SIRK

IIA Norge

Styring – Internrevisjon – Risiko – Kontroll

Nr 1 2018

REDAKTØRENS SPALTE

ELLEN BRATAAS

Connecting the World Through Innovation var tittelen på den internasjonale IIA-konferansen som i mai fant sted i Dubai. Her var en håndfull nordmenn og jeg til stede sammen med 3 500 deltakere fra nærmere 100 nasjoner. Konferansen viser i praksis hvor global IIA virkelig er og hvilket mangfold medlemmer representerer. De kulturelle forskjellene er mange, mens interessen for faget er fellesnevneren som bringer oss sammen.

Ved åpningen av konferansen var statsminister og visepresident i De forente arabiske emirater og enehersker av Dubai, Mohammed bin Rashid Al Maktoum, også kjent som Sheikh Mohammed, til stede og la sin beskyttende hånd over konferansen. I praksis vil det si at Sheik Mohammed overvar nasjonalsangen før han forsvant med følget sitt ned den røde løperen og konferansen startet. Det er så ulikt her hjemme og så fascinerende å erfare hvor stolte emiratene er av landet sitt. Et relativt nytt land i hurtig endring der høyest, raskest, bredest, flest og mest ser ut til å være sentrale drivkrefter bak den formidable fremveksten. «Vi har 500 år å ta igjen på resten av verden», sa Mohamed Alabbar, grunnleggeren av Emaar, et av verdens største eiendomsutviklingsselskaper. I en raskt voksende økonomi vil forretningsmodellene kontinuerlig endres og dette krever en kultur der de ansatte er «connected» 24/7. Alabbar er tydelig på at det ikke handler om digitalisering, men om mennesker. Teknologien vil alltid være der, men vi som brukere må utvikle utnyttelsen av de teknologiske løsninger. «Artificial Intelligence is brainpower!»

De siste årene har digitalisering og kunstig intelligens preget både næringslivets og den politiske agendaen, og vi kan forvente store og raske endringer i forretningsmodeller og måten vi jobber på. Innflytelsesrike yngre aktører som Mark Zuckerberg, Elon Musk, Emmanuel Macron, Justin Trudeau, for å nevne noen, er i ferd med å overta styringen i verden. Nye generasjoner vokser opp med og utnytter teknologi på en helt annen måte enn vi gjorde bare få år tilbake. Et ekstremt eksempel er kanadiske Tanmay Bakshi, Neural Network Architect, Honorary IBM Cloud Advisor, som tok scenen med storm i Dubai. Til tross for sin unge alder (14 år!) fremstod han som en velreflektert Gandalf som gjennom et energisk foredrag gav oss innsikt i alle fordeler kunstig intelligens kan bringe til menneskeheten.

Så, hvor står internrevisorene opp i det hele? Som de fleste foredragsholdere i Dubai tror også jeg at internrevisorer med sin forretningsforståelse er godt posisjonert for fremtidige endringer. Likevel er det behov for ny kompetanse og mer entreprenørskap i form av endrede arbeidsprosesser og verktøy. Hvis man skal overleve i systemet må man kjenne forretningen fra utsiden og inn, ikke innenfra og ut. Og dette krever et annet tankesett enn tidligere. Med dette nummeret av SIRK håper vi å kunne bidra til noe av utviklingen.

Benytter samtidig anledningen til å ønske alle medlemmer og lesere en riktig god sommer, og avslutter med et sitat fra Richard Chambers, President & CEO, IIA global:
"Internal audit will have to undergo a radical mindset change in order to be relevant. We cannot afford to rely on how things have always been done if we are to navigate a disruptive landscape and meet growing stakeholder demands. Innovation and transformation will require visionary leadership, trial and error, commitment, and courage. This alteration — likely to be more evolution than revolution — will invariably redefine the profile of the typical internal auditor."

SIRK ønsker sine lesere en riktig god sommer!

STYRELEDER HAR ORDET

INGUNN VALVATNE
STYRELEDER
IIA NORGE

Det er et rekordtykt SIRK dere nå har i hånden, på hele 80 sider. Mens aviser og magasiner sliter med opplagstall for sine papirutgaver, opplever SIRK økt interesse fra lesernes side, og ikke minst fra bidragsyterne. Vi kan være stolte av det høye engasjementet fra medlemsmassen. Det er i fagnettverk og grupper produksjonen skapes, og her skal medlemmene hente sin faglige inspirasjon.

Mange av oss jobber i små avdelinger. Selv om internrevisjonen skal bidra løpende i verdiskapingen i virksomhetene, er kontrollaspektet ved internrevisjonen fortsatt viktig. Styrene får økt ansvar for styring og kontroll og har behov for gode støttespillere.

Uavhengig av de som kontrolleres. Det kan noen ganger oppleves ensomt, og derfor er foreningen et viktig fellesskap for deling, og det er dette som kommer til uttrykk i frivilligheten og engasjementet. Vi ser det i interessen for SIRK og ikke mindre for de årlige konferansene, som har blitt en stadig viktigere arena for møter og meningsutvekslinger.

IIA Norges styre skal på sin side gi føringer for aktiviteten og sikre at vi trekker i riktig, og i samme, retning. Det har gitt opphav til mange gode diskusjoner i styret; hva skal foreningen være? For hvem? Og hvor bredt skal det faglige nedslagsfeltet være? Diskusjonen kan ses i lys av utvikling i profesjonen generelt, og tilsvarende diskusjon utspiller seg i IIA globalt. Virksomhets- og risikostyring er viktige komponenter i internkontrollen og inngår som en viktig komponent i internkontrollen. Det samme gjelder etikk og etterlevelse.

På årets generalforsamling vil jeg gi stafettpinnen videre til Mette Storvestre og et engasjert styre som sikrer at foreningen er i gode hender. De skal ta diskusjonen videre inn i ny strategiperiode. Hele tiden i perspektiv av at foreningen skal være nyttig for medlemmene og at internrevisjonen er kjernefaget vårt.

Jeg vil takke for tre inspirerende år som har gitt anledning til kontakt med gode kollegaer her hjemme og internasjonalt. Jeg vil også oppmuntre til videre engasjement, gjerne også i foreningens styrende organer. Her vil det være behov for alle gode krefter i videreutvikling av IIA Norge.

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

Magnus Digernes
Director, KPMG AS

Marit Trodal
Prosjektleder, IIA Norge

Neste utgivelse er desember 2018

Årsabonnement: Kr. 150

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

Opplag: 1200
Meninger 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

Går pengene til formålet?

Det krever at tilskuddsforvaltningen er ivaretatt på en god måte.

Det samlede omfanget av tilskudd fra den norske staten er blant de høyeste i verden sett i forhold til innbyggertallet. Tilskuddsforvaltningen skal i første omgang sikre at tilskuddet gis til riktig målgruppe og benyttes til formålet.

BDO Utredning og analyse tilbyr spesialiserte tjenester for alle faser av tilskudds-forvaltningen. Vi kan gjennomføre utredninger,kontroller og analyser samt gi råd og oppfølging for å sikre en helhetlig og god tilskuddsforvaltning.

Vi tilbyr tjenester til tilskuddsgivere og -mottakere i privat og offentlig sektor, samt samfunnsnyttige/ideelle organisasjoner.

Kontakt oss gjerne for en uformell prat.

KONTAKT

Morten Thuve
morten.thuve@bdo.no
+47 916 47 115,

Øistein Harsem
oistein.harsem@bdo.no
+47 905 53 294

Tina-Irene Amundsen
tina-irene.amundsen@bdo.no
+47 993 57 800

INNHOLD

RISIKOSTYRING

COMPLIANCE

VIRKSOMHETSSTYRING

KONTROLL OG SIKKERHET

48

20

30

13

6

INTERNREVISJON

FASTE SPALTER

Hva har skjedd i kjølvannet av Metoo?

#metoo

#Metoo-kampanjen har satt seksuell trakassering på dagordenen og skapt mye debatt og bidratt til åpenhet. Vi tok en prat med noen utvalgte virksomheter for å høre hva de har gjort i kjølvannet av kampanjen.

Arbeidsgiver har plikt til å forebygge og forhindre seksuell trakassering. Dette følger av den nye likestillings- og diskrimineringsloven § 13 samt arbeidsmiljøloven § 4-3 (3). Arbeidsgivers plikt til å forebygge trakassering, herunder seksuell trakassering ivaretas som en del av det systematiske helse-, miljø- og sikkerhetsarbeidet (HMS) i virksomheten.

OSLO KOMMUNE:

Har Oslo kommune sett behov for å forsterke innsatsen i kjølvannet av metoo?

På sentralt nivå har Oslo kommune sammen med fire forhandlingssammenslutninger utarbeidet en felleserklæring om seksuell trakassering, hvor partene gir utrykk for en tydelig holdning om at arbeidstakere i Oslo kommune ikke skal utsettes for seksuell trakassering eller annen utilbørlig adferd. Det er også understreket betydningen av en kultur basert på åpenhet og tillit samt betydningen av å bygge en kultur hvor det er trygt å melde fra dersom trakassering forekommer. I erklæringen har partene sluttet seg til råd utarbeidet av NHO, LO, Arbeidstilsynet og Likestillings- og diskrimineringsombudet. Virksomhetene i kommunen er bedt om å gjøre erklæringen kjent og følge den opp i samarbeid med tillitsvalgte og vernetjenesten. Erklæringen var også tema på forum for HR-medarbeidere i desember 2017. Det er tatt inn en omtale av seksuell trakassering i kommunens personalhåndbok.

I tillegg har vi en rekke planlagte tiltak. Det er igangsatt arbeid for å vurdere et kurstilbud knyttet til trakassering, herunder seksuell trakassering og varsling. Retningslinjene for lokale varslingsordninger, (Oslo kommune har en sentral ordning samt lokale ordninger i samtlige virksomheter), er også under revisjon. Det vurderes å ta en inn tydeliggjøring av temaet i retningslinjene.

Byrådet ivaretar et overordnet tilsynsansvar på HMS-området. Det blir derfor årlig gjennomført revisjoner i enkelte utvalgte virksomheter. På bakgrunn av fokuset på området vil trakassering, herunder seksuell trakassering, bli et av temaene i neste HMS-revisjon.

Det vurderes også en egen rapporteringsordning, samt å ta opp temaet i forbindelse med seminarer. Videre vurderes det ulike tiltak for holdningsskapende arbeid, herunder å legge til rette for erfaringsutveksling.

Det er for øvrig Byrådsavdeling for finans ved Seksjon for personalledelse som har ansvaret for tiltakene som er beskrevet over. Internrevisjonen er sekretariat for kommunens sentrale varslingsordning. Fra og med i år er seksuelle trakassering lagt inn som en egen kategori.

I forbindelse med den årlige innhentingen av informasjon om omfanget av varslingssaker fra de lokale varslingsordningene, er det også bedt om særskilt rapportering av varsler om seksuell trakassering. Formålet med dette er dels å få en oversikt over hvor mange som benytter varslingsordningen som kanal for å si i fra, samt å rette oppmerksomheten på at varslingsordningene også kan benyttes som en av flere kanaler for å si i fra dersom varsling i linjen er vanskelig.

Har dere sett behov for å gjøre noen endringer i de etiske retningslinjene?

Nei, det er ikke blitt gjort endringer i kommunens etiske retningslinjer.

ELLEN CECILIE BRAATHEN, LEDER INTERNREVISJONEN

NAV:

Har NAV sett behov for å gjøre noe i kjølvannet av metoo?
Temaet ble tatt opp av NAVs toppleder i ledergruppen i januar i år. Det var ønske om å vurdere at vi har på plass det vi bør i forhold til eventuelle «Metoo»-lignende saker.

Hvilke tiltak har dere gjort? Hvem har i så fall vært involvert?
Det ble nedsatt en tverrfaglig gruppe bestående av representanter for HR, kommunikasjonsavdelingen, personvernombudet og internrevisjonen. Gruppen ledes av HR-direktør. Arbeidet til gruppen ble blant annet koblet opp mot etatens varslingsrutiner. Det er forøvrig internrevisjonen som «eier» denne rutinen. En rekke tiltak har blitt gjort eller er igangsatt på initiativ fra arbeidsgruppen, deriblant er temaet blitt tatt opp fra HR i samling med hovedverneombudene. Vi har også jobbet med å tydeliggjøre problemstillingen i eksisterende rutiner/regelverk, deriblant oppdaterte vi varslingsrutinene slik at det fremkommer at også seksuell trakassering er en av flere årsaker som gir grunnlag for berettiget varsling. Vi har også utarbeidet et case som nå er del av vår etikkopplæring og laget en egen side på intranett som omhandler hva seksuell trakassering er, nulltoleranse for dette, reaksjoner ved overtredelser, etc.

Hvilke konkrete endringer har dere eventuelt gjort i egne etiske retningslinjer?
NAV har ikke egne etiske regler, men følger de statlige reglene.

TERJE KLEPP, LEDER INTERNREVISJONEN

IF FORSIKRING:

Har If sett behov for å gjøre noe i kjølvannet av metoo?
Det er nok ingen som ikke har fått med seg denne kampanjen under høsten 2017.
Dette har helt sikkert vært et samtaletema på mange arbeidsplasser og private hjem.
Hos oss har det helt klart høynet fokus og oppmerksomheten knyttet til seksuell trakassering, men også om det skulle være snakk om andre former av trakassering.

Hvilke tiltak har dere gjort? Hvem har vært involvert?
Her i If ble det satt et tydelig fokus. Først og fremst via vår Nordiske HR leder som publiserte temaet på vårt intranett, men også fra vår øverste ledelse.

HR har blant annet gitt en beskrivelse av hvordan seksuell eller annen type trakassering kan rapporteres internt;

Det er gitt oppfordringer til den som av ulike årsaker ikke er bekvem med å snakke direkte med sin leder, til å kontakte sin leders leder, eventuelt ta direkte kontakt med en HR Partner, en tillitsvalgt eller verneombud. Det er også muligheter for å melde ifra via en anonymisert telefonsamtale.

Vi har også en egen side på intranettet for varslinger, som bygger på alle typer kritikkverdige forhold som berører selskapet og våre ansatte. If gjennomfører en utredning av opplysninger som måtte fremkomme, og en langsiktig kartlegging av seksuell trakassering/krenkende særbehandling i hele selskapet.

HR har også utarbeidet materiale for ledere om hvordan man blir oppmerksom på, og håndterer seksuell trakassering på arbeidsplassen. Vi har også ytterligere tydeliggjort guidelines i forhold til bruk av alkohol. Det videre fokuset vil være innenfor bygging av ønsket kultur, verdier, adferd og respekt for enkeltindividet. Aktiviteter knyttet til dette er under kontinuerlig utvikling.

Det er også besluttet å re-etablere og oppdatere introduksjonskursene for nye medarbeidere og ledere. Opplæringen vil skje i det enkelte land hvor vi har vår virksomhet. Dette for å sikre at vi snakker om å bygge den rette kultur og at vi sikrer en trygg arbeidsplass der dårlig adferd og mobbing ikke er akseptert.

Sist, men ikke minst, ble det i høst også gjennomført en egen medarbeiderundersøkelse knyttet til seksuell trakassering. Denne konkuderte med at If ligger svært godt an sammenlignet med virksomheter i landet for øvrig når det gjelder andelen som har opplevd seksuell trakassering.

Hvilke konkrete endringer har dere eventuelt gjort i egne etiske retningslinjer?
Det har så langt ikke vært behov for å gjøre noen større endringer i våre etiske retningslinjer for If. De endringer som er gjort er mer semantiske endringer for ytterligere å tydeliggjøre språket. Vår policy står trygt og dekker svært godt alle former for adferd, både de som ikke er ønskelige så vel som det vi bør stå for. Det kanskje mest overordnede og viktige å nevne i fra Ethical Guidelines for If, er;

«We work actively against discrimination, harassment and bullying. We do not tolerate any form of discrimination, harassment, bullying or any other form of physical or verbal mistreatment.»

RUNAR PETTERSEN, GROUP INTERNAL AUDIT

Hvordan identifisere og evaluere compliance-risiko?

Av
MARIT TRODAL
Prosjektleder IIA Norge

Compliance-nettverket inviterer jevnlig til Compliance & Kaffe, en uformell møtearena for presentasjon og diskusjon rundt aktuelle temaer. Et tema som opptar mange innenfor risiko og compliance er hvordan virksomheter identifiserer og evaluerer compliance-risiko. Dette var tema for et Compliance & Kaffe arrangement i februar.

Siri Simenstad, Compliance Officer i Aker Solutions og advokat Cecilie Wetlesen Borge i Haavind presenterte det juridiske bakteppet, styrets ansvar, metodikk og eksempler fra blant annet Aker Solutions, hvor prosjekter i en rekke høyrisikoland krever at virksomheten har høy fokus på risiko for korrupsjon, hvitvasking, overtredelse av internasjonale sanksjoner, overtredelse av konkurranserettslige begrensninger og handel med politically exposed persons (PEPs). Det konkrete compliance-risikobildet er opp til enhver virksomhet å identifisere. Virksomhetens bransje, størrelse, internasjonale virksomhetsområde og sektor er noen faktorer som kan eksponere virksomheten for lovovertredelse. Organisering av salgs- og innkjøpsprosesser er også relevant for hvilke elementer virksomhetens compliance-system bør inneholde. I tillegg kan internasjonale sanksjoner bidra til at forståelse av compliance-risiko blir et enda mer bevegelig og sammensatt mål.

Det er utarbeidet en rekke veiledninger som kan være nyttige å bruke, deriblant ble det henvist til Transparency International UKs «Diagnosing Bribery Risk». Selv om denne er rettet mot korrupsjonsrisiko kan mye av det som sies om utvikling av et compliancesystem overføres til andre områder. En effektiv risikovurdering starter uansett med at en representativ gruppe med god kjennskap til virksomheten vurderer en rekke spørsmål og kartlegger virksomhetens verdikjede ned i detalj (se eksempler neste side).

Videre er det viktig for compliance-funksjonen å komme tidlig inn i prosjekter og beslutningsprosesser. Det kan bli vanskelig å få nødvendige avklaringer på plass hvis funksjonen kun blir en siste instans for å sjekke av at alt er på stell når en kontrakt er i ferd med å inngås. Integrity Due Diligence (IDD) av potensielle forretningspartnere brukes til å eksemplifisere problemstillinger og mulige fremgangsmåter. En risikobasert IDD-prosess justerer dybden og bredden av undersøkelser etter hvor risikabelt et forretningssamarbeid vurderes å være, og gjør virksomheten i stand til å prioritere begrensede ressurser på forretningssamarbeid med størst risiko. Eksempler på tema som kan påvirke risikonivået er prosess for valg av forretningspartner, bestemmelser om eksklusivitet, partnerens compliance-forpliktelser, land og region hvor prosjektet/ samarbeidet/investeringen skal finne sted, forretningspartnerens modenhet, internasjonale sanksjoner av betydning for involverte parter eller produkter, tredjepartsrepresentasjon, og kompensasjonsmodell. Evalueringen danner grunnlaget for fremgangsmåten og hvilke kilder som benyttes. Relevante informasjonskilder for slike bakgrunnssjekker er offentlig tilgjengelige kilder, Google-søk, abonnementsdatabaser, egenevalueringsskjemaer, intervjuer og rapporter via eksterne leverandører. Ved bakgrunnssjekk av enkeltpersoner er personvernet et moment som må vurderes; regler for personvern vil påvirke aspekter som hvilken type informasjon som kan innhentes og brukes, hvordan og hvor lenge informasjon lagres, og hvem som kan få innsyn i informasjonen.

Når har vi tilstrekkelig bakgrunnsinformasjon?

IDD-prosessen gir utfyllende informasjon som påvirker risikovurderingen, gir retning for oppfølgingsbehov, og fungerer som dokumentasjon dersom regelbrudd skjer på et senere tidspunkt. Mangelfull informasjon når man foretar en integrity due diligence kan være en utfordring. Dersom man ikke finner noe informasjon om en potensiell samarbeidspartner i et gitt land, betyr det at det

ikke er noen 'røde flagg', eller må man nettopp da grave dypere? Her er det ikke noe fasitsvar – risikovurderingen avgjør hvor dypt man må grave.

– Å stille nærgående spørsmål til potensielle forretningspartnere kan oppleves som ukomfortabelt og krevende for førstelinjen, forteller Siri Simenstad. – Denne rollen kan gjerne vi i compliance-funksjonen ta, slik at førstelinjen kan bevare en god tone og relasjon med den potensielle partneren, samtidig som vi innhenter informasjon som er nødvendig for en fullstendig IDD.

Due diligence krever skjønnsmessige vurderinger og avhenger av hvilke ressurser og verktøy compliance-funksjonen har tilgang til. Begrenset ressurstilgang er ofte en utfordring innen compliance, og kan også kobles til «tonen fra toppen». Det er viktig at styret, og ledelsen på alle nivåer, har compliance på agendaen og at tilstrekkelig med ressurser er gjort tilgjengelig for å kartlegge risiko, sikre god respons, og planlegge og sikre oppfølging. Selv om compliance er vanskelig målbart, må virksomheter også sikre god rutinemessig intern rapportering, samt ha eskaleringsmekanismer for enkeltstående tilfeller hvor ledelsen må ta stilling til en konkret risiko eller hendelse. Den eksterne rapporteringen må også inngi tillit til at virksomheten har god oversikt og kontroll over sine compliance-risiko. For som en rekke virksomheter som har trådd feil sikkert vil skrive under på:

«If you think compliance is expensive, try non-compliance».

Tidligere U.S. Deputy Attorney General Paul McNulty

DIAGNOSING BRIBERY RISK:

- What do we do as a business?
- Do we operate in a range of businesses or markets which are sufficiently different from each other to have wholly or partially distinct risk profiles? • What interactions with the outside world do our business activities involve?
- Whom do we interact with? In particular, what interactions do we have with central or local government and public officials generally?
- What do we need from third parties that is particularly critical to our business?
- Are we able to interact directly with such third parties, or do we rely on intermediaries to help us?
- How many such intermediaries do we engage and what do they do for us?
- Where do we do business and are customs or practices in those places likely to expose us to risk?

Kilde: Transparency International UK

Test yourself

How important is risk culture to you and your organisation?

First give points to score each question below as follows:
1. No.
2. Rather not
3. I do not know
4. Rather yes
5. Yes

Then add up the total score

Question		Score
1.	My work is related to risk and the successful outcome of my work depends on the approach I take in relation to risk	
2.	The risk that my organization takes depends largely on my behaviour / actions	
3.	The concept of risk management is important to my work in the organization and this in turn affects the organisation's performance	
4.	Culture is an important element of my attitude to risk	
5.	Culture can be changed to help the organization better achieve its goals	
Total score		

Evaluation of total score
- 18+ points - You are sure that risk culture is important to you and your organization
- From 13 to 17 points - You doubt whether risk culture is important to you and your organization
- Less than 12 points - For you, culture is not relevant to you and your organization

Read further the article on risk culture on page 10 of the magazine

Risk culture – are internal auditors meeting the challenge?

By
SVETLOZAR KARANESHEV
MSc in Business Administration

Svetlozar is Head of Internal Audit at the Bulgarian American Credit Bank and a member of IIA Bulgaria. His role as Head of Internal Audit is to assess the risks of the organization and audit corporate and risk governance, strategic, control and operational management systems and functions, as well as critical business and operational processes and functions. His previous achievements are in a variety of fields including risk management, mergers, acquisitions and post-merger integration, business development, organization development, restructuring and turnaround, investment portfolio management, the design and implementation of management and control systems as well as business process design and reengineering. He is Co-Founder of the Risk Culture Lab.

svetlozar.karaneshev@gmail.com

INTRODUCTION

Risk culture has been identified as a key element of an institution's risk management by regulators and supervisors. To do their job better to audit risk culture internal auditors need knowledge not only of organizational culture, but how it interacts with strategy and governance. Communicating and co-operating with other stakeholders – Risk, HR and Compliance specialists is a good way to develop trust and a common language between stakeholders.

> Chance favours the prepared mind
>
> *Louis Pasteur*

What is driving organizations to pay more attention to their risk culture?

There could be two answers to this question: 1) driven from the outside (regulatory pressure) or 2) driven from the inside (corporate problems or enlightened, forward thinking CEO's and their management team who think culture can solve problems or add value)[1]. If changes to risk culture are driven from the inside we would expect the typical development of the process to follow the innovation adoption curve[2] and the market to decide whether the concept is viable and how fast it will be adopted. However, when regulators and supervisors influence the process, the adoption curve could be accelerated. In fact, regulators and supervisors are sending clear signals – they are requiring financial organizations to pay more attention to risk culture. Culture is one of the top ten priorities for internal audit for 2018 according to «European Report: Risk in Focus Hot Topics for Internal Audit 2018» which begs the question: «Does the internal audit function have the necessary skills and experience to assess culture and behavioural metrics? [3]».

Why are regulators and supervisors paying increasing attention to risk culture in recent times?

The answer to this question is that weaknesses in risk culture were deemed to be at the basis of the global financial crisis in 2008 and behind the misconduct of many institutions[4]. The crisis demonstrated that risk management frameworks, standards and processes are important, but not sufficient on their own to ensure that organizations reliably manage their risks. The behavioural element – why individuals, groups and organizations behave the way they do and how this affects risks, was underestimated. Regulators and supervisors realized that to assess financial enterprises' health, it is no longer sufficient to look just at facts and figures, but must include the people behind these figures and facts[5].

As a consequence, risk culture is identified as an important element of corporate governance. The Guidelines for internal governance[6] of the European Banking Authority (EBA) define risk culture as a key element of an institution's risk management. A sound risk culture enables sound and informed decision

making and financial institutions should develop an integrated and institution-wide risk culture through policies, providing examples, communication and staff training. Institutions have the obligation to develop an integrated and institution-wide risk culture based on the full understanding and holistic view of the risks they face. Sound risk culture should include good practices in the following areas[6,7]:

- *Tone from the top* – the management body should be responsible for setting and communicating the institution's core values and expectations and promote, monitor and assess the risk culture of the institution;
- *Accountability* – the staff should know and understand the core values of the institution and the institution's risk appetite and risk capacity and must be held accountable for their actions in relation to the institution's risk taking behaviour;
- *Effective communication* and challenge – sound risk culture promotes open communication and challenge regarding the decision-making process;
- *Incentives* – incentives should pay a key role in aligning risk taking with the institution's risk profile and long-term interest.

As the internal audit function has the obligation to evaluate the effectiveness and to contribute to the improvement of the risk management function[8], there are clear consequences from the EBA Guidelines: (1) risk culture, as a key element of the institution's risk management, must be in scope of the audit plans and activities and (2) to ensure that the institution's risk culture is sound, internal audit should assess the tone from the top, accountability, effective communication, the appropriateness of incentives and whether operational and strategic decisions are challenged.

Does the internal audit function have the necessary skills and experience?

Risk culture is the «bank's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks.

The integrative perspective of behavior and culture, governance and strategy & business model (source De Nederlandsche Bank)

Figure 1

Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume[9]». Familiar terms like risk awareness, risk-taking, risk management, controls are combined with not so familiar terms like norms, attitudes and behaviours. Culture and behaviour are influenced by multiple internal and external processes and factors[5]. Organizational culture interacts with external factors – regulators, customers, macro-economic developments, financial markets and internal factors – governance (organizational framework, risk management framework and processes, internal control framework) and strategy & business model (figure 1). The strategy, structure, processes and culture of the organization are formed by a central purpose and complement each other. The practical implication from this insight is that to assess and audit culture and risk culture internal audit needs knowledge not only of organizational culture, but how it interacts with strategy and governance.

Organizational culture is not a new concept for internal audit. According to the COSO integrated framework for internal control, organizational culture supports the control environment by setting expectations on behaviour that reflects commitment to integrity and ethical values, oversight, accountability and performance and evaluation[10]. To establish the reliability and validity of the approach to auditing risk culture there is a need to develop a conceptual model and a common language for risk culture. This will allow the effective identification and mitigation of behaviour and cultural risks[5]. This is not an easy task as there are a lot of organizational culture theories and models[11] and there is no common view as to which is best. Organizational culture theories and models are not ready to be implemented in the assessment of risk culture without adjustments. There is

1. *Chartered Institute of Internal Auditors. Culture and the role of internal audit. Looking below the surface, 2014 https://www.iia.org.uk/media/598939/0805-iia-culture-report-1-7-14-final.pdf*
2. *Everett M. Rogers, Diffusion of Innovations, 5th Edition, Simon and Schuster, 2003*
3. *European Report: Risk in Focus Hot Topics for Internal Audit 2018, 2017 https://global.theiia.org/news/Pages/European-Report-Risk-in-Focus-Hot-Topics-for-Internal-Audit-2018.aspx*
4. *Alessandro Carretta, Paola Schwize, Risk Culture in the Regulation and Supervision Framework, in Risk Culture in Banking, Palgrave Macmillan Studies in Banking and Financial Institutions, 2017*
5. *De Nederlandsche Bank, Supervision of Behaviour and Culture, 2015 https://www.dnb.nl/binaries/Supervision%20of%20Behaviour%20and%20Culture_tcm46-334417.pdf*
6. *European Banking Authority, Guidelines on internal governance, 2017 https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-*
7. *The Financial Stability Board, (FSB), Guidance on supervisory interaction with financial institutions on risk culture, 2014 http://www.fsb.org/2014/04/140407/*
8. *International Professional Practices Framework, Standard 2120 – Risk Management, 2016*
9. *Basel Committee on Banking Supervision, Corporate governance principles for banks, 2015 https://www.bis.org/bcbs/publ/d328.htm*
10. *COSO, Internal Control — Integrated Framework, 2013 https://www.coso.org/Pages/ic.aspx*
11. *Some of the most popular organizational culture models can be viewed on: https://www.ocai-online.com/blog/2017/Culture-Models-Overview*

no single method and no «one-size-fits-all» solution to auditing risk culture[12, 13]. Internal auditors need to understand their organization's culture and risk culture to be able to develop an audit approach and indicators for risk culture. There is a vast amount of literature on organizational culture and a growing literature on risk culture, of these I would especially mention two sources that will help internal auditors to understand better organizational culture and risk culture and the approaches to assess and audit them. The first is «Risk culture - Resources for practitioners» developed by the Institute of Risk Management (IRM)[13] and the second is «Supervision of Behavior and Culture» published by the De Nederlandsche Bank[5]. Both are giving solid theoretical foundation and practical insights and tools as to how to assess and measure risk culture.

Governance (organizational framework, risk management framework and processes, internal control framework) is a more familiar topic for internal auditors but it is complex and subject to dynamic development and change. Regulators focus on the link between risk culture and risk management. Risk culture should be developed based on a full understanding and holistic view of the risks and taking into account the organization's risk appetite[6]. Internal audit needs to understand and assess the organization's risk management framework, to give an opinion on its effectiveness, maturity and compliance with legal and regulatory requirements. Knowledge of risk management standards, frameworks and maturity models and exploring good practices are crucial for the success of internal auditors work in giving assurance in respect of risk management and risk culture.

It is common sense that strategic risks are the greatest risks for every organization, but the focus of internal audit on them is not sufficient – strategic risks represent 86% of losses in market value, but only account for 6% of the time spent by internal audit[14]. Regulators and supervisors are currently paying greater attention to strategy and the organization's business model than before. For them it is important to undertake an analysis of the institution's financial projections and strategic plan to understand the assumptions, plausibility and riskiness of its business strategy[15]. To assess and audit behaviour and culture auditors need to understand the process of identification, assessment and mitigation of risk in relation to strategy[5].

Meeting the challenge

Assessing and auditing risk culture is a serious challenge for internal audit, but it is a great opportunity too. As organizations, especially those from the financial services industry, are under increasing pressure to demonstrate their commitment to improving standards of behaviour «internal audit can be a key player in giving confidence to boards that measures put in place to change culture and thus behaviour are actually working, and that the tone at the top is reflected at all levels»[1]. To meet this expectation internal audit needs to strengthen its capacity in risk culture and its related fields of behaviour and culture, governance and strategy.

Internal auditors can do their job better in relation to risk culture assessment and audit by actively participating in the process of discovering, promoting and adopting good practices for risk culture. For this reason, they need to communicate and co-operate with other stakeholders, in the first instance with risk managers and officers, HR and Compliance managers and specialists. Creating communities of good practice in assessing and auditing culture and risk culture is a good way to put different views and perspectives on the topic, to develop trust and a common language between participants and to facilitate communication on achievements, problems and solutions.

The Risk Culture Lab is one such example of a product from Bulgaria which aims to connect experts to build knowledge on the role of Culture and Risk Culture in organizations and society and to experiment and explore Culture and Risk Culture in the context of today›s reality. May be this initiative is something for Norwegian internal auditors should consider as a tool for building knowledge by sharing experience and practice in the area of risk culture?

The Risk Culture Lab

The Risk Culture Lab is a non-commercial initiative, aimed to create opportunities through a series of events and projects, connecting experts to build knowledge and sharing local and global best practices and experiences on the role of Culture and Risk Culture. Partners of the initiative in Bulgaria are the Bulgarian Risk Management Association (BRiMA), ISACA Sofia Chapter, the Bulgarian Association for Human Resources, Society for Organizational Learning Bulgaria and the Bulgarian Association for Management Consulting. It is an open format community and the expansion of the initiative will reflect the interest and willingness of individuals and organizations to join and contribute to the initiative.

12. *The Institute of Risk Management (IRM), Risk culture - Resources for practitioners, 2013 https://www.theirm.org/media/1605851/Risk-Culture-Resources-for-Practitioners.pdf*
13. *The Chartered Institute of Internal Auditors, Board briefing: Culture and the role of internal audit, 2016 https://www.iia.org.uk/resources/audit-committees/board-briefings/board-briefing-culture-and-the-role-of-internal-audit/*
14. *Harvard Business Review, How to Live with Risks, July–August, 2015*
15. *European Banking Authority, Guidelines for common procedures and methodologies for the supervisory review and evaluation process (SREP), 2014*

Virtuell krigføring og kryptiske aktører

I 2017 stiftet flere virksomheter og organisasjoner kjennskap med Wannacry, NotPetya og en rekke andre datavirus. Det var bare begynnelsen…

Av
MARIT TRODAL
Prosjektleder IIA Norge

Hørt om Wannacry?

På ECIIA-konferansen i september 2017 fikk forsamlingen på rundt 700 deltakere spørsmål om de hadde kjennskap til Wannacry. Spørsmålet kom fra en foredragsholder som jobbet med datasikkerhet. Responsen var noen ytterst få hender i været, etterfulgt av en tirade fra foredragsholderen om at dette burde internrevisorer vite langt mer om.

Den 12. mai 2017 spredde et krypteringsvirus seg i et forrykende tempo. Over 200 000 datamaskiner i 150 land ble infisert av en type skadevare som enkelt forklart krypterer filer. At filer er kryptert vil si at de ikke lar seg lese uten en bestemt krypteringsnøkkeI som kun de som står bak angrepet har. Ved å holde data som gissel kunne bakmennene skape kaos og stille krav til løsepenger – utbetalt i kryptovalutaen bitcoin. Dette var Wannacry.

Virksomheter som FedEx, Deutsche Bahn og the National Health Service i Storbritannia ble berørt. I Tyskland hersket det kaos på togstasjoner mens systemer ble slått ut. Storbritannia ble enda mer berørt. Wannacry skapte kaos ved en rekke sykehus og institusjoner over hele landet. Rundt 19.000 medisinske konsultasjoner ble kansellert, inkludert rundt 600 kirurgiske inngrep.

Enkelt fortalt utnyttet Wannacry en svakhet i eldre operativsystemer fra Windows. Informasjon om denne sårbarheten var kjent for The National Security Agency (NSA) i USA, men hadde bevisst ikke blitt kommunisert tilbake til Microsoft. Da en gruppe hackere som kaller seg The Shadow Brokers offentliggjorde informasjon stjålet fra NSA i april 2017, inkluderte dette også info om denne sårbarheten. NSAs evne til å beskytte data havnet i et veldig dårlig lys, og de fikk mye kritikk. Når informasjon om denne sårbarheten lakk ut, åpnet det også muligheten for andre aktører å ta i bruk samme 'bakdør.' Wannacry var ikke et veldig sofistikert datavirus, men til gjengjeld var det effektivt! Ved å lure en intetanende person til å åpne et vedlegg i en mail, laget for å lure mottakeren, ble maskinen til vedkommende infisert. Hovedårsaken til at angrepet var vellykket var at Microsoft ikke hadde en sikkerhetsoppdatering som tettet dette hullet, også kalt «Eternalblue» på tidspunktet som Wannacry herjet. Dataormen scannet automatisk nettverket for å identifisere andre datamaskiner med tilsvarende svakheter. På den måten snodde ormen seg videre til andre datamaskiner og datasystemer i et forrykende tempo.

Hva stoppet spredningen? Marcus Hutchins, en 23 år gammel IT-spesialist

oppdaget tilfeldig en 'kill switch' i den skadelige programvaren. Hutchins ble hyllet for sin innsats i Storbritannia. En ung hacker som fortsatt bodde på gutterommet hjemme hos sine foreldre ble en 'accidential hero.'

Metoder og gråsoner

Tilbake til foredragsholderen under ECIIA, som for øvrig heter Jaya Baloo, CISO i KPN Telecom i Nederland og internasjonalt anerkjent innenfor informasjonssikkerhet og cyber risiko. Baloo skisserte spørsmål hun og hennes team umiddelbart stiller når nettverk utsettes for dataangrep og de må vurdere hvordan de skal håndtere angrepet. Hva er taktikken som benyttes? Er det et mønster som kan sammenlignes med tidligere angrep? Har vi sett det før? Er det et ondsinnet angrep? Krever de løsepenger?

For å bekjempe dataangrep må man ha inngående kjennskap til skadelige datavirus, hvordan de er utviklet, metoder, eksempler. Uavhengige datasikkerhetsspesialister kan selv være involvert i handel og infiltrere forum for å skaffe seg informasjon og holde seg oppdatert. Dette er metoder som rettslig er forbeholdt et lands politi eller etterretningstjeneste. I denne gråsonen kreves det meget god manøvrering, noe helten fra Wannacry også skulle oppdage. Tidlig august 2017 ble Hutchins arrestert av FBI-agenter i Las Vegas, hvor han deltok på Defcon, en internasjonal hacking konferanse. FBI mistenker Hutchins for å stå bak utviklingen og salget av Kronos, en type skadelig programvare designet for å stjele informasjon om kunder fra banker. Utfallet er ennå ikke klart. Saken er per mars 2018 ikke brakt inn for retten i Los Angeles, hvor Hutchins nå oppholder seg i påvente av rettsaken. Strafferammen i USA er på 40 år, dersom han blir funnet skyldig på alle tiltalepunktene.

Kryptovaluta og kaos

Det er fortsatt ikke kjent hvor mye skade Wannacry forårsaket i løpet av disse fire dagene i mai 2017, men løsepenger som ble utbetalt til bitcoin wallets var på totalt 140 000 USD. Disse løsepengene ble senere tatt ut og trolig kjørt gjennom en såkalt 'bitcoin mixer', en hvitvaskingsprosess som skjuler spor slik at bitcoins anonymt skal kunne omsettes til hard valuta.

Mulighetene til å få løsepenger utbetalt i kryptovaluta er imidlertid mildt sagt en lukrativ business som er i voldsom vekst. Fra 2015 til 2017 økte antall dataangrep med 2000 %, ifølge Malwarebytes Labs, et internasjonalt datasikkerhetsselskap. Men selv om det ble fremmet krav om løsepenger fra aktørene bak Wannacry, så anslår en rekke eksperter at Wannacry var politisk motivert – primært for å skape kaos. Dette skulle også den danske shippinggiganten Maersk få erfare da selskapet i juni 2017 ble utsatt for et dataangrep omtalt som NotPetya, som benyttet seg av samme sårbarhet som Wannacry, men som primært var ute etter å forvolde skade og ødeleggelser. Dataormen spredde seg raskt gjennom sentrale IT-systemer og lammet terminaler og deler av virksomheten. Midt oppi dette kaoset måtte ansatte likevel håndtere containerskip på vei inn og ut av havner. Omtrent hvert 15. minutt i gjennomsnitt er et Maersk containerskip på vei inn i havn et eller annet sted i verden med mellom 10-20 0000 containere klar til å bli losset. Maersk måtte håndtere denne logistikken i 10 dager uten IT-systemer til hjelp. Samtidig måtte hele IT-infrastrukturen reinstalleres, noe som innebar 4000 servere, 45 000 PCer og 2500 applikasjoner. I sin tale på World Economic Forum i vinter beskrev Møller-Maersk styreleder Jim Hagemann Stabe arbeidet som en heroisk innsats som i verste fall kunne tatt seks måneder, men som ble gjort i løpet av 10 dager. Takket være enorm innsats fra ansatte, opplevde selskapet kun en reduk-

DET SVAKESTE LEDD

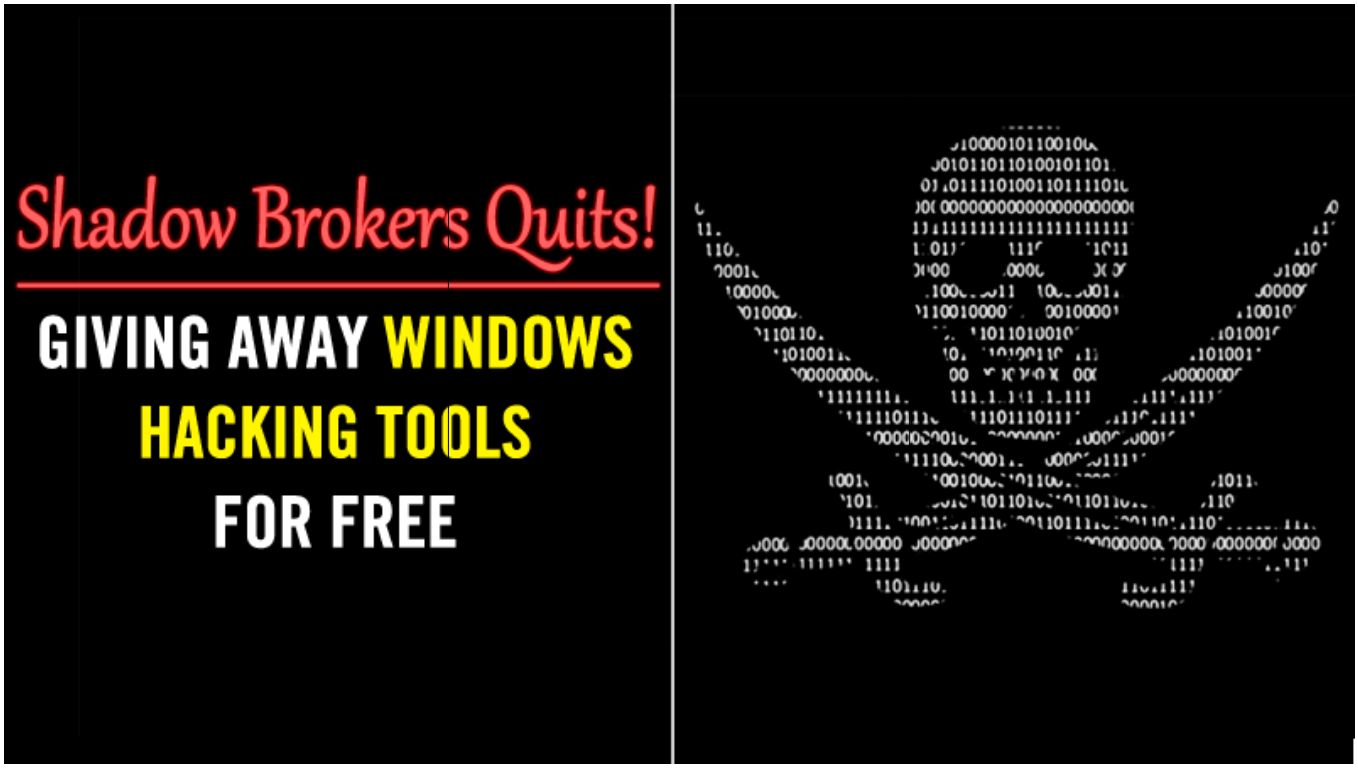
SKREVET AV FRANK ULFSBY ERIKSEN – SENIOR MANAGER I EY

Oppgradering av IT-systemer er et viktig tiltak for å sørge for at kjente sårbarheter ikke utnyttes, men hva skal til når kriminelle aktører utnytter hittil ukjente sårbarheter?

En moderne virksomhet er i dag tilknyttet internett på en eller annen måte, med alt fra e-post til leveranse av digitale tjenester til sine kunder. Dette betyr at virksomheten har en økt eksponering mot trusler som Hackere, Wannacry eller annen skadevare.

Tekniske tiltak alene er ofte ikke godt nok, da de kriminelle ofte ligger et lite hestehode foran slik at de kan utnytte hittil ukjente sårbarheter. Ved å utnytte dette sammen med det svakeste leddet som er mennesket, trenger de kriminelle ikke å bryte seg inn via brannmurer og andre tekniske tiltak. De trenger kun en person som trykker på en lenke i e-post for å få fotfeste. I praksis betyr dette at de kriminelle går mot det svakeste ledd, den ansatte. Virksomheten er dermed ikke sterkere enn det svakeste ledd. I praksis betyr dette at virksomheter må ha en helhetlig tilnærming og kontinuerlig fokus på informasjonssikkerhetsarbeidet for å minimere konsekvensen når en slik hendelse inntreffer. For en slik hendelse vil skje før eller siden, spørsmålet er om virksomheten er forberedt, kompetent og reagerer raskt nok til å håndtere hendelsen når den inntreffer.
Man ville tro at selskaper som Maersk hadde god kontroll på dette, og det hadde de trolig også. Men allikevel hadde NotPetya-viruset store konsekvenser, både økonomisk og omdømmemessig. Still dere spørsmålet, hvorfor det? Kan det ha noe med det svakeste leddet å gjøre? Maersk fikset problemet veldig raskt og trolig med minimale skader gitt situasjonen. Vil andre virksomheter klare dette, eller kan en slik hendelse være kroken på døra?

Hovedpoenget her er at et utelukkende fokus på teknisk sikkerhet og oppgradering ikke er tilstrekkelig. Man må se på informasjonssikkerhet som noe alle virksomheten bidrar til, og det er kombinasjon av menneskelige, organisatoriske og tekniske tiltak. Har man en slik tilnærming, vil man trolig være mye bedre rustet til å oppdage hendelser tidsnok, håndtere de og begrense skaden slik at det påvirker virksomhetens omdømme og økonomi i minst mulig grad.



sjon på 20% i volum, mens de resterende 80% ble håndtert manuelt inntil systemene igjen fungerte. Maersk har i etterkant estimert med at NotPetya kostet selskapet nærmere 300 millioner USD.

Hvem står bak?

Svaret er sjelden opplagt. Er det aktører som er støttet av myndigheter i Russland? Nord-Korea? Andre land? Eller opererer de på egenhånd? Verden har etter hvert stiftet bekjentskap med blant annet the Shadow Brokers og the Lazarus Group. Utover navnene de opererer under kjenner man ikke identiteten til dem som står bak, men sistnevnte gruppe tror mange eksperter er støttet av Nord-Koreas regime. Nord-Korea har etter hvert fått et avansert cyber program med en egen hær av hackere. Disse sitter ikke nødvendigvis i Nord-Korea, men opererer ut fra for eks. Kina. Nord-Korea har lite å tape på å føre cyber krig og landet trenger hard valuta i statskassa. De senere årene har grupper som knyttes til Nord-Korea gjennomført en rekke større ran av kryptovaluta internasjonalt. Den virtuelle arenaen er en yndet plass å operere i grunnet tilnærmet anonymitet. Der spionasje tidligere ble forbundet med fysisk tilstedeværelse og en del risiko, foregår vår tids spionasje i det virtuelle rom uten større risiko. I tillegg gir det også en mulighet for aktørene bak å demonstrere hvor sofistikerte de er og hva de evner å gjøre.

Oppgradering er ikke nok!

Så hva har Wannacry lært oss? Dataviruset var ikke spesielt sofistikert, men illustrerte hvor viktig det er å ha den beste beskyttelsen mot et angrep – til enhver tid. Dersom du unnlater å kontinuerlig oppgradere IT-systemene gjør det de mer sårbar – OG hackere har sannsynlig tilgang til informasjon om denne sårbarheten. Så fremt vi er koblet mot internett så er vårt digitale fotavtrykk tilgjengelig for alle som ønsker å vite mer. Men siden mai 2017 har dataangrep imidlertid blitt mer sofistikerte og Wannacry har inspirert en type angrep som går under betegnelsen 'zero-day attacks'. Kort forklart kan det oppdages ukjente sårbarheter i programvare, et ørlite hull i en brannmur som gjør det mulig å bryte seg inn i datamaskinen. Når leverandøren får kunnskap om dette hullet eller selv oppdager det, kan den utvikle en 'patch' og anmode brukere om å oppgradere. Oppgradering er imidlertid ofte ikke tilstrekkelig da angrepet kan ha skjedd før sårbarheten er tettet. Så lenge vi legger digitale fotavtrykk og blir mer og mer digitalisert, så øker også sårbarheten.

Kilder:
https://www.youtube.com/watch?v=O_k9W14F76s TEDxRotterdam 'Cybersecurity every day' Jaya Baloo, Nov 2017
https://www.wired.com/story/2017-biggest-hacks-so-far/
https://www.calyptix.com/top-threats/biggest-cyber-attacks-2017-happened/
https://nrkbeta.no/2017/05/15/nrkbeta-forklarer-dataormen-wannacry/
https://www.bloomberg.com/news/articles/2018-01-16/north-korean-hacker-group-seen-behind-crypto-attack-in-south
https://www.nytimes.com/2018/02/18/technology/virtual-currency-extortion.html
https://phys.org/news/2018-03-bank-england-chief-slams-cryptocurrencies.html#jCp
https://www.tv2.no/a/9722595/
https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-finally-cashed-out-about-140000-in-bitcoin/
https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/
https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper

Internrevisjon av cyber security

– hvordan benytte angrepssimulering for å avdekke de reelle risikoene

Av
MAGNUS FELDE
Magnus er manager i Deloitte Cyber Risk Services hvor han leder fagområdet strategi og risikostyring. Han har en mastergrad innen informasjonssikkerhet samt en Master of Management fra BI, og har lang erfaring med gjennomføring av risikovurderinger og revisjoner på tvers av ulike sektorer.

Av
LINN KRISTIN KLAUSEN
Linn er konsulent i Deloitte Cyber Risk Services, og har en master i etterretning og internasjonal sikkerhet fra King's College London. Hun arbeider med trusseletterretning og informasjonssikkerhet.

Innovasjon, informasjonsdeling og tillit er tre fundamentale vekstdrivere for virksomheter i dagens digitale samfunn. Digitalisering introduserer forretningsmuligheter gjennom fremvekst av nye virksomheter, endring av eksisterende virksomheter, nye produkter og tjenester. Begrepet cyber kan oversettes på norsk til det digitale rom. Økt digitalisering introduserer nye risikoer som må identifiseres og håndteres.

Mange nye virksomheter baserer sin forretningsidé på omfattende innsamling og analyse av data, ofte i samarbeid med tredjepartsaktører. Disse er spesielt utsatt for lekkasjer eller misbruk av informasjon. Facebook-skandalen er et nylig eksempel på dette. Slike hendelser vil medføre tap av tillit og kunne trigge behov for økt regulering. Digitalisering medfører en større forretningsmessig avhengighet av IT-løsninger. Nedetid vil kunne medføre store forretningsmessige- og økonomiske konsekvenser. Banker og telekom-virksomheter har erfart viktigheten av å sørge for oppetid av systemer.

Enkelthendelser, være seg tilsiktede eller utilsiktede, vil kunne resultere i store negative konsekvenser for virksomheter. Eksemplene på slike saker er mange. Mærsk har rapportert et tap på 300 millioner dollar som følge av at deres IT-systemer ble utilgjengelige etter å ha blitt utsatt for et løsepengevirus kalt «NotPetya» [1]. Facebook er i hardt vær som følge av at informasjon om 85 millioner av deres brukere ble delt med Cambridge Analytica, som igjen har brukt informasjonen til analyser. Disse er solgt til klienter. Hva de endelige konsekvensene av saken vil innebære for Facebook gjenstår å se, men etter at nyheten ble kjent har markedsverdien av virksomheten blitt redusert med 100 milliarder dollar [2].

En viktig premiss for enhver revisjon vil være å avdekke hvorvidt hensiktsmessige tiltak er implementert i tråd med etablert risikoappetitt, og hvorvidt tiltakene fungerer som tiltenkt. Den økte cyber risikoen knyttet til digitalisering fordrer at internrevisjonen vurderer virksomhetsstyring og kontroll av sikkerheten i det digitale rom. Spørsmålet er hvordan man best bør gå frem for å avdekke dette.

Et komplekst digitalt økosystem bestående av en rekke aktører kombinert med høy endringstakt tilsier at det vil være utfordrende for enkeltpersoner å vurdere den faktiske sikkerhetstilstanden i organisasjonen. Deloitte benytter et spesialtilpasset rammeverk for dette. I tillegg gjennomfører vi angrepssimulering med hjelp av et teknisk ekspertteam kalt «red team» for å avdekke sikkerhetshull. Vår erfaring er at denne kombinasjonen av aktiviteter gir et svært godt bilde av dagens situasjon i virksomheten, og danner et godt grunnlag for å definere en tiltaksplan som er med på å redusere den reelle risikoen.

Trusselbildet i det digitale rom er i stadig endring, og kompleksiteten tilsier at man må håndtere cyber-sikkerhet nyansert og dynamisk. Trusselnivået og risikoeksponeringen må forstås opp mot spesifikke komponenter som inngår i et helhetlig styringssystem for cyber sikkerhet – og bør være integrert i den totale virksomhetsstyringen. I utarbeidelse av styringssystem er det viktig å forstå trusselbildet, og se dette opp imot hvilke kapabiliteter som er nødvendig å ha på plass for å sikre informasjonsverdier hensiktsmessig. Disse komponentene kan deles inn på ulike måter, og det finnes en rekke rammeverk og god praksis som beskriver slike komponenter.

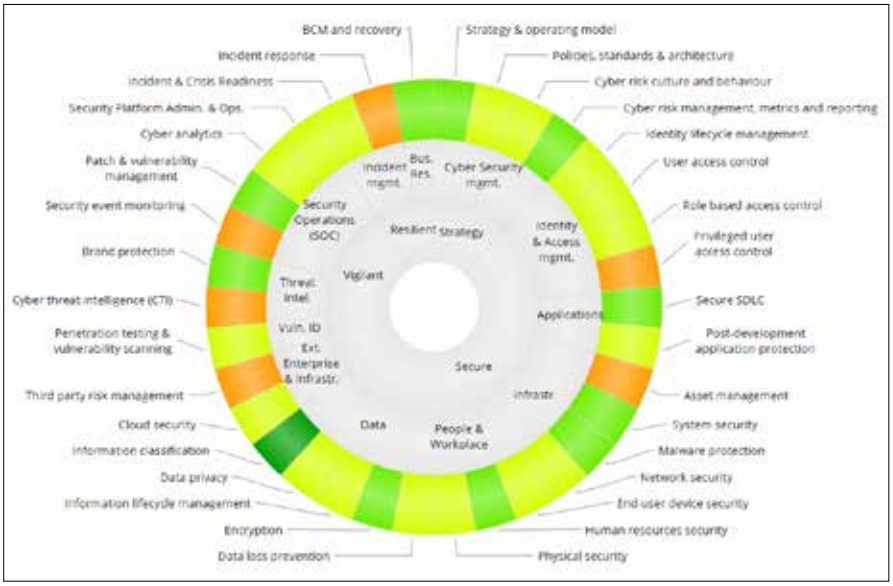
Deloittes rammeverk, kalt *Cyber Strategy Framework (CSF)* inneholder god praksis ift. cyber-kontroller knyttet opp mot risiko og type virksomhet. Et dedikert team sørger for å oppdatere dette i tråd med utviklingen av cyber-risiko og vår erfaring. Rammeverket muliggjør en strukturert og risikobasert tilnærming for å vurdere cyber tilstanden i virksomheten,

og med utgangspunkt i dette utarbeide handlingsplaner. Rammeverket hjelper oss med å identifisere verdier, trusselaktører og manglende eller mangelfulle kontroller.

Innen cyber-sikkerhet eksisterer det en rekke ulike standarder og rammeverk som benyttes for å etablere hensiktsmessige sikkerhetstiltak, og det er viktig å bruke et metodeverk som er dekkende og tilpasset den aktuelle virksomheten. International Organization for Standardization (ISO) 27001/2, Control Objectives for Information and Related Technologies (COBIT), Information Technology Infrastructure Library (ITIL), og Information Security Forum (ISF) Standard of Good Practice for Information Security er alle eksempler på rammeverk som benyttes for å ivareta cyber-sikkerhet.

Uavhengig av hvilken standard eller rammeverk som er benyttet for å håndtere cyber-sikkerhet kan CSF benyttes for å utføre en vurdering av etablerte tiltak. CSF kan benyttes selvstendig eller som en kartlegging mellom andre rammeverk. Videre vil resultatene fra CSF-vurderingen automatisk kunne presenteres opp mot ISO 27002, NIST Cybersecurity framework og CIS Top 20 Controls.

Center for Internet Security (CIS) er en ikke-for-profitt organisasjon som regelmessig utarbeider 20 sikkerhetskontroller for cyber, i prioritert rekkefølge. Ved å implementere kun de fem første kontrollene estimeres det at cyber-risikoen kan reduseres med omtrent 85%. CSF er bygd opp på tilsvarende måte, og oppdateres jevnlig for å være aktuell opp mot det gjeldende trusselbildet og god praksis. Hvert område innen cyber rangeres på en modenhetsskala fra 1-5, der etablering av de grunnleggende kontrollene på nivå 1-3 vil redusere brorparten av risikoen. Grunnet stadig mer sofistikerte angrep og flere digitaliserte løsninger, ser



CSF-hjulet.

vi likevel at området i stor grad er hendelsesdrevet. Risikostyring på området blir dermed ofte vilkårlig. I mange tilfeller er avanserte kontroller på plass mens det helt grunnleggende mangler. For å vite hvilke komponenter som burde være på plass anbefaler vi en risiko-basert tilnærming til cyber-sikkerhet, med forståelse for forretningskontekst og trusselbilde.

Deloitte deler opp en cyber-modenhetsvurdering i fem faser som vist under.

I den innledende fasen kartlegges forretningskonteksten og bedriftens viktigste informasjonsverdier (kalt bedriftens «kronjuveler»).

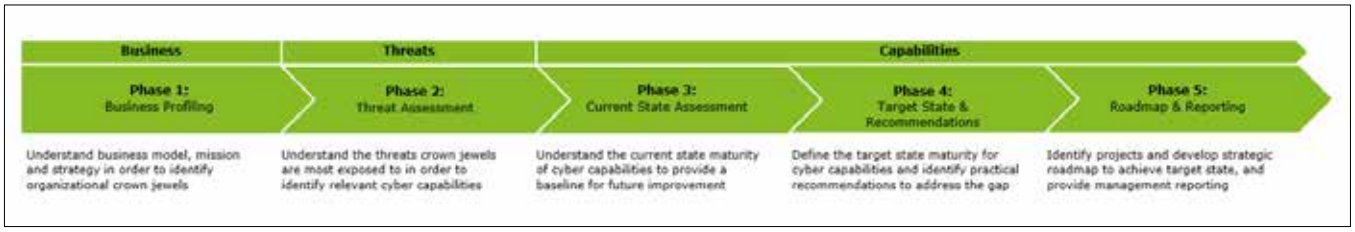
Fase 1 blir et naturlig bakteppe til fase to, hvor en trusselvurdering utarbeides. Det er viktig å identifisere aktuelle trusselaktører, deres taktikker, teknikker og prosedyrer, samt sannsynlige angrepsvektorer og trusselscenarioer. Disse utarbeides basert på tidligere angrep på bedrifter med linkende profil og eksponering.

Fase tre er en analyse av virksomhetens modenhet, med de to foregående fasene (forretningsprofilering og trusselvurdering). Denne fasen er en gjennomgang av virksomhetens nåværende modenhet. Dette kan gjøres på flere forskjellige måter. Cyber sikkerhet deles opp i 34 kapabiliteter som i kombinasjon vurderer tiltak for å forhindre, oppdage og respondere på sikkerhetshendelser.

Disse områdene blir gradert på en modenhetsskala fra 1-5, fra ad-hoc og varierende praksis til systematisert og optimalisert styring med kontinuerlig forbedring gjennom både inkrementelle og innovative endringer.

For å fastsette modenheten kan flere forskjellige metoder benyttes.

1) Vi gjør en dokumentgjennomgang og gjennomfører intervjuer innenfor de ulike kapabilitetene med nøkkelansatte i linjeorganisasjonen. De kan ofte hjelpe til med å identifisere svakheter i styringen, som kan ha mange forskjellige årsaker. Disse svakhetene rangeres. Resultatet sammenliknes med tilsva-



Cyber modenhetsvurderingens fem faser.

rende bedrifter; i samme industri, fagområde, av tilsvarende størrelse og trusselprofil. Dette gjøres via et stort datagrunnlag – all informasjonen vi henter inn anonymiseres og aggregeres for sammenlikning og kalibrering – og er nyttig for virksomhetene da det viser hva som er beste praksis i markedet i dag innenfor cybersikkerhet.

2) Deloitte tar ofte stikkprøver for å teste kontrollene som er implementert. Slike tester er viktig, og viser effekten av implementerte tiltak. De gir imidlertid ikke svar på om en hacker kan omgå tiltaket.

3) For å avdekke hull i sikkerhetsarkitekturen til virksomheten utfører Deloitte en angrepssimulering med et ekspert team kalt «red team». Med utgangspunkt i informasjonen vi identifiserer i de to første fasene vil vi kunne definere scenarioer og mål som angrepssimuleringen skal forsøke å oppnås. Dette vil typisk være scenarioer som vil få store konsekvenser for virksomheten dersom en angriper lykkes. Dette kan være å teste om vi kan overføre en betydelig pengesum fra en finansinstitusjon eller stoppe trafikken hos en infrastrukturoperatør ved å tilegne oss tilgang til kjernesystemene i virksomheten.

Angrepssimuleringen blir skreddersydd til den enkelte virksomhet, og i likhet med reelle angrep blir «minste motstands vei» utnyttet for å oppnå sluttmålet. Her vil inngangsporten kunne være å fysisk lure seg inn, utnytte eksternt eksponerte IT systemer eller sende såkalt «spear phishing» e-poster til ansatte. Angriperen vil bruke ervervede tilganger for å komme seg videre inn i organisasjonens infrastruktur på jakt etter hovedmålet. Nettopp fordi målet er å oppnå adgang til kjernesystemene er det viktig at angrepsteamet har en tett dialog med nøkkelpersonene i virksomheten for å sikre en god og trygg prosess.

Ettersom det ikke vil være mulig å forhindre ethvert angrep vil det også være viktig å ha kapabiliteter til å oppdage og respondere på hendelser som inntreffer. Som en del av angrepssimuleringen er det derfor som regel ønskelig å teste organisasjonens evne til å oppdage slike angrep. Dette fordrer at kun noen utvalgte nøkkelpersoner er gjort kjent med testen på forhånd slik at testen blir så realistisk som mulig. I etterkant av testen vil det være mulig å raskt identifisere hvor angrepet burde ha vært oppdaget slik at etablerte tiltak kan forbedres, samt identifisere områder som krever økt overvåking.

Resultatene fra en slik test gir således svært håndfaste observasjoner som kan brukes for å definere anbefalte tiltak. Resultatene fra testene vil videre være svært virkningsfulle ved at man har bevist at et konkret scenario faktisk er mulig, og ikke bare «sannsynlig». Dette er svært nyttig for å gi helt konkrete anbefalinger til forbedringer av sikkerhetsarkitekturen.

Fase 1-3 legger grunnlaget for en handlingsplan som fastsettes i fase 4, og et transformasjonsprogram som fastsettes i fase 5.

I fase 4 vurderes det om eksisterende sikkerhetstiltak er hensiktsmessige. Dersom vi i fase 3 avdekket manglende eller lite effektive tiltak vil vi etablere en handlingsplan som definerer hvilke tiltak virksomheten på kort og lang sikt bør etablere for å operere innenfor en akseptabel risiko. Det er viktig at denne fasen utføres i tett samarbeid med virksomheten, og at det vurderes hvordan anbefalingene passer opp mot forretningskontekst og øvrige handlingsplaner.

Fase 5 – transformasjonsfasen - er typisk et omfattende omstillingsprosjekt og dekker som regel alle de 34 kapabilitetene som er identifisert innenfor cyber-sikkerhet. Denne fasen utføres derimot ikke i tradisjonelle internrevisoroppdrag, og omtales derfor ikke videre i denne artikkelen.

De iboende cyber-risikoene som økt digitalisering medfører må som nevnt identifiseres og håndteres. Rammeverket som er beskrevet i denne artikkelen hjelper organisasjoner med å avdekke hvorvidt hensiktsmessige tiltak er implementert og om disse fungerer som tiltenkt – for således å kunne vurdere om risikoen ligger på et akseptabelt nivå.

Grunnet stor endringstakt, et dynamisk trusselbilde og stadig nye sårbarheter som kan utnyttes, er det viktig å jevnlig vurdere om man har de riktige tiltakene på plass. Rammeverket med tilhørende verktøy gir mulighet for enkelt å foreta en ny evaluering for å se utviklingen av pågående arbeid eller avdekke hvorvidt nye tiltak er nødvendig. Dette vil bidra til å styrke styring og kontroll av risikoene i det digitale rom (cyber risikoer).

Modenhet	Beskrivelse
1	Grunnleggende: kapabilitetene er udokumenterte og i konstant forandring (ad-hoc)
2	Gjentagende: repeterende kontroller, men ikke fullt dokumenterte eller dekkende for området – det er fortsatt noe grunnleggende.
3	Definert: definert styringssystem, formell dokumentasjon, fastsatt scope og eierskap til prosesser, rutiner eller systemer. Styringen er gjeldende på tvers av bedriften.
4	Styrt: tilsier aktiv styring der ytelse måles regelmessig og tiltak identifiseres.
5	Optimalisert: kapabiliteten er under kontinuerlig forbedring gjennom både inkrementelle og innovative endringer. Det er avanserte og industri-ledende implementering med full dekning.

[1] https://www.ft.com/content/a44ede7c-825f-11e7-a4ce-15b2513cb3ff
[2] http://fortune.com/2018/03/26/facebook-stock-ftc-investigation-cambridge-analytica/

KOMMENDE AKTIVITETER HØSTEN 2018

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

INTRODUKSJON TIL INTERNREVISJON

11. september 2018, 09.00 – 16.30

På denne dagen vil vi gi en innføring i internrevisors roller og ansvar, begrepsavklaringer og definisjoner, samt hvilke etiske regler og hvilke krav som ligger i internrevisjonens standarder.

Formål med kurset:

Gi deltagerne grunnleggende forståelse for internrevisjonsrollen og det faglige rammeverket rollen og arbeidet baseres på. Innholdet i kurset er nødvendig basiskunnskap for kurset Praktisk Internrevisjon.

Kurset dekker følgende:

- Internrevisjonsprofesjonen
- Internrevisjon – roller og ansvar
- Internrevisjonens formål og nytteverdi
- Governance, risikostyring og internkontroll
- Samspill med andre bekreftelsesfunksjoner
- Det profesjonelle faglige rammeverket med hovedfokus på standardene
- Sertifiseringer inne profesjonen

PRAKTISK INTERNREVISJON

25. – 27. september 2018, 09.00 – 16.00

I løpet av disse dagene vil vi gi innføring i planlegging, gjennomføring og rapportering av internrevisjonsprosjekter. Ved hjelp av case og diskusjoner vises god praksis for gjennomføring av enkeltprosjekter, men også knytningen til virksomhetens helhetlige risikostyring, revisjonens årsplan og rapportering til ledelsen og styret berøres i kurset.

Kurset dekker:

Praktisk gjennomføring av det enkelte revisjonsprosjekt, herunder:

– Planlegging
– Gjennomføring
– Rapportering
– Oppfølging
– Dokumentasjon
– Kvalitetssikring

Kurset vil også gi deltagerne forståelse for koblingen til risikodrevet årsplanlegging, rapportering til ledelsen og styret og omtale spesielle forhold relatert til IT- og mislighetsrevisjon.

SKRIV RAPPORTER SOM SELGER!

17. oktober, 09.00 – 16.30

Hva bør en revisjonsrapport inneholde og hvordan få frem det viktigste budskapet til de ulike interessentene? Mye hardt arbeid legges i å skrive rapporter, men rapportene får ikke alltid den gode virkningen vi hadde håpet på. Hvordan skrive rapporter som blir lest og fulgt opp?

Dette får vi lære mer om av Christine Calvert, tekstdoktor med over 25 års erfaring som skribent, underviser Digital markedsføring på Westerdals Oslo ACT. Forfatter av "Skriv for nettet – kort og godt" og "Skriv så det selger"

MEDLEMSMØTE STATLIG SEKTOR

13. juni og 30. august

Mer informasjon om tematikken på disse nettverksmøtene finner du på nettet.

We proudly present Stephen Maycock CFIIA, CRMA, CIRM, a professional trainer, writer and consultant. His broad international experience spans a number of sectors, and this has provided him with some fascinating case studies which he uses to bring his training to life.

TECHNIQUES FOR EFFECTIVE TESTING

13th and 14th November 2018, 09.00 – 16.00,

This course will help you design testing activities that are efficient, effective and appropriate to each situation. You will learn how to focus on clear objectives throughout the testing process and use this to produce sound conclusions that are more likely to be accepted by management. Upon completion you will be able to:

- appreciate the role of testing within the context of the internal audit process
- design tests focused on achieving test objectives and meeting assurance requirements
- select and apply sampling techniques that will help to ensure test objectives are achieved
- appreciate the different ways in which a range of Computer Assisted Audit Tools and Techniques (CAATTs) can be used to support testing activities
- conduct tests and document test results in a manner that will help to ensure accuracy, efficiency, integrity and confidentiality
- interpret test results and develop conclusions that are supportable with appropriate evidence
- present test results to management in a manner that will contribute to obtaining agreement on any actions that may be required
- understand how to develop and preserve relationships whilst maintaining high ethical standards

AGREEING FINDINGS AND ACTIONS – A CLOLLABORATIVE APPROACH

15th November 2018, 09.00 – 16.00

The most challenging aspect of an assurance process is often the stage in which assurance providers discuss their findings and recommendations with management and seek to agree the actions that management will take. This course provides a clear structure for approaching this task and contains many tips that will help to ensure success. Upon completion you will be able to:

- identify the key aspects of a finding
- interpret the results of your work and develop findings that are supported by appropriate evidence
- link findings to business risks
- develop recommendations that will add value to the organisation
- anticipate and deal with challenges related to findings and recommendations
- agree actions with management that are achievable and valuable

Register at **www.iia.no/aktiviteter**.

IT-skandalen på Transportstyrelsen

– Er internrevisor en varsler?

Hele førerkortregisteret, inklusive de med hemmelig identitet, lå åpent tilgjengelig for ansatte hos outsourcingspartner når Transportstyrelsen i Sverige satte ut IT-driften. Flere IBM-ansatte hadde full tilgang til alle data og logger, noe som gav mulighet til å kopiere og sende videre informasjon for senere å slette alle spor. Regjeringens håndtering av saken førte til at det i 2017 ble fremsatt mistillitsforslag mot tre statsråder og det ble flere utskiftninger i den svenske regjeringen i tillegg til at direktøren i Transportstyrelsen måtte gå.

Av
ELLEN BRATAAS
Generalsekretær IIA Norge

Annette Olofsson som ledet internrevisjonen i Transportstyrelsen rapporterte gjentatte ganger over tre år om brudd på flere svenske lover uten å få gehør hos ledelsen. Hun forsøkte også å informere styret om hva som var i ferd med å skje. Under granskingen påsto både styret og direktør at de «ikke kjente til» at de brøt med lover eller hvor alvorlig det de gjorde var. Annette på sin side, kunne dokumentere at hun gjorde sin jobb og at styret kjente til direktørens beslutninger.

Annette ble innkalt til en høring i Konstitutskottet (Sveriges svar på kontroll- og konstitusjonskomiteen) hvor hun i 70 minutter redegjorde for arbeidet hun hadde gjort og kom med sin versjon av saken. Høringen kom inn på mange interessante utfordringer som internrevisorer, spesielt i norske statlige virksomheter, også vil kjenne seg igjen i, som blant annet rapporteringslinjer og ledelseskultur. Opptaket er tilgjengelig på nett for de som er interessert.

«Det är många som inte klarar av att stå upp och stå emot när det behövs som mest», sier Annette Olofsson til et intervju med Ekspressen. «Och problemet», mener hun, «handlar om mer enn en IT-skandal. Det har handlat om bristande riskanalys, riskhantering och proaktivitet. Det har behövts mer transparens och medvetenhet i kultur- och ledningsfrågor».

> «Problemet handlar om mer enn en IT-skandal. Det har handlat om bristande riskanalys, riskhantering och proaktivitet»
>
> *Annette Olofson, internrevisjonsleder i Transportstyrelsen*

I Sverige utnevnes årlig en GRC-profil som er en utnevnelse til individer som har gjennomført enestående innsats innen GRC - governance, risk og compliance. I 2018 ble flere medarbeider fra Transportstyrelsen nominert til denne prisen, for sitt arbeid med å styrke og beskytte virksomheten og ta vare på landets og skattebetalernes interesser. En av de nominerte var leder av internrevisjonen, Annette Olofsson. Dette falt ikke i god jord hos ledelsen i Transportstyrelsen, som forbød sine medarbeidere å motta utmerkelsen av følgende grunn: «Medarbetare hos oss ska inte ens kunna misstänkas för att låta sig påverkas av ovidkommande önskemål eller hänsyn i sitt arbete. I aktuell situation är det därför ur ett myndighetsperspektiv problematiskt – utifrån principen om orubbad saklighet och opartiskhet – att ta emot priset och delta vid det aktuella tillfället.»

I en kommentar på IIA Sveriges nettside sier generalsekretær Linda Lundin: «Jag hade, i likhet med Transportstyrelsens medarbetare, mycket svårt att se hur detta skulle kunna vara ett hot mot medarbetarnas opartiskhet och saklighet. Det är ju ett branschpris som tilldelas av en jury bestående av framstående GRC-profiler, med branschens förtroende. Å andra sidan, kanske det är jag som inte ser det Transportstyrelsens ledning ser?»

Saken gikk videre til Etikknemnden i IIA Sverige som etter en nøye vurdering konkluderte med at «Det inte är i strid med Yrkesetisk kod att delta i evenemanget eller att, om de skulle vinna, acceptera priset.» . Den 1. februar 2018 ble kåringen foretatt og prisen gikk følgende gruppering i Transportstyrelsen: Annette Olofsson, leder av internrevisjonen, Tobias Ander, Chief Information Security Officer, Johan Eriksson, tidligere Chief IT Security Officer og Jens Johanson, Chief Security Officer.

Den 26. april i år ble Annette Olofsson tildelt den prestisjefylt prisen «Årets varsler» fra Transparency International i Sverige. Prisen gis til personer virksomme i Sverige «som på ett aktivt sätt visat på missförhållanden, som ligger inom Trans-

parency International Sveriges intresseområde – korruption i vid mening. Att personen i fråga visat prov på civilkurage är en viktig faktor för bedömningen.»

Det er første gang en internrevisor er tildelt denne prisen. Men til IIA Sverige sier Annette at hun selv er tvilsom til prisen:

«Som internrevisor känns det ju lite märkligt att bli utnämnd till visselpipa – tankarna för till visselblåsare och det är jag ju inte. Jag har bara gjort mitt jobb, följt interna rapporteringsvägar och dokumenterat det.»

> «Jag har bara gjort mitt jobb, följt interna rapporteringsvägar och dokumenterat det»
>
> *Annette Olofsson, internrevisjonsleder i Transportstyrelsen*

IIA Sveriges generalsekretær Linda Lundin sier på foreningens nettsider:

«Det är roligt, både för Annette och för professionen, att en så erkänd organisation som Transparency International väljer att uppmärksamma även internrevisorer. Annettes insatser faller ju väl inom Transparency Internationals definition för Årets visselpipa: Annette har aktivt visat på missförhållanden rörande korruption i vid mening, och visat statstjänstemannaskap i genomförandet av sitt arbete.

Även Internrevisorernas standards berör ämnet. Internrevisionschefen förutsätts normalt följa rapporteringskedjan, det vill säga i det aktuella fallet rapportera via Generaldirektör till styrelse. Om internrevisionschefen som «sista utväg» ser det som nödvändigt att rapportera till någon annan, så betecknas man som visselblåsare. Det är därför mycket viktigt att betona att Annette inte är en visselblåsare, inte ens enligt våra egna standards.

Internrevision är ett yrke som ofta verkar i det tysta och det är sällan en internrevisor får offentligt erkännande och uppmärksamhet för ett väl utfört arbete. Nu har Transportstyrelsen hamnat i medialjuset och det är glädjande att se hur mycket uppskattning internrevisionen har fått, inte minst i justitierådet Thomas Bulls utredning och i KU-förhören. Det har gjort att allt fler har fått upp ögonen för vilken viktig roll internrevisionen spelar. Vi har en stark yrkeskår som varje dag levererar värde med integritet, professionalitet och mod.»

> «Internrevision är ett yrke som ofta verkar i det tysta och det är sällan en internrevisor får offentligt erkännande och uppmärksamhet för ett väl utfört arbete»
>
> *Linda Lundin, generalsekretær i IIA Sverige.*

Annette er enig i at det er gøy med oppmerksomhet rundt internrevisjonsprofesjonen:

«Jag ser priset som ett erkännande för alla internrevisorer. Transparency International visar genom utmärkelsen att även de ser att internrevision är en viktig del i arbetet mot missförhållanden.»

Hvor ble det av rotårsaksanalysen?

Av
Y. AYSE B. NORDAL
Fagansvarlig – risikostyring,
Undervisningsbygg Oslo KF
MSC, BSC METU, Licentiat NHH
Sertifisert - Akkreditert Risk Manager QMCE
Styringsgruppen for Nettverk Risikostyring i IIA Norge

Bakgrunn

Mange virksomheter benytter gode og egnede prosesser og verktøy for bestemmelse av kontekst dvs. for å fastsette de eksterne og interne parameterne som de skal ta hensyn til i risikostyring og for å kunne identifisere, rangere, analysere og evaluere sine risikoer og muligheter. [1][2] Scenario -og SWOT-analyser og risikomatriser er eksempler på slike verktøy, som bidrar til å forstå og dokumentere potensiell usikkerhet.

Virksomhetene trenger også egnede verktøy for å forstå og analysere bakenforliggende årsakene av en negativ hendelse/ utvikling, som har vært sterkere enn forutsatt og påvirket virksomhetens måloppnåelse i en negativ retning, eller av en «overraskende» positiv utvikling som har bidradd til måloppnåelsen.

Rotårsakanalyse er et slikt verktøy som vi kunne ha brukt hyppigere.

Gode japanske bidrag som ikke krever investering til verktøy

Selv om virksomhetene etablerer periodiske vurderinger av negativ og positiv usikkerhet og igangsetter tiltak for å håndtere denne, har de behov for å forstå «overraskelser». Hvorfor går vi med underskudd når ordrebøkene er fulle og det er døgn-kontinuerlig produksjon? Hvorfor har vi en feilprosent på produksjonen som er større en forventet verdi? er problemstillinger som vi møter eller hører om.

Svaret på disse spørsmålene er det mulig å komme nærmere ved å bruke en analysemetode som har sin opprinnelse fra Japan. Rotårsaksanalyse benyttes til å identifisere årsaken til en hendelse ved å bruke visuelle tilnærminger. [3,4] Metoden krever ikke noe annet verktøy enn en blyant, et ark og noen engasjerte mennesker, selv om det også finnes software for de som foretrekker disse. Ideen er å fjerne virksomhetens oppmerksomhet fra symptomene og muliggjøre en grundig analyse av hendelsen. Det er ulike metoder som kan benyttes for dette formål. De mest kjente er fiskebensdiagrammer og 5-ganger hvorfor som kan benyttes hver for seg eller i kombinasjon med hverandre.

Fiskebens-diagrammet er oppfunnet av Karou Ishikawa i 1968 og vurderes som en av de 7 verktøy i kvalitetsarbeid. Metoden benyttes ved hjelp av workshopper og idemyldring. Deltagere i en workshop kan være prosesseiere, risikoeiere, ledere eller nøkkelpersoner. Analysen består som regel av følgende trinn:

- En fasilitator identifiserer problemstillingen på en entydig og klar måte uten forklaringer, forbehold og bisetninger.
- Problemstillingen plasseres i hodet på fisken.
- Gruppen identifiserer hovedkategorier som kan benyttes til å klassifisere og systematisere årsakene til problemet. Medarbeidere, Organisasjon, Prosesser, Materialer kan være eksempler på slike kategorier.
- Nøkkelpersoner diskuterer mulige årsaker til forhold som er synliggjort i hovedkategoriene.
- Alle de underliggende/mindre årsakene plasseres under hovedkategoriene/ større årsakene.

Nedenfor gjentar jeg et eksempel som jeg har benyttet i IIAs innføringskurs i risikostyring i januar 2018.

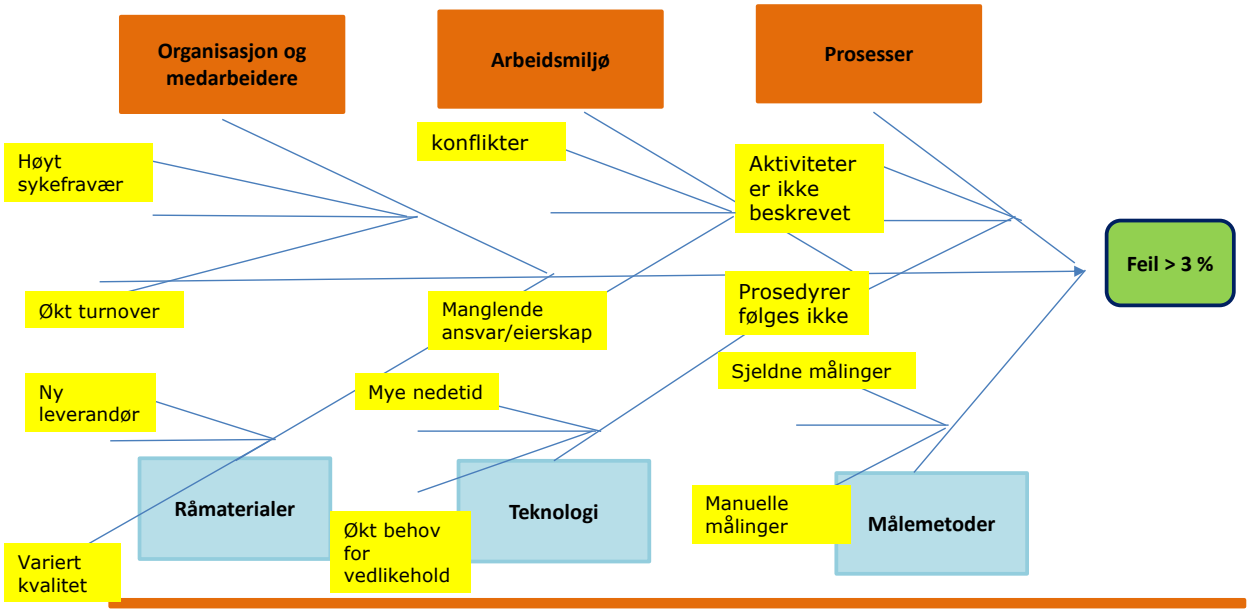
- Bedrift A har en målsetning om å ha maks. 3 % feil i produksjonen mens resultatene viser et høyere tall.
- Nøkkelpersonene i bedriften mener at årsakene til dette kan ligge i følgende områder: Organisasjon og medarbeidere, Arbeidsmiljø, Prosesser, Målemetoder, Teknologi og Råmaterialer.
- Fasilitator initierer en kreativ prosess som er fokusert på bakenforliggende årsaker innen hvert område.

Kilder:
[1] For bestemmelse av kontekst og risikovurdering Standard Norge NS-ISO 31000:2009, 2.9 og 5
[2] For risikovurdering COSO, Enterprise Risk management, Integrating with Strategy and Performance, Performance, June 2017 pp: 65-89
[3] DFØ, Veiledning i rotårsaksanalyse, versjon 2. 2015
[4] Christina Vik, Rotårsaksanalyse, Akkrediteringsdagen 2015

Rotårsaksanalyse

Fiskebein-diagram benyttes ved å spørre «hvorfor», gjentatte ganger….

Eksempel: Bedrift A prøver å finne ut hvorfor den ikke når kravet om maks. 3 % feil i produksjonen.



Fremskritt gjennom deling av kunnskap

- Dette bringer virksomheten nærmere til rotårsakene. På området «Organisasjon» identifiseres eksempelvis «økt turnover» og «høyt sykefravær» som mulige årsaker. Ved å spørre flere ganger hvorfor, kan virksomheten analysere rotårsakene til økt turnover og sykefravær nærmere, og kan iverksette relevante tiltak til å håndtere de egentlige utfordringene.

Sakichi Toyoda, grunnleggeren av Toyota Motor Company, utviklet «5 hvorfor» prosessen, en årsaks-analyse for å identifisere og løse problemer som oppsto i selskapet. Det har siden blitt brukt som en del av Lean, Kaizen, og Six Sigma metodikk. Antallet 5 er veiledende, og det er erfaringsbasert. Enkelte problemstillinger kan kreve flere/færre trinn. Det er vanlig å integrere metoden i gjennomføring av «fiskebenanalyser». Metoden benyttes slik:

- Arbeidet starter med å spørre hvorfor ut fra den opprinnelige problemformuleringen.
- Det kan foreligge ett eller flere svar på dette spørsmålet.
- Gruppen stilles på nytt spørsmålet hvorfor.
- Prosessen fortsetter til det ikke er mulig å gjenta spørsmålet.

Hvilken nytte kan virksomheten forvente?

Det å fokusere rotårsakene til et problem gir gevinster i form av at det settes relevante tiltak for å håndtere problemer og utnytte muligheter. Virksomheten får mulighet til å behandle årsaker og ikke symptomer. Men disse analyser har også andre og mer langsiktige sidegevinster. Disse er:

A. Metoden bringer kvalitetsledelse og risikostyringsmiljøene nærmere. I enkelte virksomheter fungerer disse miljøene som siloer. Den nye standarden ISO 9001: 2015 Ledelsessystemer for kvalitet stiller krav til risikobasert tilnærming. Bruk av en metode som er anerkjent av begge miljøene kan bidra til økt samarbeid.
B. Bruk av metoden bidrar til en kultur hvor det er mulig og hvor det er forventet å spørre hvorfor.
C. Bruk av metoden bidrar til tverrfaglige analyser og iverksettelse av tiltak.
D. Analysen krever ikke anskaffelse av systemer og verktøy.
E. Metoden kan kombineres med bruk av andre metoder. Virksomheten kan benytte risikomatriser, kost-nytte analyser og bow-tie diagrammer i kombinasjon med rotårsaksanalyser, for å identifisere sine risikoer/muligheter, for å vurdere sine tiltak og kontroller.

Ikke glem modellrisikoen!

En modell er en forenkling av virkeligheten og brukes blant annet til å forklare fenomener, identifisere mønstre og forutsi hendelser eller preferanser. Modeller er nyttige og i takt med økt prosesseringskraft, får de stadig større utbredelse. Med modellene følger imidlertid også risiko, både for feil resultater og feiltolkninger.

Av
HELGE BENUM
Senior konsulent i Transcendent Group

Hva er modellrisiko og er den noe å bry seg om?

I denne artikkelen skal jeg gi en overordnet presentasjon av modellrisiko og gi noen anbefalinger om hvordan virksomheter kan sikre seg at de har styring over risikoen. Før vi kommer så langt er det viktig å se litt nærmere på hva en modell er og hva modellrisiko egentlig omfatter. Office of the Comptroller of the Currency, tilsynsmyndigheten for finansbransjen i USA, definerer modell som følger:

En modell er en kvantitativ metode, system eller tilnærming som bruker statistiske, økonomiske, finansielle eller matematiske teorier, teknikker og forutsetninger til å gjøre om datainput til kvantitative estimater.

Dette er en veldig bred definisjon som omfatter et stort antall prosesser og beregninger. I praksis må virksomheter prioritere hvilke av modellene som skal gis størst oppmerksomhet og underlegges strengest styring. Definisjonen er likevel nyttig for å forstå omfanget av modellrisiko.

En modell består av tre komponenter; *input* (forutsetninger og data), *prosessering* (formler som omgjør input til estimater) og *rapportering* (omgjøring av estimater til forretningsinformasjon). Vi snakker altså om et sett av formler som omdanner forutsetninger og data til forretningsinformasjon.

Modeller er i bruk innenfor de fleste bransjer og støtter en rekke ulike oppgaver. Innenfor finansbransjen brukes modeller blant annet i stresstesting, til måling av risiko, i prisings- og kredittvurderingsprosesser og til kapitalallokering. Her er modellrisiko ansett som en del av den operasjonelle risikoen Finanstilsynet pålegger virksomhetene å vurdere kvaliteten på. En vanlig bruk av modeller er støtte til å *optimalisere allokeringen av ressurser,* for eksempel til å forutsi forbruks- eller forbrukermønstre eller beregne optimal distribusjon innenfor varehandelen. Modeller er også i bruk på samfunnsnivå, for eksempel i den makroøkonomiske styringen og i klimaforskningen.

Modellrisiko er produkt av sannsynligheten for at hendelser eller feil inntreffer, og konsekvensen av dette. Modellrisiko kan oppstå innenfor selve modellen, knyttet til input, prosessering eller rapportering, eller i form av feiltolkninger eller bevisst misbruk av resultatene.

Identifikasjon og vurdering av modellrisiko

Som med annen operasjonell risiko, starter vurderingen av modellrisiko med å kartlegge mulige feil eller hendelser. Feil eller hendelser kan oppstå i forbindelse med:

- Input: Dette omfatter feil i forutsetningene (for eksempel feil antagelser eller manglende oppdatering) og feil knyttet til data (for eksempel feil i dataformat, komplekse og ustrukturerte datasett eller feil i manuell innlesing)
- Prosessering: Dette omfatter alt som skjer «inne i» modellen og kan dreie seg om feil i formler, forenklinger som gir feil resultater, svikt i kalkuleringer eller feil på grunn av manuelle beregninger.
- Rapportering: Feil her er ofte knyttet til forenklinger eller snarveier som gir upresise resultater. Det kan også oppstå feil på grunn av ulik kompetanse og fokus hos de som kjører beregninger og de som skal bruke resultatene i forretningsmessige beslutninger.
- Feil- eller misbruk av resultater: Dette omfatter både bevisst misbruk av resultater og at resultater feiltolkes eller gis for stor gyldighet på grunn av manglende forståelse av premissene og modellens begrensninger.

For å kunne prioritere mellom risikoene og sikre at fokuset rettes mot de viktigste feilene, er det viktig å vurdere hvor sannsynlig det er at hendelsene eller feilene inntreffer, og hvor stor konsekvens de vil få. Hendelser eller feil i modeller vil typisk gi finansielle konsekvenser. For eksempel kan feil i en modell som beregner kapitalavsetninger i en bank gjøre at bankens risikoeksponering blir overvurdert og at det allokeres for mye kapital. I siste instans har dette en finansiell konsekvens for banken i form av lavere avkastning på bankens kapital. Innenfor dagligvarebransjen kan en modellfeil innebære at det distribueres for mye av enkelte typer varer, noe som igjen gir økt svinn og redusert lønnsomhet.

Feil eller hendelser kan imidlertid også skade en virksomhets omdømme (noe som senere også kan gi finansielle tap). For eksempel vil feil i modellene til virksomheter som er basert på salg av innsikt om forbrukeres vaner og preferanser kunne føre til at kjøperne av informasjonen prioriterer feil. I neste omgang vil dette skade tilliten til den innsikten som selges og gjøre at kundene velger alternative leverandører.

Håndtering av modellrisiko

Det er ikke mulig å fullstendig eliminere modellrisiko. Virksomheter bør derfor fokusere på å definere hvilken mengde risiko de er komfortable med å bære (risikoappetitt) og sette mest mulig konkrete rammer for dette. Tiltak for å redusere risiko bør primært rettes mot de bakenforliggende årsakene, men kan også tilordnes feilene eller hendelsene direkte. Risikoreduserende tiltak kan for eksempel omfatte å:

- Kartlegge omfanget av modeller og etablere en samlet oversikt
- Sikre at det eierskapet til modellene er tydelig plassert og definere roller og ansvar for øvrig
- Få på plass overordnede styringsprinsipper i form av policyer og retningslinjer
- Etablere prosesser for (uavhengig) validering av modeller, før lansering og deretter regelmessig når modellene er i bruk
- Sette standarder for kommunikasjon av resultater med fokus på modellenes forutsetninger og begrensninger
- Øke ledelsens kompetanse om modellene og hvordan resultater kan tolkes og anvendes
- Implementere og dokumentere internkontroll relatert til hver enkelt modell, herunder identifisere risikoer og sette inn kontroller.

Internrevisjonens rolle i styring av modellrisiko

Modellrisiko bør underlegges samme styring som andre typer (operasjonell) risiko. Det overordnede ansvaret for modeller og tilhørende risiko bør ligge hos ledelsen, og det er også ledelsens ansvar å etablere tilstrekkelig kontroll. Risikostyringsfunksjonen (eller tilsvarende støttefunksjon) bør støtte ledelsen i gjennomføringen av prosesser og med metodikk. Internrevisjonens oppgave er å gjøre selvstendige vurderinger av risikoen for å sikre at virksomhetens styre og toppledelse gis et mest mulig reelt bilde av risikosituasjonen.

Internrevisjonens første oppgave er å anerkjenne at modellrisiko utgjør en vesentlig risiko som må innlemmes i virksomhetens revisjonsunivers. For å danne seg et bilde av risikoen, bør internrevisjonen undersøke hvordan virksomheten forholder seg til modellrisiko på overordnet nivå. Er det stor bevissthet om modellrisiko? Er det etablert en policy for modellrisiko? Er eierskap plassert? Har virksomheten oversikt over modellene sine og risikoen de innebærer?

I revisjoner av spesifikke modeller bør internrevisjonens innledende spørsmål være om virksomheten har dokumentert selve modellen, hvordan den kontrollerer modellrisikoen og (hvis ikke) hvilken kontroll som faktisk utøves. Revisjonsprogrammet bør bygges opp rundt modellens komponenter, og kan omfatte spørsmål som:

- *Har det blitt identifisert risiko knyttet til modellen?*
- *Har risikoene og behovet for tiltak blitt vurdert?*
- *Er det etablert kontroller knyttet til inndata?*
- *Er forutsetninger og premisser klart beskrevet og omforente?*
- *Valideres resultatene av en uavhengig (av de som har bygd og/eller bruker modellen) tredjepart?*
- *Hvordan formidles og brukes resultatene?*

I virksomheter hvor det er lavt fokus på modellrisiko og hvor betydningen av denne risikoen ikke er godt forstått, har internrevisjonen et ansvar for å illustrere betydningen for toppledelsen og styret. For å nå fram med budskapet, bør internrevisjonen gi en mest mulig presis vurdering av potensielle tap. Om mulig i kroner og øre. I foretak som er spesielt avhengige av tillit og renommé, bør internrevisjonen bestrebe seg på å illustrere hvordan feil i modeller kan svekke kundenes tiltro til framtidige vurderinger og på den måten svekke virksomheten.

Internrevisjonen har altså en viktig rolle i styringen av modellrisiko. Modeller er i bruk i de fleste bransjer og utbredelsen øker, så internrevisjonen bør ta en aktiv rolle for å løfte modellrisiko opp i lyset og inn i ledelsens bevissthet.

MODELLRISIKOENS ROLLE I FINANSKRISEN

Et av de mest spektakulære eksemplene på hva feil i modeller kan føre til stammer fra finanskrisen i 2007/2008.

Tidlig på 2000-tallet hadde matematikeren David X. Li som den gang jobbet for JPMorgan Chase, etablert en formel som ble kjent som «Gaussian copula function». Formelen ble brukt til å beregne risikoen i obligasjoner som var basert på privatpersoner og bedrifters gjeld. Formelen inngikk etter hvert i modellene til en lang rekke banker, ratingbyråer og finansinstitusjoner over hele verden.

Det sentrale elementet i formelen var knyttingen mellom prisene på såkalte «Credit Default Swaps», en forsikring mot mislighold som ble omsatt på det åpne markedet, og hvordan sannsynligheten for mislighold ble priset inn i obligasjoner. Denne knytningen gjorde prisingen av obligasjoner mye enklere enn tidligere og fjernet tilsynelatende usikkerheten rundt hvor mye risiko ulike obligasjoner hadde i seg. Tilnærmingen fungerte strålende i en periode på 2000-tallet da de amerikanske boligprisene var jevnt stigende, og medførte en eksplosiv økning i denne typen obligasjoner.

Når boligmarkedet begynte å falle og stadig flere amerikanere ble tvunget til å gi opp husdrømmen, ble det imidlertid klart at modellene ikke hadde gitt et riktig bilde av hvilken risiko det innebar å eie denne typen obligasjoner. I 2008 brøt store deler av det internasjonale finansmarkedet sammen, og resten er historie.

Hvordan kunne det egentlig gå så galt? I en artikkel «Recipe for Disaster: The formula that killed Wall Street» peker forfatteren Felix Salmon blant annet på at de som tok forretningsmessige beslutninger generelt ikke forsto modellene eller de «kvantitative» argumentene for modellenes svakheter. Dessuten tjente aktørene svært gode penger på obligasjonene. Etter at boligprisene hadde begynt å falle fôret mange aktører modellene med eldre data for at risikoen skulle framstå som lav og dermed holde prisen på obligasjoner nede. Kort oppsummert: Feil forutsetninger, feil input (også bevisst), og manglende forståelse/ feiltolking av resultater.

Strategisk risiko – den glemte risikoen

Av
HERMANN KRISTIANSEN
Ass. operativ leder i
NSB Trafikk og Teknikk
Executive Master of Management
ved Handelshøyskolen BI 2008-2018

Strategisk risiko er årsak til tap i 63% av tilfellene

I forrige utgave av SIRK skrev jeg om risikotyper og verditap basert på en oppgave jeg skrev ved Handelshøyskolen BI. Etter å ha studert kursdata i perioden 2010-2015 og hendelser i en tredel av de største norsknoterte selskapene i 2015, viste det seg at strategisk risiko kunne tilskrives som årsak til verditap i 63% av tilfellene. Strategisk risiko medførte tap av lik størrelsesorden som operasjonell risiko når den inntraff, imidlertid inntraff den dobbelt så ofte. I internasjonale undersøkelser er forskjellen enda større.

Strategisk risiko er altså meget betydningsfull, og det synes utslagsgivende å vie den tid og ressurser for å trygge oppnåelsen av strategiske mål. I denne sammenhengen betyr det å hindre verditap ved uønskede hendelser. Men hvor går grensene for ansvar og nedslagsfelt når internrevisor skal vurdere hvorvidt risikostyringen er adekvat, og hvor godt risikostyringen håndterer strategisk risiko? Hvilken betydning har disse sammenhengene for internrevisjonens arbeid?

Operasjonell risiko – den lettest kvantifiserbare og målbare risikoen

Fokuset på strategisk risiko er økende rundt om i organisasjoner. En av årsakene til at likevel de fleste bedrifter fremdeles har hovedfokus på operasjonell risiko, synes å være at operasjonelle problemstillinger ofte oppleves som mer relevante og konkrete enn mer utfordrende problemstillinger av strategisk art[2]. Det operasjonelle er normalt det lettest kvantifiserbare og målbare fordi økonomiske og erfaringsbaserte data er lett tilgjengelige. Hendelser forårsaket av strategisk risiko er derimot oftere av en sort som ikke inntreffer på jevnlig basis, og som av natur er mindre forutsigbare[3].

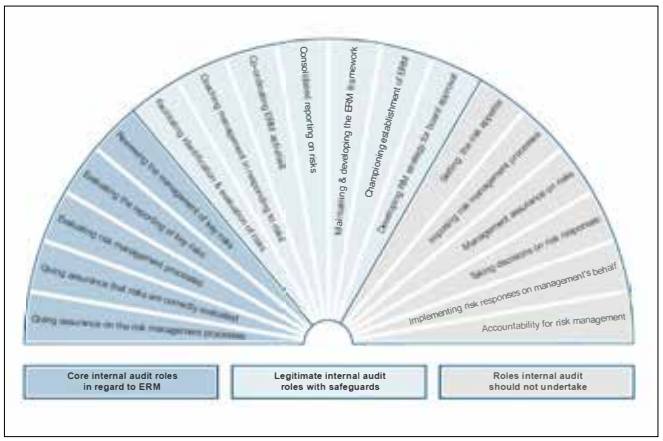
Operasjonell risiko oppstår i den daglige driften gjennom prosesser, rutiner, mennesker og teknologi. Det gir få begrensninger for internrevisors oppfølging. Strategisk risiko oppstår ved beslutninger fattet av et styre eller toppledelse. Det gir utfordringer med hensyn til evaluering og styring av risikoen, vurdering av risikostyringen og kommunikasjon med risikoeier fordi kilden til risiko kommer fra et nivå høyere opp i organisasjonen. I tillegg kommer utfordringene som ligger i risikotypens natur. Internrevisor skal ha integritet, autoritet og legitimitet gjennom strategisk kompetanse for å kunne evaluere risikostyringen i strategiske beslutninger tatt av toppledelsen. Hos en organisasjon med moden risikostyring er dette ofte integrert i beslutningsprosessene, men ikke like ofte metodisk dokumentert. Det kan by på vesentlige utfordringer i å kartlegge hvor godt strategisk risiko er håndtert. I denne sammenhengen blir viften med internrevisors roller og avgrensninger relevant (Figur 1).

I kontakten mellom internrevisor og bedriftens øverste beslutningstakere kommuniseres risiko og vurdering av risikostyringen oftest i form av enveisrapportering. Relevante

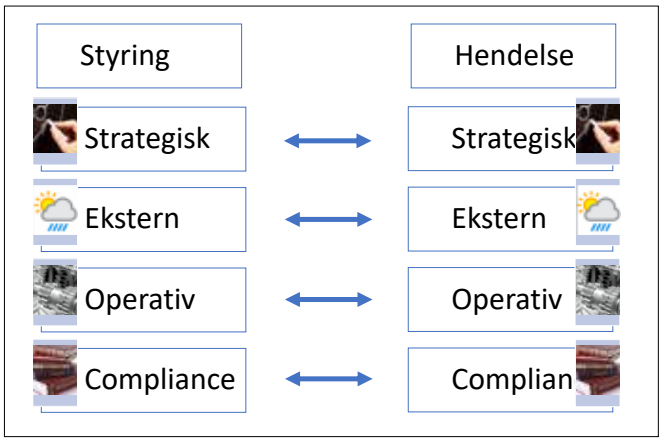
ET FERSKT EKSEMPEL DER INTERNREVISOR FRASKRIVER SEG ENHVER BEFATNING MED STRATEGISK RISIKO

I januar gikk britiske Carillion konkurs etter store finansielle problemer med mye gjeld og kontrakter som var verdsatt 845 millioner pund for høyt. Til slutt ble mange av kontraktene til tapskontrakter, og banken skrudde igjen kranen for den stadig økende gjelden. KPMG hadde eksternrevisjonsoppdraget, og signerte regnskapene i mars 2017 som «a true and fair view» av selskapets eiendeler. Deloitte hadde internrevisjonsoppdrag for entreprenørkjempen som blant annet bygger veier, sykehus og leverer skoletjenester til det offentlige i Storbritannia. I etterspillet uttaler Deloitte tydelig at de ikke var ansvarlige for ledelsens beslutninger eller selskapets strategi1 som til slutt førte til opphøret. De henviste til eksempler på deres revisjonsarbeid der de fokuserte kun på operasjonelle risikoer, som f.eks om lastebilsjåfører i Canada hadde gyldig bilforsikring.

Hendelsen medførte enorme tap for eierne, myndighetene og 43.000 ansatte. Daglig leder av IIA UK uttalte seg på omtrent følgende måte til pressen: «altfor ofte har internrevisorer vært opptatt av detaljene i mindre alvorlige risikoer, og har ikke fokusert på det som virkelig betyr noe». Han etterlyser også i sakens anledning et lignende Code of Practice som i dag gjelder for finansnæringen, for å håndtere denne typen risikoer4.



Figur 1 The role of internal audit in ERM



Figur 2 Risikodekningsmodell

risiko og informasjon om risikostyringen formidles oppover, kanskje ofte uten å påpeke håndtering av risikoeksponering som konsekvens av bedriftens strategiske valg. Dette fører til at aktiviteten risikostyring blir værende et stykke ned i organisasjonen, adskilt fra opphavet; toppen. Det medfører at strategiske beslutninger lettere kan bli tatt i et klima med lite faglig fundert risikoorientering om ikke toppledelsen har bakgrunn fra risikostyring. Om risikostyringen ikke fanger opp strategisk risiko, og toppledelsen ikke håndterer det, faller det hele mellom to stoler.

Målet bør være en risikostyring så integrert at enhver beslutning i bedriften er risikobasert

Internrevisor er antakelig den rollen utenfor toppledelse og styre, med et mandat som rettferdiggjør en nærhet til de største beslutningenes opphav best. Funksjonen er ikke nødvendigvis å finne øverst i organisasjonskartet, men har et naturlig potensiale til å knytte organisasjonen sammen vertikalt med sin tilknytning til styret eller øverste leder. Med sin objektivitet og uavhengighet fra linjen for øvrig, er det å opptre som en politisk nøytral part på tvers av avdelinger og nivåer en viktig måte å bidra med verdi til organisasjonen. Når internrevisor rapporterer om risikostyringen, er det dermed viktig at budskapet oppleves som mest mulig relevant for den øverste ledelsen og deres beslutninger.

Målet for organisasjonen bør være en risikostyring så integrert at enhver beslutning i bedriften er naturlig risikobasert. Beslutningsprosesser med gode verktøyer som ivaretar deler av risikostyringen er her uvurderlig. Dette forutsetter også at jobben med å vurdere og beskrive risikoene riktig og presist er gjort i forkant. Dette er et anliggende for ledelsen, hvor internrevisjonen kan bidra til å stille relevante spørsmål om risikostyringen. Internrevisor kan også støtte opp om og gi anbefalinger til gode governance-prosesser, for eksempel strategisk risikostyringsworkshop gjennomført av toppledelsen. Dette må da være relevant med hensyn til beslutningsprosessene om det skal kunne gi verdi. Det er også like viktig å vurdere hvor tett forhold en risikostyringsfunksjon har til toppledelsen, slik at risikoinformasjonen kan flyte både effektivt og objektivt oppover.

Det ovenstående handler i stor grad om modenhet i både risikostyring og beslutningsprosesser. Å evaluere dette, forutsetter overordnet kunnskap om begge deler. Man bør evne å formidle hvorfor dette er viktig ved mangler, og hvilken betydning det kan ha for målsettingene. Internrevisor kan her påpeke mangler ved prosesser, og eventuelt flagge risikoer som er anbefalt å gjøres tiltak på og som ikke følges opp. Det må oppfattes relevant nok av ledelsen til at det tas på alvor, og utfordrende nok til at det vekker den nødvendige bevissthet. En måte å utfordre toppledelse og styre på, kan være å utarbeide en spørsmålsliste. Det utløser mer effektivt tankeprosesser enn en passiv rapport alene, og kan fungere som en sjekkliste for begge parter. En slik sjekkliste kan for eksempel bygge på risikodekningsmodellen fra min forrige artikkel (figur 2), for å søke å forstå om bedriften er godt dekket mot relevante risiko. Om det inntreffer få uønskede hendelser i egen organisasjon, kan man da hente inn data fra andre sammenlignbare virksomheter for å se om egen risikostyring kunne forhindret eller begrenset skadevirkningene av en lignende hendelse. For internrevisor vil kjennskap til dette kunne støtte revisjon av risikostyringen, og bidra til en kompetent og relevant rapportering oppover.

Mangel på strategisk risiko i risikovurderinger må være internrevisors oppgave å påpeke, like mye som manglende vurderinger av compliance-og operasjonell risiko. På samme måte som at styring av operasjonell risiko må være til stede for forretningsprosessene, må styring av strategisk risiko være til stede for beslutningsprosessene.

Med takk til gode diskusjoner med Jørgen Bock og Cecilie Thorberg i Internrevisjon i Universitetet i Oslo. Takk til Martin Stevens i Gjensidige for initiativ, fasilitering og gode diskusjoner.

[1] *Madison Marriage, "MPs turn fire on KPMG and Deloitte partners over Carillion", Financial Times 22.02.2018*
[2] *R. Funston, "Avoiding the value killers», Treasury and Risk Management, april 2004, s. 11*
[3] *A. Wilkinson & R. Kupers, "Living in the futures", Harvard Business Review, mai 2013*
[4] *Dr. Ian Peters, "Internal audit has failed to look at the bigger picture", Financial Times, 28.02.2018*

Undervisningsbygg:

Ekstern kvalitetssikring av outsourcet internrevisjon

Av
MARIT TRODAL
Prosjektleder
IIA Norge

IIA Norge gjennomførte tidligere i år en eksternevaluering av internrevisjonen i Undervisningsbygg. Denne funksjonen er ivaretatt av BDO og ledes av Øyvind Sunde, Director. Dette er første gang et revisjonsselskap har tatt initiativ til en ekstern kvalitetskontroll.

Hvorfor ba du om en ekstern kvalitetskontroll (QAR)?

Min motivasjon for å be om en ekstern kvalitetskontroll var todelt:
1. Et krav i IIA-standarden.
2. Læring.

Jeg ivaretar på BDOs vegne en outsourcet internrevisjonsfunksjon i et kommunalt foretak. Det er ikke til å stikke under stol at standarden på sett og vis er krevende, men at den, etter mitt syn, må tilpasses den virksomhet som revideres. Det må kunne være mulig å imøtekomme IIA-standarden i en funksjon på 1-2 årsverk, selv om mange internrevisjoner som ansatte i virksomheten normalt har mange flere årsverk til disposisjon. Dimensjoneringen her var jeg opptatt å få fram forut for kvalitetskontrollen.

Øyvind Sunde, BDO og Ellen Brataas, IIA Norge. Foto: Marit Trodal

Er ikke en intern kvalitetskontroll i revisjonsselskapene nok?

Jeg har skjønt at BDO er det første eksterne revisjonsmiljøet som har latt seg underlegge en ekstern kvalitetskontroll i Norge. Det er jo forunderlig. Vi som jobber i revisjonsbransjen, om det er den ene eller andre formen for revisjon, burde jo være de første til å forstå behovet for/nytten av en ekstern kontroll med hvordan du utøver yrket! Jeg hører, også fra mine egne foresatte, at vi i revisjonsbransjen har så gode og omfattende interne kvalitetskontroller, at behovet for en ekstern kontroll ikke er nødvendig. Da setter man seg jo imot IIA-standarden. Dessuten, hvis den interne kvalitetskontrollen er så god som man hevder, er det jo ingen fare med en ekstern kvalitetskontroll!

Jeg har jobbet i operativ revisjon i mer enn en mannsalder, både i privat og offentlig revisjon, og i forskjellige revisjonsselskaper. Min erfaring er at en intern kvalitetskontroll ikke kan måle seg med en ekstern kvalitetskontroll, den interne kvalitetskontrollen går ikke slik i dybden på arbeidspapirene og vurderer opp mot standarden. Det skal tilføyes at jeg ikke har erfart hvordan en intern, internasjonal kvalitetskontroll ville vært,

men jeg ville tro en slik kontroll i stor grad ville rette seg mot anvendelse av internasjonal revisjonsmetodikk (hvis formål naturligvis er å oppfylle IIA-standardene).

Hvorfor valgte du IIA Norge?

Valg av kvalitetskontrollør er ikke trivielt. Som et eksternt revisjonsselskap ønsker vi jo ikke å slippe våre konkurrenter inn i vårt hus. Ekstern kvalitetskontroll kan organiseres på forskjellige måter:

a) Full ekstern kvalitetskontroll.
b) Full ekstern kvalitetskontroll i samarbeid med andre internrevisjoner.
c) Ekstern validering av egenkontroll.

En ekstern kvalitetskontroll er ikke gratis, det vet også vi som av og til gir tilbud på slik QAR for internrevisjoner. Prisen på disse formene for kvalitetskontroll synker med grad av egeninnsats, der alternativ b) og c) har størst innslag av dette. BDOs valg falt på ekstern validering av egenkontrollen, og engasjement av IIA Norge som kvalitetskontrollør. Da begrenset vi prisen og unngikk konkurrenter inn i vår organisasjon.

Er en egenevaluering fullt ut troverdig?

Egenevalueringen er ingen 'walk in the park'! Det er mange spørsmål som skal svares ut og dokumenteres. Ekstern kvalitetskontrollør går så gjennom denne dokumentasjonen for å se etter at den er tilfredsstillende for å oppfylle IIA-standardens krav. Uten å gå i detalj hadde jeg tilrettelagt i underkant av 30 dokumenter for å svare ut standardens krav til internrevisors egenskaper og hvordan arbeidet er gjort (egenskapsstandardene og utøvelsesstandardene). En viktig del av den eksterne kvalitetskontrollørens arbeid er også å gjøre intervjuer med mange interessenter, så som styreleder, administrerende direktør, linjeledelse, risk controller og ekstern revisor. Jeg antar, uten å vite, at formålet med disse intervjuene blant annet er å undersøke informantenes opplevelse av internrevisors uavhengighet, og om de oppfatter at internrevisjonen gir merverdi.

Fikk du noe læring av ekstern kvalitetskontroll?

BDO fikk bestått på kvalitetskontrollen. Rapporten viste meg at IIA Norge hadde gjort en grundig jobb, og jeg mener de hadde lagt til rette en god prosess mot meg som internrevisor. Jeg opplevde kontrollen som positiv. Det er læringspunkter. Kanskje det viktigste er hvordan BDO skal videreutvikle seg som internrevisor, ikke minst gjennom interne oppfølgingstiltak og at 'revisjonsuniverset' er dekket/oppdatert. Personlig synes jeg standardens anbefaling om å vurdere risiko for misligheter og kritiske IT-systemer i hvert prosjekt ikke må bli en 'tvangstrøye'. Jeg gjør en risikovurdering i hvert prosjekt relatert til prosjektets problemstillinger, men det er ikke naturlig å male mislighetsfanden på veggen hver gang. Informasjonssystemer er i dag verktøy i enhver prosess, og en risikovurdering av dette/disse kan være relevant, men ikke nødvendigvis isolert sett og i ethvert prosjekt.

Jeg har de senere årene stålsatt meg, forhåpentligvis på tilstrekkelig grunnlag, til å konkludere med at foretaket har etablert gode systemer og prosedyrer for å sikre god virksomhetsstyring og tilfredsstillende håndtering av risikoer. I dette ligger at ledelsen bidrar til god governance, risikostyring og kontroll. Jeg var sikker på at en slik uttalelse var et krav i standarden, men har nå lært at det bare er en anbefaling. Men når kunden kjøper en internrevisjonstjeneste som skal følge IIA-standardene, bør man vel konkludere på dette uansett? Det er en krevende revisjon, men jeg synes den hører med. Det innebærer at man ikke kan «dukke opp» hos kunden en gang i blant i forbindelse med prosjekter, man må da ha såpass tilstedeværelse som internrevisor at man får en god ryggmargsfølelse når disse bevingede ord skrives. Du skal ha grunnlag for å skrive revisjonsplan, evaluere risikostyringsprosesser, vurdere virksomhetsstyringen og skrive tertial- og årsrapport. I tillegg kommer altså de vedtatte prosjektene. Har du kontroll på dette årshjulet, kan du lage revisjonsprogrammet for overordnet vurdering av strategi, drift, rapportering og etterlevelse.

Og konklusjonen?

Nå kan jeg fortsatt skrive i min årsrapport til styret at internrevisjonen er utført i tråd med IIA-standardene uten forbehold!

OVERORDNET KVALITETSKONTROLL

Noe av det som skiller IIA Norges eksterne evalueringer fra andre tilbydere, er at foreningen har en egen overordnet kvalitetskontrollgruppe som gjennomgår alle sluttrapporter. Gruppen består av erfarne internrevisjonsledere som med sin lange fartstid ofte har innspill til god praksis utover det kontrollørene har observert. Et annet formål med gruppen er å sikre konformitet i alle evalueringer som gjennomføres i foreningens regi. Gruppen har siden 2013 bestått av følgende medlemmer:

Trine Tengbom
Leder Internrevisjonen
Norges forskningsråd

Jørgen Bock
Leder Internrevisjonen
Universitetet i Oslo

Reidar Døli
Leder Internrevisjonen
Oslo Børs ASA

Tor Steenfeldt-Foss
Leder Konsernrevisjonen
DNB Bank ASA

Digital arbeidskraft og internrevisors rolle

Av
MAGNUS DIGERNES
Director KPMG Risk Consulting

Av
OLE JACOB KVISSELLIEN
Manager KPMG Risk Consulting

I en tid hvor virksomheters omgivelser endres stadig raskere kan internrevisorer spille en viktig rolle. Dette krever imidlertid at internrevisjonen «følger med i timen»; har god oversikt og forstår nye typer risikoer og hvordan de bør håndteres, og selv er tidlig ute med å ta i bruk ny teknologi. I denne artikkelen ønsker vi å belyse endringer knyttet til digital arbeidskraft og hvordan internrevisor kan håndtere disse endringene på en proaktiv måte.

Hva er «roboter» og digital arbeidskraft?

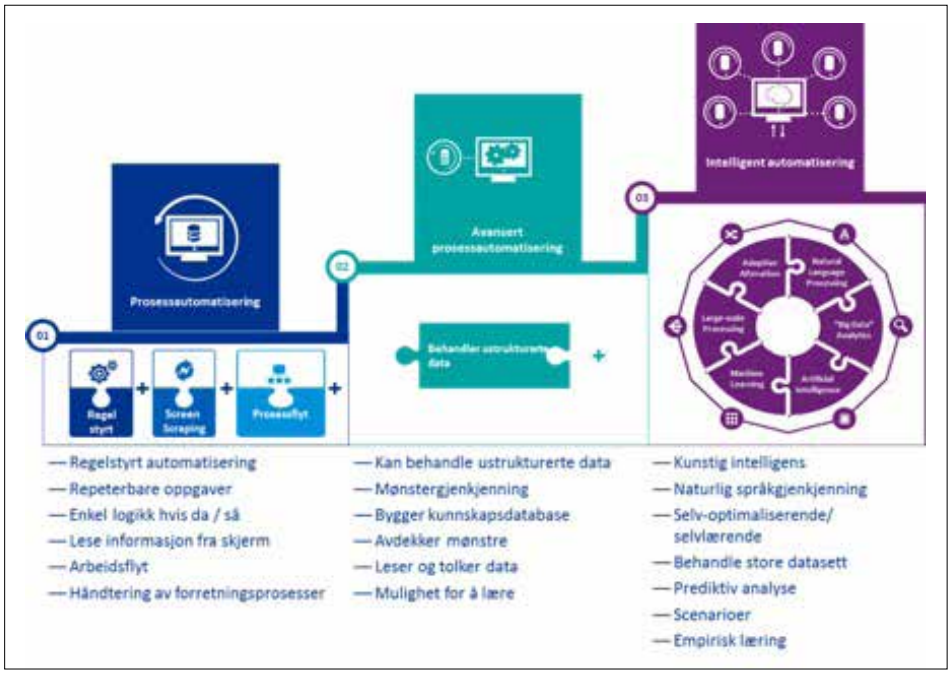
Stadig flere virksomheter investerer i prosesseringsroboter for å automatisere arbeidsoppgaver. I en undersøkelse gjennomført av KPMG (2017 CEO Outlook Survey) svarte 60% av virksomhetslederne at de vil fokusere på investeringer innen intelligent digital arbeidskraft. Teknologien er blitt billigere, og samtidig mer avansert og den er blitt kraftigere.

Risikoer

Når virksomheter implementerer ny digital arbeidskraft er det flere fallgruver. Ved å forstå disse fallgruvene kan virksomheten innføre de nødvendige forebyggende kontrollene. Ved implementering av digital arbeidskraft deler man gjerne inn fasene i; autentisering og integrering, endringer, styring og oppfølging/overvåking.

Muligheter for internrevisjonen

IIA har utgitt en veileder for internrevisjoner om kunstig intelligens (Global perspectives: Artificial intelligence) som beskriver hvilke roller og aktiviteter internrevisjonen bør vurdere ved virksomheters implementering av digital arbeidskraft;



Illustrasjonen viser en mulig kategorisering hvor bl.a. kunstig intelligens er en del av intelligent automatisering. I kategorien «intelligent automatisering» finner vi aktiviteter som kombinerer avanserte teknologier som kunstig intelligens og maskinlæring, og som kan bidra til at ansatte blir mer produktive og mer informerte.

- I alle virksomheter bør internrevisjonen inkludere digital arbeidskraft i sine risikovurderinger og i sin risikobaserte revisjonsplan.

- For virksomheter som vurderer mulighetene for digital arbeidskraft, bør internrevisjonen aktivt involvere seg i alle prosjektfasene gjennom rådgivning og innsikt for å bidra til en vellykket implementering. Imidlertid må internrevisjonen være påpasselig med å ivareta sin uavhengighet og objektivitet og ikke eie eller være ansvarlig for implementeringen av et prosjekt for digital arbeidskraft.

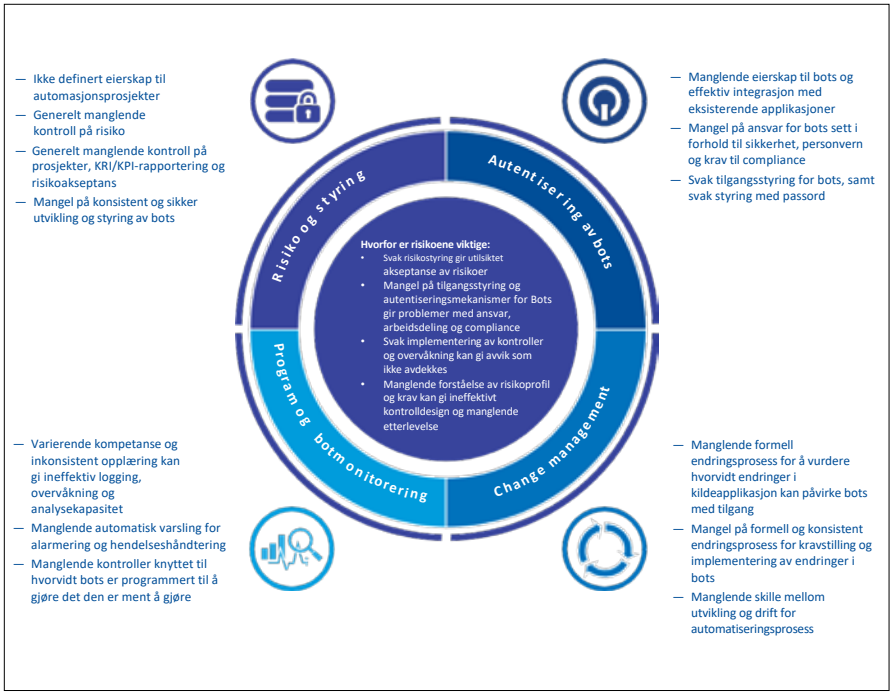
- For virksomheter som i noen grad har implementert digital arbeidskraft enten i sine driftsprosesser (slik som vareprodusenter med roboter i en fabrikklinje), eller innebygget i en vare eller tjeneste (slik som forhandlere som tilpasser produkttilbudet basert på kundens kjøpshistorikk), bør internrevisjonen kvalitetssikre risikostyringen knyttet til pålideligheten i de underliggende algoritmene og for de dataene som benyttes som underlag for disse algoritmene.

- Internrevisjonen bør sikre at moralske og etiske problemstillinger som kan ha betydning for virksomhetens bruk av f.eks. kunstig intelligens er ivaretatt.

- Som ved bruk av andre store systemer, bør det være styringsstrukturer/styringssystemer på plass og internrevisjonen kan kvalitetssikre denne styringen.

Videre bør internrevisjonen benytte seg av bidragene fra digital arbeidskraft til å øke sin egen effektivitet og produktivitet.

Internrevisjonsfunksjonen har gode muligheter til å bli en viktig bidragsyter til virksomhetens aktiviteter knyttet til bruk av digital arbeidskraft. Internrevisjonen bør være i stand til å evaluere aktiviteter hvor digital arbeidskraft benyttes og gi intern kvalitetssikring for ledelsens vurderinger av risiko. Med rett innsikt og tilnærming har internrevisjonen muligheten til å bli ansett som en pålitelig rådgiver som kan gi støtte til ledelsen ved innføring av digital arbeidskraft.



I fasene er det ulike utfordringer som skissert i illustrasjonen.

Eksempler på internrevisjonsprosjekter ved implementering av digital arbeidskraft er illustrert i tabellen under.

Fase	Rådgivningsoppdrag	Bekreftelsesoppdrag
Planlegging	Vurdere valg av plattformsløsninger og arkitektur	Vurdere integrering av prosedyrer og standarder Oppfølging av leverandører
Designe	Vurdere identifisering av risiko og kontrolldesign	Vurdere prosedyrer for akseptansetesting av «robotene»
Implementering	Vurdere definering og innbygging av kontroller	Operasjonell ytelse og kvalitet
Oppfølging	Evaluering av risikoappetitt	Effektivitet i prosesser for kontinuerlig forbedring

Vurdere én gang, teste én gang, tilfredsstille mange

Hvordan redusere compliance-kostnader ved å samkjøre kontrolltestingen ved ISAE3402, SOC2, GDPR attestasjon og ISO/IEC 27001 sertifisering?

KEVIN F. MCCLOSKEY
CISA, CIA, CRMA
Kevin er Director i Deloitte og har over 27 års erfaring med Third Party Assurance (TPA), IT-revisjon, internrevisjon, Sarbanes Oxley og IT-basert internkontroll.

TPA-rapportering vokser med 10% hvert år

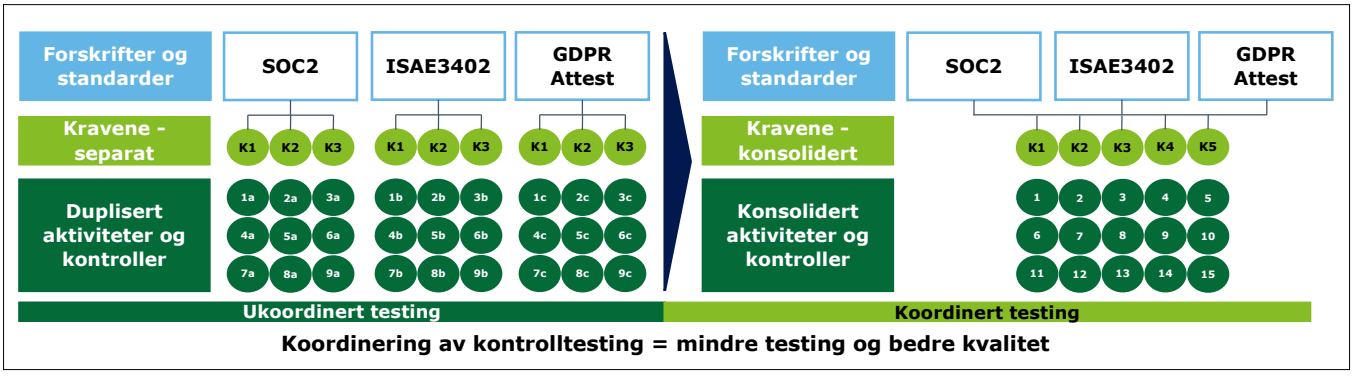
Flere virksomheter enn tidligere velger å outsource deler av sin virksomhet inkludert IT til en Outsourcing Service Provider (OSP). Når OSP-ens engasjement med kunden er av en betydelig størrelse, har OSP-ens interne kontrollmiljø ofte en stor innflytelse på kundens internkontroll. Som en følge av dette har etterspørselen etter ulike tredjepartsbekreftelser, såkalt Third Party Assurance (TPA)-rapportering på internkontroll hos OSP-ene økt kraftig de siste årene. Basert på en analyse av vår database av TPA-rapporter utstedt av Deloitte globalt, øker det totale antallet TPA-rapporter med rundt 10 prosent hvert år.

Complianceutfordringer

Fra en OSP sitt perspektiv har kravene til uavhengig attestasjon, sertifisering og revisjon også økt kraftig. OSPs er under konstant press for å møte behovene til deres kunder og tilsynsmyndigheter med hensyn til å ha tilstrekkelige kontroller på plass. De må også forbli konkurransedyktige, noe som kan bety at de må sørge for at de nyeste og beste sertifiseringene innen internkontroll er på plass. Det er blitt mer vanlig for kunder å inkludere klausuler i kontraktene som enten krever revisjonsrettigheter eller spesifikke rapporteringskrav rundt internkontroll som er relevante for tjenestene som kjøpes av OSP-en.

Med de kommende GDPR-kravene vil det bli enda større behov for å bevise for kunder og andre at organisasjonen har de rette kontrollene på plass for å sikre personopplysninger. Trolig vil dette ende opp i en eller annen form for attestasjon. Vi har sett utvikling rundt dette i Danmark hvor FSR Danske Revisorer har utarbeidet utkast til rapporteringsstandard basert på ISAE3000 med et standard sett av kontrollmålsetninger og anbefalte kontroller fokusert på beskyttelse av personopplysninger. Deloitte jobber nå med maler og metodikk rundt GDPR-attestasjonsrapporter og forventer at dette blir en standard måte å dokumentere overfor kunder og samarbeidspartnere at selskapet etterlever kravene i GDPR.

Ulike kunde- og regelverkskrav relatert til internkontroll fører til at et selskap ofte setter i gang flere ressurskrevende aktiviteter for å oppfylle disse kravene. Dette kan inkludere workshops, spørreundersøkelser, sjekklister, stikkprøvetester,



kartleggingssamtaler med videre. Mange OSP-er har derfor behov for en mer strømlinjeformet tilnærming for å håndtere alle kravene på en effektiv måte.

Gjenbruk av kontrolltesting for å dekke flere attestasjonsoppdrag og sertifiseringer

Det er flere måter å rapportere på og mange sertifiseringer tilgjengelig. Disse har ulike formål og bruksområder. Noen av de mest vanlige og relevante attestasjonstypene og sertifiseringene som vi ser hos klienter er oppsummert i tabellen.

Mange selskaper som ønsker å produsere en attestasjonsrapport har allerede en av ISO-sertifiseringene, enten innenfor sikkerhet eller kvalitet. Med riktig kunnskap om ulike standarder, kan man spare mye tid og penger hvis flere av disse rapportene skal utarbeides eller man har mulighet til å koordinere attestasjonsprosjektene med sertifiseringsprosesser. Hvis man kan teste basert på de strengeste kravene man må etterleve, trenger man ikke å teste kontrollen mer enn én gang. Hvis prosjektene ikke er koordinerte, noe som skjer ofte, er det sannsynlig at kontrollen testes flere ganger.

Med oversikt over kravene til rapportering og sertifisering, god planlegging og en strukturert måte å angripe dette på kan man oppnå ganske mye i løpet av relativt kort tid. OSP-er er ofte oversvømt med sikkerhetsspørreskjemaer fra kunder, forespørsler om kundespesifikke TPA-rapporter, og krav om å tilrettelegge for besøk av kundens revisor. Et gjennomtenkt og velorganisert TPA-rapporteringsprogram burde dekke mange, hvis ikke alle, disse behovene. Kombinert med at OSP-er skal oppfylle egne interne krav (f.eks. i samsvar med Sarbanes-Oxley (SOX) eller andre regelverk), er det lett å se hvorfor det er nødvendig å finne måter å lette byrden på.

Ledende praksis

For å kunne realisere fordelene av en god prosess rundt TPA-rapportering og sertifisering av enkelte områder kreves det en helhetlig tilnærming som best mulig kan utnytte en OSPs ressurser.

Mange OSP-er er i reaktivt modus når det gjelder å administrere TPA-forespørsler. En del av problemet stammer fra at de ikke har en god oversikt alle sine interne og eksterne kontrollkrav. Å lage en oversikt over alle kontrollbehov i virksomheten er det første trinnet i både å identifisere hull og finne fellesområder. Oversikten skal inneholde internt identifiserte krav, industrikrav og krav som inngår i eventuelle TPA-rapporter. Til slutt bør oversikten inneholde krav som dekkes av eventuelle spørreskjemaer eller servicenivåavtaler (SLA).

Når man har oversikt over kravene kan man kartlegge hvilke kontroller som oppfyller dem, og avgjøre hvilke krav som kan dekkes gjennom TPA-rapporter. Hvis man for eksempel har en enkelt kontroll som dekker fysisk tilgang til datasenteret, kan det tilpasses flere forskjellige krav, både interne og eksterne. Ved å kartlegge hvert krav en kontroll oppfyller, bør testingen kunne gjøres mer effektivt.

Få mer valuta for pengene

Hvis man håndterer kunderapporteringskrav og sertifiseringsprosesser som separate prosjekter risikerer man å gå glipp av viktige synergier. Når man har en katalog over gjeldende krav og hvilke kontroller som dekker disse kravene, er man i stand til å realisere betydelige effektiviteter under kontrolltesting. Snarere enn å teste hver gang et krav kommer inn fra en kunde eller gjennom en sertifiseringsprosess, trenger man bare teste hver kontroll én gang for både interne og eksterne formål og dokumentere resultatene for alle krav som kon-

Rapporttype / sertifisering	Type	Beskrivelse
ISAE3402 / SOC1	Attestasjonsrapport	Sikkerhet over internkontroll relevant til prosessering av finansielle informasjon
SOC2	Attestasjonsrapport	Sikkerhet over kontroller hos en serviceorganisasjon som er relevant for sikkerhet, tilgjengelighet, integritet, konfidensialitet eller personvern
SOC2+ GDPR	Attestasjonsrapport	Ikke utgitt ennå, men under utvikling og vil være en utvidet SOC2 rapport for å oppfylle kravene til GDPR
ISAE3000	Attestasjonsrapport	Attestasjonsoppdrag som ikke er revisjon eller forenklet revisorkontroll av historisk finansiell informasjon - Sikkerhet over spesifikke internkontrollrutiner uten behov for detaljert beskrivelse som i en ISAE3402 / SOC1
ISO/IEC 27001	Sertifisering	Markedsrelatert, for å vise kunder at man har implementert et sikkerhetsstyringssystem
PCI DSS	Sertifisering	Nødvendig for å kunne behandle kredittkorttransaksjoner/informasjon
ISO9000	Sertifisering	Markedsrelatert, for å vise at selskapet har implementert kvalitetsrutiner
CSA Selvvurdering	Spørreskjema	Markedsrelatert, for å vise at selskapet har kontroll over sikkerhet med fokus på cloud computing

trollen gjelder. Det er viktig at dokumentasjon av testene er tilstrekkelig for å dekke behovene for den strengeste krav som skal rapporteres på.

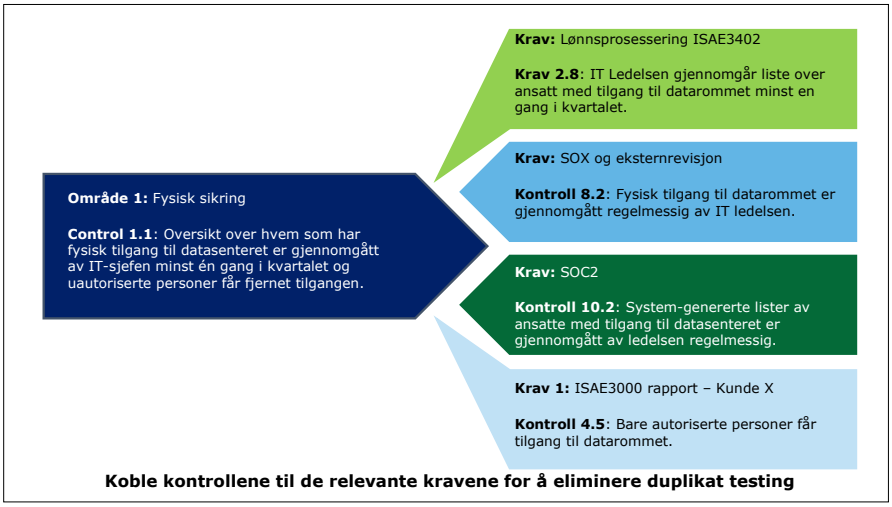
Mange TPA-rapporter har felleselementer. Man kan derfor oppnå ekstra effektivitet ved å utstede TPA-rapporter under flere standarder hvis man kan gjenbruke testing utført for en rapport i en annet. Evnen til å utstede disse rapportene under flere standarder er en viktig fordel for globale leverandører.

Virksomhetens katalog over krav og kontrolltester kan være spesielt nyttig for rask sammenstilling av klientspesifikke rapporter, siden resultatene av hver test allerede er koblet opp mot alle relevante krav. En annen måte å få effektivitet på er å tilpasse rapporteringsperioder som dekkes av de ulike TPA-rapportene, slik at de overlapper så mye som mulig. Da kan du dele tester på forskjellige rapporter og oppnå betydelige tidsbesparelser.

Vær proaktiv og fremoverlent

TPA-kravene utvikler seg stadig og kundenes behov for bekreftelse endres ved bestilling av nye tjenester eller ved endring i regelverk. Kundene bør behandle sine lister med krav til sin OSP som et levende dokument som revideres regelmessig. Fra OSP-er sin side kan det å sende ut årlige TPA-rapporter uten å revurdere innhold resultere i at man bruker tid på problemer som ikke lenger er reelle for kundene. Alternativt kan man oppdage at vesentlige områder ikke er dekket av rapporten fordi kundens behov har endret seg. OSP-er og selskaper som utsteder attestasjonsrapportene / sertifiseringene må derfor være proaktive når det gjelder å holde seg oppdatert på regulatoriske endringer og kundenes behov.

Når TPA-rapporteringsprogrammet utvikles, bør det samme gjelde kontrollopplegget. Denne prosessen burde faktisk gi virksomheten en mulighet til å gjøre noe som de fleste ikke få til: fjerne enkelte kontroller helt, ikke bare fjerne dem fra rapporter. Hvis kontrollene er overflødige eller ikke lenger nødvendige, er det fortsatt sløsing med verdifulle ressurser, spesielt hvis de involverer manuelle aktiviteter. Dette forutsetter at man finner en mer effektiv kontroll i prosessen enn den som fjernes og kanskje en kontroll som dekker flere risikoer.



Koble kontrollene til de relevante kravene for å eliminere duplikat testing

Hva bør en som attesterer på en TPA-rapport spørre utsteder om?

Det er viktig at en virksomhet som velger å utstede en attestasjonsrapport velger riktig rapporttype og evt. sett med målekriterier. Et feil valg kan bety at de ikke oppnår målsetningen med å lage rapporten. Noen av de første spørsmålene vi i Deloitte spør en ny attestasjonskunde om er derfor:

- ***«Hvorfor vil dere gjøre dette?»*** Hvis selskapets egen markedsavdeling ønsker å kunne svare på mange henvendelser fra kunder vedrørende Cloud Security Alliance (CSA)-undersøkelser er kanskje dette en mulighet for lage en SOC2+ rapport med vekt på CSA. Er det en av kundens regnsapsansvarlige som har bedt om rapporten kommer trolig ønsket fra kundens eksternrevisor og da kan en ISAE3402 rapport eller lignende være passende. Hvis det er kundens IT-ansvarlig som ønsker dette, kan en SOC2-rapport eller en ISO-sikkerhetssertifisering derimot passe

OMRÅDER Å FOKUSERE PÅ NÅR MAN SKAL OPTIMALISERE TPA

Som en del av ditt TPA optimaliseringsprogram bør du adressere følgende spørsmål:

- Hvilke krav har vi for rapportering?
- Hvilke rapporter skal vi utvikle? Hvorfor?
- Kan vi velge standarder eller rammeverk selv eller er det bestemt?
- Hvis vi får velge, er det noen måter å rapportere på som kan dekke flere behov?
- Er det noen kartlegging av de forskjellige standarder som jeg kan / må ta i bruk som kan bidra til en effektivisering av dette arbeidet?
- Hvilke metoder er best for å oppnå en effektiv rapporteringsprosess?
- Hvilken av rapportene / sertifiseringene har de strengeste kravene? Det er denne som er minimumskravet mitt, og det er denne som skal gjenbrukes.
- Hvordan skal vi best synkronisere utgivelse av disse rapportene?
- Hvordan skal vi mappe kravene til kundebehovene?
- Hvor ofte skal vi revurdere angrepsvinkelen vår?
- Er det noe vi kan avvikle?
- Er vi 'up-to-date' når det gjelder de siste rapporteringskravene?
- Er det noen interne aktiviteter som er relevant for dette som vi burde koordinere med?
- Kan vi ta i bruk teknologi for å effektivisere prosessen?

bedre. Hvis kunden, som mange andre, er bekymret for OSP-ens behandling av personinformasjon, er det sannsynlig at en SOC2 + GDPR eller en ISAE3000 rapport med riktig målekriterier i bunn vil være mest effektivt.

- ***«Hva skal de som mottar dette bruke den til?»*** Skal mottaker utgi egen attestasjon og bruke rapporten vår som underlag så trenger de en rapporttype som inkluderer riktig testmetode for deres bruk og tilstrekkelig detaljer om kontrollmiljøet. ISAE3402 vil ofte være løsningen. Hvis de skal bruke den til eget formål kan de leve med en 'kortere' rapporttype. En ISAE3000 rapport kan gjerne være på noen få sider, mens en ISAE3402 rapport ofte er over 30 sider.

Ekspert vs. salgsperson

Vi som attesterer på disse rapportene har et ansvar for å gi våre kunder råd om valg av rapporteringsform som er riktig og dekkende for deres behov. Vi må gi ekspertråd også når kunden kan velge å gjøre mindre. Vi er tjent med å levere god kvalitet med god integritet. En forlengelse

Kilde: Deloittes bibliotek.

av dette, for oss, er å se etter muligheter for effektivisering. Da er det viktig å finne ut hva virksomheten har av sertifiseringer og attestasjonsrapporter for å kunne finne ut om det er noen muligheter for «gjenbruk».

Konklusjon

Siden selskaper i økende grad utvider bruken av OSP-er for styring av virksomhetskritiske operasjoner og forretningsprosesser, er etterspørselen etter TPA-rapportering økende. Samtidig øker presset for å kunne vise frem riktige sertifiseringene og sertifikater for å kunne være konkurransedyktige. Kunder og myndighetene etterspør mer og mer informasjon fra OSP-er om deres internkontroll, for å sikre at kvaliteten på tjenestene de leverer er tilstrekkelig i henhold til lovkrav, for å etterleve krav i kundeavtaler og for å sikre at de opererer i henhold til beste praksis. Noen ganger vil kunden kjøre egen revisjon hos sin OSP. Noen ganger krever kunden at OSP-en fyller ut lange spørreskjemaer. Ofte er en TPA-rapport en god løsning for å dekke behovene fra flere kunder. Sertifiseringer er en god måte å vise nåværende eller framtidige kunder at OSP-en har møtt minimumskravene til et spesifikt sertifiseringsområde. Man kan velge å kjøre alle disse rapportering- og sertifiseringsprosessene som separate prosjekter, men det kan være ineffektivt. Hvis man samler prosjektene, bruker tid på å finne ut hva de har felles og organisere kontrolldokumentasjonen, prosjektplanlegging, kontrolltesting og rapporteringsprosessene, kan man realisere gevinster i form av bedre kvalitet og mer effektiv ressursbruk.

Det er mange fordeler med å optimalisere TPA-rapporteringen	
God dekning	OSP-er kan gi sikkerhet til et variert spekter av kunder med en enkel rapport eller sett av rapporter.
Integrerte krav	OSP-er kan «teste én gang», og bruke resultatene på tvers av flere rapporter / sertifiseringer. De kan også potensielt utnytte resultatene til interne krav.
Tids- og kostnadsbesparelser	OSP-er kan utstede egne rapporter og kartlegge eller justere dem mer spesifikt til kundens krav. Dette sparer dem tiden det tar for å svare på flere «engangs» spørreskjemaer fra kunder og imøtekomme revisjoner fra kundenes revisorer.
Sterkere tillit	Når kundene er komfortable med en OSPs rapporteringsprosess, er det mindre sannsynlig at de vil be om ytterligere informasjon om sine kontroller.
Rask skreddersøm	OSP-er kan raskt tilpasse rapporter for både eksisterende og potensielle kunder.
Kundens verdiskapning	En strømlinjeformet TPA-prosess kan være et betydelig fortrinn over konkurrentene for OSP-er som markedsfører sin fleksibilitet og evne til å raskt møte kundenes krav gjennom en rekke TPA-rapporter kartlagt (eller skreddersydd) mot spesifikke industristandarder og forskrifter.
Forbedret evne til kryssalg	Med en helhetlig, tverrfaglig tilnærming til TPA-rapportering, kan OSP-er strukturere rapporter for å kommunisere til kunder hele spekteret av tjenester de tilbyr. Dette kan potensielt føre til forespørsler om tilleggstjenester.
Forbedring av forretningsprosesser	Effektivisering av TPA-rapporterings-/sertifiseringsprosessene kan også bety en effektivisering av kontrollene og en identifikasjon av når enkelte kontroller er overflødige. I tillegg til å fjerne kontrollene fra rapporteringsrammen kan ledelsen ha mulighet til å eliminere de tilknyttede arbeidsaktivitetene helt, slik at disse ressursene kan omfordeles til mer verdiskapende aktiviteter.

PwC State of the Internal Audit Profession 2018

Drone-observasjoner og kunstig intelligens benyttes til å planlegge preventivt vedlikehold. Blockchain-matematikk påstås å eliminere iboende risiko for feil i transaksjonsprosessering. Smartklokker overvåker utvikling i biometriske data og optimaliserer medikasjonsbruk. PwCs globale internrevisjonsundersøkelse 2018 tegner et revisjonslandskap i endring, og gir konkrete råd til hvordan internrevisjonen bør opptre for å tilføre nytte.

Av
JONAS GAUDERNACK
Partner PwC

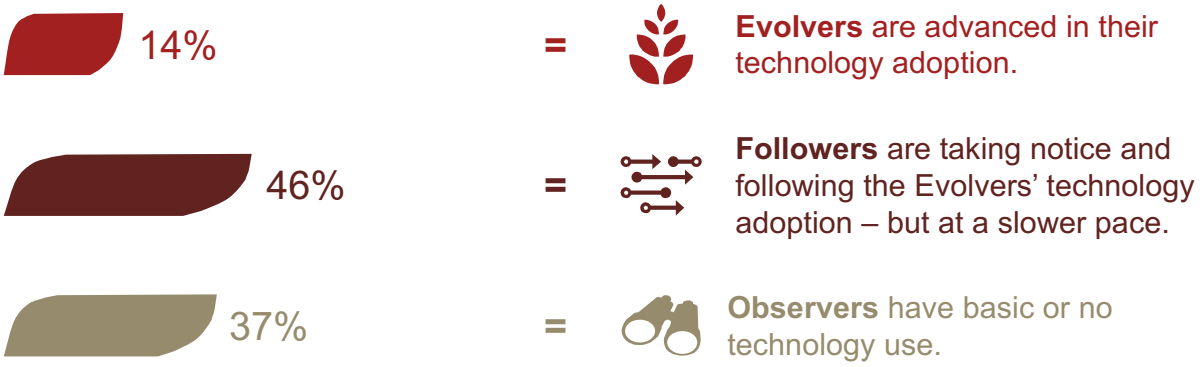
Endringstempoet i samfunnet er raskt og økende, og planleggingshorisonten blir for alle bransjer kortere og kortere. Styret og ledelsen må ta mange kompliserte og risikable valg om produkter, teknologi og allianser, og de trenger råd. Har internrevisjonen en plass rundt bordet? Svaret er at det varierer. De som det lyttes til viser seg å ha noen fellestrekk vi alle kan lære av.

Teknologisk avanserte IR-funksjoner oppleves mer nyttige

PwCs årlige internrevisjonsundersøkelse dekker 92 land, med innspill fra over 2500 styremedlemmer, toppledere og internrevisorer. I undersøkelsen klassifiseres internrevisjonen i tre modenhetskategorier ut fra hvor sofistikerte de er i forståelse for og anvendelsen av

> The real pitfall of Internal Audit is if they don't stay current on new technologies they won't have a seat at the table, and won't be perceived to be adding value.
>
> *Audit Committee Chair*

Figure 2a: Evolvers lead in tech sophistication and span industries, geographies and company sizes



> RPA and AI are the next big technologies. It will be important for Internal Audit to understand these technologies and be able to push the business in how to implement new solutions in the future. With new technology comes new security risk, and this should be a concern of boards going forward.
>
> *– Audit Committee Chair*

teknologi. Undersøkelsen viser at kun 14% av internrevisjonsfunksjonene har en avansert tilnærming til teknologibruk, men at en betydelig høyere andel av disse oppleves å tilføre nytte enn de mindre teknologisk kyndige internrevisorene (figur 2a og 2b).

Kjennetegn ved teknologisk avanserte IR-funksjoner

De avanserte internrevisjonsfunksjonene bidrar allerede i dag med råd om styring og kontroll rundt robotisert automatisering (RPA), bruk av kunstig intelligens (AI), droner, etc. De bruker mer avanserte samarbeidsverktøy for å komme tettere på organisasjonen. De baserer revisjonsarbeidet på en høyere grad av selvstendige datauttrekk, dataanalyser, og datavisualisering, og de bruker AI og maskinlæring for å kunne by på innovativ og verdifull innsikt i organisasjonen (se figur 6). I sum svarer de ut styrets og toppledelsens ønske om å ha meninger om mulighetsrommet nye teknologier tilfører, risikoene som følger med og kontrollregimet som bør være på plass.

Figure 2b: Percentage of organizations who view the IA function as providing significant value

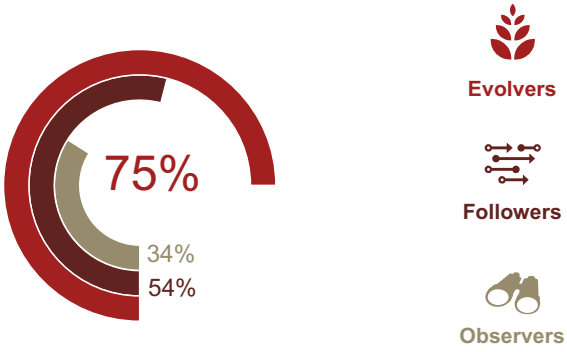
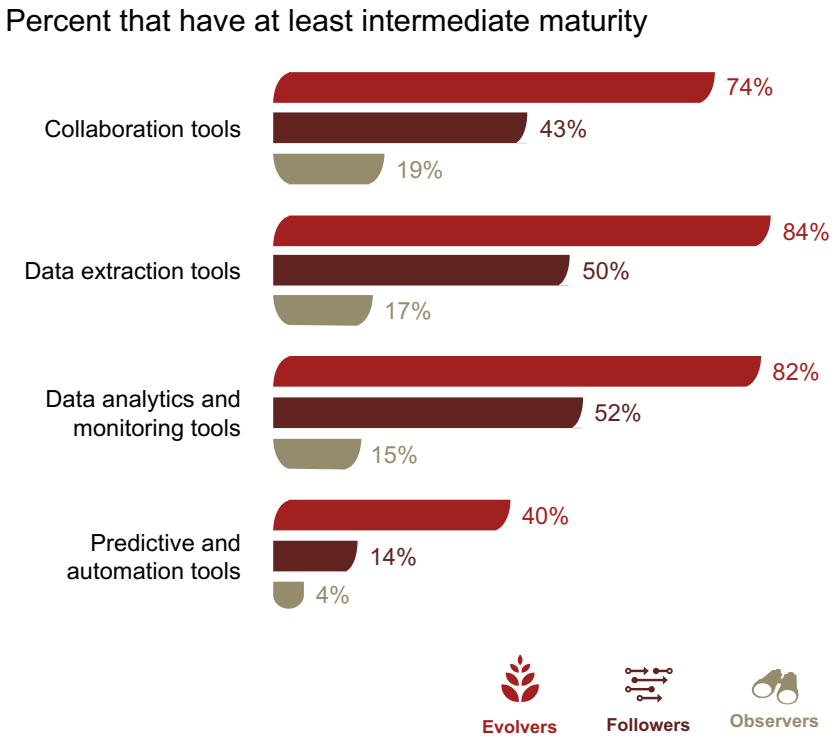


Figure 6: Evolvers' tech maturity crosses tool categories



Rekruttering og medarbeiderutvikling

Undersøkelsen viser at alle internrevisorer må ha teknologiske grunnkunnskaper som overgår gårsdagens «generelle IT-kontroller» tilnærming. Kjerneegenskapen man må besitte er teknologisk nysgjerrighet og en vilje og evne til å kontinuerlig oppdatere seg på nye teknologier, muligheter og risikoer. Den gode nyheten er at den store majoriteten besitter denne viljen, og ser at de har et individuelt ansvar for å ta tak i egen utvikling. De ledende internrevisjonsfunksjonene har en god kompetansemix, med systematisk og dedikert kursing og utvikling

rettet mot nye teknologier (figur 9). Undersøkelsen peker mot RPA og AI som to viktige kommende områder å oppdatere seg på.

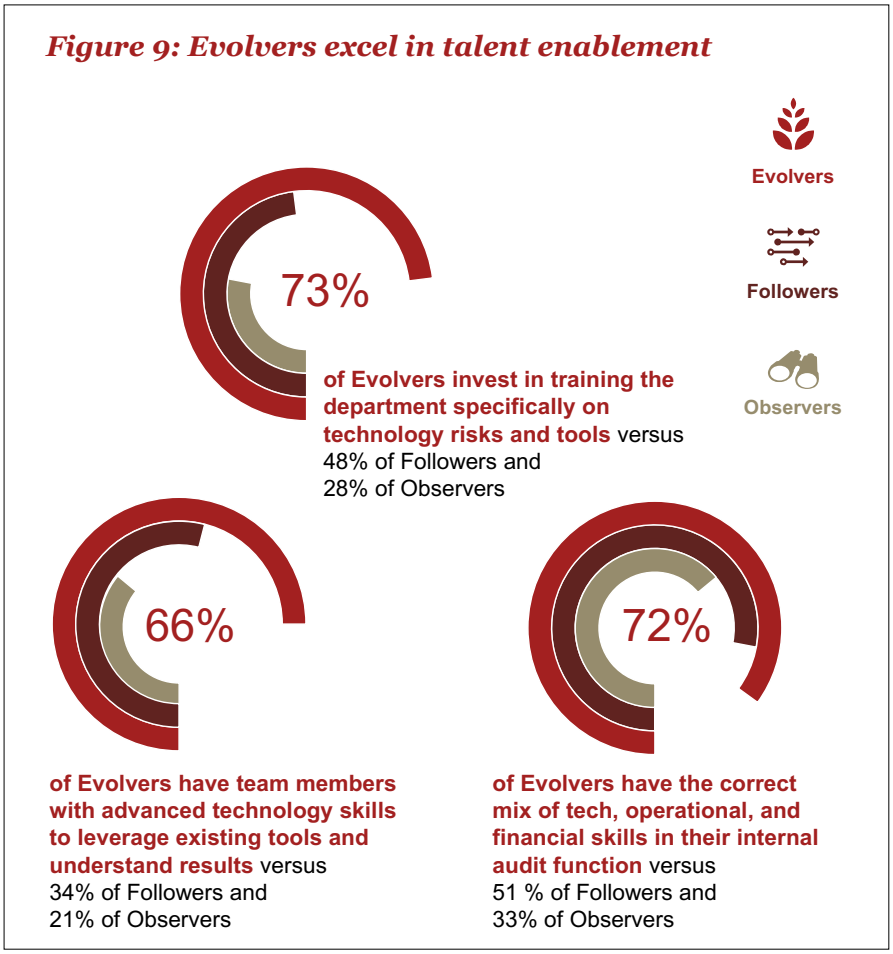
Hvor står Norge

De mindre modne funksjonene er ofte kommet delvis i gang, men er begrenset av tilgang til teknologi, mangelfull datakvalitet, manglende investeringsvilje, eller en organisasjon som ikke er kulturelt klar for å ha en teknologisk avansert internrevisjon. Min opplevelse av den norske internrevisjonsstanden er at det er stor nysgjerrighet og vilje på teknologiområdet, men at man ligger etter i forhold til ledende internasjonal praksis. I mange virksomheter verdsettes fortsatt trygghetsskapende bekreftelser av eksisterende prosesser, eller råd om mer grunnleggende styrings- og kontrollutfordringer. Imidlertid opplever jeg økende forventninger om at internrevisjonen selv burde kunne navigere datasystemene til virksomheten ved egen hjelp, gjøre mer avanserte analyser, komme med prediksjoner, samt visualisere trender, anamolier og risikoforhold. Jeg tror det foreløpig er begrensede forventninger om at internrevisjonsarbeidet skal robotiseres eller gjøres via AI, men gitt utviklingen på andre fagområder, som eksempelvis innen regnskapsrevisjon, burde man begynne å utforske mulighetsrommet.

Anbefalinger

Undersøkelsens hovedanbefaling er å omfavne de teknologiske endringene, og ta i bruk mulighetene i eget arbeid. Strategiene og utviklingsplanene for internrevisjonen må ha fokus på både teknologi og bygging av internrevisjonsteamets kompetanse. Man må innovere måten man arbeider på, og tørre å være «revolusjonær». Se aksjonsplanen nedenfor eller les mer på: https://www.pwc.com/us/en/services/risk-assurance/library/internal-audit-transformation-study.html

Figure 9: Evolvers excel in talent enablement



Actions to take today

Assess where Internal Audit stands with its tech-enabled foundation

- Is your organization using or does it plan to use any emerging technologies such as Blockchain, AI or robotics?
- Does your internal audit function have access to the skills needed to provide risk and controls advice with regard to those emerging technologies?
- Is your internal audit function taking advantage of collaboration, data extraction, analytics and visualization tools?
- Does your internal audit function have a technology skills and tools roadmap as part of its strategic plan?

Fuse technology and talent into a single strategy

- Let the objectives you are trying to accomplish direct the company´s technology and talent investments.
- Invest smartly today for tomorrow´s needs.
- Assess the digital skills available to Internal Audit.
- Develop and source the technology skills needed for tomorrow.

Innovate and be revolutionary whenever possible

- Rethink how things could be done versus making incremental improvements.
- Find ways to share or leverage other´s technologies and talents to leap forward.
- Remember that today´s issue is not tomorrow´s; engage with the organization´s innovation agenda to ensure that Internal Audit keeps pace.

Slik er IIA Norge skrudd sammen

Av Ellen Brataas, generalsekretær

IIA Norge er en ideell organisasjon der hovedtyngden av aktivitetene drives frem av engasjerte medlemmer, for medlemmer. Med et sekretariat hvor to av tre ansatte har vært ansatt i mer enn ti år, er det lett å glemme at selv om medlemstallet ligger relativt stabilt på 800, vil det alltid være noen som er nye og andre potensielle medlemmer som ikke er kjent med hva foreningen kan tilby gjennom nettverk og komiteer.

«IIA Norge skal gi sine medlemmer et solid faglig fundament og styrke kunnskapen i norske virksomheter om styring, kontroll og internrevisjon», er formålet til foreningen. Med et så bredt fagområde, er det en viss fare for silo-tendenser mellom nettverkene, og kanskje er det bare sekretariatet og styret som ser hele spekteret av den fantastiske «dugnadsjobben» som finner sted.

I tråd med foreningens eget motto – «Fremskritt gjennom deling av kunnskap» - kommer her en kort innføring i hvilke komiteer og nettverk foreningen omfatter, samt hva de forskjellige har ansvar for.

I dag er det om lag 70 tillitsvalgte i foreningens forskjellige organer. Alle blir formelt valgt på generalforsamlingen i juni. Det er styret som fastsetter foreningens strategi og beslutter hvilke handlinger som skal prioriteres for å støtte opp om strategien. Sekretariatet er bindeleddet mellom foreningens komiteer og nettverk, mens det er de tillitsvalgte som får ting til å skje.

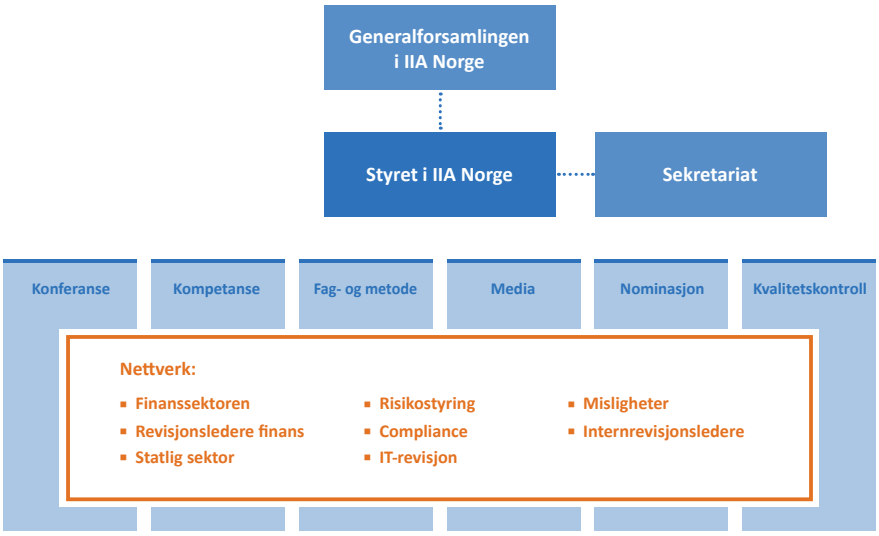
Nominasjonskomiteen: Nominerer aktuelle kandidater til foreningens tillitsverv.

Konferansekomiteen: Arrangerer foreningens årlige konferanse.

Kompetansekomiteen: Utarbeider og arrangerer kurs og medlemsmøter.

Mediakomiteen: Utgir fagbladet «SIRK», samt kommuniserer og promoterer via nettsider, blogg og sosiale medier.

Fag- og metodekomiteen: Pådriver for utviklingen av internrevisjonsprofesjonen i Norge ved å bidra til å gjøre aktuelle fagtema kjente og tilgjengelige.



Kvalitetskontroll: Gjennomgår alle sluttrapporter fra eksterne evalueringer for å sikre konformitet.

Nettverkene: Er møteplasser for medlemmer med interesse for de ulike fagområdene. I nettverkene tilrettelegges det for kunnskapsdeling av fagrelevante problemstillinger gjennom møter, seminarer, kurs, utgivelser/publisering av veiledninger og kunnskapsformidling av nye trender innen fagområder & bransjer. Nettverkene bidrar med faglig innhold til foreningens tidsskrift, nettsider og sosiale medier. Det er viktig for foreningen som helhet at aktiviteter i de enkelte nettverk støtter opp under foreningens strategiske mål.

Per i dag har vi følgende nettverksgrupper:
- Finansnettverket
- Statlig nettverk
- Compliance
- Risikostyring
- Misligheter
- IT-revisjon
- Ansatte internrevisjonsledere
- Revisjonsledere finans

Det er en kontinuerlig vurdering av om nettverksstrukturen møter de behov medlemmene har. Til nå er ingen nettverk faset ut eller slått sammen, men fler har kommet til. Det betyr likevel ikke at slik vil strukturen være for alltid, spesielt ikke i en verden som endres raskt. I blant hender det også at nettverkene går sammen om å arrangere noe rundt et tema som treffer bredt.

What's in it for me?

Fra første arbeidsdag i foreningen har jeg vært utrolig imponert av disse drivkreftene som er tillitsvalgte. Hva får en travel hverdagshelt til å legge ned ytterligere tid på fag? Jeg fikk følgende svar da jeg ropte i skogen: «Vel, som tillitsvalgt får jeg jobbe med akkurat de faglige problemstillingene jeg synes er mest viktig. På jobben kan noen kanskje synes jeg er en fagnerd, så derfor er det utrolig givende å jobbe med andre som er like opptatt av samme faglige utfordringer som meg. Jeg bygger nettverk og blir utfordret på roller jeg normalt ikke ville tatt. Det er gøy å bidra med aktiviteter vi ser er nyttige for flere av medlemmene. Jeg mener den erfaringen jeg får som tillitsvalgt i IIA Norge vil være verdifull hvis jeg på et tidspunkt ønsker å bidra som tillitsvalgt internasjonalt.»

Sitter du med ubesvarte spørsmål om nettverk, komiteer eller det å være tillitsvalgt, ta kontakt på post@iia.no.

Statlig fellesavtale om kjøp av internrevisjonsbistand

Gjennom felles innkjøpsavtale for internrevisortjenester legges det til rette for enklere innføring av internrevisjon for flere statlige virksomheter.

Av
HENRIETTE TORGERSEN
Seniorrådgiver - innkjøp og avtaleforvaltning Statens innkjøpssenter

Avtalen om felles innkjøp ble signert 19. desember 2017 og trådte i kraft 1. januar i år. Det var Difi ved Statens innkjøpssenter som inngikk avtalen på vegne av staten, som vi også har gjort for kjøp av forbruksmateriell og reisebyråtjenester. Fellesavtalen består av fire parallelle rammeavtaler med følgende leverandører, i prioritert rekkefølge: KPMG AS, Ernst & Young AS, Transcendent Group AS og PricewaterhouseCoopers AS.

Hvorfor felles innkjøp av internrevisjon?

I 2015 ble alle virksomheter med inntekter eller utgifter over 300 millioner pålagt å vurdere bruk av internrevisjon i egen virksomhet ved Rundskriv R-117 *om Internrevisjon i statlige virksomheter* (R- 117). Det har gitt økt behov for internrevisjonsbistand blant statlige virksomheter. Markedet ble på kort tid fordoblet og innkjøpskompetansen på fagområdet er trolig varierende.

Målet med fellesavtalen er å bidra til etablering av internrevisjon i staten og å spare staten for utgifter.

Hvilke gevinster kan oppnås med avtalen?

Fellesavtalen forventes å gi en prisbesparelse på 10 – 12 prosent sammenlignet med hva et utvalg av statlige virksomheter tidligere har oppnådd.

De forventede indirekte gevinstene for virksomhetene med å ha en statlig fellesavtale for internrevisjon er vel så viktig som pris. Vi forventer at Fellesavtalen vil:

- gi bedre kvalitet til brukerne
- bidra til lavere transaksjonskostnader
- legge til rette for innføring av internrevisjon i staten
  - o internrevisjon effektiviserer staten og vil bidra til indirekte besparelser i den enkelte virksomhet, samt effektivisere arbeidet til Riksrevisjonen

Hvilke tjenester omfattes?

Fellesavtalen skal dekke statlige virksomheters behov for internrevisjonsbistand i henhold til anerkjente standarder for internrevisjon. Internrevisjonsbistanden skal utføres i tilknytning til en internrevisjonsfunksjon eller et internrevisjonsoppdrag. Alle utførte internrevisjonstjenester skal utføres i samsvar med R-117. Utover internrevisjonstjenestene skal leverandøren på forespørsel bidra med utvikling gjennom rådgivning og kurs.

Mange har hjulpet oss

Fellesavtalen om internrevisjonsbistand har blitt til med bistand fra virksomhetene som er omfattet av ordningen. Disse har bidratt i alle anskaffelsens faser, fra planlegging og konkurransegjennomføring til avtaleforvaltning.

Vi har også et godt samarbeid med DFØ, som er gitt myndighet til og ansvar for å forvalte kravene i R-117, og IIA Norge. Vi samarbeider tett om å klargjøre roller og lage veiledningsmateriale for virksomhetene. Dette legger vi fortløpende ut på internettsidene våre: https://www.anskaffelser.no/statens-innkjopssenter/inngatte-avtaler/internrevisjon. Dere finner også mye god veiledning på DFØ og IIA Norges hjemmesider.

Virksomhetenes rolle

Den enkelte virksomhet er oppdragsgiver og vil ha det operative ansvaret for rammeavtalen gjennom kjøp av internrevisjonstjenester, oppfølging av leveransen og betaling. Den enkelte virksomhet er en part i avtalen. Hver virksomhet skal melde inn en lokal avtaleforvalter som skal stå for kommunikasjonen med oss. Lokale avtaleforvaltere kan sende en slik henvendelse til internrevisjonsbistand@difi.no for å registrere seg og få oversendt kontraktene.

Vår rolle

Statens innkjøpssenter er avtaleeier. Vi har ansvar for strategisk avtaleforvaltning. Den stra-

Fra venstre: Kjetil Østgård, Dag Strømsnes, Barbro Bottheim, Steffen Sutorius, Henriette F.V. Torgersen, Lars Reidar Vold- Andersen fra Transendent Group AS, Petra Liset fra PricewaterhouseCoopers AS, Ole Willy Fundingsrud fra KPMG AS og Aina Karlsen Røed fra Ernst & Young AS.
Gruppebilde fra kontraktsignering hos Statens innkjøpssenter den 19. desember 2017.

tegiske avtaleforvalteren for avtalen er Henriette F.V. Torgersen. Vi følger opp leverandørene på overordnede og gjentakende problemstillinger som er av interesse for alle som er omfattet av avtalen. For eksempel følger vi opp på lønns – og arbeidsvilkår slik at hver enkelt virksomhet slipper denne jobben.

Dette er et nytt område for mange innkjøpere, og vi vil strekke oss ekstra langt i å bistå og veilede på bruken av Fellesavtalen. Send eventuelle spørsmål om avtalen til internrevisjonsbistand@difi.no

Hvordan kjøpe tjenester?

Kjøp av tjenester omfattet av avtalen gjøres ved et såkalt avrop. Det er to forskjellige måter å gjøre avrop på, avhengig av verdien på avropet.

Avrop med estimert verdi inntil kr 100 000 eks. mva. skal foretas direkte hos rammeavtaleleverandørene. Den leverandøren som ved tildelingen er rangert øverst skal forespørres først. Det vil si at KMPG skal forespørres først. Dersom KPMG har saklig grunn i form av manglende kapasitet eller kompetanse til å avslå oppdraget, forespørres leverandør nr. to, altså Ernst & Young, deretter Transcendent Group og deretter PricewaterhouseCoopers.

Det skal gjennomføres mini-konkurranser for avrop med en estimert verdi som er lik eller over kr 100 000 eks. mva. Reglene for hvordan mini-konkurransene skal gjennomføres fremgår av avtalen. Det er satt opp en liste med lovlige tildelingskriterier som virksomhetene kan bruke. Hvilke kriterier som brukes og hvordan de vektes er opp til den enkelte virksomhet, og bør velges ut ifra hva som best vil dekke virksomhetens behov. Maler for konkurransegrunnlag for minikonkurranser er under utarbeidelse.

Standardavtalene ***bistandsavtalen (SSA-B) og oppdragsavtalen (SSA-O)*** skal brukes ved inngåelse av avtale med valgt leverandør, avhengig av om tjenesteleveransen er definert som bistand eller oppdrag (full utkontraktering).

Virksomhetene trenger deres hjelp

Internrevisjon er nytt for mange og kompetansen på kjøp av bistand varierer blant virksomhetene. Det er derfor ekstra viktig at internrevisjonsmiljøet bistår innkjøperne som skal gjøre avrop i prosessen. Vi oppfordrer derfor på det sterkeste alle til å samarbeide godt med innkjøpsavdelingene for å få til gode behovsbeskrivelser, slik at dere får gode tilbud som dekker behovet.

Tatt i bruk av to

Det er allerede to virksomheter som har gjort avrop på Fellesavtalen. Vi er svært fornøyd med å registrere at avtalen et tatt i bruk, og vi er spente på fortsettelsen.

Bruk av internrevisjon fra to departementers perspektiv

INTERVJU MED
THOMAS NEBY BAARDSENG OG ARNE LUNDE

Av
OLA OTTERDAL OG GUNNAR JACOBSEN
begge seniorrådgivere i
Forsvarsdepartementets internrevisjon

Antall internrevisjoner i statlig sektor har doblet seg de siste årene. Dette har virksomhetene i stor grad anbefalt selv, etter at de ble pålagt å vurdere behovet i 2016 med hjemmel i rundskriv 117 (R-117). Men departementene, som etatsstyrer disse virksomhetene, har også hatt en regi på det som har skjedd på internrevisjonsområdet.

Vi har tatt en prat med de to ringrevene Thomas Neby Baardseng i Helse- og omsorgsdepartementet (HOD) og Arne Lunde i Kunnskapsdepartementet (KD). De har vært tilretteleggere for vurderinger av internrevisjon (IR), behandlingen av vurderingene i sine departementer og etablering av nye internrevisjoner. Arne jobber i fellesstaben i KD, i prosjekt digitalisering. Digitalisering er interessant mht. internrevisjon både fordi det skaper større transparens og sårbarhet, og fordi det åpner for nye måter å gjennomføre internrevisjon på. Thomas er nestleder i budsjett- og økonomiavdelingen i HOD og har ansvar for riksrevisjonssaker, RNB og nysalderingen på høsten, samt råd og veiledning til etatsstyrende avdelinger, herunder etablering og bruk av internrevisjon.

Har R-117 fungert som en katalysator for etableringene?

Thomas Neby Baardseng: Det har vært en lang ferd for opprettelse av internrevisjoner i HODs sektor. DFØ kom med en kartlegging i 2009 som blant annet bidro med begrepsavklaring. Etter det har HOD avventet utredningsarbeidet i regi av Finansdepartementet og Direktoratet for økonomistyring (DFØ). HOD var positiv til reguleringen som ble lagt ut på høring i 2014. Det hadde neppe blitt etablert så mange nye internrevisjoner dersom R-117 ikke hadde kommet.

Rundskrivet både sørget for at det ble foretatt en vurdering av behovet for å ha internrevisjon, og rundskrivets modeller har påvirket innrettingen. Modellene har vært utgangspunktet.

Arne Lunde: I universitets- og høgskolesektoren, hvor de nye internrevisjonene i kunnskapssektoren har kommet, har kompleksitet og størrelse vært viktig for valgene. Selv om det var enkelte internrevisjoner i virksomheter under KD før 2016, så var det lite fokus på dette før R-117. Rundskrivet legitimerte behovet for internrevisjon.

Da Lunde tidligere jobbet i Polarinstituttet var det i internkontrollsammenheng mye fokus på transaksjonskontroll. Utviklingen med blant annet digitalisering har økt behovet for formaliserte løsninger og kvalitetssikring og også økt oppmerksomhet på etterlevelse av lov- og regelverk. Personvern har også kommet mer i fokus. Ofte er ikke risikostyringen helhetlig og godt nok avstemt mellom ulike deler av virksomheten. En internrevisjon må forholde seg til hele virksomheten.

Baardseng og Lunde understreker begge at IIAs standarder har vært «bånnplanken».

Hva slags rolle inntok dere da virksomhetene som ikke hadde IR fra før skulle gjøre en vurdering av behovet for en IR?

Thomas Neby Baardseng: Rundskrivet var veldig forsiktig med hensyn til å legge føringer på prosessen. Det var virksomhetene som skulle vurdere og beslutte. HOD mente dette var en såpass viktig prosess at det

Thomas Neby Baardseng og Arne Lunde

aktivt tok stilling til vurderingene. Det ble kommunisert ut i forkant av vurderingene at departementsråden ville ta den endelige beslutningen etter at virksomhetene hadde sendt sine vurderinger. Tre av fire vurderinger gikk igjennom som foreslått av virksomhetene. En virksomhet ønsket å avvente etablering av egen internrevisjon, siden de var i en omstillingsprosess, men departementet var uenig. Men noen ganger kan overstyring fra departementet sette fart på ting. Folkehelseinstituttet ble den første blant virksomhetene som skulle ha internrevisjon, til å etablere. Helsedirektoratet var positive til etablering av IR, men ville trekke det lenger ut i tid enn 1.1-18. Det var ikke HOD enige i.

Det var ikke så populært da helseforetakene ble pålagt å etablere internrevisjon i 2005, men etter dette har vel alle hatt stor glede av det. Så dette kan være en modningsprosess. Her har internrevisjonen blant annet bidratt til at de ulike kontrollmekanismene jobber bedre sammen.

Selv om Statens legemiddelverk var under innslagspunktet for vurdering, ble de også bedt om å gjøre en vurdering. De

ønsket ikke å etablere internrevisjon grunngitt i allerede veletablerte rutiner for kontroll og kvalitetssikring. Dette ble akseptert av HOD.

Arne Lunde: Det er viktig at man har internkontroll sånn rimelig godt på plass dersom internrevisjon skal ha noe for seg. KD arrangerte noen samlinger for å legge opp til en god prosess og bevisstgjøre om hva dette gikk ut på. Siden alle de aktuelle virksomhetene under KD har styrer, har det vært styrene som har tatt valget om etablering av internrevisjon og modell. Departementet ga tydelig signal om at det ser positivt på etableringen av egne internrevisjoner, der størrelse og kompleksitet tilsier det. Innenfor høgskolene har det vært noen fusjonsprosesser som har forsinket etableringen noe, men som har økt relevansen og betydningen av å etablere funksjonen.

I kunnskapssektoren har man erfart at det er krevende å etablere egne enheter for internrevisjon i virksomhetene. Derfor har løsningen blitt ulike former for outsourcing, enten full outsourcing eller at en internrevisjonssjef i virksomheten kjøper tjenester fra konsulentbransjen.

Hva var inntrykket av kvaliteten på vurderingene som ble sendt departementet?

Thomas Neby Baardseng: HOD var fornøyd og mente alle virksomhetene hadde gjort gode vurderinger. Det var ikke behov for noen ekstra runder. Det var nok også en modningsprosess og mange ble nok mer positive til internrevisjon underveis i prosessen.

Arne Lunde: I sektoren under KD er det et betimelig spørsmål hva internrevisjon skal bidra med og det er blant annet et spørsmål hvor langt en internrevisor skal gå i å vurdere det faglige. I denne sektoren er fagfellevurdering en utbredt metode og man har lang erfaring med kvalitetssikringsregimet i regi av NOKUT. Helse og utdanning har noe til felles her. Dette er sektorer hvor fag betyr mye. Men internrevisjon kan over tid bidra til mer helhet i kvalitetsarbeidet. Administrativt har man i universitets- og høgskolesektoren slått sammen enhetene til mer robuste og effektive miljøer.

Bør IR-sjefene delta på etatsstyringsmøtene?

Thomas Neby Baardseng og Arne Lunde er enige om at det må bli opp til etatsledelsen hvem de tar med i disse møtene.

Har dere noe nettverk mellom IR i sektoren?

Thomas Neby Baardseng: I HOD er det ikke tatt initiativ til det. Jeg ser særlig IIAs nettverk for statlig sektor som aktuelt og relevant.

Arne Lunde: Jeg er ikke kjent med at det er etablert noe eget nettverk for KDs internrevisjoner, selv om departementet har oppfordret til dette.

Er det etablert noe samarbeid om outsourcingen mellom de som har valgt modell 5?

Arne Lunde: Dette har i stor grad skjedd innenfor rammene av den nye fellesavtalen for internrevisjon i regi av Statens innkjøpssenter.

Har dere diskutert praktiske ordninger for «sikkerhetsventil» (gå sammen til departementet for avklaring dersom internrevisjonssjef og virksomhetsleder er uenige)? På hvilken måte?

Thomas Neby Baardseng: Det er lagt opp til at etatssjef og IR-sjef sammen kan gå til departementet for eksempel ved uenighet om håndtering av vesentlig risiko. Dette er skrevet inn i instruksene for Folkehelseinstituttet, Direktoratet for e-helse og Helsedirektoratet.

Arne Lunde: Det er styrene som har hovedansvaret her. Det er også slik at ved betydelige avvik, kan departementet ha kontakt med internrevisjonen.

Har dere vurdert å opprette internrevisjon i departementet?

Thomas Neby Baardseng: Dette har vi ikke vurdert som aktuelt og det ville ikke vært effektiv ressursbruk. Det er nok heller ikke hensiktsmessig at internrevisjonen reviderer oppgaven som sekretariat for politisk ledelse. Viktige oppgaver som tilskuddsforvaltning er flyttet fra departementet til direktoratene. HOD har også en kontrolldirektørfunksjon som har både fokus på interne forhold og oppfølging av blant annet tilskuddsforvaltningen på direktoratsnivå. Denne funksjonen dekker forhold som tilskuddsregelverk, forskriftsfesting eller ikke. Dette er områder som de nye internrevisjonene også kan se på. HOD har ikke en kontrolldirektørfunksjon.

Arne Lunde: I forbindelse med omorganiseringen i KD har fokus vært på å forbedre internkontroll og en eventuell etablering av en internrevisjon i KD har ikke vært en aktuell problemstilling. KD har en kontrolldirektør.

Hva slags forventninger har dere til de nyetablerte internrevisjonene?

Thomas Neby Baardseng: Jeg håper ledelsen i virksomhetene, som har fått nye internrevisjoner, bruker anledningen til nytekning og mer systematisk arbeid med ting som ikke står øverst på prioriteringslisten, men som likevel er viktige. Målrettet bruk av IR kan være et grep som bedrer virksomhetens interne kontroll, og som forebygger merknader fra Riksrevisjonen. Jeg har også en forventning om at IR-enhetene vil balansere rollen sin og være både uavhengige og rådgivende. Den rådgivende delen er viktig. Jeg forventer også at de som jobber med etatsstyring i departementet etterspør informasjon om virksomheten og bruker informasjonen konstruktivt. Opplegget for oppfølging har sammen med nye retningslinjer for årsrapporten (R-115) blitt mer konsistent. Jeg forventer en profesjonalisering av styringsrelasjonene. Det blir stadig vanskeligere å si man ikke visste.

Arne Lunde: I forbindelse med R-117 kom det også nye krav til innholdselementer i årsrapport fra virksomheten til departementet. Mye av styringen ligger jo i oppfølgingen av disse rapportene. Departementet må kreve rapportering og bruke den. IR er interessant for KD og kan gi informasjon om gjennomføring og etterlevelse i virksomhetene. KD har ikke mottatt rapporter fra de nye internrevisjonene, men det henvises til resultatene av internrevisjonsarbeidet i årsrapportene. Det blir spennende å følge med.

Nye internrevisjoner under HOD:
- Helsedirektoratet,
- Nasjonalt folkehelseinstitutt
- Direktoratet for e-helse

Nye internrevisjoner under KD:
- NTNU
- Universitet i Tromsø
- NMBU
- Høyskolen i Sør-øst Norge
- Høgskolen på Vestlandet
- Høgskolen i Østfold

Kryptoteknologi

Kan det være måten å realisere en drøm om å gi eierskap av egne data tilbake til kunden?

Av:
ANDERS REKVE
M.Phil Teknologi, Innovasjon og Kunnskap UiO, Ansatt Turner & Townsend. Utleid til europeisk kunde som prosjektleder for implementasjon av nytt designkonsept i Norden.

ANTONIO MARCUS LAAKE
MSc Finance (Cass Business School), Master I Risikostyring og analyse UIS, Diplomøkonom BI (økonomi og administrasjon), Senior Analytiker/Manager Risikostyring Konsern i Gjensidige med over 13 års arbeidserfaring fra finans, risikostyring, risikomodellering og governance

Forberedelser til innføringen av GDPR (det nye personvernsdirektivet) har det siste året ført til tildels omfattende gjennomganger av bedriftens rutiner for å sikre etterlevelse av det nye regelverket. Parallelt har det i løpet av det siste året også skjedd en utvikling i bruk av kryptovalutaer som til eksempel Bitcoin, Ethereum, m.fl. Siden kryptovalutaer går for å være en hel del sikrere enn andre lignende løsninger, finnes det noen gode løsninger på GDPR problematikk innenfor kryptoteknologi? Er det for eksempel mulig å nyttiggjøre seg av kryptorelaterte løsninger for å kunne sikre sensitive kundedata?

Maidsafe

Det amerikanske sikkerhetsselskapet Identillect Technologies tror at det er mulig å anvende kryptoteknologi for å tilfredsstille GDPR-kravene. I mars 2018 inngikk Identillect Technologies en lisensieringsavtale med det skotske selskapet Maidsafe der de sammen tar sikte på å utforske bruken av Maidsafe sin teknologi for å løse problemstillinger relatert til GDPR.

Maidsafe sitt produkt er et nytt *autonomt* nettverk «SAFE Network». Et autonomt nettverk styrer og administrerer seg selv uten mulighet for menneskelig påvirkning. Det finnes ingen tredjeperson som kan hackes, påvirkes eller kompromitteres for å få ulovlig tilgang på data. Data du har lastet opp er kryptert og distribuert over nettverket med avansert kryptering. Nøkkelen som dekrypterer dataene har aldri forlatt enheten du lastet dataene opp fra. Det er ingen som kan tyvlytte eller hacke tredjepersoner på internett på leting etter tilgang til dine data. Det er som et nettverk lagd for GDPR: Ingen kan få tilgang til dataene med mindre du eksplisitt har gitt noen tilgang til den.

Maidsafe er en forkortelse av ordene *Massive Array of Internet Disks, Safe Access For Everyone.* Målet til Maidsafe er å lage et nettverk, «SAFE Network», som nyttiggjør seg av ledig lagringskapasitet på allmenhetens internett-oppkoblede elektroniske enheter. Hvis Maidsafe:

1. Finner en måte å koble enhetene sammen til et stort nettverk
2. insentiviserer folk til å stille enhetene sine til disposisjon til fellesskapet

– da har man i praksis oppnådd et fungerende *Massive Array of Internet Disks.*

Hvis Maidsafe i tillegg:

3. lager en løsning som er teknisk sikker som gjør at folk er villig til å lagre dataene sine på andre mennesker sine enheter - da har de også oppnådd *Secure Access For Everyone.*

Maidsafe er allerede på god vei til å gjennomføre dette. De har arbeidet over 10 år med FoU; neste iterasjon av testnettverket (Alpha 3) er ventet snarlig, og de har sikret seg flere defensive patenter på teknologien sin, samtidig som de skalerer opp organisasjonen for økt produksjon av datakode og tilrettelegging for eksterne applikasjonsutviklere.

Fordeler ved bruk av Massive Array of Internet Disks

Et hav av ledig kapasitet

Hvis du tenker deg om, hvor mange elektroniske enheter har du hjemme som er

INSPIRASJON TIL TV-SERIE

Richard Hendricks (Thomas Middleditch) i den amerikanske situasjonskomedien og tv-serien Silicon Valley. Teknologien i forretningsideen til Richard sitt fiktive selskap «Pied Piper» er basert på SAFE Network.

Figure 1: https://spectrum.ieee.org/view-from-the-valley/telecom/wireless/a-2-million-contest-seeks-a-real-world-pied-piper

koblet opp mot internett? De fleste av oss har kanskje en smarttelefon, bærbar PC, lese-/nettbrett, stasjonær datamaskin, en smartTV, osv. Estimatene spriker litt, men ett estimat sier at det innen 2020 vil være over 30 milliarder oppkoblede enheter. Alle estimater viser en enighet om at antallet vil øke betydelig de neste årene. Det er dette som er *Internet of Things (IoT)*, på norsk Tingenes internett.

Felles for alle enhetene er at utnyttelsesgraden av disse er forholdsvis lav. De fleste bruker kanskje bærbar PC og mobil flittig. Men om natten, ca. en tredjedel av døgnets 24 timer, så ligger begge oftest ubrukt. Og selv om de er i aktiv bruk, belastes ikke enhetene 100% hele tiden. Så hva hvis delingsøkonomien kunne bli brukt for å utnytte denne ressursen? Aggregert vil de utgjøre en betydelig reserve i form av lagringsplass og prosessorkraft. Dette er ressurser som kan stilles til nettverkets disposisjon til en marginal kostnad for den enkelte som er tilkoblet nettverket. Dette fordi enheten er allerede:

1. betalt for, så det innebærer ingen innkjøpskostnad som må nedbetales
2. skrudd på, så den konsumerer bare marginalt mer strøm ved økt utnyttelsesgrad
3. koblet til internett som i de fleste tilfeller har en fast kostnad uavhengig av bruk.

Enheter som er koblet sammen i «SAFE Network» vil dermed kunne yte tjenester til brukere av nettverket for en kostnad lik den økte kostnaden et marginalt høyere strømforbruk representerer. Sett i kontrast med kostnaden ved å lagre data i datasentrene der

1. Det må investeres i bygging av datasenteret, infrastruktur og maskinvare
2. Driftskostnader inkluderer kostnader til sikkerhet, redundans, kjølingskostnader osv.

så er merkostnaden i form av høyere strømforbruk på eksisterende digitale enheter beskjeden i forhold. På en annen side blir eierne av enhetene kompensert i form av «SAFE Network» sin kryptovaluta «safecoin». Så lenge denne kompensasjonens kroneverdi tilsvarer eller er høyere enn den økte strømkostnaden, så er individet insentivisert til å stille enhetene sine til disposisjon.

Data lagres én gang

Det finnes millioner av duplikater av filer lastet opp på nettet. Se for deg en liten videosnutt som går viralt. Etter kort tid ligger denne videoen lagret på servene til flerfoldige nettsteder; Facebook, blogger, osv. En fil på 10MB duplisert 1.000 ganger ender opp med å oppta 10GB med total lagringsplass. Ifølge Åse Dragland i Sintef ICT ble 90% av verdens data produsert de siste 2 årene (i 2013). Hvor mye av dette er lagret i duplikater på internett?

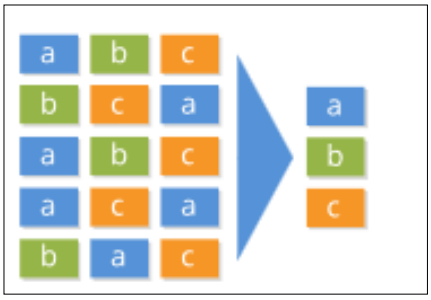
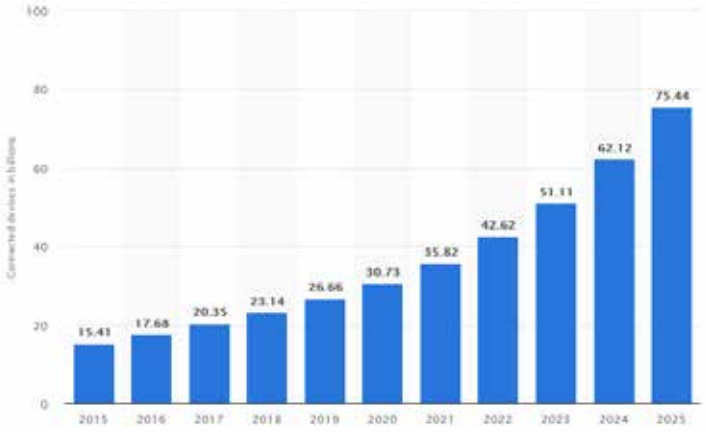


Figure 2: https://maidsafe.net/features.html

På «SAFE Network» lagres unike filer kun en gang. Når brukere lagrer en fil som allerede ligger på nettverket, så vil brukerne bli referert til filen som allerede ligger på nettverket. Dette skjer ved at nettverket tar et fingeravtrykk, «hash», av filen



Tingenes internett (IoT)

Wikipedia beskriver IoT som «et nettverk av oppkoblede fysiske enheter, kjøretøy, husholdningsapparater og andre ting som inneholder elektronikk, programvare, sensorer, aktuatorer og nett-oppkobling som muliggjør at enhetene kan kommunisere og utveksle informasjon».

Figur 1: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

du ønsker å lagre på nettverket – og sjekker om fingeravtrykket allerede ligger på nettverket.

Effektivitet

SAFE Network tar i bruk *delingsøkonomien* for å skaffe tilgang til ressurser og utnytter ubenyttet kapasitet til enhetene i Tingenes Internett. Samtidig sørger teknologien for at data ikke blir lagret i duplikater - som effektiviserer lagring ytterligere. Resultatet er ett nettverk som kan stille nettverksressurser til disposisjon til en langt lavere ressurskostnad enn dagens arkitektur som er avhengig av store datasentre.

I tillegg til mindre ressurskrevende lagring, bidrar SAFE Network med mindre ressurskrevende sikkerhetsopplegg for den enkelte bedrift som må etterfølge GDPR. Datasikkerhetsfunksjonene som muliggjør etterlevelse etter GDPR er en sentral egenskap av nettverket. En kan tenke seg at spesielt for nykommere vil det være interessant å se hvordan SAFE Network kan senke inngangskostnadene til å tilby tjenester innenfor etablerte segmenter – der konkurrentene har gjort betydelige organisasjonsmessige og materielle investeringer.

Sikkerhet: Blokkjede vs. SAFE Network

Sikkerhet og lagring i blokkjede

SAFE Network og blokkjede er ikke direkte sammenlignbart. De utfører forskjellige funksjoner. Ved hjelp av blokkjede kan man etablere en uforanderlig historikk over hendelser uten å være avhengig av en sentral autoritet som verifiserer at hendelsene tok sted (som en bank ville gjort med transaksjoner). Den iboende *sikkerheten* i blokkjede er at ingen skal kunne endre historikken om hva som har hendt. For eksempel er det svært vanskelig å endre på transaksjonshistorikken til Bitcoin.

Blokkjede er «en voksende liste med databaser kalt «blokker» som er lenket sammen ved hjelp av kryptografi» ifølge Wikipedia. Forenklet består den kryptografiske lenken i at hver blokk inneholder et «hash» av den foregående blokken.

Det er svært vanskelig for en uærlig aktør å endre på data som er skrevet inn i blokkjeden. Hvis en uærlig aktør ønsker å gjøre en endring på transaksjonene som ligger i databasen til blokk #32, så vil «hashen» av blokk #32 som ligger i blokk #33 ikke lenger stemme. Da vil heller ikke «hashen» av blokk #33 som ligger i blokk #34 stemme. Og så videre. Se tekstboksen i denne artikkelen for et inntrykk av hva selv den minste forandring i den underliggende dataen betyr for den assosierte «hashen».

HVA ER EN HASH?

En hash kan fungere som et fingeravtrykk av data, uten å avsløre hva slags data det er snakk om. Dette skjer ved hjelp av spesielle hash-funksjoner som til eksempel Secure Hash Algorithm (SHA). I eksemplene under blir setningene «hashet», og vi får en «hash» (et fingeravtrykk av setningen) representert med tall og bokstaver. Legg merke til endringen i «hashen» (fingeravtrykket) der kun en bokstav endres i setningen.

SHA1(«The quick brown fox jumps over the lazy dog»)
= 2fd4e1c6 7a2d28fc ed849ee1 bb76e739 1b93eb12

SHA1(«The quick brown fox jumps over the lazy cog»)
= de9f2c7f d25e1b3a fad3e85a 0bd17d9b 100db4b3

Eksempel hentet fra Wikipedia, https://no.wikipedia.org/wiki/SHA-sjekksumsfunksjoner, 25.04.2018

> «Blockchain´s killer app is bitcoin, the rest is mostly pure marketing»
>
> *-David Irvine, Maidsafe*

Blokkjede er uovertruffen til å skape en uforanderlig historikk. Men den fungerer dårlig til lagring av data. Databasen til hver blokk i blokkjeden har kun kapasitet til en veldig begrenset mengde informasjon. Det er ikke realistisk å lagre et bilde til en blokk i en blokkjede, men noen tusen linjer med tekst går fint.

Det siste året har det vært en «hype» der blokkjede har vært løsningen som lette etter problemer å løse. Det kan være greit å opplyse om at kypto-sfæren består av mer enn kun blokkjede. Blokkjede er en fantastisk teknologi for å skape desentraliserte og sikre betalingsløsninger, men dårlig på svært mye annet.

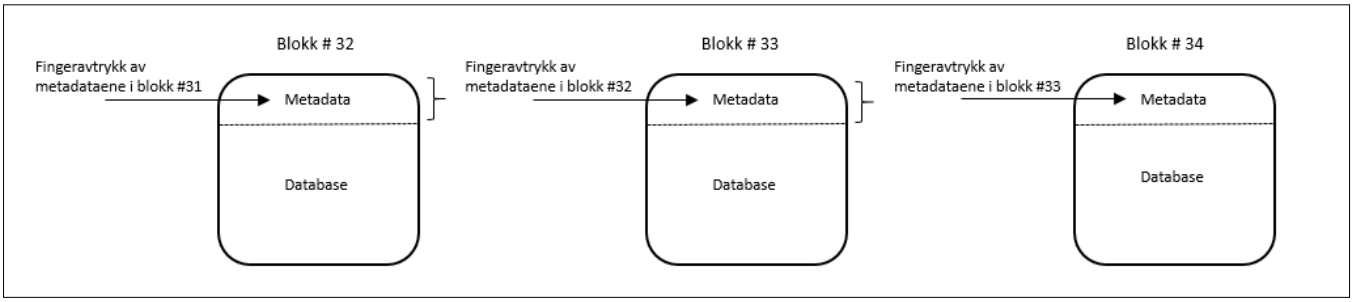


Figure 3: inspirert av https://www.pluralsight.com/guides/software-engineering-best-practices/blockchain-architecture

Sikkerhet og lagring i SAFE Network

SAFE Network er et autonomt nettverk, der nettverket styrer og administrerer seg selv. Det er et desentralisert nettverk uten et sentralt sted som en uærlig aktør kan angripe for å påvirke nettverket. Det regulerer selv hvor, hvordan og når data blir lagret. Det regulerer selv prisen den kompenserer enhetene i nettverket slik at det alltid er et tilstrekkelig tilbud av ressurser i reserve. Ingen kan vite hvilke enheter og hva slags data ligger lagret, selv ikke nettverket selv. Datasikkerhetsmessig fjerner dette kanskje den største kilden til at data kommer på avveie: Det er ingen mennesker til å begå feil, kompromitteres eller ødelegge med vilje.

Hvis du tar et bilde med telefonen din og ønsker å lagre dette på nettverket, så deles bildet først opp i flere mindre biter. Deretter krypteres det med to svært sikre krypteringsmetoder, der nøkkelen for å dekryptere bildet aldri forlater telefonen din. Etter dette blir de krypterte bitene av bildet lastet opp til tilfeldige enheter på nettverket.

Siden passordet ikke forlater telefonen, betyr det at passordet ikke er lagret et annet sted. Dette betyr igjen at:

1. Ingen kan tyvlytte på kommunikasjonen din for å finne passordet
2. Ingen kan hacke stedet der passordet ditt er lagret
3. Ingen har nøklene til dataene utenom personen som lastet opp dataene.

I 2012 ble Linkedin hacket, og rundt 6.5 millioner passord ble stjålet av hackere. Disse passordene sammen med brukerinformasjon kan igjen åpne opp for at uvedkommende får tilgang til brukerkontoer andre steder. Slike scenarioer er ikke mulige på SAFE Network, da det ikke finnes et sentralt mål for hackere å angripe. Passord og brukerinformasjon er ikke lagret noe sted unntatt på enheter kontrollert av brukeren. Hvis passord kommer på avveie, så er det sannsynlig som følge av brukerfeil.

«SAFE Network» og GDPR – En mulig løsning

Grunntanken er at kundens sensitive data hele tiden ligger på «SAFE Network» og aldri er i bedriftens kontroll. Bedriften tilrettelegger for at kunden kan legge til sine data til «SAFE Network» og gi bedriften midlertidig lesetilgang til denne. Dette gjøres ved hjelp av en applikasjon som bedriften har utviklet ved hjelp av utviklerverktøyene til Maidsafe. Bedriftens applikasjon abstraherer vekk kompleksiteten ved SAFE Network for kunden. Den sørger for at kunden innehar reelt og faktisk eierskap til dataene sine. Den sørger også for å strukturere informasjonen som bedriften er interessert i, på samme måte et hvilket som helst skjema ville gjort.

Når det er nødvendig for å fullføre en gitt forretningsprosess etterspør bedriften lesetilgang på relevant data fra kunden. Det er kunden som kontrollerer informasjonen hele veien, og det er kundens ansvar å administrere tilgangskontroll til denne informasjonen. Når forretningsprosessen er overstått sitter bedriften igjen med produktet av forretningsprosessen, men ikke dataene som inngikk i den.

En kan spørre seg om ikke dette ville latt seg gjøre uavhengig av «SAFE Network»? Kan ikke bedriften be om at kunden oppbevarer dataene sine hos en ekstern leverandør av skylagringstjenester? Begge tilfeller resulterer i at kundedata er lagret utenfor bedriftens systemer. Og på samme måte som i eksempelet ovenfor, så etterspør bedriften lesetilgang til kundens data når den trenger det.

Forskjellen ligger i at kundedata lagret hos underleverandør er data i bedriftens kontroll, og dermed også ansvar for med tanke på datasikkerhet. Kundedata på «SAFE Network» ligger innenfor kundens kontroll.

Utvikling fremover

Personene bak «SAFE Network» har store ambisjoner. Det er spennende å se systemer som knytter sammen såpass mange utviklingstrekk i dagens samfunn: Generelt fokus på eierskap og kontroll av data; et autonomt og desentralisert nettverk; *kryptografisk* sikret data; nyttiggjøring av *delingsøkonomien* for å skaffe til veie ressurser i *Tingenes Internett* (IOT) samt nye metoder for å lagre data uten duplikater som igjen adresserer den massive økningen i dataproduksjon. Den fiktive COO til «Pied Piper» Jared Dunn i den amerikanske situasjonskomedien og tv-serien *Silicon Valley* uttrykte det på en veldig bra måte – se boksen.

Konklusjon

I disse tider blir Facebook beskyldt for å lagre for mye av våre data og selge de videre til tredjepersoner. Vi leser om nettsteder som blir hacket og sensitiv kundedata som kommer på avveie. Personlige data er blitt en ettertraktet ressurs for legitime og illegitime aktører. Gitt denne bakgrunnen er det spennende å få øynene opp for alternative måter å organisere data på slik at individet – kunden - du selv - eier og forvalter egne data. I sammenheng med innføringen av GDPR blir det spennende etter hvert å se hvordan kryptoteknologier kan utvikle seg til å være en løsning av utfordringer - med en tilsvarende stor mulighet for innovasjon av varer og tjenester. Kanskje vil dette ikke være den første og siste gangen du hører navnet «SAFE Network» og utnyttelsen av kryptoteknologi i personvernsammenheng?

I AM SURE YOU ARE AWARE OF THE GREAT LONDON HORSE MANURE CRISIS OF 1894?

In the 1890s the industrial revolution had people flocking to the city. And more people equals more horses and more horses equals manure. And it was predicted that by the middle of the next century there would be 9 feet of manure covering the streets. But what no one saw coming was a new technology that would completely obliterate those concerns - the car. Overnight the manure problem vanished.

And the internet as we currently know it is rife with identity theft and SPAM and hacking - so it is manure. And we believe that in success, our new entirely decentralised internet will be just as significant as the car.

«Pied Piper» sin COO Jared Dunn (Zach Woods)

Why gather intelligence?

After a career in police investigations based out of London, Shaun moved to Trondheim where he now works as a consultant with his own company Reardon Consulting Services advising in the areas of Information Security, Quality Management Systems, Investigations, Business Intelligence, Risk and Business Continuity.

By
SHAUN REARDON

Introduction

In this article, I will examine more closely what we mean by intelligence and how that differs from information. I will also address how to deal with the information acquired. It should be noted that in this article I am addressing issues generically and when considering action to be taken it must, of course, be tested against the legality of what is permissible in the jurisdiction in which you are operating.

Part of identifying and assessing risk must surely be to anticipate what the opposition have access to and what their capabilities are. If it works for them it can work for you, so a systematic approach to gathering information and turning it into intelligence is needed. It doesn't have to be the stuff of fiction or Hollywood films; this is not the Bourne Trilogy and you don't have to look like Matt Damon.

There are many companies that provide intelligence gathering services for their clients. Brand protection is but one reason for this. A lot of the intelligence gathering takes place on the internet and you would be truly surprised at what can be found. There are many books written on the subject of Open Source Intelligence (OSINT) and there are hundreds, if not thousands of free tools available on the internet to gather and mine this information. Some nation states employ tens of thousands of people to gather and exploit information. Countries such as Norway have a reputation for technology and innovation so they especially present themselves as an attractive target.

As a penetration tester, I spend a lot of time gathering information before even attempting to test a system. Figure 1 shows the result of OSINT gathering and then visualizing it to aid understanding. Each node is information freely obtained and shows the links between people, companies, hobbies etc. Put together this information can either make you stronger or destroy your business.

Some nation states employ tens of thousands of people to gather and exploit information. Countries such as Norway have a reputation for technology and innovation so they especially present themselves as an attractive target.

Intelligence vs information

So, everyone knows what information is! It's anything you can sense, see, touch or hear. It can be rumours, speculation or even the truth.

Intelligence, on the other hand, is something more, well, intelligent. It is the collection and receipt of information, assessing it for reliability and provenance, identifying gaps, obtaining and analysing the additional information. Just because it is on the internet or in the papers doesn't make it true. Besides, what is important to one organization may not be important to

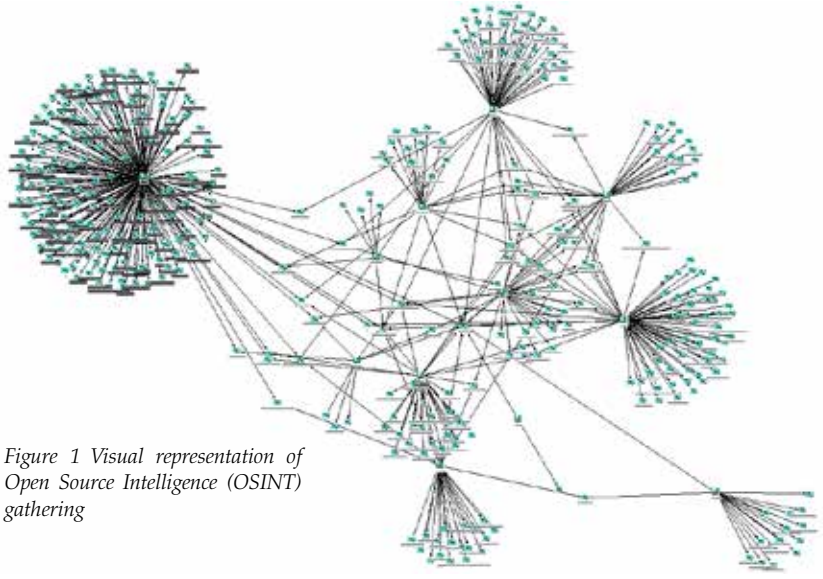


Figure 1 Visual representation of Open Source Intelligence (OSINT) gathering

yours. The end result is something that informs your business processes.

Let's now step through the first stages that can be adopted to make you more 'intelligent'.

Are you vulnerable?

Consider how many sources of information you have access to. The list is endless. Now consider what could give you a warning that something untoward is about to happen to your business. Then ask yourself why someone would want to do this?

It could be that you have just launched a new product which 'flattens the competition'. It could be that your product or service will 'provoke' special interest groups or your Research and Development process is enviously regarded. So firstly, ask the question 'Where will they get information?' In other words 'Espionage'. Your web site seems a good place to start.

Disclosing the hidden traces

Putting aside such illegal methods as blackmail, kidnapping, burglary and theft, consider what information is openly held, where it is and how they could access it. The first point of their intelligence gathering could be your internet presence.

You hopefully have decent logging enabled, not to mention protection from attacks. Does the coding in your web page reveal sensitive information? You would be surprised what people write when they think it can't be seen. I have seen 'secret' email addresses as well as comments that refer to the location of sensitive data.

In one case, an international group of paedophiles used virtually untraceable email addresses to communicate. They then used several other internet tools to split the information up. However, just leaving information in the web page circumvented their security and resulted in some pretty lengthy stays as a guest of the state.

People gathering information will, in all probability, have left traces on the internet during previous activities. This can help you build an assessment of their motivation and capabilities. Having a structured way to gather this information,

and turn it into intelligence, seems like a good idea. Better to know that someone is looking than get surprised.

Consider cause and effect. Again, risk identification and planning are essential. As the old saying goes: It's too late to learn to dance five minutes before the party.

Evaluation

Time now to apply some thought. The first thing to assess is the source of the information. This could be graded as follows:

- Always Correct
- Almost Always Correct
- Often Mistaken
- Believed to be False
- Unable to Assess.

You could assign a value to these assessments either by a letter or a number. Either way, be sure to evaluate each piece of information on its own.

The second step is to evaluate how the source knows this information? Again, the criteria could be:

- Knows it personally.
- Told by others
- Heard a rumour
- Made an assumption / inference.

A third step may be desirable and is used for determining who or where the intelligence should be disseminated to. It could be that the source or the information is 'business sensitive' and it should be protected. This is a matter for you, but again a grading system could be adopted.

An Example (Details changed to protect the guilty)

You are an organisation who produces a successful range of designer furniture. You have had some protests from environmental groups in the past due to the use of hardwood from non-sustainable forestry sources. The protests previously have been nonviolent and involved the use of social media and letters to some of your retailers. However, a threat was made that should this continue then 'other action' may be taken. You are just about to launch a new line of furniture and will announce it on your website.

This example is used to illustrate the potential sources of information to be collected and evaluated during your risk assessment.

- Monitor the media used by the protesters on a previous occasion. Have the number of 'likes' or comments increased?
- Consider monitoring other social media feeds i.e. Twitter
- Use search engines to form a profile of the group
- Try to form an opinion on whether they are a 'risk' or a 'threat' and what your vulnerabilities are.
- Try and establish a 'normality picture' for your website. This may help identify activity such as attempts at altering your web page, 'web defacement'

- Inform the IT department of the forthcoming 'product campaign' and task that they notify unusual or unexpected events.
- Poll your staff to find out if any unusual requests have been received and ask security about any security events however minor.
- Similarly consider other sources of information such as press articles or information from industry sources.
- Remember, some people are motivated by ideology not profit so their techniques may encompass multiple attack vectors, physical and cyber.

Above all, have a systematic plan to collect, record and evaluate and deal with the consequences. Make sure all interested parties have access to it, and if possible, exercise your plan so everyone knows what their role is.

Collect and record

By now you should be well on the way to appreciating the information you already have access to, be aware of the additional sources of information available and understand the importance of applying a defined and structured method of evaluation to this data.

Realising that this intelligence may come in dribs and drabs, a method of storing and collating data is needed, and this is where the thorny question of data protection law comes in to play. I can only encourage you to comply with your own country's laws and regulations. Compliance is always a risk element to be considered and mitigated given its potential to damage your organisation's bank balance and reputation.

The system should be capable of being searched for words and ideally utilise basic search logic such as AND or OR statements. Each piece of information should have the source and evaluation criteria attached. At the very least, a spreadsheet will suffice. This can be incorporated into your overall risk planning although it is very dynamic by nature. Remember you can´t avoid an investigation but you can at least think about it and plan for that eventuality. For those of you that remain to be convinced consider the GDPR regulations that came into effect in May 2018. Many companies are NOT ready and I would predict that there will be several investigations by the regulators into breaches of information security, some of which could have been prevented by defined intelligence gathering procedures.

Once you have overcome this potential barrier you can proceed to the next stage which is analysis. This function comes in several different flavours ranging from simple to that requiring a PhD. For our purposes, we'll use the KISS principle (Keep It Simple, Stupid).

Gap Analysis

In the context of this article this means 'What do we know now, and what would we like to know in the future?›. The bit in between is the gap that needs filling. The gap can be to find out more about a competitor's product, to determine why your share prices are changing unexpectedly or to understand the capability and intent of people opposed to your product, as mentioned in the first part of this article.

The result of this analysis could drive another round of collection, evaluation and collation, but this time with a specific task in mind. You are intelligently tasking, and that is more efficient in terms of time and resources.

Once you have sufficient data, you can proceed to other more complex types of analysis. This can be timelines, cause and effect studies, business modelling etc. The type will depend on your needs and abilities. It is at the analysis stage that the mists should start to clear and a clearer picture of the situation emerge.

One of the quirks of analysis is that you will rarely get all the answers written in stone. Some things you will know as facts, and others you will have to infer.

One of the quirks of analysis is that you will rarely get all the answers written in stone. Some things you will know as facts, and others you will have to infer. The evaluation methods shown in this article will certainly help in this respect, as you will have a set of criteria to assess the information against. Inferences are useful when formulating working theories.

Tasking

I mentioned above that tasking is an important part of the intelligence process. Tasking (and the reasons) should be recorded and this applies whether you yourself perform the task, or you assign it to someone else. In fact, any decision taken

should be recorded with as full a rationale as possible.

If you are subject to an investigation, they will want to know why certain actions were taken. Having a contemporaneous record of a decision, whether right or wrong, is better than "I can't remember" or worse; making your answer fit the circumstances in hindsight.

Some people run dedicated written 'decision logs' covering a range of topics such as media, communications etc. However, as long as it's recorded somewhere, can't be altered and is available, then any medium will suffice. It will help to answer those horrible questions such as 'when did you know' and 'why did you do that'.

In my experience, the post incident review often involves much finger pointing, people running for the bushes and putting extra clothing on that part of the body that we sit on!

Decisions

So, you've put all this effort in, you've identified risk or threat, you have collected, evaluated, collated, analysed, tasked and analysed again. Now it's decision time:

- Have you identified something that can be exploited for your organisation's benefit?
- Have you identified a risk that you can mitigate by implementing control measures?
- Have you identified something that can form part of your contingency and crisis response plans?
- Now do you see the need for effective information gathering and intelligence development?

This is where all efforts can come to naught because the information is not disseminated or shared to those who need it.

Dissemination

So, what should the output be from all of this work? If everyone has the ability to feed information in should they also have the right to see the resulting intelligence? Not surprisingly the answer to that question is an emphatic no.

One principle that should always be adopted is the 'need to know principle'. There is some information which should not be freely available because once information is released, it is impossible to know how far it has gone, who now has it, and what they will do with it.

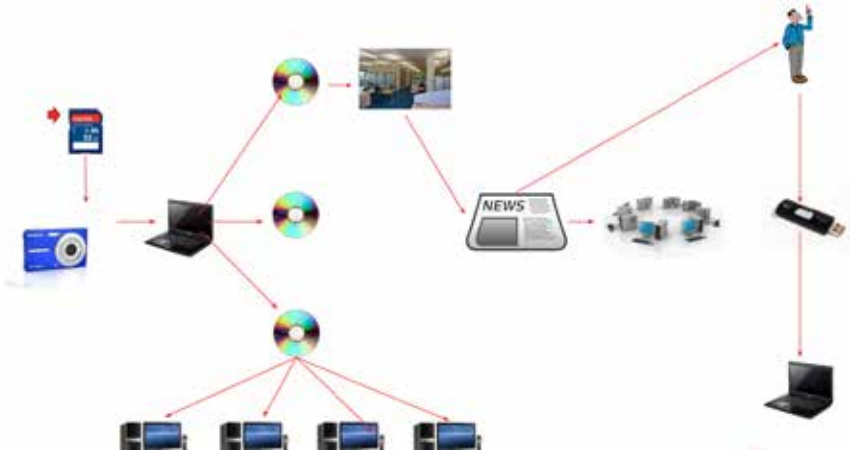


Figure 2 Computer forensic investigation

Research suggests that the biggest threat to corporate or organizational security comes from within, and this includes espionage. If you have ever 'misplaced' sensitive data, then your priority will surely be to conduct 'propagation analysis'. A potentially costly and sleep depriving exercise, which I will illustrate by describing a case I worked on involving the loss of sensitive data.

Research suggests that the biggest threat to corporate or organizational security comes from within, and this includes espionage.

Figure 2 shows the result of a very fast time computer forensic investigation to determine whether the data contained in the SD card shown on the left had been copied and, if so, who else had access to it. Apart from the sensitivity of the data I would suggest that the primary objective was to determine the degree of propagation and assess the risk to the data subjects. By following the forensic clues coupled with ´good old detective work´ I managed to trace the data flow, identify who had seen it and ring fence it within 36 hours. My confidence level was high that the information was safe but had it gone any further the outlook would have been quite pessimistic. The point here is "Need to Know".

During your intelligence process you may have adopted a grading system for each piece of information relating to its dissemination. Even if you have not done this, then you should consider whether the final report should be protectively marked with something like 'Commercial – Sensitive' and restrict its circulation.

If this report forms part of your general contingency planning, then extracts or a summary can be made freely available. You can also store the report within your crisis management system and restrict access by role or a named individual. Again, assess the risk of disclosure and any possible impact.

Conclusion

This article has focused on the need for a systematic approach to gathering information, assessing it and turning it into actionable intelligence. The techniques described, albeit briefly, are tried, tested and battle-proven across a whole range of activities from intelligence agencies to the largest corporations.

Business intelligence (BI) is intelligent business. BI drives many functions from client selection, acceptance and product development, to risk, contingency and crisis management.

This article was previously published as a blog on the website administered by One Voice.

Pilotarbeid rundt kampflyanskaffelsen

Teori ble til praksis da Forsvarsmateriell fikk på plass et COSO-basert internkontrollsystem.

> Dokumentering av et system for internkontroll i en kompleks virksomhet

Av
FRANK ALVERN
Spesialrådgiver Forsvarsdepartementet, utlånt til Forsvarsmateriell frem til april 2018

Av
DOROTHEE SAUER
Tjenesteleder for risikostyring, internkontroll og internrevisjon i BDO

Forsvarsmateriell har ansvar for anskaffelsen av kampflyene F-35. I 2017 kom Riksrevisjonen med en revisjonsberetning for 2016 som fastslo at det ikke var mulig å bekrefte anskaffelseskostnaden for kampflyene i virksomhetsregnskapet til Forsvarsmateriell. Årsaken var hovedsakelig manglende dokumentert internkontroll. Det måtte det gjøres noe med!

Innførte periodisert virksomhetsregnskap

Forsvarsmateriell (FMA)[1] ble etablert 1. januar 2016 gjennom en utskillelse fra Forsvarets logistikkorganisasjon. Fra samme dato innførte Forsvaret, og dermed også Forsvarsmateriell, periodisert virksomhetsregnskap. Konsekvensene av omleggingen av regnskapsprinsipp ble kraftig undervurdert. Da Riksrevisjonen konkluderte med at den ikke kunne uttale seg om årsregnskapene for 2016 for de to etatene, ble det iverksatt et stort arbeid. For å sikre bedre internkontroll i Forsvarsmateriell påla Forsvarsdepartementet å dokumentere etter prinsippene i COSO. COSO er et rammeverk for virksomhetsstyring som fokuserer på målrettet drift, pålitelig regnskapsrapportering og overholdelse av lover og regler, og ligger til grunn for økonomiregelverket i Staten.

Portal med beskrivelser

Sluttproduktet var et internkontrollsystem i form av en intern nettportal. I portalen dokumenteres COSOs 17 prinsipper og hvordan prinsippene er anvendt i Forsvarsmateriell. Det var 2013-versjonen av internkontrollrammeverket som ble lagt til grunn. COSO publiserte i 2015 en veileder kalt «Leveraging COSO Across the Three Lines of Defense»[2]. I dette dokumentet anbefaler COSO hvem i organisasjonen som bør ha ansvar for hvilke kontrollaktiviteter. Dette ble også vurdert, og tatt inn i portalen.

- Jeg tror ikke det er mange som har klart å kombinere teori med praksis slik vi har klart i dette prosjektet, sier Frank Alvern, som har hatt ansvaret for prosjektet i Forsvarsmateriell.

Innfallsvinkler og prinsipper

– Vi fikk anledning til å anvende velkjente rammeverk helhetlig, og hentet ut praktisk nytte fra generelle veiledere om risikostyring og internkontroll, sier Alvern.

– Internrevisorene som leser dette bør være kjent med hva COSO mener internrevisjonens oppdrag bør være, prinsipp for prinsipp, mener han.

I tillegg tipset Riksrevisjonen om at deres amerikanske kollegaer, Government Accountability Office (GAO), hadde oppdatert sin COSO-baserte internkontrollstandard med virkning fra 2016. Denne standarden, Green Book, konkretiserer forventningene til alle 17 prinsippene og utdyper hva de ser som spesielt viktig. Alvern oppfordrer de som har interesse til å laste ned dokumentet fra GAOs hjemmesider[3].

IKT-risiko og mislighetsrisiko

Det er to risikoområder COSO behandler særskilt, nemlig mislighetsrisiko og IKT-risiko. Førstnevnte ble dekket gjennom COSOs ferske veileder om Fraud Risk Management[4].

– Når det gjelder IKT-risiko valgte vi å hente støtte fra COBIT 5[5] og konkret veiledning rundt oppfølging av tjenesteutsatte leveranser. Det har sammenheng med at Forsvarsmateriells IT-systemer i stor grad forvaltes og driftes av Cyberforsvaret. For de som jobber i virksomheter med et lignende oppsett anbefales det å ta en titt på COBIT-rammeverket for ekstra støtte med tanke på IKT i prinsipp nr 11.

Stor implementeringsjobb

Det nye internkontrollsystemet i FMA dokumenterer hvordan alle COSO prinsippene er utkvittert. Videre dokumenteres hvem i organisasjonen som eier og hvem som bidrar til ønsket risikonivå inn mot COSOs målkategorier; drift, rapportering og etterlevelse. Når dokumentasjonen var på plass begynte arbeidet med å teste både kunnskapen om og etterlevelse av prinsippene. Det var en stor implementeringsjobb som ble gjort før lanseringen 1. oktober 2017.

Viktig med informasjon og opplæring

Informasjon og opplæring er en kritisk suksessfaktor i endringsprosesser, også når

[1] *www.forsvarsmateriell.com*
[2] *https://www.coso.org/Documents/COSO-2015-3LOD.pdf*
[3] *https://www.gao.gov/assets/670/665712.pdf*
[4] *https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf*
[5] *www.isaca.org/cobit*
[6] *https://kahoot.com/*

det gjelder internkontroll. Det ble derfor tidlig bestemt at det ville være nødvendig å prioritere kommunikasjon av internkontrollsystemet til ledere generelt, og til de som arbeider med virksomhetsstyring spesielt. Det ble blant annet gjort gjennom en serie med halv-dags workshops.

Spillbasert læringsplattform

For å gjøre COSO, risikostyring og internkontroll mer spennende og engasjerende ble den spillbaserte læringsplattformen Kahoot![6] valgt som verktøy.

– Engasjement fra deltagerne er en forutsetning for å lykkes med formidling av tørre temaer som internkontroll. Jeg hadde tidligere i flere forskjellige sammenhenger oppnådd veldig god læring og engasjement blant deltagerne med Kahoot! som pedagogisk verktøy, sier Dorothee Sauer i BDO, som var rådgiver og sparringpartner i prosjektet. Hennes erfaring er at man må legge ned arbeid i å lage gode spørsmål og svaralternativer, men at effekten da vil være høy.

– Vi pirret konkurranseinstinktet til deltagerne og oversteg forventningene. Dermed fungerte en workshop i internkontroll hos FMA, selv på en fredagsettermiddag, bekrefter Frank.

Workshop i COSO

Workshopen ble gjennomført med en tradisjonell innledning for å etablere et felles startpunkt, felles mål og en felles forståelse av utfordringen. Resten av workshopen var det frem med mobiltelefonene. Prinsipp for prinsipp ble COSO gjennomgått med spørsmål og svar på skjermen.

–Vi valgte å holde en og samme workshop for alle, fordi COSO-rammeverket for internkontroll henger sammen i en helhet, forteller Alvern. Nærmere 100 personer var totalt sett gjennom denne halve opplæringsdagen, og det inkluderte toppledergruppen hvor flere fikk sitt første møte med Kahoot! som verktøy.

Læringspunkter

Portalen for internkontrollsystemet fikk navnet FMA IK FELLES, og trådte formelt i kraft 1. oktober 2017.

– Resultatet bekrefter at COSO er et godt verktøy for å implementere tilfredsstillende internkontroll på en systematisk måte, også på komplekse områder eller virksomheter, sier Dorothee Sauer. Hun mener at den interaktive opplæringen var en sentral suksessfaktor.

– Vi oppnådde kunnskapsøkning om internkontroll på alle nivåer i FMA. Med fullt fokus, riktig prioritering og engasjerte medarbeidere oppnår man mye i løpet av bare ett år, sier hun.

– Internkontroll er en prosess og ikke et engangsarbeid. Etableringen av FMA IK FELLES var nødvendig for å ramme inn og koble sammen risikostyring og internkontroll på tvers av virksomheten, forteller Alvern. Workshopene gjorde at vi kom godt i gang – og nå må dette repeteres og holdes ved like, sier han.

Forfatternes kontaktinformasjon:
frank.alvern@fd.dep.no og
dorothee.sauer@bdo.no

FAKTA OM KAMPFLYANSKAFFELSEN

(MER INFORMASJON FINNER DU PÅ WWW.KAMPFLY.NO)

Kampflyet F-35 er det største anskaffelsesprosjektet som noensinne har vært gjennomført i Norge. Norge skal kjøpe inntil 52 fly av typen F-35A som produseres i Texas og leveres i perioden 2015-2024. Hovedbasen for de nye flyene blir på Ørland, med en fremskutt base på Evenes. Joint Strike Fighter-partnerskapet som Norge deltar i består av ni forskjellige land. Partnerlandene bidrar med midler til utviklingen av F-35, og deltar i beslutningene rundt utviklingen og produksjonen av flyet.

Hele anskaffelsen er beregnet til 71,5 mrd reelle kr i 2017-verdi. Dette skal ikke bare betale for flyene, men skal også dekke alle kostnader direkte relatert til å stille en ny kampflykapasitet ferdig og klar til overtakelse for Luftforsvaret når anskaffelsesperioden er over. Da må man også anskaffe våpnene og alt utstyret og de første reservedelene som skal brukes for å vedlikeholde flyene. Vi skal også betale for integrasjonen av de riktige våpnene til flyet og anskaffe et helt nytt simulatoranlegg for å sikre at vi kan trene og operere med flyene mest mulig effektivt. Dette gjør at selve flyene faktisk er bare litt over halvparten av den totale anskaffelseskostnaden.

For å legge forholdene til rette for at Riksrevisjonen skal få gjort sitt viktige arbeid har det vært nødvendig å «ramme inn» og dokumentere systemet som skal sikre forsvarlig forvaltning av midlene tildelt til Forsvarsmateriell for kampflyanskaffelsen både i virksomhetsregnskapet og i kontantregnskapet. Dette systemet bygger på og kompletterer FMA IK FELLES, og består av tre hoveddeler; 1) Virksomhetsbeskrivelse og organisering, 2) Regnskapsmessig behandling og 3) Tillegg vedrørende internkontroll. Først med dette på plass var det mulig for vår eksterne revisor å gjennomføre en målrettet revisjon av denne komplekse anskaffelsen. Med fasit i hånd etter 2017-revisjonen kan vi slå fast at det lykkes vi veldig godt med! Forsvarsmateriell har derfor besluttet å dokumentere internkontrollen for de store prosjektene på tilsvarende måte fremover.

F-35A flyr over Rondane. Foto: Morten Hanche / Forsvaret

Corporate Governance «Theatre» and the possibility of a continuing Assurance gap

By
JAMES C PATERSON
Director Risk & Assurance Insights Ltd. former Head of Internal Audit, author of "Lean Auditing" (J Wiley & Son), speaker at courses for many IIA Institutes including a number of times here in Norway.

Crises in the past, crises today

I've been working in the field of corporate governance, auditing and assurance for the past 15 years; 7 years as a Chief Audit Executive (CAE) and 8 years as a consultant. Through that time, we have seen many corporate governance and assurance crises. Specifically:

- In 2001/2002; Enron/WorldCom (concerning Financial Accounting standards and external audit quality).
- In 2007/2008; the financial crisis (concerning, inter alia, issues with understanding the risk of certain financial instruments and inadequate liquidity / capital reserves in financial services).

Since then we have other corporate governance crises including:

- BP (Deepwater Horizon, in 2010), Volkswagen (with the diesel emissions scandal, in 2015)
- And in 2018 we have seen the collapse of Carillion in the UK (a going concern failure) as well as numerous scandals in the charity sector.

Of course, the full list of disappointments, crises and collapses over time is very substantial.

Responses to these, some more substantial than others

Each of these governance and assurance failures was met with some sort of enquiry followed by recommendations for change. In the case of Enron and Worldcom, the USA enacted the Sarbanes Oxley legislation. It sought to address, amongst other things, concerns about the rigour of financial reporting and the independence of external auditors. Similar legislation has been enacted in some countries (notably Canada, Japan and France), but it is worth noting that the rigour of these accounting/auditing standards has not been adopted across all countries.

In relation to the Financial crisis, the root causes were attributed to factors such as «greedy bankers» influenced by a «bonus culture», «weak board oversight» as well as short-comings in regulations and regulatory supervision and - again - a range improvements were proposed and many of these were implemented in relation to the banking and insurance sector. Again, it is worth noting that implementing lessons learned from the financial crisis was mostly confined to the financial services sector, and not used to significantly strengthen the corporate governance of other industry sectors.

In the case of «one off» corporate governance and audit scandals since then (e.g. BP, Volkswagen, Carillion etc.), enquiries are carried out, reports are written and specific actions are recommended and implemented, often by the companies concerned (if they are still in existence), or, sometimes by regulators and other oversight bodies.

Are we making progress? And how might we make more?

From one perspective, you can look at where we are now, with more rules and regulations and «lessons learned» reports and argue that things have improved and we won't have these same problems again. From another point of view you could argue whilst some lessons are being learned, overall we don't seem to be able to head off major, even catastrophic, corporate governance and assurance issues,

despite rafts of regulation, governance bodies (e.g. boards and risk committees), pages and pages of internal policies and procedures and many inspection and audit bodies (e.g. internal auditors, external auditors and regulatory bodies).

One analysis of these failures in corporate governance and assurance is to argue that individual boards, and/or executives, and/or auditors have failed; but this risks scapegoating those specific individuals or groups. Another perspective is to blame the whole set up - e.g. collapses or short-comings in commercial enterprises are used to argue that the whole capitalist system does not work; or disappointments in the way public services operate are used to attack the whole notion of public services. In each case, prior beliefs, political leanings and other motivations (such as commercial interests) may colour our ability to look dispassionately at the patterns of problems in both private and public sectors and seek a deeper understanding in relation to their root causes; specifically, why major failures continue to occur despite often substantial governance, risk and compliance (GRC) processes as well as a range of assurance activities.

The problem of governance (GRC) theatre and a continuing assurance gap

Bruce Schneier, a security expert and author of «Beyond Fear» reflected on the 9/11 (twin towers) tragedy of 2001 and the additional security measures were put in place at airports etc. and suggested that much of what has been done is «Security theatre» - measures are put in place that reassure the public, and make a good TV or radio «sound bite», but do not necessarily address serious, determined threats.

I am increasingly worrying that despite our efforts to date, there is a real risk that some, or even a lot, of the GRC activities that go on is just «theatre»; policies and processes are well-intentioned, and can catch some, even many, issues - but when it comes to the crunch - some of the most sinister and catastrophic risks and issues that are lurking, or may emerge, can be missed.

To guard against this, many will think that external audits, internal audits and regulatory inspections should act as an additional line of defence, to provide assurance that things are working, but - as we have seen up to now - there is often a gap between the assurances we think we are getting and the assurances that are actually being provided.

> There is often a gap between the assurances we think we are getting and the assurances that are actually being provided

Potential root causes and the consequences of not addressing them

Why are these issues continuing to recur? As I see it, the root causes of the problems we are seeing are multi-dimensional and often systemic. They lie beyond scapegoating individuals and the private vs. public debate. The specifics root causes of catastrophic problems occurring vary from case to case, but as I see it, a number of recurring themes can be seen:

- A blindness to identifying some risks («failure of imagination») and/or a reluctance to collect information and data that might challenge the status quo (i.e. «inconvenient truths»); and/or
- Challenges to pin down accountabilities within, and between, increasingly complex organisations (with limited understanding of, and use of, accountability mapping techniques); and/or
- Gaps between the ambition levels and appetite for change from leaders (who want to be seen to be doing something) and what is possible, (with weak feedback processes to "pierce the bubble" of their thinking); and/or
- Difficulties in talking openly and honestly about organisational dilemmas, resource and other practical constraints; and/or
- An underestimate of the human and psychological factors that are often in play, including allegiances between senior managers and board members, group dynamics (e.g. «group think», «dependency» and «fight/flight»), which can be further compounded by the ways that self-serving («foxy») managers «play the game» and/or
- Perverse incentives (e.g. banker's bonuses).

I wonder whether we are making enough effort to recognise and name these complexities and darker sides of human nature (beyond scapegoating individuals) in the way we look at what has happened. If my fears are justified, then I can quite easily imagine another long list of corporate disappointments and disasters in the next 5, 10 or even 50 years.

What would need to happen to turn the tide?

The encouraging news is that as governance and assurance failures continue with depressing regularity (e.g. safeguarding issues at charities, and the UK Carillion collapse) members of the public, stakeholders and politicians are starting to express increasing dissatisfaction about how organisations are being governed and the quality of the assurances being obtained. I believe these common-sense challenges in relation to the current levels of governance and assurance in place are justified. Bluntly put: there are still too many instances where senior managers and board members operate on a «no bad news is good news» basis; and the public, and other stakeholders, are entitled to argue that surely there must be a lot of

> There are still too many instances where senior managers and board members operate on a «no bad news is good news» basis.

«smoke and mirrors» going on for externally published governance and assurance statements to appear to be so good on the surface, while catastrophes are lurking around the corner.

As I see it real progress will require us to focus on, and more determinedly look at the subtle and various «hairline cracks» that still exist in the GRC and assurance

activities of organisations, even those regarded as leading; and to more diligently call these out and act on them on a timely basis.

Note that the implementation of a GRC system does not eliminate the possibility of GRC theatre! Such systems may have a role, but I have heard on numerous occasions risk and compliance experts and managers talking about the time and effort of «feeding the machine», with an uneasy sense they should be working on the management of real risks, rather than spending time setting up and operating the GRC system. And even when GRC systems are implemented, let's not forget the «garbage in / garbage out» challenge!

This requires us to be braver in calling out the GRC theatre that is - to this day - all around us and to probe more diligently the assurances we are given by auditors and regulators, who - at the moment - use terms such as «reasonable assurance» as a convenient «get out» clause for any short-comings in what they have missed.

A fool's errand?

Some readers of this article may worry that asking for a step-change improvement in the way we understand and learn from organisational failures is a fool's errand. You can argue that human history is littered with bubbles and bursts, of rises and falls, and it's a simply reflection of living in an imperfect world, and due to human nature, that problems occur.

My response to this is to agree that problems and disappointments will follow mankind through history; but my question, at this point in time, is: are we really learning everything that is to be learned, quickly enough, about shortcomings in governance and assurance? Are we getting to the real root causes? All too often I fear that enquiries into, and debates about, crises are tainted by the desire to scapegoat others and to grab headlines, which fills me with a sense of déjà vu when reading lessons learned reports (note that the Grenfell Tower tragedy was proceeded by the Lakanal fire, and enquiry, and numerous recommendations, not yet implemented, several years before). Often I feel we are going around in circles and I suspect this is one of the reasons that a degree of resignation, or even cynicism, can creep into discussions about crises, corporate governance and lessons to be learned.

Reasons for hope - but not optimism

But let's look at this another way: If every organisation that failed was an airplane that had crashed would we feel the same? In the past, air crashes were more frequent, but over the past decades we have - by and large - made real progress, to the point that, nowadays, we expect engineers to design quality into airplanes and to have high standards in constructing, operating and monitoring these. And to the credit of many, we have reached a state where the safety of airplanes is clearly objectively better than it has ever been.

My hope is that we can take some comfort from what has been achieved in «high precision» and «high safety» fields (such as the airline industry), and use this to work more diligently in relation to our current governance and assurance efforts, to try to reduce the frequency of catastrophic failures. I'm not especially optimistic that we will eliminate organisational failures, but I reject a pessimistic view that nothing more can be done. And when you think about the many small traders, and their families, whose lives have been destroyed by the Carillion collapse, and others who have been let down by pension fund and other collapses, it has got to be appropriate that we «try harder.»

This article was first published on LinkedIn and is reproduced by kind permission of the author.

jcp@RiskAI.co.uk

Etikk på dagsordenen!

'Hvem kjenner til de etiske retningslinjene?' var tema i en artikkel i forrige utgave av SIRK. Vi fikk entusiastisk og positiv respons fra Bærum kommune. De har satt i gang en rekke tiltak for at ansatte skal kjenne kommunens etiske standard og forteller gjerne hvordan de har jobbet med å forankre dem på tvers av kommunen.

Av
SIRI OPHEIM
Controller, Rådmannens stab, Bærum kommune

Bærum kommune er landets femte største kommune med ca. 125.000 innbyggere fordelt på 152 nasjonaliteter. Kommunen har ca. 12.000 medarbeidere (ca. 7.000 årsverk). Tjenestespekteret er stort, fra skole, barnehage og helse og omsorgstjenester, til tekniske tjenester og kultur. Vi har om lag 250 tjenestesteder.

Kommunens etiske retningslinjer ble revidert høsten 2014. Arbeidsgruppen tok utgangspunkt i de gjeldende etiske retningslinjene fra 2007. Vi kontaktet også andre kommuner og virksomheter og brukte deres etiske retningslinjer som grunnlag for vårt arbeid. Vi ble raskt enige om noen viktige prinsipper: Korte og presise formuleringer, enkelt språk – alle ansatte skal kunne forstå innholdet.

Mange var involvert i arbeidet, og utkast til nye retningslinjer var på høring både hos ledere i virksomheten, tillitsvalgte og vernetjenesten. Ny Etisk standard ble vedtatt i ledelsen i desember 2014 og lansert på rådmannens ledersamling med alle tjenestelederne 14. januar 2015.

Bildetekst

Bildetekst

For å nå ut til alle medarbeiderne har vi deretter gjort følgende:

- Opprettet «Etikk i Bærum» på kommunens intranett (ansattportal) hvor all informasjon om etikkarbeidet ble samlet.
- Samarbeid med kommunikasjonsenheten for å kommunisere etikk i internavisen Bære:Bærum. (Digital- og papirversjon som sendes til alle tjenestesteder).
- Plakat ble sendt til hvert tjenestested.
- Brosjyre/flyer ble delt ut til alle medarbeiderne.
- Alle medarbeidere må undertegne på Etisk standard. Dette er leders ansvar.

- Nyansatte signerer på Etisk standard sammen med arbeidsavtalen.
- Etisk standard, kommunens verdier og visjon er fast tema for opplæring av nye ledere, samt i opplæringen av nye verneombud.
- Utviklet e-læringsprogram om alle temaene i Etisk standard. Før utsendelse av nye leksjoner har lederne blitt informert via ansattportalen og oppfordret til å gjennomgå leksjonene med sine medarbeidere.
- Alle leksjonene er tilgjengelig på ansattportalen og er del av det nye e-læringsprogrammet for nyansatte medarbeidere.
- Obligatorisk e-læring for nyansatte ledere er tilgjengelig i Lederskolen.
- Lederavtalen, med tilhørende sjekkliste, inneholder leders ansvar for å følge opp implementeringen av Etisk standard, herunder at alle har signert.

E-læring i etikk

Det er laget 14 korte leksjoner som i løpet 2016 og 2017 er sendt til alle medarbeidere med kommunal e-postadresse. Rådmannen fronter kommunens etikkarbeid.

Målet med leksjonene har vært å gjennomgå alle temaene i Etisk standard og stimulere til refleksjon og samtale om hvert emne. Leksjonene er laget for å kunne være et redskap for lederne i arbeidet med å implementere kommunens etiske standard på eget tjenestested.

Fagpersoner fra ulike enheter bidro i utformingen av etikkleksjonene og disse ble oversendt kommunens overordnede verdigruppe på høring og kommunaldirektør for OU for å forankres med tillitsvalgte og vernetjenesten.

Etikkleksjonene (laget i Junglemap) har vært sendt ut i 2016 og 2017. Det har vært et bevisst valg for å sette etikk på dagsorden over en lengre periode.

Når en ny leksjon har blitt sendt ut, så har antall fullførte leksjoner på de forutgående leksjonene økt. De som ikke åpnet leksjonene fikk en gang i halvåret en purring/påminnelse og det har også ført til at det samlede antall fullførte leksjoner stadig har økt. I gjennomsnitt har vi nådd 3690 personer med leksjonene.

Vi har ingen oversikt over hvor mange som har brukt etikkleksjonene som grunnlag for samtale på eget tjenestested, men vet at noen tjenester har brukt dette systematisk.

Nr.	Tema	Fullført
1	Etikk i Bærum - introduksjon	4922
2	Arbeidsmiljø	4511
3	Profesjonalitet	4317
4	Åpenhet, dialog og brukermedvirkning	3847
5	Mobbing, trakassering og diskriminering	3641
6	Interessekonflikter	3620
7	Gaver og representasjon	3476
8	Innkjøp	3170
9	Miljø og klimautslipp	3268
10	Kritikkverdige forhold	3496
11	Profesjonalitet	3539
12	Penger og eiendeler	3623
13	Profesjonalitet	3399
14	Etikk i Bærum - siste leksjon	2832

Oversikt over fullførte leksjoner per 25.01.2018

Informasjon til lederne

Tjenestelederne har før utsendelse av hver leksjon blitt oppfordret via Lederinfo (intranett) til å gå igjennom leksjonene og bruke dem som grunnlag for samtaler/diskusjoner på eget tjenestested. Der medarbeidere selv ikke har tilgang til leksjonene (de som ikke bruker sin kommunale e-post adresse) er ledere spesielt oppfordret til å gjennomgå leksjonene på avdelingsmøter eller andre egnede fora. I rådmannens årsbrev til virksomheten for 2015 var implementering av Etisk standard et viktig budskap.

Opplæring av ressurspersoner

Kommunen har gjennom flere år gitt opplæring til ressurspersoner, kalt etikkveiledere. Målet med opplæringen er å gi disse veilederne begreper og metoder slik at de selv kan dra i gang etisk refleksjon og dilemmatrening på egen arbeidsplass. Deltagerne er i all hovedsak fra helsesektoren, likevel er kurset åpent for alle ledere og ansatte. Kurset er praktisk rettet og vektlegger øving på refleksjon over konkrete dilemmaer fra deltagernes egen hverdag. De siste fire årene er det gitt opplæring til omlag 180 etikkveiledere fra i alt 85 ulike avdelinger/tjenestesteder. I tillegg arrangeres introduksjonskurs i etisk refleksjon for personalgrupper, opplæring i helse-juss, nettverkssamlinger for etikkveiledere, veiledning og workshops. Kartlegging tyder på at om lag 40 avdelinger/tjenestesteder bruker systematisk etikkrefleksjon.

Årlig risikovurdering

Alle ledere og politikere oppfordres til å registrere sine verv i Styrevervregisteret, og å ha fokus på habilitet og arbeidsdeling i saksbehandlingen. Alle tjenesteområder har gjennomført risikovurdering i forhold til korrupsjon og misligheter. Denne skal årlig oppdateres. Som oppfølging av risikovurdering er det gjennomført interne revisjoner på området anskaffelser og delegasjon av myndighet og fullmakter i kommunens systemer.

Etikk på dagsorden i folkevalgte organer

Rådmannen sender årlig en politisk orienteringssak om arbeidet med etikk, antikorrupsjon og internkontroll. Kommunestyret hadde i august 2017 etikkseminar og dilemmatrening basert på Transparency International Norge sin Antikorrupsjon Dilemmasamling. I det påfølgende kommunestyremøtet, hvor rådmannens orienteringssak om arbeid med etikk, antikorrupsjon og internkontroll ble behandlet, fikk både rådmannens arbeid og seminaret mye fokus og god omtale. «Etiske normer for Bærum kommunes folkevalgte» inngår i de regler som gjelder for folkevalgte organer.

Veien videre

Som oversikten over fullførte leksjoner tydelig viser når vi ikke ut til alle med e-læringer.

Skal vi nå alle medarbeidere er det viktig at ledere på alle nivåer også fremover bruker e-læringene som verktøy og grunnlag for samtale.

Hvordan kan ledelsen i Bærum kommune fremover sikre at etikkarbeidet videreføres?

- Ledelsen fortsetter å ha etikk på dagsorden i hele organisasjonen. Samarbeide på tvers av faggrupper for å sikre at etisk refleksjon knyttes til arbeidsoppgavene og ikke gjøres til noe eget.
- Ansvaret for oppfølging og utvikling av etikkarbeidet er tydelig plassert i organisasjonen. (HR-direktør og koordinator for etikkarbeidet, overordnet verdigruppe).
- Lederavtalen og sjekkliste inneholder leders ansvar for å følge opp etikkarbeidet. Lederne har ansvar for sikre at alle medarbeidere kjenner Etisk standard i tillegg til at alle nyansatte og innleide skal undertegne Etisk standard.
- Fremheve gode eksempler fra virksomheten kan motivere andre ledere til dialog og samtale om etikk i det daglige.
- Etisk standard med tilhørende leksjoner legges i kommunens nye kompetanseportal i 2018 (Dossier) og blir obligatorisk opplæring for alle ansatte. Det utarbeides nå «kontrollspørsmål» til alle leksjonene.
- Etikk leksjonene som er laget hentes frem igjen og sendes på e-post til alle medarbeidere når det oppstår situasjoner eller saker i media som gjør at tema kommer på dagsorden
- Skape møtepunkter for personalet til å reflektere over vanskelige dilemmaer som oppstår i hverdagen for å finne måter å håndtere situasjonene på.
- Oppfordre til at flere tjenestesteder utdanner etikkveiledere og benytter etisk dilemmatrening etter SME metoden (Senter for medisinsk etikk) som verktøy i det daglige arbeidet.

Refleksjoner rundt etiske dilemmaer bidrar til at ansatte i fellesskap kan finne løsninger på vanskelige situasjoner og få en felles forståelse for hvordan praksis bør være. Bedre samarbeid og mer konstruktiv kommunikasjon, bidrar til tryggere ansatte og har trolig positiv effekt både på sykefraværet og kvalitet i tjenesten.

Arbeid med implementering av Etisk standard og utvikling av etikkleksjonene har vært utfordrende. Mange har vært involvert, og prosessen har vært tidkrevende. Den største utfordringen har vært å skrive kort, konsist og i et språk som er forståelig for alle medarbeiderne. Nå er det viktig at ledere på alle nivåer i organisasjonen fortsatt setter etikk på dagsordenen.

HEDERLIG OMTALE

Ved utdeling av Etikkprisen for 2015 fikk Bærum kommune hederlig omtale for vårt arbeid. Etikkprisen deles ut av prosjektet «Samarbeid om Etisk kompetanseutvikling» som er et samarbeid mellom Helse- og omsorgsdepartementet, Yrkesorganisasjonene innen helse, Helsedirektoratet, Senter for medisinsk etikk v/Uio og KS.

Fra juryens begrunnelser:

«Bærum kommune har etablert et systematisk og langsiktig etikkarbeid for ansatte og ser etikk i sammenheng med annet arbeid. Juryen berømmer kommunen for bred forankring politisk og administrativt, på alle nivåer. Kommunen legger stor vekt på brukermedvirkning i utviklingen av Etisk standard, og dette er implementert i handlingsprogrammet for 2016-2019. Det er definert klare og konkrete mål for etikkarbeidet, noe som gir et tydelig styringssignal ut til tjenestene. Kommunens etikkprogram er under stadig utvidelse. Ambisjonen er at alle tjenestesteder og sektorer skal omfattes. Alle medarbeidere ansvarliggjøres blant annet ved å undertegne Etisk standard.»

Foto: Terje Lien (KS)
Fra venstre: områdedirektør KS Helge Eide, Helse- og omsorgsminister Bent Høie, Bærum kommune: Gunvor Erdal, Siri Opheim og Siri Swierstra Bie.

Det var en gang

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

FOR 40 ÅR SIDEN – DEN INTERNE KONTROLL

Det er kanskje lett å glemme at internkontroll var et tema lenge før COSO så dagens lys. Statsautorisert revisor Kaare Eimhjellen innledet årskonferansen til Norsk Bankrevisorforening i Tromsø i 1978 med et foredrag om dette temaet. Artikkelen ble senere trykt i Bankrevisoren.

Han innleder med en statusoppsummering at bankrevisjon i stor utstrekning var basert på relativt omfattende bilagskontroll og avstemmings- og beholdningskontroller. Han ser at det etter hvert er blitt klart at stadig flere revisorer nedlegger betydelig arbeid ved gjennomgåelse av forretningsgangen og vurdering av den interne kontroll, primært for å foreta en hensiktsmessig revisjonsinnsats innen de forskjellige kontrollområder, men også for å gjøre ledelsen oppmerksom på svakheter i kontrollsystemene med det siktepunkt at disse blir forbedret.

Selv om man skulle tro at dette var nytt «stoff» for mange av tilhørerne så påpeker han at Thorleif Andenæs så tidlig som i 1946 utga boken «Revisjon og Indre kontroll». Denne ble etterfulgt i 1953 av Thomas Kjeldsbergs første bok om «Intern kontroll».

Han påpeker at etter hvert er det blitt en av revisjonens hovedoppgaver å overvåke at de kontrolltiltak som er etablert, fungerer som forutsatt. Han foreslår at svakheten oppdaget ved gjennomgangen av forretningsgangen bør listes opp på spesiell blankett, blant annet for å få ensartet registrering og for at skjemaet danner et oppfølgingsregister.

Han anbefaler at revisor skal gjøre det til ufravikelig regel å føre opp følgende svakheter der hvor det er aktuelt:

1. Det foreligger ikke beskrivelse av ansvars- og arbeidsområde for avdelingen.
2. Det foreligger ikke skriftlig instruks for avdelingsleder, eventuelt at den ikke er fullstendig eller ikke ajour.
3. Det er ikke utarbeidet skriftlig rutinebeskrivelse, eventuelt at beskrivelsen ikke er fullstendig eller ikke ajour.
4. Svakheter ved blanketter som benyttes, f.eks bruk av ikke autoriserte blanketter, ikke ajourførte blanketter ved endring av rutinen.

Etter nettopp å ha avsluttet en operasjonell revisjon i et vesentlig forretningsområde kan jeg nikke gjenkjennende. Mye stemmer den dag i dag med den forskjell at vi ikke benytter blanketter lenger men maler! Plus ça change, plus c'est la même chose!

FOR 20 ÅR SIDEN – INTERNREVISJON I FREMTIDENS POST-MODERNE VIRKSOMHET – EN UMULIGHET ELLER VIKTIGERE ENN NOEN GANG

Ikke desto mindre har arbeidslivet forandret seg de 20 årene fra 1978 til 1998 i takt med at mennesker gjennom automatisering av prosesser er blitt frigjort fra gjentagende og ikke mentalt krevende arbeid. I 1998 ble det utgitt en artikkel av Bente R. Løwendahl, Hun var den gang førsteamuensis i Strategi Handelshøyskolen ved BI og hun utfordrer internrevisjon til å tenke nytt om internkontroll.

Bente ser at en av de kanskje viktigste utfordringene for svært mange av fremtidens bedrifter ikke er kun å styre bruken av ressursene i riktig retning og kontrollere at alle gjør det de skal, men også å trekke til seg og motivere kreative og høyt kompetente mennesker til å bruke sin tid og energi til beste for akkurat vår virksomhet. Hun påpeker videre at «dessverre er det ikke alltid slik at de tiltak som bidrar til økt styring og kontroll samtidig bidrar til økt motivasjon og kreativitet.»

Hun gir et bilde av den nyere tidens endringer i strategifaget der konseptet «value creation» har erstattet «value appropriation». Begrepet «intellektuell kapital» legger vekt på usynlige ressurser som utgjør både «input» og «output» i produksjonsprosessen og er i svært stor grad eiet av andre enn bedriftens eiere. Særtrekk for usynlige ressurser er altså at de utvikles mens de brukes og at de eies ofte ikke av bedriften. Hun setter fingeren på følgende fire punkter som hun mener er utfordringer for intern revisjon:

1. Måleproblemer knyttet til usynlige ressurser som kompetanse og renommé
2. Støttefunksjonenes utfordrende rolle i de etter hvert svært flate, fragmenterte og «løst koblete» organisasjonsformer, der støttefunksjoner samtidig bygges ned.
3. Konflikten mellom kontroll og motivasjon og hvordan man kan best mulig støtte opp under kreativ verdiskapning til kundens beste, uten at man mister kontrollen og styringen.
4. Kontroll av eksterne ressurser der store deler av verdiskapningen baserer seg på ressurser som ikke eies av bedriften, med nye utfordringer når det gjelder å trekke til seg, å motivere og å holde på relasjonene.

Denne artikkelen virker forutseende i forhold til den utviklingen vi står midt oppe i i dag med en ubønnhørlig utvikling i digitalisering. Mitt håp er at internrevisoren forstår viktigheten av internt miljø og bedriftskultur både når det gjelder virksomhetens internkontroll og dens fremtid.

Martin Stevens

Finansiell klimarisiko

Klimarisiko går fra å være et langsiktig miljøproblem til en mer nærliggende finansiell utfordring. Finanssektoren ber om økt rapportering og selskaper bør derfor begynne å vurdere sin finansielle klimarisiko.

ANETTE RØNNOV
Director, KPMG Sustainability Services

JØRGEN WESTRUM THORSEN
Manager, KPMG Sustainability Services

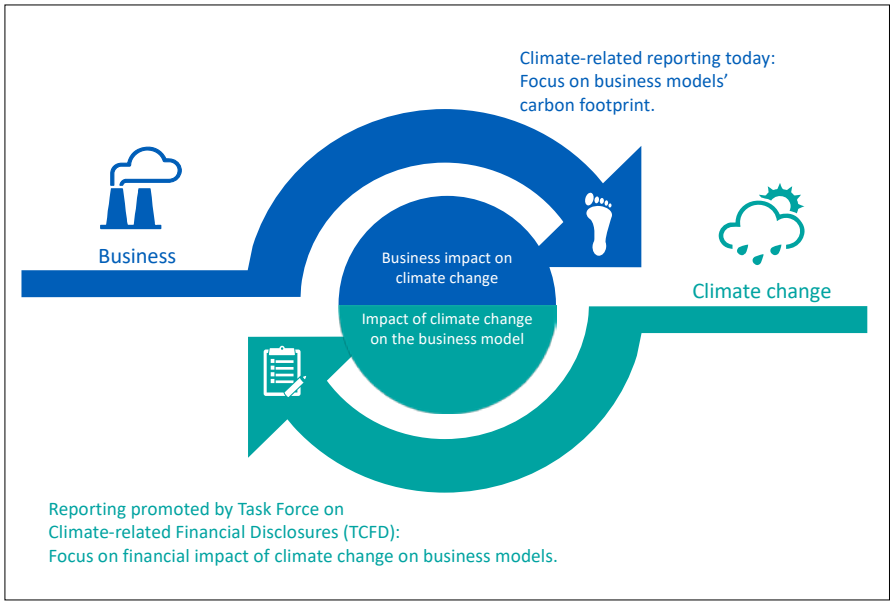
Parisavtalen i 2015 bekreftet viktigheten av å redusere klimagassutslippene slik at den globale oppvarmingen holdes godt under to grader sammenlignet med førindustriell tid. Vi ser allerede at konsekvensene av klimaendringene øker, og i World Economic Forums globale risikorapport for 2018 dominerer klimarelaterte risikoer. Klimaendringene har også finansielle konsekvenser ikke bare på selskapsnivå og kan ifølge Mark Carney, sentralbanksjefen i Storbritannia, faktisk true stabiliteten i finanssystemet!

For selskaper innebærer dette at mens fokus tidligere var på hvordan selskaper påvirker miljøet gjennom sin virksomhet, er fokus i økende grad på hvordan endringer i klima kan få finansielle følger for selskapenes forretningsmodell:

For å vurdere de finansielle følgene av klimarisikoer, er det nyttig å se på de følgende tre typer av risikoer:

1. **Overgangsrisiko** som knyttes til utviklingen av policy og teknologi. Hvis vi tar utgangspunkt i at myndighetene vil innfri Paris-avtalen, kan vi forvente oss et nytt nivå på klimareguleringer som gjør det dyrere å slippe ut klimagasser og forhåpentligvis enklere og billigere å utarbeide klimavennlige løsninger og produkter. Samtidig vil utvikling av ny teknologi redusere verdien av mange investeringer og forbrukere stiller høyere krav til klimavennlige produkter og produksjon og endrer dermed etterspørselen etter produkter og tjenester. Denne utviklingen sees allerede tydelig i markedet bensin og dieselbiler versus elbiler.
2. **Fysisk risiko** knyttes til potensiell fysisk skade, slik som oversvømmelse, tørke, varmestress og stigende havnivå. Denne risikoen kan skape produksjons- og operasjonsforstyrrelser for eksempel via kraftforsyning og trans-

Kilde: KPMG



port, forstyrrelser i leverandørkjeden, fysisk skade på eiendeler og stigende priser på råvarer og forsikringspremier. Det kraftige regnværet i området til Hydros raffineri i Brasil er et aktuelt eksempel.

3. **Ansvarsrisiko:** «Forurenseren betaler» er et prinsipp som har vært på plass lenge og blir forsterket ved at selskaper og deres ledelse i større grad blir stilt til ansvar når det gjelder klima. For eksempel uttalte myndighetene i Australia nylig at retten nå vil se på mange klimarisikoer som forutsigbare og at sjefer kan bli stilt ansvarlige for å svikte sin aktsomhetsplikt i fremtiden. Allerede er Exxon under etterforskning av New Yorks Attorney General for om selskapet har løyet til investorer og offentligheten om klimatrusselen, mens flere byer i California saksøker oljeselskaper for å kompensere byen for følgene av klimaendringer. Hva utfallet av disse sakene blir er ennå uklart, men en økning i klimarettsaker kan ventes.

KPMG utfører hvert annet år en undersøkelse av rapporteringen på bærekraft blant de 100 største selskapene i en rekke land og verdens 250 største selskaper. I forbindelse med vår analyse i 2017 av , fant KPMG det betimelig å spesifikt se på hvorvidt selskaper har begynt å rapportere på finansiell klimarisiko. Resultatet viste at de færreste anerkjente denne risikoen i sine årsrapporter; i underkant av halvparten av de største globale selskapene og færre enn 30% av de 100 største selskapene i 49 land gjorde det. Av de selskapene som anerkjente finansiell klimarisikoer ga flere en overordnet beskrivelse av risikoen, men veldig få kvantifiserte den potensielle finansielle effekten eller beskrev scenarioanalyser. Det internasjonale resultatet gjenspeiles i Norge; 72% av de største norske selskapene anerkjente ikke finansiell klimarisiko i sin årsrapport og av de som anerkjente klimarisiko, var det kun 2% som rapporterte den potensielle risikoen i finansielle termer.

Kostnadene forbundet med disse risikoene kan bli store og det er behov for at finanssektoren tar høyde for de finansielle følgene av klimarisikoene i sine vurderinger og beslutninger. The Financial Stability Board (FSB), på vegne av finansministerne og sentralbanksjefene i G20 landene etablerte derfor en arbeidsgruppe for å analysere hvilken informasjon finansaktører trenger fra selskapene for å vurdere finansiell klimarisiko i sine beslutninger. Arbeidsgruppens anbefalinger ble fremlagt sommeren 2017 og innebærer følgende anbefalinger for selskapers rapportering:

Det norske Finansdepartementet sammen med Klima- og miljødepartementet fulgte opp og etablerte et norsk utvalg som skal evaluere klimarelaterte risikofaktorer og deres betydning for norsk økonomi og finansiell stabilitet. Utvalget ledes av siviløkonom Martin Skancke, og skal levere sin innstilling innen 14. desember 2018.

Forventinger til selskaper om å ta inn over seg finansiell klimarisiko og rapportere på disse vil derfor øke fremover. Når det er sagt, er dette et nytt område og mange selskaper er usikre på hvordan de skal gå frem. Vår anbefaling er å komme i gang med å stille følgende spørsmål:

Governance:
- Er selskapet klar for å ta tak i klimarisikoene og anbefalingene til rapportering?
- Hvem i selskapet er ansvarlig for å identifisere, vurdere, styre, måle og rapportere på klimarelaterte tema?
- Er det god kommunikasjon på tvers av funksjonene så som finans, risikostyring, strategi, juridisk og bærekraftsavdelingene?

Strategi:
- Har selskapet vurdert hvilke følger klima kan strategisk?
- Hvilken del av strategien er mest sårbar?

Risikostyring:
- Inkluderer risikostyringen klima?
- Hvordan vurderer selskapet potensielle finansielle følger av klimarisiko?

Arbeidsgivers ansvar ved varsling fra arbeidstakere

Av
ERLING GRIMSTAD
Advokat og daglig leder i Advokatfirmaet Erling Grimstad AS.
Foto: privat

Arbeidsgivers tilrettelegging for varsling har stor betydning for ytringsklimaet i virksomheten. Gode kanaler for varsling og oppfølging gir også muligheter for å avdekke eventuell trakassering, diskriminering, mobbing, maktmisbruk eller økonomisk kriminalitet. Ifølge Varslingsutvalget representerer varsling en verdi.

Hva varsles det om?

Arbeidstaker velger selv hva det skal varsles om. Varsling kan for eksempel gjelde anklager om seksuell trakassering, andre former for trakassering, diskriminering, mobbing, rasisme, kritikkverdig forskjellsbehandling, brudd på interne regler/rutiner/retningslinjer, maktmisbruk, misbruk av stilling eller posisjon, økonomisk kriminalitet (bokføringslovbrudd, skatteunndragelse, arbeidslivskriminalitet, tyveri, underslag, eller korrupsjon) og brudd på krav til helse-, miljø og sikkerhet.

Det er varsleren som arbeidstaker selv som bestemmer hva vedkommende oppfatter som kritikkverdige forhold det som bør varsles om. Arbeidsgivere som forsøker å begrense hva det kan varsles om, eller ikke respekterer ansattes rett til å avgjøre hva som er kritikkverdig, bør tenke seg godt om. Slike signaler kan få motsatt effekt dersom intensjonen var å legge til rette for en god ytringskultur i virksomheten. Som arbeidsgiver bør du respektere de krav varslerne setter for å gi informasjon. Ikke lov varsler noe du ikke kan holde.

Man bør være forsiktig med å kategorisere det varsler selv har definert som varsling - som noe annet enn, nettopp varsling. Arbeidsgivers handlinger og unnlatelser ved håndtering av varslingssaker, kan få stor betydning for tilliten medarbeidere har til leder.

Kan arbeidsgiver bestemme hvordan arbeidstakere skal varsle?

Svaret er nei. Arbeidsgiver kan utarbeide tydelige retningslinjer om hva som regnes som forsvarlig varsling. På den måten kan arbeidsgiver utøve en viss påvirkning av hvilke typer av kritikkverdige forhold ansatte vil varsle om. Ved å åpne for flere kanaler for varsling, kan man gjøre det enkelt for ansatte å varsle i og utenfor arbeidstiden.

Ledere kan bidra til å skape en organisasjonskultur som tilrettelegger for at ansatte vil benytte virksomhetens varslingsordning. Lederskapet avgjør langt på vei om arbeidstakerne oppfatter at de har et trygt og godt fysisk og psykososialt arbeidsmiljø. Noen velger å varsle utenom virksomhetens egne varslingskanaler. Derfor går noen varslere direkte til kontrollmyndigheter eller til journalister med den informasjonen de har. Dersom varsler ikke er trygg på at arbeidsgiver vil gjøre nok for å avsløre og/eller stanse de kritikkverdige forholdene, øker muligheten for at varsler går eksternt.

Hvorfor velger noen å varsle?

Årsaken til at noen velger å varsle er sammensatt og helt avhengig av situasjonen.

Arbeidsgiver bør forsøke å forstå hva som forårsaker varsling. De fleste varslere har en sterk overbevisning om at varsling er det eneste som nytter for å avsløre noe som er kritikkverdig. Det betyr at varsleren ikke har tillit til at det eksiterer andre reelle kanaler for å ta opp kritikkverdige forhold på arbeidsplassen. Varselet kan gjelde noe som kun berører eller går ut over varsleren selv. Men det kan også være noe varsler har oppdaget på arbeidsplassen og som gjelder flere personer. I

Alle virksomheter med flere enn fem ansatte skal ha rutiner for varsling av kritikkverdige forhold. Disse rutinene bør skape god forutsigbarhet for den som varsler og den det varsles om. Det er arbeidsgivers ansvar å påse at håndteringen av varslingssaker skjer på en trygg måte for varsler og den det varsles om.

mange tilfeller kan det være varslers egen samvittighet som gjør det umulig å fortsette som før eller late som om ingen ting har hendt. Min erfaring er at varsling kan synliggjøre noe som mange vet, men som ingen andre tør å ta tak i på arbeidsplassen. Bestemte hendelser kan utløse varsling om forhold som ligger langt tilbake i tid.

Det er sjeldent at varselet er oppdiktet eller gitt kun for å skade noen. Slike tilfeller er relativt enkelt for arbeidsgiver å oppdage om fakta undersøkes.

> Kunnskap om fakta er det beste utgangspunkt for å starte den møysommelige prosessen med å løse vanskelige eller innbitte konflikter på arbeidsplassen.

Klarer arbeidsgiver å håndtere varsler på en god måte?

Svaret på det avhenger av om arbeidsgiver ser på varsler som en pest og plage, eller som en viktig verdi og ressurs for å rette opp i feil, dysfunksjonelt arbeidsmiljø, dårlig ledelse, ulovlige eller kritikkverdige forhold.

I mange tilfeller gjelder varselet mistillit til noen i virksomheten. Det kan være mistillit til ledere eller kollegaer på samme nivå. Det er ikke uvanlig at varselet har et følelsesladet bakteppe der subjektive oppfatninger gjør det vanskelig for andre å beskrive de faktiske forholdene. Arbeidsgiver må derfor respektere at ansatte oppfatter samme faktum på ulike måter. Det kan vise seg svært krevende å avdekke hva som er de objektive fakta. Undersøkelsene må også ta hensyn til hvordan personene selv har opplevd hendelsen. I tilfeller der varselet gjelder konflikt mellom enkeltpersoner, starter konfliktløsningen med å identifisere fakta som partene kan enes om. Kunnskap om fakta er det beste utgangspunkt for å starte den møysommelige prosessen med å løse vanskelige eller innbitte konflikter på arbeidsplassen. Dersom det ikke er noen som helst enighet om hendelsesforløpet, er det svært vanskelig å løse konflikter på arbeidsplassen.

En god håndtering fra arbeidsgiver krever en vilje til å rydde opp i de kritikkverdige forholdene. Derfor blir det et feil utgangspunkt dersom arbeidsgiver er mer opptatt av *hvem* som har varslet enn hva det varsles om.

Arbeidsgiver må være klar over at varsling ofte handler om *mot til å si ifra* om ubehageligheter, der andre velger å se en annen vei. Derfor opplever varsler ofte å stå alene, uten støtte fra andre som har sett det samme. Det er en svært krevende situasjon å komme i. Isolasjon som skjer som følge av at man har varslet, kan oppfattes krenkende og svekke selvtilliten hos de fleste av oss. Kritikken fra varsler er ofte knyttet til prosessen og ikke alltid innholdet i hva det varsles om.

Hvilke rutiner bør varslingsordningen omfatte?

Arbeidsgiver bør etablere flere kanaler for varsling, men dette er ikke noe lovkrav. God praksis tilsier at det etableres tre ulike kanaler der minst en av kanalene for varsling er tilgjengelig for ansatte utenfor eget arbeidssted og utenfor kontortid. Alle kanalene bør være satt opp på en måte som sikrer at varselet kommer frem til rette vedkommende uten innsyn fra uvedkommende. Det er vanlig å etablere en kanal for varsling per telefon, postforsendelse og et elektronisk varslingsmottak.

Arbeidsgiver bør ha tenkt gjennom hvordan varslingsordningen skal gjøres kjent i virksomheten og sikre at alle lovbestemte plikter er oppfylt i de rutiner som utarbeides. Rutinen bør blant annet gi varsler en viss veiledning om hva varsling er, hvilke plikter arbeidsgiver har og hvordan ledelsen saksbehandler varselet. Rutinene bør omtale hvordan kommunikasjon med varsler og den det varsles om, skal foregå under saksbehandlingen av varselet.

Det er en helt sentral rettssikkerhetsgaranti at den personen det varsles om blir gjort kjent med kritikken og får anledning til å kommentere og forsvare seg mot anklagene. Men det er ikke åpenbart når slik mulighet bør gis til den personen kritikken rammer. Dersom anklagene gjelder åpenbare straffbare forhold, bør det først vurderes om saken skal anmeldes til politiet før den mistenkte orienteres. Husk at den mistenkte kan forspille bevis eller påvirke vitner. De valg du gjør før politiet kobles inn, kan avgjøre om saken oppklares. I en straffesak er det opp til politiet å avgjøre når mistenkte skal informeres og om hva.

DEN 15. MARS 2018 BLE VARSLINGSUTVALGETS UTREDNING OM VARSLING I ARBEIDSFORHOLD LAGT FREM (NOU 2018:6).

Varsling har størst verdi dersom:
- varselet blir tatt på alvor,
- varsleren blir tatt vare på,
- det blir iverksatt undersøkelser for å avklare om det foreligger kritikkverdige forhold, og
- det kritikkverdige forhold opphører.

Alle virksomheter som jevnlig sysselsetter minst fem arbeidstakere plikter å utarbeide varslingsrutiner. I denne beregningen inngår faste ansatte, midlertidige og innleide. Rutinene skal angi fremgangsmåten for mottak, behandling og oppfølging av varsling i virksomheten.

Informasjon om rutinene bør ligge lett tilgjengelig for ansatte, dvs. på virksomhetens intranett eller annet sted der det er enkelt å finne den. Varsleren bør enkelt kunne skaffe seg informasjon om hvem som saksbehandler varselet slik at varsleren selv kan vurdere om noen av de som normalt behandler varselet er inhabil eller uskikket til å behandle varselet.

Saksbehandling av varsel

Bestemmelsene om varsling i arbeidsmiljøloven innebærer i seg selv ingen plikt til å saksbehandle varsler, men det anbefales sterkt at alle varslersaker saksbehandles. I noen tilfeller har arbeidsgiver plikt til å undersøke påstander fra varslere etter andre bestemmelser enn bestemmelsene om varsling i arbeidsforhold. Innholdet i varselet kan for eksempel være av en art som innebærer plikt for selskapets styre og daglig ledelse å undersøke opplysningene etter aksjelovens regler. Saksbehandlingen bør innrettes slik at den inngir tillit hos den eller de som varsler. Men det er selvsagt måten saksbehandlingen gjennomføres på som avgjør om arbeidstakere vil ha tillit til ordningen og følge virksomhetens varslingsrutiner.

Det bør være noen få og faste personer som saksbehandler varslingssaker. Årsaken er at slike saker krever en bestemt kompetanse og kan inneholde sensitiv informasjon. Arbeidsgiver bør ha god kontroll med hvem som mottar informasjon om varslingssaken. Den det er varslet om bør selv ikke delta i saksbehandlingen, men skal selvsagt ha anledning til å forsvare seg mot anklagene.

Det bør føres logg for saksbehandling av varslingssaker slik at arbeidsgiver kan redegjøre for alle beslutninger og aktiviteter i saken. Saksbehandlingen bør innrettes slik at andre kan etterprøve hva som er gjort og ettergå kritikk som kan komme. Ofte vil et separat elektronisk saksbehandlingssystem, adskilt fra andre arkiv eller oppbevaringssteder, være løsningen for å ivareta disse hensynene.

De som skal behandle varselet bør ha kompetanse til å saksbehandle varselet på en måte som sikrer en forutsigbar prosess i samsvar med varslingsrutinene. Dette krever kunnskap om bevisvurdering og regler om hvem som har bevisbyrden, krav etter arbeidsmiljøloven, personvernregler (GDPR), kunnskap om hva som utgjør lovbrudd, kompetanse til å innhente fakta gjennom elektroniske lagret informasjon, dokumenter eller intervjuer, og kompetanse til å rapportere funn på en nøktern, balansert og korrekt måte.

Varslingsmottaket bør ha ressurser til å kunne behandle varslersaken umiddelbart om det kreves. Varslingssaker bør ikke bli liggende uten at noen har ansvar for å håndtere dem. Erfaring viser at enkelte varslingssaker kan avgjøres på svært kort tid. Andre kan henvises til behandling hos personalavdelingen, til en bestemt leder eller til behandling i etablerte fora og faste møter i virksomheten. Noen saker kan vise seg svært krevende og omfattende. Det er ikke uvanlig at enkelte varslingssaker tar mer enn ett år å saksbehandle. I sjeldne tilfeller søker varsler råd hos advokat, noe som kan medføre at det rettes krav mot arbeidsgiver fra varsler.

> Kritikken fra varsler er ofte knyttet til prosessen og ikke alltid innholdet i hva det varsles om.

Hva om varselet gjelder noen i den øverste ledelsen?

Rutinene bør åpne for muligheten til å kunne varsle forbi daglig ledelse dersom varselet gjelder daglig leder/øverste ledelse. Det bør derfor tilrettelegges for at det for eksempel kan varsles til styreleder, enkeltpersoner i styret eller eksternt varslingsmottak der det ikke er noen annen naturlig løsning for varsling til noen over øverste leder.

Anonym varsling

Dersom det tilrettelegges for at varsler rutes til virksomhetens varslingsmottak i samsvar med varslingsrutinen, anbefales det å åpne for saksbehandling av anonym varsling. Men det er ingen plikt for arbeidsgiver å tilrettelegge for eller saksbehandle anonyme varsler. Dette er et av mange valg arbeidsgiver må gjøre ved etablering eller ajourføring av varslingsordningen i egen virksomhet.

Eksternt eller internt varslingsmottak?

Intern varslingsordning er løsninger der mottak og saksbehandling av varslingen foregår av ansatte i virksomheten. Ekstern varslingsordning innebærer at mottak av varslinger går til noen som ikke er ansatt i bedriften og/eller at saksbehandlingen utføres av personer som selv ikke er ansatt i virksomheten.

Mange mindre virksomheter velger å kun etablere interne varslingsordninger der det ikke er noen eksterne aktører som har noen rolle som mottak av varsel eller saksbehandling av varselet. Noen bedrifter har både intern og ekstern varslingsordning. Andre velger kun ekstern varslingsordning der mottak av varsel og saksbehandlingen skjer utenfor virksomheten.

Varsling og personvern

Arbeidsgiver skal ivareta personvernhensyn for varsler og den eller de personer varselet gjelder. Dette kan vise seg å være en krevende balansegang. Varsler vil ofte inneholde sensitive personopplysninger og må behandles deretter. Arbeidsgiver må derfor vite om det er lovlig grunnlag for å behandle varselet, sørge for god informasjonssikkerhet og oppbevare opplysningene slik at ingen andre enn de som må behandle disse, har tilgang. Dersom virksomheten velger eksternt varslingsmottak opptrer den eksterne enheten som databehandler.

Tillitsbasert styring og ledelse i Oslo kommune

Av
JOAR SÆTERDAL VIK
Fagsjef, seksjon for org. og ledelse, Byrådslederens kontor

Tillit er ikke noe nytt. Ei heller tillitsbasert styring og ledelse og debatten om målstyring og new public management. Det som er nytt i norsk sammenheng er Oslo kommunes satsning på tillitsbasert styring og ledelse. «Stoppeklokken» i eldreomsorgen skal erstattes med økt fokus på omsorg og kvalitet gjennom involvering og medvirkning av brukeren og de ansatte.

Byrådet i Oslo har vedtatt at tillit skal være et bærende prinsipp for styring og ledelse i hele kommunen. For tiden gjennomføres det piloter i noen deler av kommunens tjenestetilbud for å implementere dette. Det er viktig å finne den rette balansen mellom styring og ledelse, kontroll og oppfølging. I byrådsvedtaket fra mai 2017 fremgår det blant annet at detaljstyringen skal reduseres og at innbyggerne skal være delaktige.

TILLITSBASERT STYRING OG LEDELSE I OSLO KOMMUNE SKAL KJENNETEGNES AV:

- Få og tydelige mål
- Redusert detaljstyring
- Gode beslutningsgrunnlag
- Bred deltakelse fra innbyggere
- Åpenhet og god kommunikasjon
- God samhandling mellom ledelse og medarbeidere og deres organisasjoner
- God utnyttelse av medarbeidernes kompetanse og kreativitet
- God samhandling og samordning på tvers
- Innbyggerorienterte digitale tjenester

Inspirasjon fra andre

Det som i byrådsplattformen omtales som en «tillitsreform» er en viktig satsning for kommunen. Arbeidet ble startet opp etter at de rød-grønne vant kommunevalget i 2015 og henter inspirasjon og læring fra både akademia og andre deler av offentlig sektor, samt tilsvarende reformer gjennomført i Sverige og Danmark. I Danmark ble det opprettet en ledelseskommisjon som har vært operativ en tid og som kommunen har hatt noe dialog med. Som en del av dette forbedringsarbeidet har det vært viktig å få til godt lederskap. Kommunen deltar i et samarbeidsprosjekt med København kommune for å se på mulighetene for å utvikle offentlig lederskap videre.

Tillit, kontroll og målstyring

Representanter fra Danmark og Sverige presenterte sine erfaringer med tillitsreformer på DFØs styringskonferanse i januar i år. De var tydelige på at dette ikke innebærer å slutte med målstyring, men at tillitsbasert styring og ledelse skjer innenfor rammen av målstyring. Dette er også en viktig premiss for arbeidet i Oslo kommune. Ett av kjennetegnene for tillitsarbeidet er få og tydelige mål. Det jobbes med styringsdialogen og tildelingsbrevene, der det nå legges til rette for mer strategisk styring. Felles føringer og mal for tildelingsbrev er utarbeidet sentralt i kommunen i tråd med intensjonen om tillitsbasert styring og ledelse. I tillegg er det etablert et eget nettverk for virksomhetsstyring blant byrådsavdelingene.

«Tillitsbasert styring og ledelse innebærer ikke at det er fritt frem for medarbeiderne hvordan de vil jobbe. Det er fortsatt slik at strukturer, systemer og styringslinjer er viktige for at innbyggerne i hovedstaden skal ha tillit til måten kommunen styres og ledes. Et annet viktig aspekt i arbeidet med tillitsbasert styring og ledelse er å utvikle tjenestene sammen med innbyggerne. Styrket brukerinvolvering er en av hovedhensiktene med dette arbeidet.»

Kommunen ser også et potensiale i digitalisering. Dette kan blant annet føre til at styringsdata fremskaffes mer kostnadseffektivt og gi muligheter for å redusere behovet for manuelle kontroller.

Det er ikke lagt opp til en systematisk nullpunktmåling som grunnlag for å evaluere tillitsarbeidet, men byrådsavdelingene blir utfordret på om de vet om styringen på sitt område fungerer. Noen evalueringer eller målinger eksisterer allerede og disse legges til grunn.Effektmåling av et slikt arbeid er utfordrende, både fordi det vil ta noe tid før man kan anta at et slikt arbeid tar effekt, samt at det er utfordrende å isolere effekter av arbeidet. Sammen med en del sentrale tiltak jobbes det også med tillitsbasert styring og ledelse omkring i hele organisasjonen. Lokale initiativ, tiltak og utviklingsarbeid er definitivt en viktig del av utøvelsen.

Behov for kulturendring

Tendenser til detaljstyring ligger i politikkens og styringssystemets natur. Når man ser på styringsprosesser både på kommunalt og nasjonalt nivå er det ofte i detaljene at sprengkraften i sakene ligger. Dette er en utvikling som også mediene naturlig nok bidrar til. At politisk ledelse har behov for å sette seg detaljert inn i ulike saker, eller sågar må detaljstyre fra tid til annen har kommunen forståelse for. Det er nødvendig med en balansegang mellom politikk og administrasjon, slik at både fagkompetanse og den byråkratiske kraften utnyttes best mulig for å få gjennomført den politikken de folkevalgte ønsker.

«Arbeidet med tillitsbasert styring og ledelse er også en kulturendring. I så måte er arbeidet noe som naturlig nok ikke

HVA BETYR TILLITSREFORMEN FOR INTERNREVISJONEN?

Wenche Jensen, Spesialrådgiver, Oslo kommune, Byrådslederens kontor, Internrevisjonen

Internrevisjonen har fortsatt ikke vært særlig involvert i dette arbeidet. Dette er forbedringsarbeid som må modnes over tid og som vil være vanskelig å se effektene av arbeidet på kort sikt. Kommunens virksomheter er i gang med å tta inn tillitsbasert styring og ledelse som en del av virksomhetenes styring. Det vil etter hvert være naturlig for Internrevisjonen å gjennomføre revisjoner ved å kartlegge og vurdere hvordan virksomhetene arbeider med å operasjonalisere og integrere tillitsbasert styring og ledelse i virksomhetsstyringen. I våre revisjoner må vi først kartlegge hvordan virksomheten planlegger og utøver tillitsbasert styring og ledelse for så å vurdere hvordan effekter og resultater måles. Metodisk vil det handle om hvordan tillitsbasert styring og ledelse utøves med tanke på god risikostyring og internkontroll. Har virksomhetene gode systemer for risikostyring og internkontroll mener vi de vil ha et godt utgangspunkt for hvilke områder det kan utøves styrket tillitsbasert styring og ledelse med færre mål samt mindre grad av rapportering og oppfølging. Internrevisjonen vil ta dette inn i revisjonsprosjekter slik at vi kan gi tilbakemelding om status i arbeidet både til byrådsavdeling og virksomhetene. Internrevisjonen har også hatt temaet «kontroll i et tillitsperspektiv» i et nettverksmøte som arrangeres for ansatte i kommunen.

endres over natten. At vi hele tiden jobber med å forbedre tjenester og arbeidsprosesser er kritisk viktig for å bidra til at detaljstyringen kan reduseres.»

Betydningen av kompetanse

Oslo kommune har et lederutviklingstilbud til toppledere som består av tre hovedelementer. Det ene elementet handler om ledergruppeutvikling. Å sikre at ledergruppen bruker tiden på de rette sakene, at de har gode arbeidsprosesser og at de oppnår den effekten de ønsker. Det andre elementet kalles refleksjonsgrupper. Disse gruppene er sammensatt på tvers av sektorer og fagområder. Dette er en arena som bidrar til læring og innsikt på tvers av sektorer. Det tredje elementet kalles leder- og temasamlinger. På disse samlingene løftes strategiske viktige temaer og politisk ledelse deltar også på noen av disse samlingene. Samlingene skal gi faglig kompetansepåfyll og bidra til deling av god praksis på tvers av sektorer og virksomheter.

Operasjonalisering av godt lederskap

Arbeidet med tillitsbasert styring og ledelse i kommunen tar ikke utgangspunkt i spesifikke metoder, teknikker eller arbeidsmodeller. Tillitsbasert styring og ledelse er operasjonalisering av godt lederskap.

Pilotprosjekter på utvalgte tjenesteområder er allerede igangsatt. Det var logisk å starte med eldre, helse og arbeid. Her er det utstrakt kontakt med brukerne og det er også her «stoppeklokkene» har vært i bruk. Gjennomføringen av pilotprosjektene har pågått en tid og skal evalueres. Evalueringen vil foreligge til medio mai 2018.

HVA MENER DFØ OM MÅL- OG RESULTATSTYRING?

Hilde Singsaas, direktør i DFØ

Mål- og resultatstyring (MRS) handler om å løfte styringen fra detaljerte instrukser om ressursbruk og enkeltoppgaver, og i stedet rette blikket mot de faktiske effektene man ønsker å oppnå for samfunnet og befolkningen. Styringsprinsippet bygger på en overbevisning om at vi får mest velferd for fellesskapets ressurser hvis de overordnede myndighetene konsentrerer seg om hva som skal oppnås, og så overlater til nivåene under å finne ut hvordan målene best kan nås.

Styringen skal tilpasses behovet. Det er ingen felles oppskrift som tvinges på alle. Dette er basert på tillit til at departementer og virksomheter finner gode løsninger basert på sine ulike behov. MRS forutsetter delegering av myndighet, altså at underliggende nivåer gis et reelt handlingsrom. Det er ikke nok at departementene delegerer myndighet til underliggende virksomheter. Ledelsen i virksomhetene må i neste omgang gi handlingsrom til sine mellomledere og medarbeidere.

Samtidig må handlingsrom og frihet i oppgaveløsingen følges av en rapportering tilbake. Her er vi inne på et annet tillitsforhold, nemlig befolkningens tillit til staten. For å ha legitimitet, må staten kunne dokumentere hva som er oppnådd og hvordan fellesskapets ressurser er brukt. I tillegg er det viktig å bruke kunnskap om resultatene til læring og utvikling i den enkelte virksomhet.

Det er praktiseringen og ikke de gode styringsprinsipper som avgjør om styringen er basert på tillit eller ikke. For at delegeringen skal fungere, er det viktig med en felles forståelse av utfordringer og mål, og da er en god og åpen dialog mellom den som styrer og den som blir styrt helt avgjørende. Dersom styringen rettes inn mot måltall, overdreven kontroll og detaljerte instrukser, går det på bekostning både av tilliten og evnen til å løse samfunnsoppdraget. Derfor er en av DFØs viktigste oppgaver å støtte og veilede statlige virksomheter slik at praktiseringen kan bli best mulig.

Finn mer informasjon på www.dfo.no

Internrevisors selvbilde

Av
MARTIN STEVENS
medlem av mediekomiteen

Det er blitt sagt at den største løgnen internrevisor kan komme med er at «jeg er her for å hjelpe deg». Vi kan være hellig overbevist om at vår rolle bidrar til forbedringer i virksomhetens risikostyring og internkontroll, men personen vi reviderer kan oppfatte oss som politi, ute etter å finne feil, påpeke svakheter og dårlige prioriteringer..

Spørsmålet er om vi internrevisorer burde vært mer bevisst på hvordan vi fremstiller oss selv i forhold til resten av organisasjonen. PWC gjennomfører årlig en globalundersøkelse som kartlegger trender innenfor internrevisjonsprofesjonen og internrevisjonens evne til å møte interessentenes forventninger (ref. artikkel i SIRK nr. 2, 2017, side 66-67). Resultatene fra 2017 viser at de internrevisjonsfunksjonene som scorer høyest er de som løfter blikket og er mer fremtidsrettede, endringsvillige eller agile. Det forventes et større fokus på strategiske og nye risikoer samt samarbeid med andre kontrollenheter som Risikostyring og Compliance. Hvordan kan vi skape et bilde av oss selv som er mer i tråd med disse forventninger?

En kategorisering av internrevisorers ulike selvbilder

I 2016 ble det utgitt en artikkel av Sarens, Lenz og Decaux1 som tar for seg hvordan internrevisorer fremstiller seg selv. De tok utgangspunkt i 141 tilbakemeldinger på et spørsmål de postet på en IIA-sponset LinkedIn side. Undersøkelsen ble utført i 2010. Basert på dette arbeidet beskrev de hvordan internrevisorer velger å presentere seg selv dvs. hva internrevisorens selvbilde fordelt på fem kategorier og oppsummerte med forslag til hvordan de mener internrevisorer bør kommunisere sin rolle og profesjon.

FEM TYPER AV SELVBILDE:

1. Negativt bilde

Tradisjonelt bilde av internrevisor som definerer seg selv som ledelsens eller styrets øyne og ører. Ønsker å oppfattes som «politi» og fremhever seg selv som den gode i forhold til kjeltringene i resten av organisasjonen.

2. Identitetsløs, nedgradering av egen rolle

Dette bildet karakteriseres av ord som «jeg er den du ønsker jeg skal være» og «vi sikrer at du fremstår i et positivt lys». Det kommuniseres ikke hvordan internrevisjon kan virkelig bistå til positive endringer i organisasjon.

3. Banale og tomme ord

I dette bildet fremhever internrevisor IIAs definisjon av internrevisjonen som «...en uavhengig, objektiv bekreftelses- og rådgivningsaktivitet som har til hensikt å tilføre merverdi og forbedre organisasjonens drift...osv.» Med denne definisjonen fremhever internrevisorer den merverdien den gir gjennom revisjonsanbefalinger. De oppfatter seg selv som pålitelige rådgivere til virksomheten, ikke minst med utgangspunkt i sin uavhengighet. Men de er ikke de eneste eller nødvendigvis de beste rådgivere for virksomheten, og det er ikke alltid at kontrollene må forbedres, kanskje noen ganger er det godt nok.

4. Overambisiøs (supermann/superkvinne)

Her promoterer man et bilde av å være lege eller spesialist som undersøker, diagnostiserer og anbefaler medisinen som kan rette opp problemene i organisasjonen. Problemet er at man ikke alltid har forutsetning og tilstrekkelig kunnskap for å uttale seg på enkelte områder.

5. Utgjør en forskjell

I dette bildet fremhever man mer realistiske ambisjoner. Her fremheves at man forsøker å gi et nytt perspektiv med ønske om å utfordre virksomheten til å lykkes. Her er internrevisor en bidragsyter i styrking av organisasjonen mot et fellesmål. Her fremheves et åpent sinn fremfor uavhengighet og objektivitet.

Internrevisor som bonde

Til slutt fremmer artikkelforfatterne sitt eget bilde av internrevisoren; En bonde. Å overleve som bonde innebærer at man må spille på lag med naturen. Man trenger ydmykhet, fleksibilitet og en kontinuerlig søken etter forbedringsmuligheter. En bonde er en leder uten tittel. Tilsvarende har en internrevisor liten formell autoritet, men må trekke på ledelsesteknikker innenfor kommunikasjon, lytting og overbevisning. En bonde sår frø som gror til gress og gir mat til hønene som verper. På tilsvarende måte opererer internrevisor indirekte i organisasjonen. Det er andre som får det til, men de kan påvirkes positivt av internrevisoren. En bonde måler sin prestasjon igjennom resultater korn som er høstet mv. og ikke sin egen innsats. Slik bør det også være med internrevisoren.

En typisk internrevisor

Det viktige er at vi som internrevisorer klarer å presentere oss selv på en måte som fremhever de egenskapene vi innehar og de verdiene vi kan bidra med. Vi er ikke verdensmestre dog mener jeg at vi utfyller en viktig rolle i våre organisasjoner. Kanskje bonde er et passende bilde av oss selv?

Det er innhentet tillatelse fra copyrighteier Taylor and Francis til å henvise til artikkelen og herunder gjengi en oppsummering av hovedelementer i den aktuelle artikkelen.

[1] *INSIGHTS INTO SELF-IMAGES OF INTERNAL AUDITORS by Gerrit Sarens, Rainer Lenz AND Loïc Decaux utgitt i The EDP Audit, Control, and Security Newsletter issue no. 54, 2016 to which further reference should be made https://www.tandfonline.com/doi/full/10.1080/07366981.2016.1220226*

Using airline methods to manage financial and legal risk

How many industries took inspiration from airline loss prevention

About the authors:
JODI LEE AND TERJE LØVØY
worked in aviation for 27 years. Jodi for American Airlines as supervisor and cabin crew. Terje as Captain and Vice President in SAS Scandinavian Airlines. He was also a US Federal Aviation Administration examiner for the Boeing Factory. Today, Jodi and Terje are management systems lecturers and consultants working in various industries for Lovoy AS.

www.lovoy.info
jodi@lovoy.info
terje@lovoy.info

In this article Jodi Lee and Terje Løvøy explain how they started high in the sky with aviation, moved to shipping and then even deeper down to diving. They help different industries use their method to manage operational, financial and legal risk. The Lovoy method improves compliance by making procedures and other documents more user friendly. It is not a software. It is a new way to write and structure information so we quickly find, read and understand what we need.

All large companies face the risk of losing something. This can be loss of life, money, polluting the environment, breaking the law and so on. These companies may have many procedures with large amounts of information. When something goes wrong, the problem is seldom a lack of information. In most cases the problem is solvable because a known solution is available, but for some reason not used.

In the old days people listened to stories told by the eldest members of the group. This was their primary form of entertainment and education. Stories passed from one generation to the next, often reflecting critical knowledge. This verbal passing of collective knowledge prevented losses and helped people survive.

20 Years of Experience or one Year's Experience 20 Times?

Why is knowledge sharing important? Some may say it is like having 20 years of experience rather than one year's experience repeated 20 times. It is about learning from past mistakes. Knowledge sharing is as important today as in the past. But today information is so complex that verbal sharing alone is not enough.

Companies handling risk must have procedures stored in a management system. We also call this standardization, which in effect is collecting years of experience from many people, and getting their acceptance of the best practices. It builds on the principle that the collective knowledge is better than the impromptu suggestion of one individual.

Human error causes more than 80% of accidents in most industries, often because people do not follow procedures. We spent 27 years in aviation trying to understand why so many accidents have "procedure not used" as a cause. Since 2009 we also work with other industries analyzing numerous management systems with thousands of documents.

Many clients complain that their management systems and procedures are too complex to read and follow. As a consequence, employees avoid using them. When the writing is too complex to understand, employees end up transferring knowledge verbally. This means that colleagues pass good and bad habits along, including

unstandardized techniques. This is a big setback – it takes us back to the old days.

How Did Airlines Improve Safety More Than 100 %?

Many of our clients want to learn from airlines because air travel is very safe. But before we continue, how safe is it to fly? In the early 1960's we had 30-40 hull loss accidents per million departures. In 2015 we had 0.32. This makes flying one of the safest things you can do. You must fly one trip every day for more than 8000 years to statistically experience an accident. Many industries are asking how airlines managed to improve safety by more than 100 %. There are two answers. In the first years, technical improvements; and after the 1970's, better ways to manage human error. Our clients asked if we could transfer these concepts to other industries. We found the answer by looking back at what the airlines did to improve their safety records.

Use Experience – not Checklists

Use experience – not checklists, was an unwritten rule for most pilots 30 years ago. Pilots had experienced having to choose between good airmanship and too long checklists. Airline checklists would typically have many non-critical items and pilots perceived them as more of a nuisance than an aid. Since voice recorders watched them, they always read the checklists, but fast and superficially. Today, pilots do not read the checklist fast because they have to – but carefully because they want to. What changed?

In 1998, Swissair had a fire in the video entertainment system. Faced with heat and smoke, the pilots still circled and read the complex lists. This took too long, they crashed and lost all onboard.

What did we learn? Unnecessary complex text competes with common sense and experience. We made the text shorter and clearer. If unable to control the smoke or fire, the conclusion quickly instructs the pilots to land as soon as possible.

Before and after example showing 65% reduction in wordcount. The photo is from a Teekay Shuttle Tanker which transports a significant part of the North Sea's oil production.

From Flying High to Diving Deep

We believe that even though an operation is complex, it does not mean we must explain it with difficult words and long sentences. This is an important principle regardless of which industry you are in. As an example, Haukeland University Hospital implemented a safe surgery checklist using aviation principles. This reduced complication rates and mortality by up to 42%. [i] TV2 News described it as the best invention since doctors started washing their hands. We customized a set of writing rules and tested them in various industries such as shipping, oil, gas, hospitals, rail, deep sea diving, manufacturing and insurance companies.

In 2014, Teekay Shipping's navigation procedures had just below 49,000 words. They used our method and simplified them down to just above 17,000 words. That was a 65 % reduction, but reducing words was not the goal, the goal was to be concise. This is now in use on nearly 200 vessels.

From Operational to Financial and Legal Risk

Shipping companies have complex requirements from governments, insurance companies and clients such as oil companies. As a consequence, they have a lot of procedures for their operations. At first, shipping companies had concerns about simplification. Would they lose required facts? Would governments, insurance and oil companies approve of simpler text? After seeing our method, oil companies replied that «we know what we like when we see it – and we like this». Insurance companies started running seminars and writing articles to their clients promoting the method[ii]. A diving company avoided costly government restrictions by using the methods[iii].

The most important feedback came from the end users. Seafarers evaluated the new

[i] *Haugen, Bakke, Lovoy, and Softeland. "Preventing Complications: The Preflight Checklist". European Urology Focus 2:1 (2016), 60-62. https://lovoy.info/m/articles/Preventing-Complications_-The-Preflight-Checklist.pdf*

[ii] *Terje Løvøy. "Simplifying Safety Management Systems". Signals Magazine by The North of England Protection and Indemnity Insurance Association. Issue 110 (2018) 6-7. https://lovoy.info/m/articles/Signals-Winter-2017-18_Lovoy.pdf*

[iii] *nternational Marine Contractors Association. "Simplicity Improves Safety". Making Waves. September (2016) 15. https://lovoy.info/m/articles/IMCA-Making-Waves-80-v2.pdf*

text as 70-80% more user-friendly. The results spread from operational tasks to administrative tasks. It also spread to other industries. As an example, today we are testing how to simplify instructions for underwriters in the insurance industry.

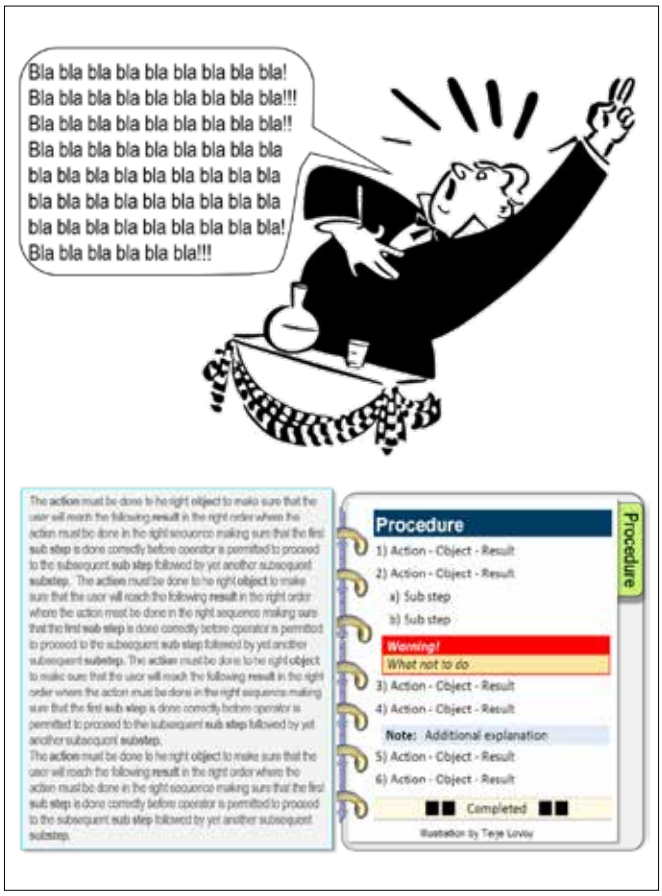
The Lovoy Method

Simplification does not happen by itself – we must design it. To do this we need methods and ways to measure the results. We developed this for writing style, layout and spagetti-like structure.

Writing Style

Writing style is about the words we use and the sentences we form. People are like text, some talk a lot but say very little. We can compare text with math, why write 12/18 when we can write 2/3? Why write «commence» when we can write «start»? We have a plain language dictionary available at www.lovoy.info

One problem is too long sentences. But how long is too long? We found that the average sentence length was 21 words. After training many writers to wash the text we found that they could improve it to 14 words or less per sentence. Passive text was another problem. Unwashed documents had more than 40% passive sentences. Our text washing improved this to more than 95% active text. Active sentences are shorter, you read them faster, understand them better and remember them longer. Passive can be unclear because one sentence can have several meanings.



Complex	Simple
Give consideration to	Consider
During the period of	During
A number of	Some
Give the recognition to	Recognize
Is concerned with	Concerns
Because of the fact that	Since

Layout

We made an easy to use template inspired by NASA research. It has a clear visual layout with notes, cautions and other styles.

Structure

People continuously add information to the management systems, but few have a clear strategy when they do this. This gives a tangled spaghetti like structure, not following logic work flows. In addition, we mix strategy and execution. We write a lot about responsibilities, but responsibility is not a verb – it is not something we can do. This makes the text abstract. It is not what we say that matters, it is what we do. The goal of a management system is to go from words to actions.

Conclusions

Most companies that manage risk can prevent losses if they make their management system text more user-friendly. Overly complex writing style reduces compliance and increases the risk of error. It is possible to train employees to write more user-friendly documents. Our research shows that clear concise text is a crucial part if you want to improve risk management. This principle is content independent, and works for operational, legal or financial risk.

Fra internrevisjon til…. stabsdirektør i Norges Bank

Av
ELLEN BRATAAS
generalsekretær IIA Norge

Mange husker nok at det stormet i og rundt Statistisk sentralbyrå i høst, noe som ledet til daværende administrerende direktør, Christine Meyers, avgang. Dette førte til at stabsdirektøren i Norges Bank ble konstituert som administrerende direktør i SSB, og slik gikk det til at Ingunn Valvatne, leder av internrevisjonen i Norges Bank, fikk tilbudet om midlertidig å fylle stabsdirektørstolen.

- Hvordan havnet du egentlig i internrevisjon, Ingunn?

Jeg har bakgrunn som sivilingeniør og tilbragte de første årene i miljøforvaltningen, der jeg arbeidet med forurensning fra oljevirksomheten til havs. Fagfeltet innebar en del internasjonale forhandlinger innenfor flere kommisjoner og internasjonale avtaler knyttet til havforurensing. Et bistandsprosjekt om miljølovgivning i Angola forsterket interessen for internasjonalt samarbeid og førte til at jeg startet i Norad, fortsatt med miljø som fagområde.

En stillingsannonse fra internrevisjonen i Hydro vakte interesse. Det brede nedslagsfeltet for rollen tiltalte meg sammen med selskapets internasjonale virksomhet og selskapets økonomiske og samfunnsmessige betydning. Deretter gikk veien videre til stilling som leder for internrevisjonen i Norges Bank. Her var det nok særlig Oljefondet som tiltalte. Internrevisjonen i Norges Bank dekker hele virksomheten, både den tradisjonelle sentralbanken og NBIM som forvalter av Oljefondet, hvilket innebærer tett og hyppig kontakt med styrende organer og med ledelse. Veksten i fondets verdi og utviklingen av organisasjon og styring vært en spennende vei.

Ingunn Valvatne

Da jeg i høst fikk tilbud om en midlertidig rolle som stabsdirektør i Norges Bank, var det lett å takke ja. Staben i Norges Bank har en viktig rolle som bindeledd mellom organisasjonen og Norges Banks hovedstyre og representantskap. Vi fungerer som sekretariat for hovedstyret og ledelsen, men også flere andre funksjoner er organisert under staben.

> Da jeg i høst fikk tilbud om en midlertidig rolle som stabsdirektør i Norges Bank, var det lett å takke ja.

- Hvilke erfaringer tar du med deg fra internrevisjon inn i den nye rollen?

Det har vært inspirerende å erfare at internrevisjonens mangfoldige virksomhet både i dybde og bredde har vært nyttig ballast for meg i stillingen, og forhåpentlig også for organisasjonen. Mange års tilstedeværelse i styremøter har for eksempel gitt god innsikt i hva som skal til for å fatte gode beslutninger. På samme måten har revisjoner av styringsmodeller og prosesser på kryss og tvers i banken gitt innsikt i styrker og utfordringer i organisasjonen. Det store interne nettverket man får som leder av internrevisjonen letter også dialogen. Gode relasjoner er et nøkkelord.

Hovedstyret i Norges Bank har 17 møter i året. Forberedelser og oppfølging mellom møtene er viktig for kvalitet i beslutningsunderlag og for oppfølging av vedtak. Her er struktur, systemer og ordentlighet som kjennetegner revisjon nyttig å ha med seg.

- Hvordan har arbeidsdagen endret seg med rollebytte?

Hverdagen i internrevisjonen kjennetegnes først og fremst ved prosjekter. Det kan være travelt, men som regel har man selv hånd om planleggingen. Jeg tror det er riktig å si at hverdagen nå i større grad preges av at andre setter agendaen. Mediehenvendelser og andre forespørsler er eksempler på ytre faktorer som ikke står i kalenderen. Jeg tror jeg vil fremheve forutsigbarhet i arbeidshverdagen som en vesentlig forskjell.

- Har dette «sidebyttet» økt din forståelse av hvordan internrevisjon bidrar til virksomhetsstyringen i Norges Bank?

Det store ansvaret styrer har, og det store omfanget av informasjon de må forholde seg til har blitt enda tydeligere. Skreddersydd og tidsriktig informasjon fra administrasjonen er helt sentralt. Internrevisjonen som fra et uavhengig ståsted hjelper med å beskrive risikobildet utgjør et svært viktig supplement i styrets arbeid. Dette har blitt enda tydeligere for meg i denne rollen. Men en plass i styrerommet fordrer en sterk bevissthet om relevans og kvalitet. For å være relevant må vi forstå det unike ved organisasjonen. Samtidig må vi ha en generell kompetanse i styring og kontroll og revisjonsmetodikk. IIA har en svært viktig rolle i å støtte medlemmene i revisjonsmetodikk som kan brukes uavhengig av slike særegenheter.

Facebook-gruppe for statlige internrevisjoner

Av
CHRISTINE VIK
Seniorrådgiver DFØ

Som et lite steg på veien for å tilrettelegge for deling og erfaringsutveksling mellom statlige internrevisjoner og bli kjent med deres utfordringer og behov, har DFØ nylig opprettet en nettverksgruppe forbeholdt statlige internrevisjoner på Facebook.

Hvorfor en Facebook gruppe?

Siden 2014 har antallet internrevisjoner i staten doblet seg. De aller fleste virksomhetene som var pålagt å vurdere bruk av internrevisjon, og som har konkludert med å etablere internrevisjon, har per april 2018 fått denne på plass eller er i oppstartsfasen. Dette betyr at det nå er 45 statlige virksomheter[1] med internrevisjon. Det er en ganske oversiktlig og liten gruppe av statens totalt 188 virksomheter. Halvparten av disse er erfarne internrevisjoner, mens den andre halvparten har begrenset erfaring med bruk av internrevisjon. DFØ ser det er et stort potensial for læring og erfaringsutveksling, både mellom de erfarne internrevisjonene, mellom de nye internrevisjonene, og ikke minst mellom de gamle og nyopprettede internrevisjonene.

Facebook gruppen «Internrevisjon i staten» er et lavterskeltiltak for å kople statlige internrevisjoner sammen. Det er helt frivillig å delta, krever ingen forpliktelser og er kun ment som et supplement, og ikke en erstatning til andre eksisterende eller fremtidige kompetansetiltak for statlige internrevisjoner.

Statlige internrevisjoner har mange fellesnevnere

Et statlig forvaltningsorgan er ikke et eget rettssubjekt, men er juridisk sett en del av staten. Staten er mangfoldig og statlige virksomheter har svært ulike oppgaver og egenart. Likevel er det flere fellestrekk som gjør det hensiktsmessig for internrevisjonene å dele erfaringer og eksempler på tvers. Noen sentrale fellesnevnere er at de:

- har samme styringsmodell, er underlagt et departement, mangler styre eller har et styre som skiller seg fra et styre i privat sektor
- er underlagt mye av det samme regelverket, herunder Offentlighetsloven
- opererer med tilnærmet like statlige årshjul med planlegging og rapportering til faste tider på året
- forholder seg til Riksrevisjonen og en rekke felles tilsyn- og kontrollorgan

Mange av de etablerte internrevisjonene har opprettet gode samarbeidsarenaer allerede, eksempelvis har både Universitet- og høyskolesektoren og Forsvarsektoren utnyttet mulighetene som ligger i deling og erfaringsutveksling. Likevel mener de statlige internrevisjonene selv at det er et potensial for økt grad av samarbeid og koordinering som kan bidra til å:

- øke kvaliteten på internrevisjonsarbeidet ved å skape faglige synergier og mer spesialisering
- skape muligheter for hospitering på tvers av internrevisjonsenheter
- frigjøre ressurser og effektivisere oppgaveløsningen gjennom stordriftsfordeler, som følge av revisjoner på felles områder, deling av planer, arbeidsprogram, funn og erfaringsnotat el
- å gi små og sårbare internrevisjonsenheter et større miljø og spille på

DFØ har gjennom en spørreundersøkelse sendt til statlige internrevisjoner i 2016 og 2017 kartlagt hvilke utfordringer og behov statlige internrevisjoner har. Gjengangere i tilbakemeldingene er utfordringer knyttet til:

- små internrevisjonsenheter og knappe ressurser (budsjett og kapasitet)

[1] *Statlige virksomheter omfatter ordinære statlige forvaltningsorganer («bruttobudsjetterte virksomheter»), forvaltningsorganer med særskilte fullmakter til bruttoføring utenfor statsbudsjettet («nettobudsjetterte virksomheter») og statens forvaltningsbedrifter.*

- rolleforståelse og grensesnittet mellom de ulike «forsvarslinjene», særlig 2. og 3. linjen
- forståelse av hva internrevisjon er og hvilken merverdi den gir (særlig aktuelt blant virksomheter med nyetablerte internrevisjoner)

Finne sin form

Vi ønsker å skape en egnet arena for uformell sparring, diskusjon og erfaringsutveksling, og har foreløpig valgt å holde gruppen lukket, dvs. ikke åpnet for konsulenthusene eller for Riksrevisjonen. Medlemmer kan stille hverandre spørsmål, komme med råd, tanker eller innspill uten at dette er åpent og synlig for alle. Eksempelvis er fellesavtalen for kjøp av internrevisjonstjenester internrevisjon helt ny og uprøvd. Kun et fåtall av de statlige virksomhetene har til nå gjort avrop. «Internrevisjon i staten» er en fin plattform for erfaringsutveksling og diskusjon uten at en trenger å ta hensyn til de kommersielle aktørene som er leverandører til denne fellesavtalen.

Det kan godt tenkes at vi skal åpne opp gruppen for konsulenthusene også etter hvert, men først må Facebook gruppen finne sin form og ikke minst selv bestemme. Tanken er at gruppen skal sitt eget liv uten at vi i DFØ holder i denne i nevneverdig grad etter hvert.

SENTRALE AKTØRER SOM JOBBER MED INTERNREVISJON I STATEN TRENGER KJENNSKAP TIL BEHOV OG UTFORDRINGER

DFØ, Difi (ved Statens innkjøpssenter) og IIA Norge (ved nettverk statlig sektor) er sentrale aktører med ulike roller knyttet til internrevisjon i staten. Med mange av de samme kundene/brukerne og målsetninger er det naturlig at de samarbeider og koordinerer sin innsats.

Disse tre aktørene er også medlemmer av Facebook gruppen. Dette forumet blir en «lytte-post» som gir aktørene indikasjoner på hva de statlige internrevisjonene er opptatte av, som et utgangspunkt for å;

- utvikle regelverket og tilby kompetansetjenester på internrevisjon (DFØ)
- bli bedre forvalter av fellesavtalen på internrevisjon (Difi)
- tilby kurs og relevante tema for nettverk statlig sektor (IIA Norge)

Her får du oversikt over hvilken aktør som kan hjelpe deg med hva på 45 sekunder
https://www.youtube.com/watch?v=8L1GFxR8lWY
Se også https://dfo.no/fagomrader/internrevisjon

DFØ, Difi og IIA Norge får også en felles kanal for å nå ut til de statlige internrevisjonene med informasjon i tillegg til de tradisjonelle kanalene som nettsider og nyhetsbrev.

MELD DEG INN VIA WWW.FACEBOOK.COM – INTERNREVISJON I STATEN

Har dere noen spørsmål eller innspill til oss som administrerer gruppen?
Ta kontakt med Christine Vik i DFØ (e-post: christine.vik@dfo.no, tlf: 95735629)

Generalsekretæren informerer

AV ELLEN BRATAAS

DIGITALISERING AV FORENINGENS AKTIVITETER OG MØTEPLASSER

Selv ikke et sekretariat med tre ansatte kan unngå å legge merke til at mye automatiseres og digitaliseres rundt forbi. Vi har opprettet en «IIA Academy» app der våre fremtidige e-læringskurs skal legges. Målet er at kursene skal bli så bra at vi kan få til et samarbeid med de andre nordiske landene og tilby flere moduler på tvers av landene. Hvis vi i tillegg kan klare å strømme flere av våre egne aktiviteter, er vi sikker på at dette vil øke tilgjengeligheten av tilbud, spesielt for medlemmer utenfor Oslo.

Vi er også på brainstormingsstadiet om å dele informasjon via korte filmsnutter og en egen podcast, samt skape et digitalt rom der medlemmer kan møtes. Det digitale rommet behøver nødvendigvis ikke bare være for norske medlemmer, men på sikt et sted man kan diskutere fritt med andre, uavhengig av landegrenser.

VERKTØYKASSE FOR INTERNREVISOR

Vi har samlet eksempler og maler som benyttes av internrevisjoner rundt om i Norge og lagt samlingen i en egen «verktøykasse» på medlemssiden. Vi håper innholdet vil være til hjelp for nyetablerte internrevisjoner i tillegg til å kunne være en kilde til inspirasjon for internrevisjoner som har vært etablert en stund. Eksemplene er hentet fra både privat og offentlig sektor og må tilpasses den enkelte organisasjon. De fleste maler er på norsk med innslag av noen engelske på enkelte områder.

Hjelp oss å utvide omfanget av verktøy: om du har maler/eksempler som kan deles, vil foreningen anonymisere tilsendte maler før de legges ut her. Materiale kan sendes til post@iia.no.

NYTT KRAV FRA 2018 – TO ETIKKRELATERTE CPE-POENG

IIA globalt har besluttet at fra og med 2018 må alle innehavere av IIA-sertifiseringer kunne rapportere at 2 CPE-poeng er relatert til etikk. Mange har allerede etikktrening på jobben, men også enkelte aktiviteter i IIA Norges regi vil relateres til etikktrening slik at sertifiserte skal kunne oppfylle det nye kravet.

COSO ERM SAMMENDRAGET OVERSATT TIL NORSK

Det har vært en formidabel utvikling i fagområdet risikostyring siden 2004 da COSOs første rammeverk for integrert risikostyring først ble utgitt, og i 2017 ble rammeverket utgitt i en oppdatert utgave. Det oppdaterte rammeverket, som nå heter Helhetlig Risikostyring - Integrering med strategi og måloppnåelse, understreker viktigheten av å vurdere risiko både i strategiprosessen og i arbeidet med å fremme måloppnåelse.

Foreningen har valgt ikke å oversette hele rammeverket til norsk, men Fag- og metodekomiteen har oversatt sammendraget i norsk språkdrakt. Den norske versjonen presenteres på frokostmøte 6. juni hos Deloitte i Oslo.

EGEN FACEBOOK-GRUPPE FOR STATLIGE INTERNREVISJONER

DFØ har etablert et forum for internrevisjoner i statlig sektor på en lukket Facebook-gruppe der medlemmer kan stille hverandre spørsmål og komme med råd, tanker og innspill.

Ansatte i Direktoratet for økonomistyring (DFØ), Direktoratet for forvaltning og ikt (Difi) og IIA Norge er også medlem i gruppen og bidrar gjerne inn i avklaringer og diskusjoner.

OPPDATERING AV VEILEDERNE

Både Veileder for Compliancefunksjonen utgitt i 2015 og Veileder for Risikostyringsfunksjonen utgitt i 2017 vil bli oppdatert i år. Dette for å ivareta utvikling i funksjonene, samt reflektere oppdaterte rammeverk som COSO ERM og ISO 31000.

KONFERANSER VERDT Å MERKE SEG

ECIIA Conference, 3. – 5. October 2018, Madrid, Spain
GRC-dagen, 11. oktober 2018, Oslo
Nasjonal Fagkonferanse i offentlig revisjon, 23. oktober 2018, Lillestrøm
IIA's International Conference, 7. – 10. July 2019, California, USA

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

The Institute of Internal Auditors | Global

VI GRATULERER FØLGENDE MEDLEMMER

Diplomert internrevisor
Per Christer Nielsen Dale, PwC AS
Katharina Erlandsen, Sparebank 1 SMN
Ida Zahl Jenssen, DNB Bank ASA
Hallstein Klimpen, Sparebank 1 SMN
Ingar Leiksett, Lørenskog kommune
Dina Robsrud, Akershus universitetssykehus
Elin Rønningen, Utenriksdepartementet
Morten Skogum, Riksrevisjonen
Miriam Tesfaghiorghis, Statens vegvesen
Marit Trodal, IIA Norge

Certified Internal Auditor (CIA)
Elisabeth Danbolt, Nordea Bank AB
Felipe Leandro Alves Pereira, National Oilwell Varco Norway AS
Veronica Storlid Kvinge, BKK AS
Sigve Økland, Forsvaret

NY STRUKTURERING AV INNHOLDET PÅ CIA-EKSAMEN FRA 2019

IIA globalt jobber for tiden med å gjøre om på innholdet i de tre delene av CIA eksamen. Den største endringen blir selve omstrukturering av innholdet i de tre deleksamenene. Til glede for mange kan nevnes at innholdet i del tre vil bli mindre omfattende. Den nye strukturen skal etter planen lanseres fra begynnelsen av 2019. For mer informasjon, se CIA Exam Syllabi Revision.

NYE VEILEDERE OG GUIDANCE FRA IIA

PRACTIC GUIDE, Financial Sector: AUDITING MODEL RISK MANAGEMENT
The growing dependence of organizations on quantitative analytical models has brought increased regulatory attention to effective model risk management (MRM). As regulatory scrutiny around model risk management increases, the internal audit activity plays a key role in assessing an organization's MRM framework.

The Institute of Internal Auditors | Global

This guidance provides an overview of the internal audit activity's responsibilities related to MRM and describes methods and processes internal auditors can use to review the design, implementation, and operation of their organization's MRM framework.

PRACTICE GUIDE: COORDINATION AND RELIANCE – DEVELOPING AN ASSURANCE MAP

The purpose of assurance activities is to provide an objective and independent assessment on governance, risk management, and control processes for the organization. Assurance maps offer a visual representation of the organization's risk coverage, and help identify gaps and overlaps. This practice guide takes the reader through the process of documenting assurance activities throughout an organization.

WHITE PAPER FROM IIA AUSTRALIA: GOOD PRACTICE INTERNAL AUDIT REPORTS

There is no prescribed standard or quality expectation for internal audit reports, or a list of what is required to be contained in an audit report, apart from what the relevant 2400 series Standards say. So, reports can vary considerably in the way audit results are presented. How can Internal Audit better report on the results of audits? This White Paper from IIA Australia look into good practice internal audit reports.

THE FUTURE OF CYBERSECURITY IN INTERNAL AUDIT

This joint research report effort from the Internal Audit Foundation and Crowe Horwath sheds light on how internal audit is adapting to overcome new and ever-changing risks to cybersecurity.

The report uses the survey responses to draw attention to key areas internal audit should focus on to successfully address cybersecurity concerns. Highlights include relationship building, goal setting for cybersecurity audit programs, and the increasing role of cybersecurity programs within the internal audit function.

AUDITING IT GOVERNANCE

Internal audits of IT governance should focus beyond the implementation of governance practices. Internal audit adds value to the organization by assessing the effectiveness of IT governance components, and providing assurance to stakeholders that principles and practices are followed and working as intended.

This GTAG has been updated to reflect the 2017 International Professional Practices Framework and to be more directly practical to internal auditors. This edition provides tools and techniques to help internal auditors build a work program and perform engagements involving IT governance.

SPECIAL THREE-PART SERIES: ARTIFICIAL INTELLIGENCE, INTERNAL AUDIT'S ROLE AND INTRODUCING A NEW FRAMWORK

This special three-part edition of Global Perspectives and Insights explores internal audit's role in Artificial Intelligence by discussing associated risks and opportunities. The papers also introduces an AI Auditing Framework comprised of six components, all set within the context of an organization's AI strategy.

Part 1: Artificial Intelligence – Considerations for the Profession of Internal Auditing
Part 2: The IIA's Artificial Intelligence Auditing Framework, Practical Applications, Part A
Part 3: The IIA's Artificial Intelligence Auditing Framework, Practical Applications, Part B

Loven fra toppen

Vi har kommet omtrent halvveis i året og så langt har 2018 vært så begivenhetsrikt at jeg må ta en pust i bakken og gjøre opp status: Hva skjer? Hvor er vi egentlig på vei?

Her kunne det vært fristende å ty til 'gudene vet' men jeg holder meg unna religion. Risikoen for å krenke noen er betydelig og det vil jeg helst unngå. Men her er vi inne på en trend! Etter flere år med fokus på dilemmatrening og opplæring i etiske problemstillinger så tror jeg behovet for opplæring i krenkelser er på rask fremmarsj. Å krenke loven er en ting, men for tiden er det også mye snakk om å føle seg krenket. Hvordan føler man seg da?

En krenkelse er en opplevelse av urettferdighet som er relatert til vår identitet og våre moralske følelser. Erfaringen av krenkelse er derfor både kognitiv og emosjonell. Tenk bare H&M og deres barnekolleksjon, med en afroamerikansk gutt ikledd genser med trykket 'coolest monkey in the jungle'. Enkelte skjønte ikke problemet, mens andre reagerte kraftig og følte seg krenket. Det som er greit for meg er kanskje ikke greit for deg. Ta et annet eksempel: Jeg er kvinne. En sen lørdagsnatt mottar jeg en melding via Messenger fra en politiker på hyttetur med gutta fra partiet. Meldingen jeg mottar er seksuelt ladet. Hvordan reagerer jeg?

A: Jøss… er han full eller?

B: Lavmål! Jeg trodde Trump var alene om den slags ytringer…

C: Hva i all verden får han til å skrive noe så ufint til meg?

Hvordan ville du reagert? Poenget er at en følelse av å føle seg krenket er høyst subjektiv og avhenger i tillegg av konteksten. Hvem var han sammen med? Hvorfor var jeg tema? Hvem sendte den? Ja, den som hadde visst det. Å ta ansvar for sine handlinger er ikke så trendy i 2018. Det som er populært nå er å klamre seg fast til maktposisjoner selv om man for eks. har hatt ansvar for et stort byggeprosjekt på Stortinget som har gått skikkelig i ball. Det var ikke min skyld! Men for all del; det er alltid fint med konkrete eksempler til bruk i opplæring både på jobb og hjemme, så jeg tar det rett inn i oppdragelsen og legger det frem over middagsbordet. Min opplevelse er at unger tar det raskt. De forstår hva som er greit og ugreit. Du skal ikke skylde på andre er barnelærdom. Tilsvarende gjelder for unnskyld.

Apropos Stortinget.

Denne ærverdige institusjonen ble tidligere i år anklaget for å ha blitt en barnehage. Den ministeren som stod bak anklagen vekket mye harme, og ikke da fra først og fremst fra sine kolleger på tinget. Nei, det var barnehagepersonell som da kom på banen og følte seg krenket. Tusenvis av barnehagebarn kunne også følt seg krenket om de hadde fulgt med i det politiske ordskiftet, men de hadde bedre ting å gjøre; inkludere hverandre i leken, lære om gjenvinning, vise omsorg for vennen som falt av huska og sånn. Russebuss hadde nok uansett vært en mer treffende beskrivelse, selv om det sikkert også hadde ført til motbør og debattinnlegg fra krenket russ. Det er strengt tatt flere likhetstrekk mellom en rekke av våre topppolitikere og russen. Russen er aktiv på sosiale medier, fester og gjør en rekke til dels upassende ting. I barnehagen er de ikke en gang på Facebook.

Seksuell trakassering har også vært i skuddet så langt i år med Metoo-kampanjen. Det er ikke rent få lunsjpauser som har gått med til å diskutere hva som er passende og mindre passende oppførsel på arbeidsplassen. Også her har en rekke norske politikere bydd på seg selv, til inspirasjon og bruk i den videre bevisstgjøringsprosessen. Hvor går grensen mellom 'å sjekke opp' damer eller unge herrer og 'maktmisbruk'? Her kan nok enkelte lett gå i surr, men en grei huskeregel er å ikke drive med sjekking i jobbsammenheng – rett og slett! Det kan oppleves som noe intenst å bli sjekket opp av en politiker fra partiledelsen i arbeidstiden. Hva så med å sjekke opp utenom arbeidstiden? Det kan være lurt å tenke hvilken rolle folk opplever at du har når du møter dem. Er du på jobbreise i din kapasitet som minister? Er du gjest i et privat bryllup? Uansett er et lite eller moderat alkoholinntak å anbefale.

Krenkelser, trakassering, diskriminering, maktmisbruk – dette er begreper vi vil bli enda mer kjent med i tiden fremover. Det kan bli litt av en øvelse å håndtere varslingskanaler fremover, ettersom det er en del rom for tolkninger innenfor dette begrepsapparatet. Lykke til!

Til slutt; Vi kommer ikke unna digitalisering, automatisering og teknologi, temaer vi har fått proppet ørene fulle av. Intet aktivt medlem av IIA Norge har vel unngått å få med seg disse temaene så langt i 2018? Det samme gjelder personvern og GDPR. Her har vi endelig noe konkret å forholde oss til hva gjelder krenking. Mitt personvern skal fra 1. juli ikke krenkes! I så fall kan det vanke klekkelige bøter til den virksomheten som ikke oppfyller kravene.

Jammen godt at noe er håndfast og på plass – snart…

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