. Revisjon vet mange av oss omtrent hva betyr, selv om vi til tross for mange års erfaring fortsatt strever med å beskrive revisjon med få ord. Jomfruer har vi hørt om, men dette begrepet kan ha flere betydninger. Det kan eksempelvis være en seksuelt uberørt kvinne, en ung ugift adelsdame, en hushjelp fra 1800 tallet (kold-) eller et kortspill (gammel-). Ved å forfølge uberørtalternativet kan jomfrurevisjon være myntet på en virksomhet uberørt av revisorhender. Det gir mening. Jeg fikk tak i forklaringen etter hvert, og den er som følger: *Den aller første revisjonen en ny internrevisjon gjennomfører må velges med omhu. Den må ikke være for komplisert, den skal gi verdi for organisasjoner og sette standarden for hva internrevisjonen kan bidra med.*

Et annet nyord er «fjernrevisjon» hvor jeg med en gang fikk assosiasjoner til et ord jeg hørte for mange år siden, nemlig «grovrevisjon». Det skulle bety noe slik som *å se over et regnskap i stor hastighet for å identifisere eventuelle åpenbare mangler.* Vi får tro at dette var en øvelse man gjorde før man gjennomførte den fullverdige revisjonen, og ikke en erstatning. Jeg tror aldri jeg fikk svar på akkurat det. Ordet fant uansett ikke feste i vår fagterminologi

Foto: Dag Oliver

og det kan vi nok være glad for. Men hva innebærer så det beslektede «fjernrevisjon»? *Fjernrevisjon er en dataanalyse som benyttes når revisjoner kan gjøres ved å analysere data fra kontoret og spare budsjetter, tid og miljøet for belastningen reising medfører.* Dette har nok mer for seg enn «grovrevisjon».

En annen nyvinning i det norske språk er «risikobasert kvalitetskontroll». Her skal betydningen være at *grundigheten av leders gjennomgang av endelig rapport varierer i takt med viktigheten av revisjonsområdet og hvor vesentlige funnene er. Om rapportene i hovedsak er grønne, overlates setningsoppbygging og korrekturlesing til revisor selv.* Det høres vel kanskje ikke så dumt ut i utgangspunktet; man skal sette inn støtet på de rapporter der det trengs mest. Det er imidlertid to haker ved denne praksisen. For det første er vi ikke tilhengere av at det gjøres revisjon på områder som ikke er viktige. Det andre er at det kan komme en overraskelse i form av den dødelige revisjonsrisikoen. Den som har gjennomført jobben kan ha gått glipp av noen vesentlige poenger som ville ha medført at konklusjonen kanskje kunne ha blitt gul, eller enda verre, den kunne vise seg være blodrød, og det vil ikke være noen hjelp i kvalitetssikringen til å identifisere forholdet.

Strømmen av nye ord ser ikke ut til å ta slutt. De aller nyeste jeg har blitt introdusert for er å komme i revisjonsklemma (avledet av tidsklemma). Det skal være *tiden mot slutten av året da alle utestående revisjoner helst skal gjennomføres før årsslutt for å komme med i årsrapporten og for å bedre internrevisjonens KPI for måling av gjennomføringsgrad.* Videre det å bli sittende revisjonsfast. Dette ordet oppsto i kjølvannet av at mange satt «askefast» i 2010, og skal bety noe slik som en *ufrivillig pause i revisjonen grunnet at de du skal intervjue er opptatt med andre ting og revisjonen blir satt på vent.* Får gjerne påvirkning på revisjonsklemma over tid.

Det aller sprekeste er likevel å ta en revisjonsdødser. Dødse betyr å stupe fra stor høyde, gjøre kreative krumspring i svevet og helst unngå et solid mageplask. I revisjonssammenheng har det ennå ikke fått fullt fotfeste og det kan enten bety *å gjennomføre (kontroversielle) revisjonsprosjekter med stor fallhøyde f.eks. se på ledelseskultur e.l.* Eller det kan innebære *å utvikle internrevisjonsfunksjonen til å bli mye mer fremoverlent i alt for stor fart uten at interessentene henger med.* Noe som for øvrig kan ende med mageplask…

Returadresse
IIA Norge
Postboks 1417 Vika
0115 Oslo

www.pwc.no

Kontaktpersoner

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

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

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

Droner, roboter og kunstig intelligens

Verden er i rask endring. Internrevisjonsverdenen er i endring, men ikke raskt nok.

Som alle andre internrevisorer er vi i tenkeboksen og utforskende i forhold til hvordan morgendagens internrevisjon bør se ut. Ta kontakt, kanskje kommer vi sammen frem til en løsning som kan passe for deg.

PwC. Vil Litt Mer.

pwc