SIRK

Styring – Internrevisjon – Risiko – Kontroll

Nr 1 2019

IIA Norge

REDAKTØRENS SPALTE

ELLEN BRATAAS

De fleste artiklene i SIRK berører risikostyringens mange fasetter. Risiko er strategi – strategi er risiko. Endring og innovasjon skaper risiko, men tilsvarende gjelder for valget om å fortsette i samme spor som tidligere. I artikkelen om merverdi kan du lese at forventinger til internrevisjonen er økende. Som internrevisor er det ikke godt nok å påpeke at en bygning brenner. Det forventes at internrevisjonen skal påpeke at risikoen for brann i bygget er stor slik at virksomheten kan håndtere risikoene før det begynner å brenne.

Ingen som jobber med virksomhetsstyring er synske, så hvordan kan funksjoner som compliance, risikostyring og internrevisjon jobbe for å bli mer forutseende og svare opp de forventinger interessentene har?

Det er sikkert mange svar på et så stort spørsmål, men tips som gikk igjen i flere foredrag på årskonferansen i mai, var at vi som enkeltpersoner må være villige til å prøve nye ting og tørre å gå ut av egen komfortsone. «Flaks er ikke tilfeldig, men et resultat av nysgjerrighet», som en foredragsholder så godt sa det. Ved å angripe en problemstilling på en annerledes måte, spørre andre til råds enn de man jobber med, være nysgjerrig og samtidig modig, er sannsynligheten for positive overraskelser stor. Og så får man heller tåle at ikke alt blir like vellykket hver gang.

Vi håper du finner ny inspirasjon i denne utgaven av SIRK – god lesing og god sommer!

STYRELEDER HAR ORDET

METTE STORVESTRE
STYRELEDER
IIA NORGE

Sommeren står for døren og IIA Norge stiller tradisjonen tro med spennende og relevant lesestoff i denne utgaven av SIRK.

Jeg vil benytte anledningen til å takke alle dere som stiller opp for IIA Norge og raust deler kunnskap med andre – enten som bidragsytere til SIRK, på våre mange nettverksmøter, kurs og ikke minst årskonferansen.

På årets IIA konferanse bidro en rekke IIA-ere ikke bare til den faglige delen, men også til det sosiale programmet.

Første dag bød på et overraskende innslag med dans fra scenen og under middagen på kvelden fikk vi høre historier fra et langt liv innen internrevisjon fra en av våre mest dedikerte influencere (les 'Just a song before I go' lenger bak i bladet), etterfulgt av bandet 'Wrong Direction' - IIAs eget boyband. Det ble stående ovasjoner, etterfulgt av litt skuffelse over at bandet kun hadde en låt på repertoaret. Vi satser på at bandet har flere låter på lager til neste års konferanse og at kreativiteten og iveren etter å bidra fortsetter å blomstre i IIA. Vi har godt av å bevege oss ut av komfortsonen – både på den faglige og sosiale arenaen. Det blir jo mye gøy av det også!

Takk til alle dere som bidrar til at IIA Norge er et så levende nettverk!

På vegne av styret i IIA Norge ønsker jeg dere god lesning og en riktig god sommer!

MEDIEKOMITEEN

Ellen Brataas
Generalsekretær
IIA Norge

Reidar Døli
Komiteens leder
Internrevisor,
Oslo Børs VPS

Martin Stevens
Internrevisor,
Gjensidige Forsikring

Ola Otterdal
Seniorrådgiver
Politiet

Esa Leporanta
Operational Risk Officer,
DNB Bank ASA

Marit Trodal
Prosjektleder, IIA Norge

Årsabonnement: Kr. 150

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

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

Grafisk produksjon:
Merkur Grafisk AS

Trykksak
2041 0672

Forsidebilde:
Foto: corgarashu/shutterstock.com

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.

INNHOLD

RISIKOSTYRING

COMPLIANCE

VIRKSOMHETSSTYRING

63

68

52

28

34

KONTROLL OG SIKKERHET

INTERNREVISJON

FASTE SPALTER

Adferdsøkonomi i regelverk og compliance arbeid.
Kan vi dytte mer for å sikre større grad av etterlevelse?

ANN CHRISTIN FLATLAND
Data Privacy Coordinator i EVRY, dipl.ir. og medlem av Nettverk Compliance i IIA Norge

JESSICA LÅNGBERG
Senior Konsulent i Transcendent Group, CIPP/E, ISO 27001 Lead Implementer

Eksterne[1] og interne[2] regler og krav kan være sammensatte og kompliserte å forstå. Selv om de fleste ansatte er godt opplært i å etterleve reglene, ser vi at enkelte likevel ikke handler rasjonelt eller riktig når de står overfor handlingsalternativer i en hektisk hverdag. Spørsmålet vi derfor stiller oss i denne artikkelen er hva som gjør at vi i praksis etterlever regler og om reglene kan utformes slik at det er større sannsynlighet for å oppnå faktisk etterlevelse?

Artikkelforfatterne har begge arbeidet med implementering av endringer i personvernkravene[3] som trådte i kraft medio 2018. Vi erfarte at organisasjonene jevnt over var positive til begrunnelsen for spesifisering av kravene og la ned mye arbeid i å sikre etterlevelse, men at det var to forhold som ble trukket frem som vanskelige. Det ene var å faktisk forstå de komplekse reglene. Det andre hvordan organisasjonene kan sikre etterlevelse under en allerede hektisk arbeidsdag. Disse observasjonene gjorde oss nysgjerrige på fagfeltet adferdsøkonomi[4] og om det er mulig å hente inspirasjon herfra som kan sikre mer effektiv og faktisk etterlevelse?

I denne artikkelen vil vi gå gjennom noen av våre innledende refleksjoner[5], og håper det kan skape nysgjerrighet, debatt og forskning rundt bruk av metoden i compliance-arbeidet fremover.

Hva er adferdsøkonomi?

Adferdsøkonomien har sin opprinnelse i B.F. Skinners forskning og ble videreforedlet av nobelprisvinner i økonomi Daniel Kahnemann. Prinsippene er gjengitt i bestselgeren hans «Thinking Fast and Slow» som kom ut i 2011. Boken oppsummerer hans forskning og kan gi verdifull innsikt og forståelse av prinsippene som ligger bak adferdsøkonomisk tenkning, men ga oss ikke så mange praktiske råd og tips som er direkte anvendelige i vårt daglige arbeid. Vi har derfor søkt praktisk hjelp i to bøker utgitt av to rådgivere innenfor dette området, Morten Münster[6] og Jon Ivar Johansen[7].

Johansen slår i sin bok fast at 90 % av alle endringer mislykkes, selv om 90% på

[1] *Lov, forskrift og pålegg fra offentlige myndigheter.*
[2] *Policy, prosesser, rutiner mv.*
[3] *Lov om behandling av personopplysninger og den europeiske General Data Protection Regulation (GDPR)*
[4] *I følge Store Norske Leksikon «Adferdsøkonomien er en retning innen økonomifaget som trekker på innsikter fra blant annet psykologifaget. Den modifiserer standardantakelsene i økonomisk teori gjennom å anta begrenset rasjonalitet og andre motiver enn snever egeninteresse».*
[5] *Våre referanser peker på sekundær litteratur vi selv har gått gjennom og mangler blant annet referanser til forskningsartikler og primærkilder.*
[6] *«Jytte fra Marketing er desværre gået for i dag» utgitt i Danmark 2018 (heretter forkortet til Jytte).*
[7] *«Mestringskoden» utgitt i Norge i 2015.*
[8] *Se Mestringskoden side 67.*

Hverdagsdytter, de gule linjene på togstasjonen holder oss på sikker avstand fra togsporene

forhånd tror de vil lykkes. Dette er nedslående tall og mange vil nok ha vansker med å akseptere denne påstanden. Gjennom nysgjerrige søken i adferdsteorien har vi lært at vi må akseptere at hjernen vår er skrudd sammen slik at vi ønsker å opprettholde status slik den er akkurat nå. Vaner og «slik har vi alltid gjort det» ligger i ryggraden vår, enten vi vil innrømme det eller ikke.

Hjernen synes ifølge Johansen det er enklest for oss å gå på autopilot[8] da dette gir en følelse av kontroll og kjennes trygt. Endringer derimot krever energi og kjennes utrygt. Gjennom autopiloten tar vi for eksempel raske valg i trafikken basert på innøvde vaner og det vi har erfart som bilfører. På jobb og hjemme gir vi raske svar på spørsmål vi blir stilt basert på hva vi allerede vet om et tema. Autopiloten kjennetegnes av at den automatisk og raskt kommer til en konklusjon «with little or no effort and sense of voluntary control» (thinking fast)[9], samt at den lar seg friste av umiddelbar belønning og unngår ubehag. Den automatiserer og handler basert på vaner.

Betyr dette at vi rett og slett kan omkode autopiloten til å gjøre de riktige tingene automatisk?

For å gjennomføre endringer og løse kompliserte oppgaver krever det at vi mobiliserer selvkontrollen[10]. Selvkontrollen kommer på banen når vi gjennomfører tyngre tankearbeid, øver inn nye vaner eller ferdigheter og assosieres med «subjective experience of agency, choice, and concentration» (thinking slow)[11]. Selvkontrollen er reflekterende og søker å motstå umiddelbar belønning og fristelser og setter langsiktige mål, samt lager planer for å oppnå langsiktige belønninger.

Mange har nok kjent på at for å få til «den der kroppen til sommersesongen som vi drømmer om hvert år» er det egentlig ikke så mye mer enn sunn mat og god trening som skal til. Likevel står vi der hver sommer og lurer på hvor tiden til å trene ble av. Hverdagen går sin gang og så lenge trening og sunn mat ikke er en del av vår «autopilot», og vi heller ikke har klart å mobilisere selvkontrollen, vil vi mest sannsynligvis ikke oppnå noe forandring i år heller.

En dytt i riktig retning

Så hvordan kan vi få selvkontrollen til å hjelpe oss med å endre vaner eller iverksette nødvendige tiltak, dersom vi egentlig ikke er motivert eller har tid? Her har forskerne etter hvert kommet frem til at vi kan designe såkalte dyttere (fra det engelske «nudges»)[12]. Dette hjelper oss med å nå våre mål, når vi synes det er mer behagelig å «fortsette som før» og la autopiloten styre.

Ved å designe smarte dyttere, som gruppen eller individet tar eierskap til, vil vi kunne arbeide mer effektivt og sikre høyere grad av måloppnåelse. Münster gjentar også flere ganger i sin bok at man må ta utgangspunkt i det virkelige liv og ikke designe noe vi tror vil fungere sett fra skrivebordet[13].

Han trekker blant annet frem et eksempel fra et selskap hvor avfallssortering i produktlinjen var svært viktig. Selskapet hadde laget en Standard Operating Procedure (SOP) for hvordan sorteringen skulle gjøres, herunder hvilket avfall som skulle i hvilken beholder. Prosedyren hadde blitt omskrevet hele 18 ganger, men uten synlige forbedringer i selve gjennomføringen eller faktisk etterlevelse av prosedyren. SOP´en ble også kommunisert og medarbeiderne ble trent i hvordan sorteringen skal gjøres, men dette hadde fortsatt ikke merkbar effekt. Münster mener at en slik prosedyre er laget for selvkontrollen og ikke for autopiloten, siden man i eksemplet satt ved pulten og designet den uten å sjekke hva som fungerer i det virkelige livet.

Etter en vurdering av adferden ved samlebåndet gjorde man noe så enkelt som å sette

[9] Kalles system 1 i Kahnemanns «Thinking Fast and Slow».
[10] Jon Ivar Johansen side 65 flg.
[11] Kalles system 2 i Kahnemanns «Thinking Fast and Slow».
[12] «Nudge» har blitt et atferdsøkonomisk begrep for tilrettelegging som får oss til å gjøre ting vi vet er riktig på en bestemt måte. Ordet kan oversettes med «dytter» eller «dult» og er blant annet beskrevet nærmere av Professor Richard H. Thaler som vant Nobelprisen i økonomi i 2017.
[13] Se for eksempel side 102 i Jytte om «Skrivebordets arrogance».
[14] Se Jytte side 141-142.
[15] Mestringskoden side 90-91.

bilder av de forskjellige typene av avfall på de ulike beholderne for å gjøre sorteringen enklere. Dette hadde mye større effekt enn alle omskrivninger av SOP´ene! Det kan høres banalt ut, men en liten dytt i riktig retning kan noen ganger føre til større effekt enn hundrevis av timer med trening og lange dokumenter.[14]

Relevante dyttere i compliance arbeidet

Ifølge Johansen kan vi dele dyttere inn tre hovedkategorier[15]:

1. Individuelle dyttere som er det du selv gjør for å påvirke egne forventninger, ubehag og stress og dermed unngå at du havner i komfortfellen og fortsetter på autopilot.

2. Sosiale dyttere som er andres forventninger til deg, eksempelvis pasientgrupper som hjelper deg med å ta sunne valg etter en operasjon, sprintmøter hver morgen under utvikling av et nytt produkt eller deltakelse i lederprogram.

3. Systemer og tekniske dyttere som kan være alt fra lover og regler, mindre tallerkener slik at du spiser mindre, SMS-varsel fra frisøren, smartklokker som måler aktivitet til innebygget personvern.

Alle disse hovedkategoriene er relevante å vurdere nærmere ved tilrettelegging av tiltak som skal sikre etterlevelse. Nedenfor skal vi se nærmere på «innebygget personvern» for å illustrere hvordan et system eller teknisk dytter kan være relevant ved etterlevelse av personvernregler.

Vi vil imidlertid først understreke at bruk av dyttere kan ha en etisk side som alltid bør vurderes, slik at ingen føler at de blir lurt til å gjøre noe som de oppfatter som uetisk eller uforsvarlig. Vi mener at så lenge man er åpen om virkemidlene, inkluderer de man ønsker å dytte i valg av akseptable dyttere, og samtidig sørger for en etisk etterprøving, er det både viktig og riktig å ta i bruk dette virkemiddelet for mer effektiv implementering av krav.

Innebygget personvern som eksempel på system eller tekniske dytter

Innebygd personvern har vokst frem gjennom beste praksis[16] og lovgiver har i forbindelse med de nye personvernreglene vedtatt prinsippet som system eller teknisk dytter. Reglen[17] er laget slik at den skal sørge for at vi tar hensyn til personvernet i alle utviklingsfaser av systemer, prosesser eller løsninger. Målet er at informasjonssystemene skal oppfylle de sentrale personvernprinsippene og ivareta de registrertes rettigheter. Innebygd personvern kan også sies å være en såkalt sosial dytter da brukeren og offentligheten forventer personvern i tillegg til brukervennlighet og tilgjengelighet.

Innebygd personvern har syv sentrale elementer[18]:

1. Forebygge fremfor å reparere.
2. Personvern som standardinnstilling istedenfor at bruker selv må sikre at innstillingene slås på.
3. Personvernet tenkes inn i designet gjennom funksjonalitetsbeskrivelse, arkitektur og forretningspraksis.
4. Full personvernfunksjonalitet fra start istedenfor å gjøre endringer etter at systemet er ferdig.
5. Sikkerhetsvurderinger er en del av løsningen og vurderingene fra start til slutt
6. Åpenhet om hvordan løsningen fungerer og hvordan den registrerte skal kunne ivareta sine rettigheter
7. Personvern gis høy prioritet.

I tillegg til å ivareta personvernet sørger prinsippene, sjekklister og veiledninger fra Datatilsynet, ICO med flere andre tilsynsmyndigheter at vi får et robust sluttprodukt og hjelp til å ta riktige valg og beslutninger underveis i utviklingen. Kravene er imidlertid ikke entydige og virksomhetene bør nok designe egne interne, mer spesifikke dyttere. Dette kan være rutiner og sjekklister som bidrar til at virksomheten automatisk og mer effektivt gjør de riktige og viktige vurderingene, så som implementering av dataorienterte og/eller prosessorienterte designkrav. Med referanse til avfallshåndteringseksempelet ovenfor er det også viktig at de som skal gjennomføre handlingen er med å designe rutinene og sjekklistene slik at de er tilpasset deres daglige gjøremål og ikke kun blir en skrivebordsøvelse.

Dataorienterte designkrav handler om å:

- Minimere og begrense antall personopplysninger («select before you collect»)
- Gjemme og skjule (kryptering, pseudonymisering mv)
- Separere (dele opp lagring slik at man for eksempel unngår å lage komplette profiler)
- Aggregere data (lage statistikk istedenfor individuell informasjon)
- Implementere standardinnstillinger som ivaretar personvernet (for eksempel aktivt velge om man vil dele informasjonen istedenfor å måtte skru av deling av informasjon med andre applikasjoner)

> Gjennom å bruke adferdsøkonomiske prinsipper i compliance-arbeidet har vi større sjanse for å oppnå faktisk etterlevelse

Prosessorienterte designkrav handler om å:

- Gi god informasjon (standardmaler, ikoner, bilder, symboler) som gjør det enkelt å forstå hva man må selv må gjøre.
- Gi den registrerte mulighet til å kontrollere egne opplysninger via en sikker nettside/app.
- Beskrive/vise hvordan regelverket håndheves og dokumenteres

Adferden eller handlingen man ønsker at skal skje må være enkelt og tydelig beskrevet og/eller implementert i systemet eller prosessen slik at det ikke er tvil om hva som forventes av den enkelte. Det er derfor kanskje bedre med en one-pager med ti kulepunkter enn et memo på ti sider?

Nedenfor vil vi illustrere dette med to konkrete eksempler:

Sending av e-post til feil mottakere blir nevnt som avvik som er meldt til Datatilsynet i 2018[19]. Ett slikt brudd er normalt mer kritisk dersom det sendes til en ekstern mottaker, dvs. utenfor egen virksomhet. Det finnes imidlertid en innstilling i Outlook som gjør at brukeren får opp et lite varsel hver gang vedkommende skriver inn en e-postmottaker som er utenfor egen organisasjon. Dette vil ikke direkte hindre vedkommende i å sende e-posten, men vil kanskje være en dytter som gjør at man reagerer på at det ikke er denne mottaker mailen skulle sendes til?

Et annet eksempel er tekniske dyttere som kan hjelpe oss slik at vi slipper å huske hele informasjonssikkerhetspolicyen og kravene til klassifisering av informasjon. «Azure protection» er et kjent eksempel fra Microsoft som gjør det mulig å legge inn virksomhetens klassifisering direkte i et dokument eller e-post og dokumentet blir automatisk beskyttet. Dvs. at hvis du har valgt å merke et dokument som «konfidensielt», og sender til en ekstern mottaker vil han eller hun for eksempel ikke kunne åpne dokumentet med mindre du spesifikt har gitt tilgang til det på forhånd.

Vil adferdsøkonomi kunne revolusjonere compliance arbeidet?

En dytt i riktig retning er et adferdsøkonomisk prinsipp som begynner å bli mer vanlig også i det norske samfunnet. Innebygd personvern er et eksempel på en tilrettelegging av reglene, slik at virksomhetene må implementere tekniske og organisatoriske tiltak (interne regler) som automatisk sikrer etterlevelse av personvernreglene. Finanstilsynet i Norge har for eksempel tatt dette i bruk i pålegget de ga kredittkortselskapene om innholdet i fakturaen som sendes til kundene. Kredittkortselskapet anmodes om å skrive hele beløpet kunden skylder på fakturaen og ikke kun minimumsbeløpet som tidligere. Denne grunninnstillingen gjør det lettere for kunden å ha oversikt over total gjeld.

Vi tror også at gjennom å bruke adferdsøkonomiske prinsipper i compliancearbeidet gjennom å forenkle de interne prosessene og prosedyrene, har vi større sjanse for å oppnå faktisk etterlevelse. Ønsket adferd og faktisk etterlevelse kan vi oppnå ved å designe kontroller (dyttere) som virker i praksis og ikke kun blir «skrivebordsregler». Dersom bekreftelsesfunksjonene[20] plasserer eierskap til å gjennomføre adferdsendringen hos enkeltindividet/gruppen i den delen av organisasjonen man ønsker å gjennomføre endringen i, er det større sannsynlighet for at vi unngår skrivebordsøvelser og at enkeltindividet og/eller organisasjonen faktisk gjennomfører den nødvendige endringen. Det er enkeltindividene som sitter med nøkkelen til å påpeke de faktiske hindringene, komme med forslag til dyttere som virker og som ved å delta i utarbeidelsen motiveres til å gjennomføre tiltakene. Ikke så ulikt det vi ellers opplever under forankring av revisjonsfunn, men her rettet mot adferdsendringer som påvirker gjentatt faktisk etterlevelse over tid. Bruk av dyttere handler med andre ord om å tilrettelegge for adferd som er ønsket og ansett som riktig, men altså vanskelig å få til i praksis.

Bruk av dyttere handler om å tilrettelegge for adferd som er ønsket og ansett som riktig, men altså vanskelig å få til i praksis

[16] *https://www.datatilsynet.no/globalassets/global/english/7foundationalprinciples_anncavoukian2.pdf*
[17] *Innebygd personvern, jf. GDPR artikkel 25.*
[18] *Se fotnote 13.*
[19] *Se tilsynets årsrapport for 2018 side 14.*
[20] *Med bekreftelsesfunksjon mener vi eksempelvis internrevisjon, samt risiko, compliance, kvalitet og internkontrollfunksjoner i andre linje.*

Hvordan kan risikostyring bidra til bedre personvern i virksomhetene?

AV Y. AYSE B. NORDAL
B Sc. og M Sc. METU, Licentiat NHH
Fagansvarlig for risikostyring og planlegging i Undervisningsbygg Oslo KF

Personvern handler mye om å ha god risikostyring. Dette er bakgrunnen til et nylig avholdt Round table diskusjonsmøte i Nettverk risikostyring i regi av IIA Norge, der jeg innledet til diskusjon, og min innledning til møtet danner bakgrunnen til denne artikkelen.

Informasjon har verdi. Den har verdi for virksomhet og den har verdi i forhold til den enkeltes behov for personvern. Rollen til Risikostyringsfunksjon er som ellers å bistå organisasjon i å ha et trygt opplegg for å forvalte denne verdien.

I artikkelen vil jeg først knytte alminnelig risikostyringsbegrepsapparat, -metoder og -verktøy sammen med lovgivningens bestemmelser. Deretter vil jeg foreslå en rekke spørsmål som virksomhetene bør stille seg for å sikre riktig bidrag fra risikostyring til personvernarbeidet.

Risikostyring, vårt begrepsapparat, metoder og verktøy

De aller fleste som arbeider med risikostyring i dag benytter en standard eller et rammeverk som innebærer innføring av *helhetlig risikostyring,* eksempelvis ISO 31000:2018 og COSO ERM: 2017. Det er også vanlig å benytte COBIT (Information System Control Standard), ITIL (Information Technology Infrastructure Library) eller ISO/ IEC 27001 (ledelsessystem for informasjonssikkerhet) for å sikre bruk av beste praksis i struktur, drift og utvikling på IKT-området.

ISO 31000:2018 og COSO ERM:2017 har følgende felles trekk:

- Risiko forbindes med virkningen av usikkerhet på måloppnåelsen. Usikkerheten kan være negativ, positiv, eller begge deler. Risikostyrer bør være like opptatt av «muligheter» som av hendelser som «kan gå galt».
- Risikostyring benyttes til å skape og å beskytte verdier.
- Risikostyring bør være integrert i alle strategiske, taktiske og operasjonelle beslutningsprosesser. [1,2]

Figur 1 Metoder som kan benyttes i arbeidet med helhetlig risikostyring

I sitt arbeid med helhetlig risikostyring har risikoleder anledning til å benytte *mange ulike metoder og verktøy* for kontekstanalyser, risikoidentifisering, risikovurdering -og håndtering. Figur 1 gir en oversikt over slike muligheter.

I tillegg kan risikoleder benytte 3-faktormodellen for å vurdere *verdier, trusler og sårbarhet* når objektsikkerhet, personsikkerhet eller informasjonssikkerhet står på dagsordenen.

Ny personvernlov med GDPR i vedlegg

Lov om behandling av personopplysninger med GDPR (General Data Protection Regulation) i vedlegg ble kunngjort den 15.06.2018, med ikrafttredelse 20.07.2018. GDPR[3] er en forordning og gjelder som norsk lov dvs. uten muligheter for lokale tilpasninger og omskrivninger som et direktiv skulle ha tillatt.

Risikoleder må forholde seg til de krav og formuleringer i loven inklusiv forordningen.

Lovens intensjon vedrørende risikostyring

I forbindelse med innføring av GDPR har European Commission utgitt publikasjonen «The GDPR: New Opportunities, New Obligations»[4]. For risikoledere har tittelen, med fokus på mulighetene, gitt assosiasjoner med helhetlig risikostyring. I publikasjonen nevnes det fem muligheter GDPR bringer til virksomhetene. En av disse er «risikobasert-tilnærming» som lover tilpasninger skreddersydd til virksomhetens risikobilde.

Lovens intensjon var å benytte risikostyring for å oppnå godt personvern bl.a. ved å dosere de tekniske og organisatoriske tiltak etter risikobildet.

Hva med lovens bokstav?

Begrepet risiko fremkommer i mange av de artiklene i forordningen. Forordningen fokuserer kun på «høy risiko» og «negative konsekvenser for fysiske personers rettigheter og friheter». Eksempler er:

Artikkel 24. Behandlingsansvarliges ansvar
Artikkel 25. Innebygd personvern og personvern som standardinnstilling
Artikkel 30. Protokoller over behandlingsaktiviteter, pkt.5
Artikkel 32. Sikkerhet ved behandlingen, pkt.1.
Artikkel 33. Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten, pkt.1

I alle disse artiklene leser vi følgende formulering:

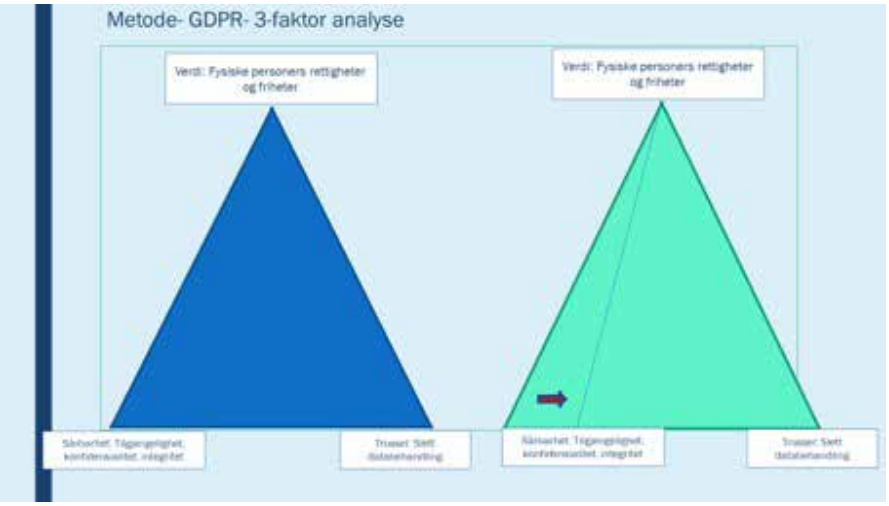
«…I det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sann-

synlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak…»

Forordningens Artikkel 32.2, pkt.2 omhandler egnet sikkerhetsnivå som impliserer bruk av 3-faktor modellen. Artikkelen lyder:

«…Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke–autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet….»

«Slett data behandling» er en trussel som påvirker tilgjengeligheten, konfidensialiteten og integriteten av personopplysninger og skaper negative konsekvenser for enkelte personers rettigheter og friheter. Ref. Figur 2.



Figur 2: 3-faktormodellen og egnet sikkerhetsnivå

Fokuset på «høy risiko» synliggjøres i Artikkel 35 Vurdering av personvernkonsekvenser, pkt.1 som sier:

«… Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og i det det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet….».

Dette er den mye siterte formuleringen om DPIA som virksomheter har høyt fokus på.

Kun i et tilfelle ser vi krav til helhetlig risikostyring i forordningen, i forbindelse med definisjon av personvernombudets oppgaver. Artikel. 39 pkt 2 sier at

«… Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, i det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i …»

Noen kritiske spørsmål for risikostyring og personvernsarbeid

Lovens bokstav åpner for følgende spørsmålsstillinger:

1. Benytter vi risikobasert tilnærming i vårt personvernarbeid og tilpasser våre tiltak til risikobildet etter tilstrekkelige analyser av intern og ekstern kontekst, størrelse av risikoer og muligheter, rotårsaker til disse i tillegg til en vurdering av eksisterende kontrolltiltak?
2. Fokuserer vi kun på «høy risiko og nedside»? Hva med å utnytte mulighetene som kan gi et bedre personvern til virksomhetene?
3. I vanlige risikoanalyser vurderer virksomhetene middelsstore (gul og oransje) risikoer etter kostnadene ved å mitigere dem. Mange ganger knyttes det proaktive tiltak til disse fordi virksomheten finner dette akseptabelt. Fokuserer vi kun på høy risiko i vårt personvernarbeid?
4. Benytter vi kun DPIA? Bruker personvernombudet tilstrekkelige verktøy for å identifisere, prioritere, analysere, evaluere og håndtere risikoene/mulighetene?
5. Har vi fokus på rotårsaker? Bruker vi analyser for å avsløre kritiske kontrollpunkter i våre prosesser?

Risikoleder bør være den egnede ressurs som kan besvare disse spørsmålene i en virksomhet og dermed sikre at personvernarbeidet får en riktig plass i virksomhetenes helhetlige risikostyring. Dette krever tett samarbeid med HR, IKT, Compliance, Juridisk og Kvalitetsmiljøene i virksomheten.

Avslutningsvis

Når personvernarbeidet gjøres som en del av helhetlig risikostyring inneholder det følgende elementer:

- *Vurderinger og analyser som identifiserer både risikoer og muligheter, risikokategorier og rotårsaker ved bruk av egnede verktøy. Disse analyser bør også omfatte manuell behandling av data. Virksomhetene bør utnytte mulighetene og innføre tiltak på «ikke høyrisiko» områdene hvis de finner preventive eller holdningsskapende tiltak fornuftige.*
- *3-faktor modell for å vurdere sårbarhet, tilgjengelighet og konfidensialitet*
- *DPIA etter en grundig vurdering av forhold som er beskrevet i Artikkel 35.*

Den nye personvern lovgivningen inneholder muligheter for å bruke kraftige bøter. Mange virksomheter fokuserer derfor på lovens bokstav i stedet for intensjonen. Det jobbes med å identifisere høy risikoområder, konsekvenser for de registrerte og DPIA. Dette bør ikke gå på bekostning av helhetlig risikostyring. Når fokus på intensjonene av GDPR er premissgivende for arbeidet med personvern, ikke frykten for bøter, betyr det at risikostyringen lyktes i virksomheten.

Referanser
[1] NS-ISO 31000:2018, Risikostyring Retningslinjer, Standard Norge 2018.
[2] COSO, Enterprise Risk Management, Juni 2017
[3] Lov om behandling av personopplysninger LOV-2018-06-15-38 Lovdata
[4] European Commission, GDPR: New Opportunities new obligations, Luxembourg 2018

Integritetssystemet i Forsvarsmateriell

FREDRIK MORTENSEN
Seniorrådgiver Forsvarsmateriell

Forsvarsmateriell disponerer store summer av fellesskapets midler, og det er viktig at disse forvaltes på en forsvarlig og etisk måte. Alle ansatte skal være kjent med og etterleve vårt verdigrunnlag og etiske regler. Denne innsatsen er organisert i vårt integritetsprogram, bestående av de tre hovedkomponentene verdigrunnlag, etiske retningslinjer og anti-korrupsjonsprogram. I tillegg følger støttekomponentene kompetansebygging og integrering i HR-prosesser. Høsten 2016 inngikk Forsvarsmateriell en samarbeidsavtale med Senter for integritet i forsvarssektoren (SIFS) for å gjøre vårt integritetsprogram best mulig.

Vårt verdigrunnlag

Kjernen i Forsvarsmateriells integritetsprogram er verdigrunnlaget. De tre kjerneverdiene er integritet, respekt og ansvar, med integritet som den førende verdien. Verdiene skal prege vår kultur. For oss i Forsvarsmateriell innebærer integritet at vi skal opptre med rettskaffenhet og ikke urettmessig la oss påvirke i etiske spørsmål. Videre skal vi kjennetegnes ved at det er samsvar mellom det vi sier og det vi gjør. Høy integritet er avgjørende for vårt omdømme og en forutsetning for at omgivelsene skal ha tillit til oss.

Hvordan demonstrerer vi disse i praksis? Vi har skissert hvordan de kan komme til uttrykk i tabellen nedenfor.

Våre etiske retningslinjer

Den etiske standard som forventes av ansatte og leverandører er definert i ulike gjeldende styrende dokumenter. Etatens egne styrede dokumenter omfatter etiske regler for ansatte og Forsvarsmateriells etiske regler for leverandører. Videre gjelder flere styrende dokumenter utgitt av Forsvarsdepartementet, deriblant Etiske retningslinjer for næringslivskontakt i forsvarssektoren som er svært relevant i etatens daglige drift. I tillegg har vi valgt å anvende Navigasjonshjulet utarbeidet av Øyvind Kvalnes og Einar Øverenget som støtte når viktige beslutninger skal fattes.

Antikorrupsjonsprogrammet

Anti-korrupsjonsprogrammet er en helhetlig og pågående prosess for å redusere risikoen for korrupsjon og andre økonomiske misligheter.

Forpliktelsen til å bekjempe korrupsjon og andre misligheter er forankret i verdigrunnlaget og våre etiske retningslinjer, samt det styrende dokumentet Direktiv for virksomhetsstyring.

Det gjennomføres hvert halvår en identifisering og vurdering av mulige mislighetshandlinger som kan ramme Forsvarsmateriell. Risikovurderingen gjøres av en tverrfaglig arbeidsgruppe og dokumenteres skriftlig. Mislighetsrisikoer som gis høy prioritet skal reduseres gjennom målrettede forebyggende og avdekkende kontroller.

Forsvarsmateriell har etablert varslingskanal som driftes av internrevisjonen. Via denne kanalen kan ansatte og eksterne, via ulike medier, rapportere om kritikkverdige forhold.

FORSVARSMATERIELLS VERDIER

Integritet	Respekt	Ansvar
Vi forstår og etterlever lover og regler	... for forsvarssektorens verdigrunnlag	... for å nå målene våre.
Vi har nulltoleranse for korrupsjon	... for den tillit som er gitt oss til å forvalte store verdier	... for egne handlinger
Vi opptrer ryddig og er til å stole på	... for beslutninger som er fattet	... for Etatens omdømme
Vi reflekterer over og deler etiske dilemmaer	... for konfidensialitet	... for trivsel og godt arbeidsmiljø
Vi sier fra om kritikkverdige forhold	Man skal behandle alle slik man selv forventer å behandles	... for kontinuerlig læring og forbedring

Forsvarsmateriell ble etablert i 2016 og har ansvar for å utruste Forsvaret med relevant og tidsriktig materiell for å bidra til økt operativ evne. Alt fra soldatens personlige bekledning til stridsvogner, ubåter, kampfly og teknologiske løsninger. Forsvarsmateriell gir råd og foretar investeringer og forvalter materiellet i hele levetiden for å ivareta ytelse, teknisk tilgjengelighet og sikkerhet i henhold til lover, regler og øvrige krav.

Kompetansebygging og integrering i HR-prosesser

Kompetansebygging omfatter ulike kommunikasjons- og opplæringsaktiviteter for å sikre tilstrekkelig kunnskap om - og eierskap til - Forsvarsmateriells verdigrunnlag, gjeldende etiske retningslinjer og antikorrupsjonsprogram blant egne ansatte og eksterne (innleide, konsulenter osv.) som jobber i Forsvarsmateriell.

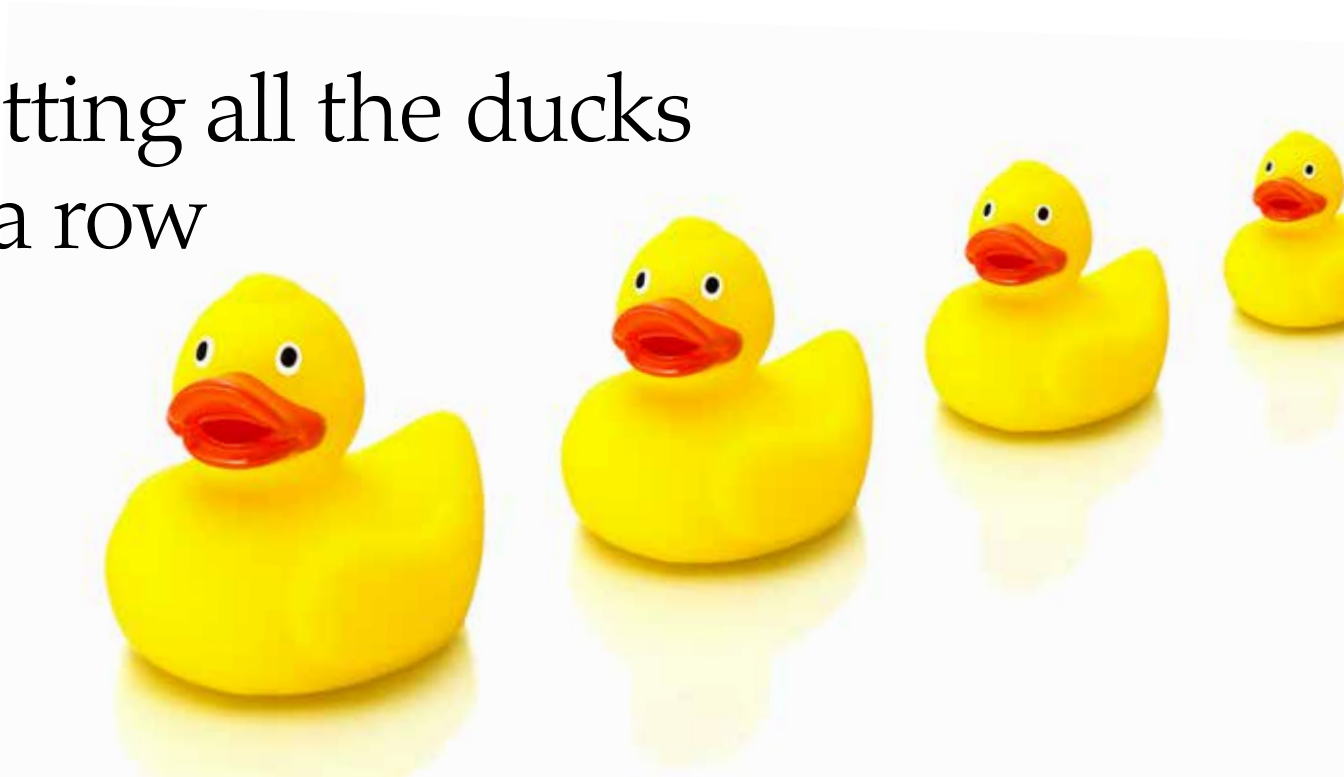
Vårt verdigrunnlag og etiske standard er bygget inn i vesentlige HR-prosesser slik som rekruttering, medarbeidersamtaler, tjenesteuttalelser og medarbeiderundersøkelser.

Evaluering

Evalueringen av hvorvidt integritetsprogrammet virker gjøres kontinuerlig i form av kontroll-aktiviteter, informasjon og kommunikasjon. Videre evalueres det i medarbeiderundersøkelser og i en årlig modenhetsvurdering.

Følg oss på sosiale medier

Getting all the ducks in a row



BY JOONAS VÄRTINEN
Chief Audit Executive, Aktia Bank Plc

How much does and should "data" play a role in running an audit function? And what do we mean when we think of data in the context of an audit function? Is it the external information that needs to be considered during an audit, or is it what we as an audit function produce at the conclusion of our day-to-day audit work?

In this article I will concentrate on addressing that part of data which an audit function produces.

What is data?

According to the Merriam-Webster dictionary data is: *"factual information (such as measurements or statistics) used as a basis for reasoning, discussion, or calculation"* This definition gives answers to the question *"What": factual information;* and to the question *"Why": for reasoning, discussion and calculation,* but it does not really answer the question "How?". How do we use the data produced in our audit work for supporting our reasoned observations? Data as such does not change anything if we do not use it: we need to process data, analyse it and report on it as well as visualise the information in order to make an impact.

Background

In the beginning of 2016 I started in my position as Chief Audit Executive in a medium sized, listed bank. I did not have previous audit experience, but I had worked over a decade within risk management and reporting. Before taking on this audit position, I was heading a unit in a multinational bank responsible for group reporting, processes and system support in the area of operational risk. The bank consisted of several business divisions and legal entities. The complexity of the organisation and the supervisory landscape made the reporting environment quite challenging.

When I started out as a CAE, I not only jumped into a new company, but also into a new area of expertise and information. One of the first tasks was to wrap-up the previous year's audit and write an annual internal control report. The purpose of this report was to give the overall opinion on the group's risks and controls.

Designing a database for audit issues

Achieving an overall picture

The bank already had a wellestablished audit function for many years. It had produced plenty of information about the organisation during those years. Obviously then, there should have been plenty of input for my overall assessment. However, quite soon I realised that building an aggregated overview was not an easy task. The key challenge was that the data was not structured but embedded into numerous and long Word-reports.

As CAE I needed to understand the key risks, critical findings and status of remediation actions. For that picture I had plenty of Word-reports containing tens of pages of important and maybe not so important information. The only way forward I could see was to read through all the reports and try to boil the information down to an aggregated view of «how things are».

After carrying out that exercise I decided that we needed to change the approach to how we handled information

as this was not an efficient way to utilise the information we had. From my previous position, I had experience of using a comprehensive GRC-system which was used to process and aggregate information. However, I was also aware of the pitfalls of such a system. I did not want to invest too much effort in the implementation and operation of a too heavy infrastructure.

A GRC system is usually a system that connects different Governance and Risk management and Compliance processes into one system and data matrix. My experience of using such a system is that their implementation is usually quite easy from a technical point of view. If you take an off-the-shelf solution, you can get a fully operational system within weeks, however, the technical implementation might just be only a part of the story. An issue is usually that the standard processes and workflows do not support the organisation's existing framework as expected. If there is a mismatch, an extensive re-configuration project might be required. The alignment of terminology and structure may also be an issue necessitating the establishment of a common taxonomy for the data in the system.

However, when you get such a system in place, the huge advantage is that all findings are in one place and you can aggregate an overall view based on various criteria (such as risk type, organisational or legal entity, or severity). The system also usually provides a structured process for follow-up.

Changing information to data and vice versa

My goal was to establish the mechanism whereby this aggregation and overall picture could be derived from a standard structure for audit findings. However, I was not sure whether I really wanted to implement a comprehensive system or rather find a quick and light solution to the problem.

From my previous experience I knew that well-structured data is in any case a prerequisite for system implementation. Working with the data will anyway pave the way for a possible implementation of a system at a later stage. Before taking any decision regarding the system, I started to think about a set of parameters that would be necessary for classifying an audit finding. These parameters could then form a comprehensive typology of "an audit finding".

Basic parameters for an audit finding

I took a very pragmatic approach to the identification of the necessary parameters. The starting point was to define "for what purpose do we need the information". This requirement would then define the necessary structures.

Functional organisation

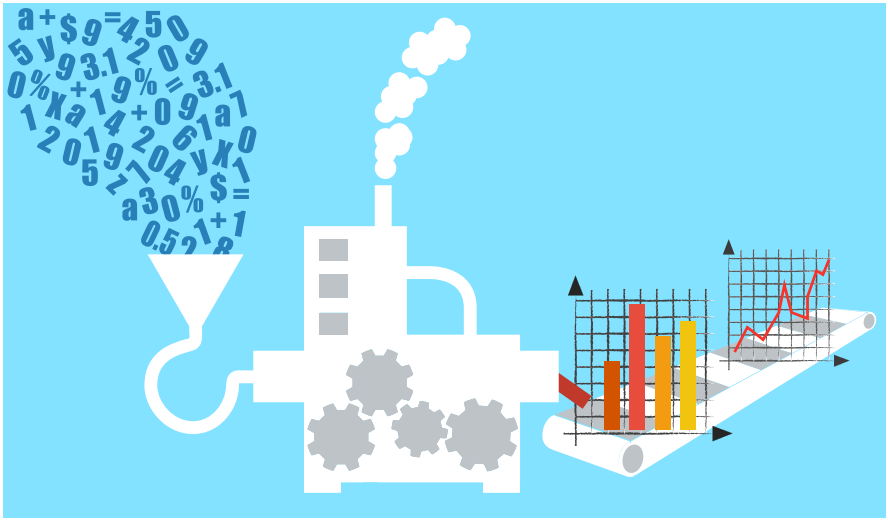
The organisation's own business organisation. This structure represents *ownership*. Business structure gives you the answer to who has the power to take decisions. Organisational levels that you implement in the data must be considered. Detailing down to a lower organisational level has the advantage of allowing granularity in reporting but will have a huge impact on maintenance. Lower levels of the organisation change constantly and following up on those changes and performing the necessary re-mapping of the data is laborious. Our decision was to define only the top two organisational levels as a structural element in the data. This means that organisational accuracy is not so good, but in a smaller organisation you can target findings manually to the right organisation even when you lack the granularity.

Legal Entities

A corporate group has also a legal structure. This structure ties very much in to *regulatory reporting* responsibilities. Formal responsibilities are tied in to the companies, and usually corporate entities are formed for certain purposes (Life Insurance, Investment Fund Company etc). Having this in the structure helps reporting especially towards internal governance bodies and external regulators.

Processes

As Wikipedia defines it, a process is a set of activities that interact to produce a result . The process produces an operational context where organisational entities, risks and controls are *connected*. This is usually the most challenging area to define. It is relatively seldom that a bank has a comprehensive process structure that encompasses the whole organisation structure and all levels. A good way to start is to utilise already existing structures. For example, processes that are identified as critical processes in Business Continuity Planning can be taken as starting point and then enriched with some additional processes.



Project
A project in this context mean an audit assignment. This is a parameter that binds interrelated findings (observations) together. Observations under a "project" form an audit report.

Observation
The description of the control weakness that was found in the audit. This parameter may be split in several pieces. We record a long and a short version of an observation. The short version is very handy, when producing reports by using visualisation tools such as Tableau.

Risk
Each finding is tied to the risk framework. This could be based on audit's own structure, but it may also be the same structure other control or compliance functions are using if the company has a commonly agreed risk taxonomy. This is a very natural connection point between assurance and control functions.

Impact or priority
This concerns the level of severity. In practise a very simple grading such as "low-medium-high" is sufficient. It would be worthwhile to try to align the levels for example with the group risk appetite or the risk management function's scaling if possible

Remediation plan
The action plan tells what is going to be done by the business owner. This parameter could be completed also with a deadline and a responsible owner (a named person).

Having identified the key parameters, there should be room for iteration. After a couple of reporting rounds you will be able to see more clearly whether you need additional elements or if there is in fact something you do not really need to maintain.

The technical platform

Establishing the data structure as such does not really solve anything. A tool will be needed in order to process and utilise the data. What exactly should the system support in respect of data processing? Wikipedia defines data processing as *"the collection and manipulation of items of data to produce meaningful information"*[1]. Roughly data processing could then be seen as a three-phased process: 1) inputting the data 2) analysing the data 3) reporting. In addition, data will usually require to be saved and maintained.

When I started to consider system support for data management, I tried to consider all the phases and weigh up the support we would like to have in each of the relevant areas, taking into account the maturity of our data structure.

Collection phase

Do you aim to include within the scope of the system the interaction between the audit function and the auditee? Our consideration was that at this point, we do not need to reach the business users through the system. We can handle the dialogue by using PowerPoint and email. This means that system usability and access control requirements could be very basic. Only the internal audit team needs to use it.

Analysis and reporting phase

We had one critical requirement: the system should easily be connected to a visualisation tool. We were already using a such system and knew the benefits of such tools.

Maintenance and development

As the data structure was new and not yet firmly established, it was clear that changes may be necessary after a while. This sets a requirement for system flexibility.

We decided to have different tools for different purposes. For collecting the data, we use PowerPoint and Outlook (eMail). In a smaller organisation these tools are used by everyone and even though they will require manual effort by the auditor (sending, asking, copy-pasting) it is still doable. For maintaining the data, we use a simple Access-database. The database has an easy interface that enables adding and updating the findings. This is done by auditors based on the input we have collected. The structure of the database is easy to restructure or modify if needed. The biggest advantage of this kind of approach is that analysing and reporting is easy because the data is highly accessible.

My experience from the GRC-solution is that the data in the system is hard to access outside the system. For analysis and reporting, the system usually provides a wide range of readymade reports. This might be adequate for the purpose. However, I wanted to have full control of the reports and analyses (flexibility) and also the possibility to connect our own data to other data (internal or external). We also connect our annual plan (which is also built up as data) to the findings.

For reporting, we use a visualisation tool - Tableau. The tool can be changed at any time, without having any impact on the collection or data management part of the process. We currently take static views from the system for our reporting, but are also able to publish dynamic reports on a server that may be accessed at any time by the report users (such as management or owners of audit findings).

Conclusion

Our initial objective has been achieved and we are now in a position where we can summarise the data supporting overall conclusions as may be required for reporting according to the various parameters. Going forward the focus regarding our own data process is to make the collection phase smoother. For example, the new Office tools have several applications / features that look very interesting and effective for audit purposes too. Again, changing a tool in one part of the process, will not have any impact on the other parts. I feel that our own ducks are now walking beautifully in a line. The next, and already ongoing task is to get the salmons to swim into a net. By this I mean more effective analysis of the data that a company produces in its operational processes which contain plenty of information for audit purposes too. But that is a different story.

Internrevisjon & merverdi

Forventningene til internrevisjonen er stadig økende. Hvordan vet internrevisjonen at den tilfører merverdi til organisasjonen og sine interessenter?

AROOJ DAR
Senior Associate, BDO

AKSANA TIKHONOVA
Internrevisor, KLP

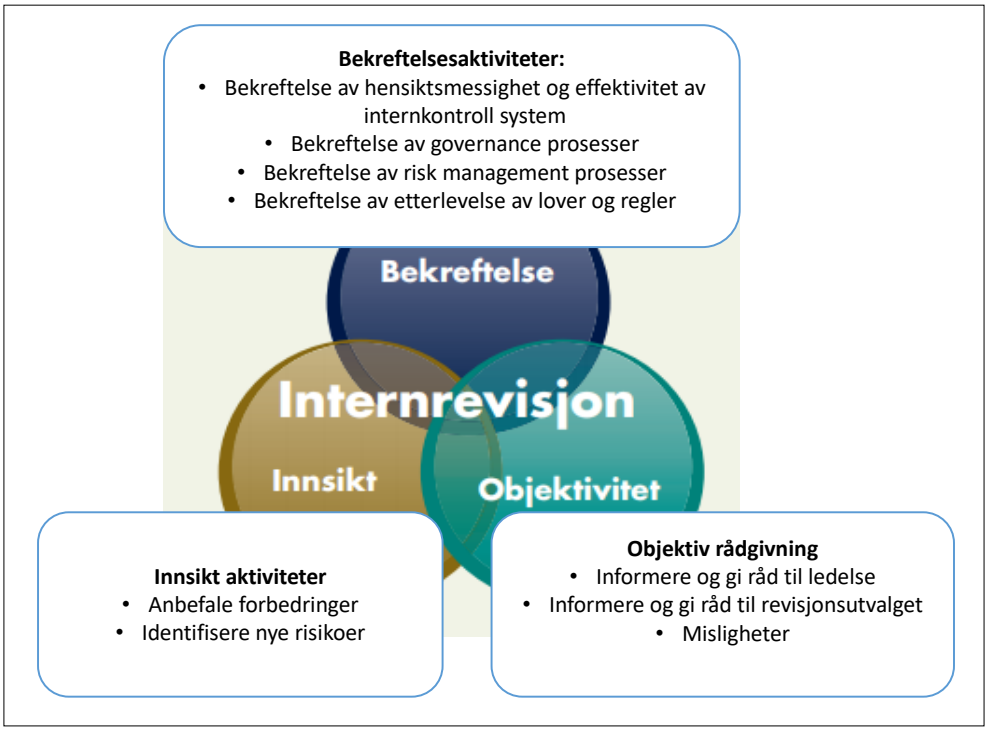
KARI ANNE GAARE
Regnskapsrevisor, Revisjon Midt Norge

Dette ønsket vi å belyse nærmere i en oppgave vi skrev ved gjennomføring av Master of Management-programmet «Intern revisjon; Governance - Risikostyring -Intern styring og kontroll» på Handelshøyskolen BI våren 2018. Vi tok utgangspunkt i fire spørsmål fra den globale undersøkelsen The Global Internal Audit Common Body of Knowledge (CBOK) fra 2015, og tilførte flere spørsmål for å gå mer i dybden. Undersøkelsen ble besvart av internrevisjonsledere i Norge. Resultatene er sammenlignet med resultatet fra den globale undersøkelsen og sett opp mot relevant teori på området.

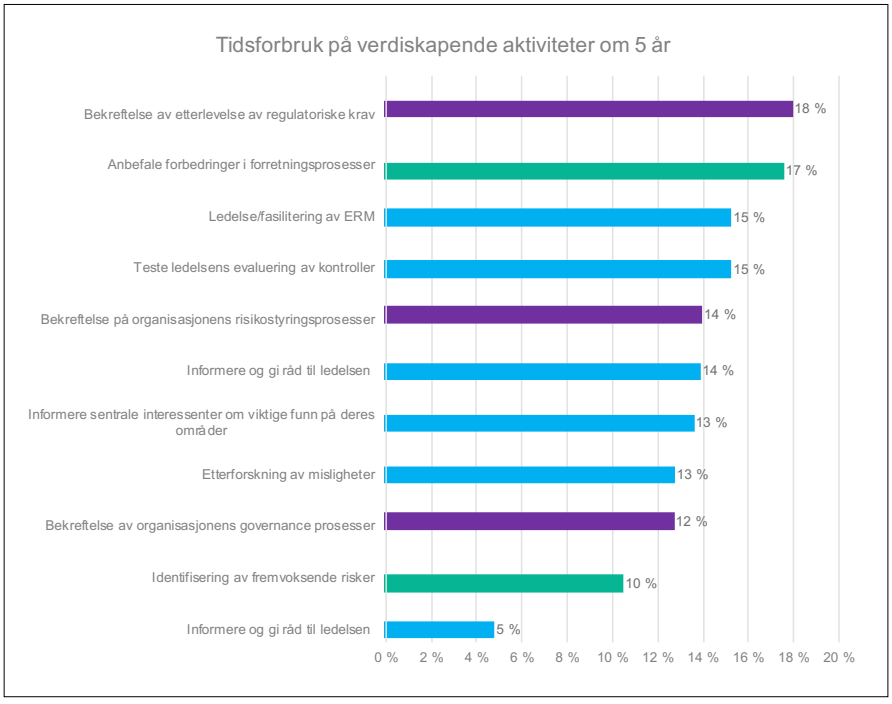
Hvilke internrevisjonsaktiviteter tilfører mest verdi?

The Value Proposition for Internal Auditing fra IIA er sammensatt av tre elementer: bekreftelse, innsikt og objektivitet. I vår undersøkelse ønsket vi å finne ut hvilke revisjonsaktiviteter norske internrevisjonsledere oppfatter som de mest verdiskapende og hvordan disse aktivitetene fordeler seg på de tre elementene i The Value Proposition. Respondentene ble bedt om å velge opp til fem alternativer de selv oppfattet som mest verdiskapende aktiviteter fra en predefinert liste med 15 alternativer. De oppgav også nåværende tidsforbruk på aktivitetene og hva de mente ville være mest verdiskapende om 5 år og hvordan tidsforbruket ville fordele seg på disse aktivitetene i fremtiden.

Revisjonsledere i Norge oppgir at bekreftelsesaktiviteter er de mest verdiskapende aktiviteter i dag. Det brukes dobbelt så mye tid på dette som både innsikt- og objektivitetsaktiviteter. Samtidig ser vi en trend som peker mot at innsikt- og objektivitetsaktiviteter vil bli oppfattet som mer verdiskapende aktiviteter i fremtiden som det vil brukes mer tid på.



Mest verdiskapende aktiviteter fordelt på bekreftelse, objektivitet og innsyn. Kilde: Tikhonova, 2018 (egenprodusert)



Tidsforbruk på verdiskapende aktiviteter om 5 år. Kilde: Tikhonova, 2018 (egenprodusert)

Hvilke målemetoder benyttes i Norge?

For å lykkes med målstyring av IRs prestasjoner er det viktig å etablere en link mellom IRs strategi, som gjenspeiler seg i de mest verdiskapende aktiviteter og som knytter måleparametere til hver av de strategiske aktivitetene. For å avgrense, strukturere, følge opp og presentere målinger på en god måte, er det også viktig å sikre at det etableres måleparametere for alle perspektiver i balansert målstyring (BMS). Typiske elementer i BMS er de fire standardperspektivene (finans, kunde, interne prosesser og vekst og læring) og balanse mellom korte- og langsiktige mål, mellom resultat- og prosessindikatorer og samt mellom eksterne og interne ytelsesperspektiver.

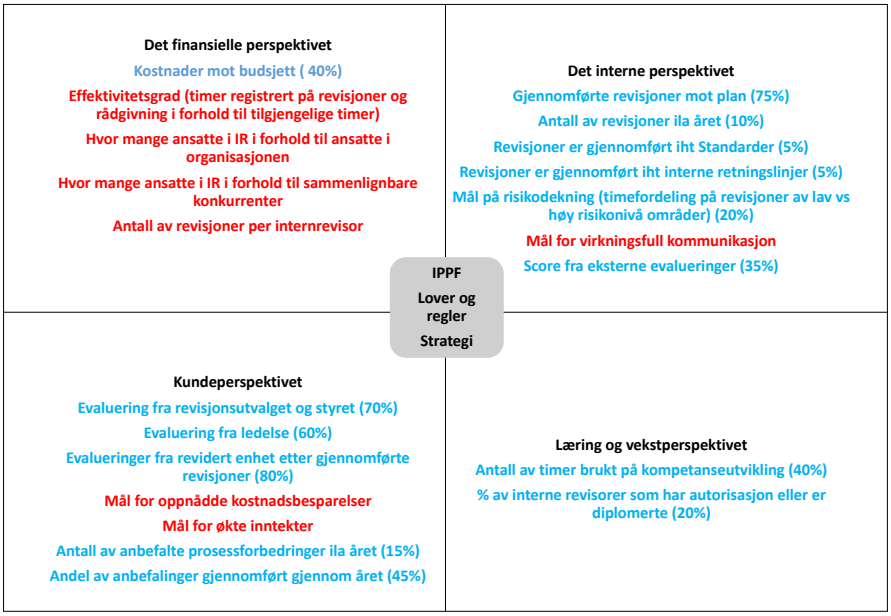
Etter å ha fått en oversikt over de mest verdiskapende revisjonsaktivitetene ville vi finne ut hvilken tilnærming respondentene hadde til evaluering av IRs prestasjoner. Over 80 % av respondentene oppgir at de bruker «egenevaluering» (en innoverrettet metode) og «tilbakemelding fra reviderte enheter etter fullført revisjon» (en utadrettet metode). Da disse to metodene representerer både innoverrettet og utadrettet metode, er dette i likhet med den globale undersøkelsen, en positiv indikator på en balansert tilnærming på evaluering. 28 % av respondentene oppgir at de bruker BMS for prestasjonsmåling. Selv om dette ligger noe høyere enn i den globale undersøkelsen, mener vi likevel at det fortsatt ligger et forbedringspotensial for å øke bruken av BMS.

Hvilke parametere egner seg best for å måle om interessenters forventninger til IR verdi blir oppfylt?

Vi ba respondentene om å oppgi alle KPI'ene de bruker for å evaluere IRs prestasjoner. Til dette svarer de fleste norske lederne (mellom 80-60 %) at de bruker følgende fire måleparametere; «tilbakemelding fra reviderte enheter etter gjennomførte revisjoner», «grad av gjennomført revisjonsplan», «evaluering fra styret og revisjonsutvalget» og «evaluering fra ledelsen». Tre av de fire mest benyttede måleparametere er utadrettede og fokuserer på forventninger og vurderinger fra interessentene. Resultatene skiller seg ganske mye fra den globale undersøkelsen, der de mest benyttede måleparametere er innoverrettede.

Etter å ha sett på hvordan måleparametere fordeler seg på innoverrettet og utadrettet, fordelte vi måleparametere etter perspektiver i BMS (figur 4.10). Det som er merket med rødt er KPI'er som ikke er brukt.

Kostnader mot budsjett er den eneste KPI'en fra det finansielle perspektivet som velges av respondentene (40%). Det virker litt merkverdig at ingen av respondentene måler effektivitetsgrad eller har andre finansielle måltall på sine målekort. F.eks. ville det vært naturlig å ha måltall på sitt timeforbruk for å vurdere og forbedre egen effektivitet.



(Figur 4.10) Mest brukte KPI´er fordelt på de fire perspektivene i BMS. Kilde: Tikhonova, 2018 (egenprodusert)

I det interne perspektivet er det «grad av gjennomførte revisjoner mot plan» som benyttes mest (70 %), mens andre KPI'er benyttes i betydelig mindre grad. Høyt fokus på fullføring av revisjonsplan kan øke risikoen for at internrevisorer prioriterer å bli ferdig med oppdragene i tide fremfor gjennomføring med riktig kvalitet, eller eksempelvis at revisjonsplanen ikke blir oppdatert når risikobildet i organisasjon endrer seg. Måling av gjennomføringsgrad av fullført revisjonsplan bør alltid understøttes med andre KPI'er, som for eksempel «mål på risikodekning» eller «revisjoner gjennomført iht. Standarder», for å forsikre seg om at man oppdaterer og fullfører planen på en hensiktsmessig måte.

Vi kan se fra figur 4.10 at norske internrevisjonsfunksjoner bruker nesten alle KPI'ene fra kundeperspektivet. 52 % av respondentene mener at «å anbefale forbedringer av forretningsprosesser» er en av de mest verdiskapende aktiviteter. Det som er interessant å merke seg er at ingen av respondentene har valgt «mål for oppnådde kostnadsbesparelser» eller «mål for økte inntekter» for å kunne synliggjøre disse forbedringene.

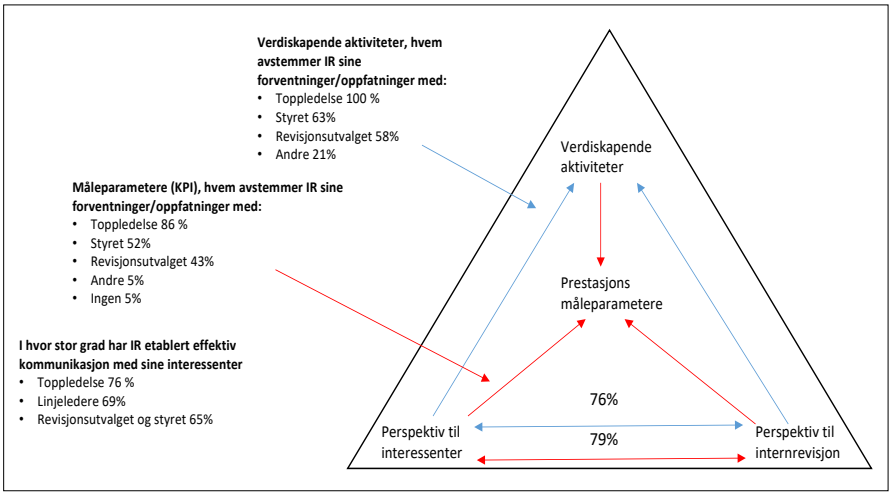
Begge KPI'ene i læring og vekstperspektivet brukes, men kun av et fåtall. Fordi både 1200-serien i IIA Standardene og de ti kjerneprinsipper for internrevisjon stiller krav til faglig dyktighet og til kompetanseutvikling, er det naturlig å tenke seg at flere IR funksjoner burde hatt KPI'er for å måle kompetanseutvikling.

Bare et fåtall (26 %) av de norske respondentene har måleparametere fra alle de fire perspektivene i balansert målstyring, og noen av perspektivene kunne derfor med fordel vært brukt mer aktivt.

Hvordan avstemme egen oppfatning av verdi mot interessentene?

For å tilføre størst mulig verdi bør IR ha en effektiv kommunikasjon med sine interessenter. Dette kan gjøres gjennom å tilpasse verdiskapende aktiviteter og prestasjonsmålinger til forventninger, og aktivt bruke resultatene av målinger til å definere forbedringsområder og iverksette effektiviseringstiltak.

Performance Measurement Triangle presenterer på en oversiktlig måte samspillet mellom internrevisjon, interessenter, verdiskapende aktiviteter og prestasjonsmålinger, og vi benyttet denne for å analysere svarene fra respondentene (figur 4.5).



(Figur 4.5) Performance Measurement Triangle. Kilde: Tikhonova, 2018 (egenprodusert)

IR må sette av tid til å skape dybdeforståelse for hvilke aktiviteter det er som oppfattes som verdiskapende av interessentene og avstemme sin egen oppfatning med dem. Da er det viktig å ha en balansert tilnærming til Value Proposition i bunnen (de blå pilene). I neste steg defineres KPI'er til hver av de verdiskapende aktivitetene (de røde pilene), og det er viktig å tenke på balanse mellom perspektiver, tilpasse antall av KPI'er innenfor hvert perspektiv, samt kombinasjonen av utadrettet og innoverrettet tilnærming.

Det er interessant å merke seg at samspill med ledelse scorer høyere på alle spørsmål enn samspillet med styret/revisjonsutvalget. Ledere av IR i Norge bør bli mer bevisst på å etablere effektiv kommunikasjon og å avstemme sine oppfatninger med styret/revisjonsutvalget, som en like viktig interessent for dem som ledelse.

Oppsummering

Det er interessentenes forventninger, oppfatninger og deres syn på hva som tilfører verdi til organisasjonen som er avgjørende. Selv om det ikke finnes et fasitsvar som passer for alle internrevisjonsfunksjoner, er det et godt utgangspunkt å følge en prosess for å identifisere og fokusere på de revisjonsaktiviteter som tilfører mest verdi for interessenter samt velge gode måleparametere. Med utgangspunkt i internrevisjonens strategi og Value Proposition, starter prosessen med å identifisere verdiskapende aktiviteter og avstemme disse mot forventningene til interessentene (styret/revisjonsutvalget og ledelse). Videre fastsettes gode måleparametere for hver av de verdiskapende aktiviteter fra de fire perspektivene i balansert målstyring. Til slutt etableres rutiner for rapportering og oppfølging av KPI'er og prosess for revurdering av innholdet i rapportering for å sikre at KPI'ene ikke blir for statiske, men at disse endres i takt med strategi og forventningene til interessenter. Det er også viktig å bruke resultatene av målinger aktivt til å definere forbedringsområder og iverksette effektiviseringstiltak.

Hvilken rolle spiller internrevisjonen i helhetlig styring av mislighetsrisiko?

AV RUNE GODTLAND
Konserncontroller Zalaris ASA
Diplomert Internrevisor

Standarder for profesjonell utøvelse av internrevisjon pålegger internrevisorer å ha tilstrekkelig kunnskap til å vurdere risikoen for misligheter, samt hvordan risikoen håndteres i virksomhetene. Internasjonal forskning tilsier at det er internrevisjoner som bidrar høyt i å avdekke tilfeller av misligheter. I en studie som ble gjennomført i forbindelse med internrevisjonsprogrammet ved Handelshøyskolen BI i 2018, så vi nærmere på sammenhengen mellom internrevisjonsfunksjonen og helhetlig styring av mislighetsrisiko i norske virksomheter.

COSO-rammeverket som teoretisk fundament

Alle virksomheter er utsatt for mislighetsrisiko, men å eliminere alle misligheter i en virksomhet er praktisk talt umulig. Formålet med implementering av prinsippene i et rammeverk for helhetlig styring av mislighetsrisiko, er å maksimere sannsynligheten for at misligheter forhindres og avdekkes i tide, samt å skape en avskrekkende holdning til å begå misligheter. Avskrekkelsesverdi oppnås ved implementering av en konsekvent og synlig styringsprosess for mislighetsrisiko, og skape en transparent og helhetlig antikorrupsjonskultur. Dette i sin tur forutsetter at virksomheten gjennomfører jevnlige og grundige vurderinger av mislighetsrisiko som utgangspunkt for utforming og implementering av forebyggende og avdekkende kontrollaktiviteter. I tillegg er det viktig å vise evne til rask handling ved mistanke om misligheter og iverksette hensiktsmessige tiltak mot de involverte parter. Det teoretiske rammeverket for undersøkelsesmodellen i studien er basert på håndboken for mislighetsrisikostyring, Fraud Risk Management Guide (FRMG), som er et anerkjent rammeverk lansert av COSO i samarbeid med ACFE i 2016.

FRMG er et selvstendig rammeverk for helhetlig styring av mislighetsrisiko. Det fungerer i synergi og er konsistent med de fem komponentene i internkontrollrammeverket som ble revidert av COSO i 2013 (se figur 1). I COSO 2013 er det definert 17 prinsipper for utforming og implementering av internkontrollsystemet hvor alle må fungere sammen for at internkontrollsystemet skal være effektivt. Prinsipp 8 i COSO

Figur 1 Helhetlig styring av mislighetsrisiko Kilde: Basert på COSOs FRMG, 2016.

2013 er rettet spesielt mot misligheter og krever at virksomheten må vurdere potensialet for misligheter når den vurderer risiko relatert til måloppnåelse. FRMG har fastsatt fem ytterligere prinsipper for helhetlig styring av mislighetsrisiko. Disse fem prinsippene representerer indikatorvariablene i undersøkelsesmodellen (se figur 1). Helhetlig styring av mislighetsrisiko er følgelig et sammensatt begrep og måles ved å ha et effektivt instrument for innsamling av data. Videre skal det utformes slik at innsamlede data har god nok og overbevisende forklaringskraft.

Har virksomheten etablert egen internrevisjon?	Har det vært avdekket tilfeller av misligheter i virksomheten siste 10 år?		
	Ja	Nei	Total
Ja	65,8 %	34,2 %	100,0 %
Nei	47,5 %	52,5 %	100,0 %
Total	57,8 %	42,2 %	100,0 %

Har virksomheten etablert egen internrevisjon?	Helhetlig styring av mislighetsrisiko		
	Frekvens	Gj.snitt	Std.avvik
Ja	81	6,09	0,89
Nei	64	5,70	0,85
Total	145	5,92	0,89

Metodisk tilnærming og statistisk grunnlag

En kvantitativ spørreundersøkelse ble gjennomført for å få en presis beskrivelse av omfanget og utstrekningen av arbeidet med misligheter. Utvalget bestod av til sammen 200 private, statlige og ikke-statlige virksomheter, hvor av 145 respondenter svarte på undersøkelsen. Statistisk faktoranalyse i SPSS viste at de fem komponentene i undersøkelsesmodellen virker sammen på en integrert måte. Reliabilitetskontrollen indikerte videre en høy grad av intern konsistens som ga grunnlag for å etablere den nye variabelen «helhetlig styring av mislighetsrisiko». På en skala fra 1 til 7 ble gjennomsnittsverdien av spørsmålene under de fem indikatorvariablene internt kontrollmiljø, risikovurdering, kontrollaktiviteter, informasjon og kommunikasjon, og monitorering beregnet til 5,92 med et standardavvik på 0,89. Dette indikerer at helhetlig styring av mislighetsrisiko er svært viktig i norske virksomheter.

Sammenhengen mellom internrevisjonen og avdekkede tilfeller av misligheter

Det er totalt avdekket tilfeller av misligheter i 57,8 % av virksomheten i løpet av de siste 10 år. Prosentandelen av totalt avdekkede misligheter fordeler seg med 65,8 % på virksomheter med internrevisjon mot 47,5 % i virksomheter som ikke har etablert egen internrevisjon.

Konklusjonen er at det er statistisk signifikante forskjeller mellom virksomheter som har etablert egen internrevisjon sammenlignet med de som ikke har det. Det er altså statistisk grunnlag for å hevde at virksomheter som har etablert egen internrevisjon avdekker signifikant flere tilfeller av misligheter sammenlignet med virksomheter som ikke har etablert egen internrevisjon.

Sammenhengen mellom internrevisjonen og helhetlig styring av mislighetsrisiko

Tabellen viser at gjennomsnittlig score for virksomheter som har etablert egen internrevisjon ligger på 6,09, mens gjennomsnittet for virksomheter som ikke har etablert egen internrevisjon ligger på 5,70.

Dette viser at det er statistisk grunnlag for å hevde at helhetlig styring av mislighetsrisiko er viktigere i virksomheter som har etablert egen internrevisjon sammenlignet med virksomheter som ikke har etablert egen internrevisjon.

Konklusjon

Resultatene fra undersøkelsen viser at styring av mislighetsrisiko er signifikant viktigere i virksomheter som har etablert egen internrevisjon sammenlignet med virksomheter som ikke har etablert tilsvarende funksjon. Årsaken til dette kan være at virksomheter med egen internrevisjon har større fokus på mislighetsrisiko som følge av at internrevisjonen er pålagt å etterleve standarder som er relatert til mislighetsrisiko.

Analysen viser også at det avdekkes signifikant flere tilfeller av misligheter i virksomheter som har etablert egen internrevisjon sammenlignet med virksomheter som ikke har etablert en tilsvarende funksjon. Dette kan tyde på at virksomheter med egen internrevisjon i større grad legger vekt på prinsippet om effektive kontrollaktiviteter gjennom forebyggende og avdekkende kontroller enn virksomheter uten egen internrevisjon. Det er ikke et statistisk forsvarlig grunnlag for å påstå dette i fra denne undersøkelsen, men et slikt funn samsvarer i stor grad med internasjonale undersøkelser som også konkluderer med at internrevisjonen er et av de elementene som bidrar til å avdekke flest tilfeller av misligheter.

Current trends in outsourcing and addressing third party risk

KEVIN F. MCCLOSKEY
CISA, CIA, CRMA, Deloitte AS

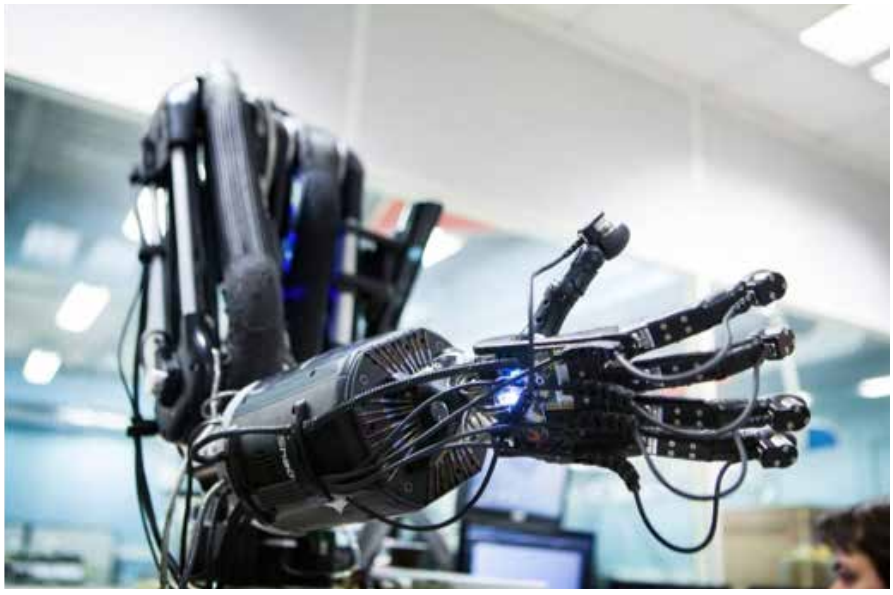


Figure 1: Source - Deloitte

Outsourcing – A growing trend

Businesses are increasingly dependent on third parties to provide mission-critical services. This may include services related to information technology (e.g., managed IT services, SaaS, security-monitoring services), finance and accounting (e.g., payroll processing and accounting services), customer service support and human resources administration, to name a few. Outsourcing has gone from being a value-protecting measure to becoming a value-creating measure.

> Outsourcing has gone from being a value-protecting measure to becoming a value-creating measure

What drives this? Simply put, companies must accept that outsourcing is sometimes required to be competitive on a global basis, to grow in the market or to reduce costs and increase quality. The increasing use of outsourcing in today´s market has made companies more dependent on a complex network of third-party suppliers. From a risk perspective, it is important that the companies themselves have an overview of the risks that affect them and manage and monitor these in a satisfactory manner. You can outsource a task but you cannot outsource the risk related to it.

The Deloitte Global Outsourcing Survey

Deloitte recently surveyed over 500 leaders from organizations of all sizes and with operations in Europe, the Americas and Asia in regards to their experiences and thoughts related to outsourcing. The survey found that while in the past organizations typically used outsourcing to improve back-office operations through cost reduction and performance improvement, today's organizations are looking to disruptive outsourcing solutions to enable competitive advantage by accelerating changes within those organizations. For these organizations, outsourcing can bring quick wins to top line growth, as well as to a more agile, effective back office. The focus has shifted from traditional 'work transfer' to upfront transformation and automation. Organizations are recognizing that disruptive solutions can revolutionize the way they do business, and that "buying" capabilities in the marketplace is generally faster and more scalable than developing capabilities internally. Emerging solutions incorporating cloud and automation are empowering organizations to work smarter, scale faster, reach new markets, increase productivity and, ultimately, to gain competitive advantage.

As with many initiatives, organizations are finding that delivering competitive advantage through disruptive outsourcing

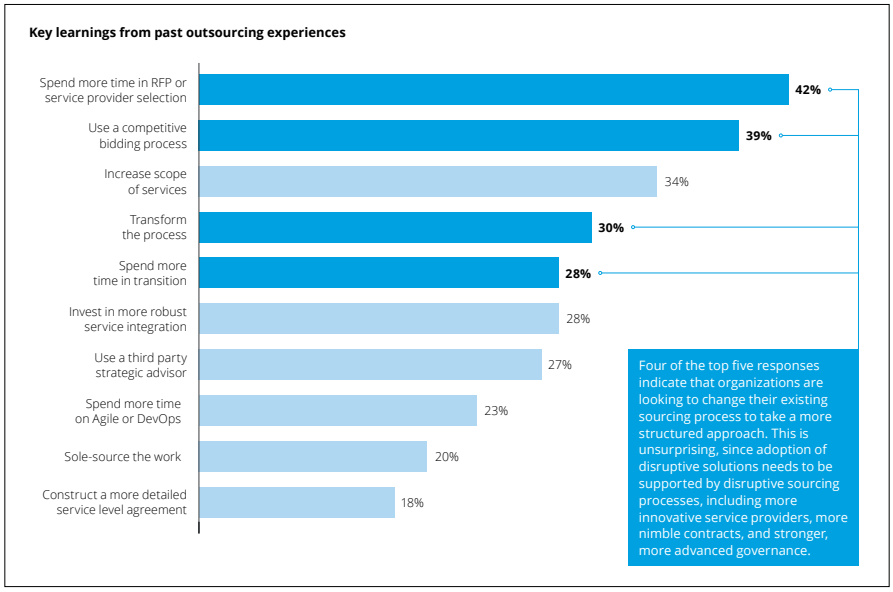


Figure 2: Source - The Deloitte Global Outsourcing Survey 2018

solutions is anything but simple; effort and expertise are needed to address security and cyber risks, changing regulations, organizational resistance, skill gaps, and to help flatten fragmented processes.

The survey itself can be found here: https://deloi.tt/2ZPd9A8

Technology drivers for disruptive outsourcing?

What are the technologies driving disruptive outsourcing? The survey found that there were three main technologies that are driving this focus on disruptive outsourcing. These are cloud computing, robotic process automation (RPA) and cognitive automation.

- **Cloud computing** is a model for providing customers access to a shared pool of computing resources (e.g., networks, servers, storage, applications and services). The model for these resources is that the ultimate user of the resource can do so with minimal management effort or service provider interaction.
- **Robotic process automation (RPA)** is basically a software that performs repetitive rules-based tasks to improve efficiency, quality and accuracy of process outcomes.
- **Cognitive automation** adds additional capabilities to RPA, including learning, judgment and 'reading' of unstructured text (e.g., handwriting, photographs, etc.).

What does this look like in Norway?

My vantage point is that of a third party assurance specialist/external and internal IT auditor. I base my observations on what I see at my clients, who are managed IT service providers, Software as a service providers, data center management providers, multinational telecom companies, financial institutions and public sector institutions, among others. What I am seeing is a clear increase in the use of all of these technologies.

- **Cloud computing**, of course, has been a hot topic for some time now and many of us use some form of cloud computing resource whether we know it or not. Cloud is one of the top-of-mind subjects when discussing areas such as IT strategy, budget and performance. It is also one of the 'black holes' in the IT auditor world. Where are my documents actually stored?
- **RPA** is very prevalent in, among others, the financial services industry, the healthcare sector, manufacturing and even agriculture sectors. These types of programmed routines present advantages for the users of the service due to the lower margin of error they provide. They also present challenges for us auditors and those tasked with managing internal control programs in user companies as to how to gain confidence in the functionality and reliability of the programmed routines themselves. Have you tried to interview a robot?
- Being the logical extension of RPA and providing true automation possibilities, **cognitive automation**, to me, can be seen as the culmination where we want to go with robotics. In my experience, this has been highly present in the financial services sector, but also in the consumer business, healthcare and pretty much all sectors when considering opportunities for automating repetitive and standard processes. Cognitive automation, also known as smart or intelligent automation, includes such exciting areas as Natural language processing (NLP) and machine learning. That 'person' answering your questions on the hotline sounds a bit metallic do they?

What does this mean from an internal control perspective?

In general, more outsourcing means more situations where someone at a user organization needs to understand controls that are outside of their company in order to fulfill their obligation to have an end-to-end understanding of internal control processes. Limited insight into the functionality and internal controls at outsourcing organizations due to contractual constraints, time and budget constraints and / or limitations in competence to understand and analyze the risks related to the use of the outsourced services can hinder a company's ability to have the right amount of control over their internal control processes from start to finish.

There is a growing need for more assurance from those providing the services and this need is being evidenced to me by numerous requests for third party assurance reports. I have seen a lot of recent requests for something called SOC2 reports (which basically provide assurance in regards to security, availability, confidentiality, processing integrity and privacy of information). I have also seen an increase in requests for ISAE3402/ SOC1 reports (focused on the areas addressing the internal control related to processing of financial information and meeting the needs of, among others, external auditors) as well as specific

ISAE3000 reports designed to meet the needs of an individual customer of the service provider.

GDPR is a hot topic these days and is getting a lot of attention from us in the audit and assurance crowd due to the drastic penalties of non-compliance. These other areas like cloud computing and RPA also present clear 'issues' for auditors and the companies they audit. The availability of third party attestation reports is currently somewhat limited but I am seeing an increase in requests for these, even from some companies I had assumed to have had such reports in place for several years based on their services and customer portfolio.

The survey found that most organizations with outsourcing initiatives that have been reviewed by internal or third party auditors in the last 12 months have completed and passed their audits. There were few completing their audits with material issues. This is promising and in my experience from the companies I have worked with this development is a natural result of the work of both the auditor performing the work and providing the opinion as well as the company being audited through their receptiveness to take advice and remediate weak controls or implementing new controls where there are gaps.

Does auditing/attestation contribute to the quality of and focus on internal control?

As a specialist in providing third party attestation services I may be biased in my opinion as to the reasoning for these good results. Of course there is an extraordinary amount of money and resources spent on security each year. My bias here would be to say that those companies that undergo a significant audit of the type required to issue a third party report or independent opinion as to the design and implementation of security controls have a tendency to learn from the audit and 'clean up' their reportable issues under the audit and, if findings are issued, afterwards. These audits generally subject the auditee to measurement against formal criteria such as the SOC2 Trust Criteria or COBIT or ISO27001 for an ISAE3402 / SOC1 report

Figure 3: Source - The Deloitte Global Outsourcing Survey 2018

using one of those standards as measurement criteria. The criteria are designed to measure a company's maturity against a set of best practice standards and when performing the audit, the auditee receives a set of control 'gaps' or weaknesses that they need to either clear or they turn into findings in the report, which will go to their customers.

In my experience, most organizations that take the step to initiate such an attestation project are receptive to observations and take them as 'constructive criticism'. This is dependent on us as the auditors and how we present our findings. If we can present findings in a manner that clearly highlights the risks the gap or weakness in controls presents to them and, if possible, come with good and constructive feedback and suggestions as to how they can remediate the issues, then the recipient of the 'bad news' has a tendency to look at the findings as positive opportunities for improvement. Through the iterative process of auditing and remediating issues, companies improve their overall internal control structure and often improve their IT Governance maturity in regards to internal control and information security.

How do companies address cyber risks with their vendors?

Based on the survey results, companies rely heavily on a regime of contractual commitment and periodic evaluation. This most likely reflects the uncertainties in the market these days in regards to various regulatory requirements and, in general, the difficulties involved in transferring some of your internal functions to an external party. Companies basically get

Figure 4: Source - The Deloitte Global Outsourcing Survey 2018

vendors to contractually commit to a form of behavior / provide a specific level of service and they follow-up that commitment with periodic assessments. There are basically 3 types of'assessments':

1) Self-assessment by the vendor (low level of security / reliance)
2) Assessment of the vendor by the customer itself (high level of security but dependent on the scope and depth of the review and also the competence and time commitment from the team performing the audit), and
3) Independent review by a specialized third party (high level of security but the receiver of any report needs to be aware of the scope of the audit performed to ensure the areas significant to them are included).

More complex organizations will most likely use a mix of these methods based on a risk-based analysis of their vendors and business partners to obtain a balanced approach to gaining assurance.

Security is foremost when choosing a cloud provider

Cloud is enabling competitive advantage by providing access to innovative technologies at the touch of a button, while avoiding many traditional roadblocks, including extensive up-front planning, capital expenditure, lengthy implementation times, and long term contracts. This is helping organizations be more agile, rapidly expand their offerings, enter new markets, and transform their internal operations.

When selecting a cloud service provider and designing solutions, executives' primary contractual concern is data security (68 percent), followed by performance/ resilience (45 percent), and providers' compliance with laws and regulations (39 percent). Data security and compliance issues can make organizations wary of adopting public cloud solutions, but this can cause them to miss out on its many benefits. A well considered cloud strategy must strike the right balance between achieving cloud's benefits and maintaining the appropriate levels of security.

CYBER RISKS WHEN MAKING OUTSOURCING DECISIONS

Nearly all respondents to the survey (95 percent) have cyber risk measures in place. About one-third (35 percent) of organizations contractually enforce data risk and security protocols with their providers and conduct period evaluations/audits. Clearly, organizations recognize the importance of proactive monitoring of cyber risk, and increasingly they are being proactive in its management.

In 2018, 78 percent of organizations reported that their outsourcing engagements were audited within the past 12 months; this is in line with 77 percent reported in an earlier survey from 2016. More audits were completed and passed (61 percent in 2018 vs. 53 percent in 2016), and fewer material issues were identified (15 percent in 2018 vs. 22 percent in 2016).

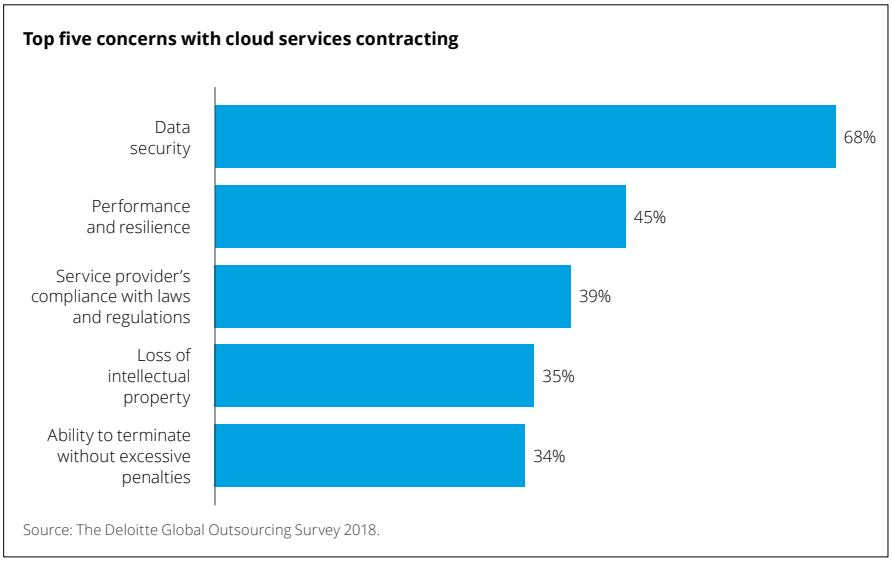


Figure 5: Source - The Deloitte Global Outsourcing Survey 2018

Security is also foremost when considering an RPA service provider

Digital labor is increasingly replacing repetitive, rules-driven tasks through automation, enabling faster, more efficient, and more accurate work at reduced costs, and fundamentally disrupting the old mantra of driving change through incremental improvements and labor arbitrage.

According to the survey, when selecting an RPA service provider and designing solutions, executives' primary contractual concern is data security (62 percent), followed by performance/ resilience (48 percent), and the providers' compliance with laws and regulations (42 percent). Approximately half of them see organizational resistance, process fragmentation, and regulatory constraints as their biggest implementation challenges. Of respondents using RPA, approximately one-third are also implementing cognitive automation, while another 59 percent plan to do so within the next 18 months.

What do the survey respondents plan to do differently in the future?

The survey asked respondents what they would do differently when launching their next outsourcing initiative based on their past experiences. The top responses were focused on the selection of providers as well as taking a more strategic planning approach.

- Service provider selection. The top responses were related to the selection process: spend more time in RFP or service provider selection (42 percent), and

use a competitive bidding process (39 percent). This may be due to the increasing maturity of both the procurement and vendor management functions within organizations.

- Strategic planning approach. Other popular answers involved taking a more strategic approach to planning a new outsourcing initiative: increase the scope of service (34 percent); transform the process rather than simply lifting and shifting (30 percent); invest in more robust service integration and transition (28 percent); and use a third-party advisor (27 percent).

What does this all mean?

My work experience is focused on the internal control aspects of outsourcing, performing third party attestation engagements (e.g., ISAE3402, SOC1, SOC2, ISAE3000), assisting clients in evaluating their maturity in regards to their vendor governance programs, performing individual vendor audits and reviewing the results of vendor audits. In the past years I have seen a drastic increase in the number of requests for independent verification / attestation of internal controls at outsourced vendors. SOC1, SOC2, ISAE3000 and ISAE3402 reports are becoming more commonplace in Norway as more companies are being required to provide them to their customers.

With global expansion for many service providers, we see that they are running into international customers that bring with them the contractual requirement of providing third party attestations and other forms for confirmation of good security or internal control. I currently deliver a number of SOC2 reports which focus on the areas of Security, Availability, Processing Integrity, Confidentiality and Privacy. The requests for these reports and the standard ISAE3402 / SOC1 reports that we generally issue are increasingly being driven by the larger, more influential and often international customers of the outsourcing service providers. This will only grow as our local Norwegian providers either expand their operations internationally through their own devices or through their being acquired by companies with an international footprint.

I fully expect the focus on outsourcing and the risks involved will be on the agenda for many years to come. One of the main areas that will continue to be in focus will be the area of information security and becoming comfortable with the vendor's internal control maturity in regards to the services being provided. Of course, GDPR trust issues between companies and security measures such as liability caps in regards to GDPR compliance risk in contracts will be driving many companies to want to prove to their customers and business partners that they are compliant. Independently produced third party attestation reports will be one of the most logical and useful methods for companies to show their compliance.

Exciting times ahead

I think that the recent developments in outsourcing outlined in the survey provide exciting opportunities for all involved parties. These new technologies present new risks and new challenges for us auditors. But if it was easy, it wouldn't be fun! Is suggest you take a look at the survey itself for more details than I have summarized here. The link is provided early in this article.

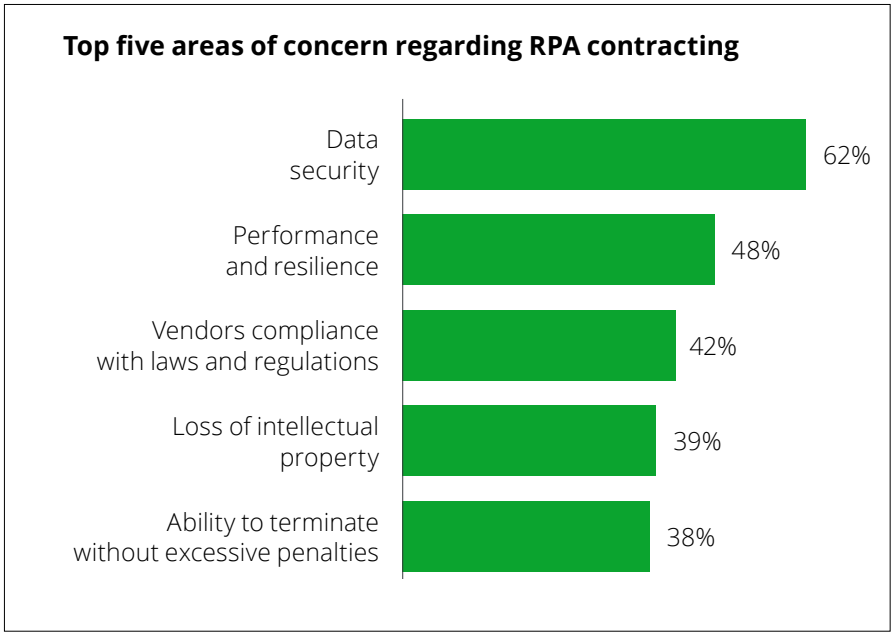
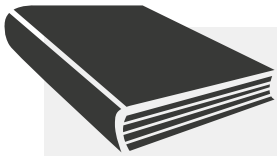


Figure 6: Source - The Deloitte Global Outsourcing Survey 2018

More organizations are conducting and passing audits with fewer material issues

76% of respondents indicated that regulations around data privacy and protection are affecting their disruptive outsourcing decisions

62% of respondents adopting RPA, and 68% of respondents adopting cloud indicated data security as an area of concern during contracting



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

Håkon Bergsjø og Ronny Windvik:

Datasikkerhet for ledere – hvordan beskytte din virksomhet

Universitetsforlaget, 2018

Den årlige mørketallsundersøkelsen som utføres av Næringslivets sikkerhetsråd viser at norske virksomheter har reelle utfordringer med datasikkerhet. Men det er ikke sikkert alle ledere vet at de har blitt utsatt for datainnbrudd. For å kunne forbedre kvaliteten i sikkerhetsarbeidet i norske virksomheter er det dermed sentralt at ledere har god bevissthet og forståelse for sikkerhet.

For å bidra til nettopp dette har Bergsjø og Windvik skrevet boken «Datasikkerhet for ledere – hvordan beskytte din virksomhet». Bokens fem første kapitler gir en grunnleggende innføring i datasikkerhet, ledelse, trusler og sårbarheter, verdivurderinger og risikovurderinger, mens de påfølgende kapitlene tar for seg ulike temaer som personvern, passord, innsidetrussel, tjenesteutsetting m. fl. og kan leses i en valgfri rekkefølge.

Trusler på internett

Etter et innledende kapittel, får leseren beskrevet hvilke trusler det finnes på nettet. Det er viktig at ledere er klar over hvem som utgjør trusselen og hvilken kapasitet og intensjon disse aktørene har. Hacktivisme er et eksempel på en ny variant som utføres for å påvirke holdninger og for å spre en ideologi, mens data-/internett-kriminalitet ifølge forfatterne er den vanligste formen for kriminalitet i Norge. Ofte dreier det seg om vanlig svindel hvor man ikke bruker datamaskiner til å gjøre innbrudd i andre datamaskiner. Et eksempel fra vårt eget land er gjerningsmennene som fikk med seg et utbytte på rundt 100 millioner etter en direktørsvindel uten at det fikk særlig stor oppmerksomhet. Spionasje er en annen form for datakriminalitet hvor formålet er å hente informasjon som er lagret digitalt. Det er ikke nødvendigvis så overraskende at forsvarsindustrien og annen høyteknologisk industri er utsatt for spionasje av aktører med høy kompetanse, men vi har normalt mye lavere bevissthet om at også informasjon om planer og beslutninger i det offentlige er utsatt for slik etterretning. Ved sabotasje anvendes datainnbrudd for å ødelegge eller forstyrre kritisk infrastruktur eller andre samfunnsfunksjoner. Heldigvis er det veldig få kjente eksempler hvor datainnbruddet har blitt brukt for å ødelegge infrastrukturen i andre land. Aktørene benytter ulike metoder. Selv om boken dekker mange ulike metoder, er det viktig å være klar over at vanlige og ofte relativt rimelige sikringstiltak, som følges opp systematisk, vil redusere risikoen betraktelig.

Kartlegge kritiske verdier

Videre viser boken en fremgangsmåte for å kartlegge og vurdere virksomhetens kritiske verdier, med utgangspunkt i virksomhetens verdikjeder. Hensikten med en slik kartlegging er å få frem en liste med sentrale verdier, datasystemer og data som får kritiske konsekvenser for virksomheter om de tapes eller reduseres. For å illustrere hvordan leserne kartlegger sine egne verdier, er det laget et eksempel i boken. I tillegg til verdier, anbefales det også å kartlegge hvilke verdikjeder virksomheten er avhengig av for egen verdiskaping og hvilke eksterne verdikjeder virksomheten er en del av.

Kontroll av risikoer

Senere beskrives det hvordan virksomheter kan kontrollere mulige avvik fra virksomhetens mål (=risikoer). Det henvises til to ulike modeller (Difi/COBIT) som både offentlige og private virksomheter kan ta i bruk. Etter at ledelsen har blitt kjent med sine risikoer, blir det lettere å iverksette tiltak ved bruk av et system for internkontroll.

Forfatterne Bergsjø og Windvik har skrevet en lettlest bok for ledere i ulike nivåer i organisasjonen, men også for alle andre som vil øke sin fagkompetanse innen datasikkerhet. Det viser seg også at det ofte nytter å beskytte organisasjonen med relativt enkle tiltak. Det som er viktigst at ledere er genuint opptatt av sikkerhet og kontinuerlig utfordrer organisasjonen ved å stille riktige spørsmål.

Ifølge sikkerhetsselskapet NTT Security anser fire av ti norske beslutningstakere at ledelsen er bedriftens største sikkerhetsrisiko[1]. Nordisk salgssjef i NTT Security, Henrik Davidsson, forteller videre at mange ledere er mer opptatt av tilgjengelighet enn sikkerhet.

Bruk av teknologi åpner for nye former for risiko. I Norge lager myndighetene og datasikkerhetsbransjen jevnlige trussel- og risikovurderinger som gir en god situasjonsforståelse for sikkerhetstilstanden både på internett og andre steder. Datasikkerhet har i løpet av de siste årene også fått stor oppmerksomhet fra journalister og hver uke skrives det om datainnbrudd i og utenfor Norge. Flere av disse kunne fått alvorlige konsekvenser dersom tilgangene hadde blitt misbrukt. Samtidig har det blitt påstått at Norge aldri har blitt angrepet[2]. Hvis ordet «angripe» betyr å virkelig skade noen via cyber, så finnes det ingen eksempler på det[3]. I det nylige angrepet mot Visma ble det også signalisert at ingen kundesystemer ble berørt av innbruddet[4]. Nå viser det seg at heller ikke dette stemmer.

Angrepet mot Hydro i mars viser at norske virksomheter i høyeste grad er utsatt for trusler som kan realiseres når som helst og ifølge en artikkel i NRK[5] er det Hydros heldigitale løsninger som har skapt utfordringer etter angrepet. Som en artig kuriositet har det samtidig vist seg at Hydro har unngått de aller største utfordringene etter angrepet takket være noen utvalgte ansatte, som ikke har stolt på datamaskiner og har arbeidet med papirbaserte løsninger.

[1] *https://e24.no/naeringsliv/datasikkerhet/fersk-undersoekelse-ledelsen-er-den-stoerste-sikkerhetstrusselen-for-bedriften/24433169*
[2] *Frem til april 2017*
[3] *Bergsjø og Windvik (2018), s. 22*
[4] *https://e24.no/digital/hacking/it-ekspert-om-maalet-med-visma-angrep-de-har-mye-informasjon-om-baade-bedrifter-og-personer/24555677*
[5] *https://www.nrk.no/norge/teknologipessimist-ble-helt-etter-dataangrep-1.14509963*

Et bestiarium for risikostyring

MARTIN STEVENS
Medlem av utvalget for risikostyring IIA Norge
og internrevisor i Gjensidige forsikring

Et bestiarium er en type litteratur som var populær i middelalderen, kun overgått av Bibelen i popularitet og utbredelse. Bøkene ble ofte rikt illustrert og tekstene skildret moralske beretninger om eksisterende dyr eller mytologiske fabeldyr som fønikser og enhjørninger. Dyrene ble tillagt menneskelige egenskaper og handlinger med den hensikt å tydeliggjøre hva som var moralsk oppbyggende, altså riktig å gjøre og hva som var motsatt – altså ondt. I de senere år er det dukket opp en del aktuelle dyr innenfor risikostyring som godt kunne trenge en tilsvarende forklaring.

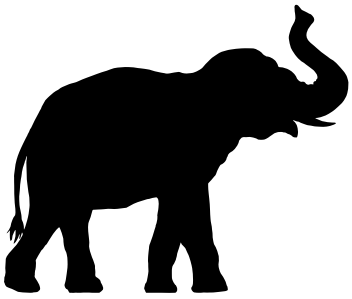
Den sorte svanen

Inntil europeerne fant veien til Australia trodde man ikke at sorte svaner eksisterte. Slik er den sorte svanen blitt et symbol på en risiko som materialiserer seg reelt nok, men som man ikke forestilte seg kunne eksistere. Ved finanskrisen i 2008 ble det fra ulike hold hevdet at man ikke hadde hatt forutsetninger for å forutse eller forestille seg at denne krisen ville inntreffe. Forfatteren av boken 'The Black Swan', Nassim Taleb mente lærdommen måtte være at 1) store hendelser kan være uforutsigbare og utenfor det vi kunne innbille oss men også at 2) beslutningstagere bør lage systemer som kan motstå store uforutsigbare hendelser. Hva er så en sort svane? Som den tidligere amerikanske forsvarsministeren Donald Rumsfeld uttalte; det er «the unknown unknowns», altså det vi ikke vet at vi ikke vet. Se også forholdet mellom risikostyring og beslutninger i figuren under som er gjengitt i Veileder for Risikostyringsfunksjonen utgitt av IIA Norge.

Beslutningstaker	Utfallsegenskaper	Utfall
Intern beslutningstaker F.eks: Å drikke en kopp kaffe	Deterministisk	Kjent og sikker – kaffekoppen er tom
Intern beslutningstaker F.eks: Estimering av antall fremtidige studenter i kommune X	Stokastisk påvirket av tilfeldigheter	Sannsynlighetsfordeling av utfallet er kjent / kan estimeres
Intern beslutningstaker F.eks: Introdusere et helt nytt produkt i et marked	Stokastisk	Sannsynlighetsfordelinge n er ukjent
Ekstern beslutningstaker – oppfattet gjennom «what if» scenarioer («known unknowns») F.eks: Opptøyer	Kaskade-, snøballeffekter, «fat tailed distribution»	«Grey Swan»
Ekstern beslutningstaker – ukjent hendelse kommer overraskende («unknown unknowns») F.eks: 9/11	Sannsynligheten kan ikke beregnes med teknikkene vi besitter i dag. Blir ikke oppdaget gjennom «what if» scenarioer	«Black Swan»

Den sorte elefanten

Den sorte elefanten eksisterer ikke i naturens verden, men innen risikostyringen er den en rar krysning mellom sort svane og elefanten i rommet. Sagt på en annen måte representerer den sorte elefanten sjeldne, men betydelige risikoer som alle har kjennskap til men helst ikke vil gjøre noe med. Eksempler kommer først og fremst fra miljøsiden med temaer som global oppvarming, avskoging, masseutryddelse mm. Elefanter er forøvrig flokkdyr og dukker sjelden opp alene……



Det grå nesehornet

Alle nesehorn i naturen er i praksis grå, selv om man i zoologien har definert to arter; de hvite og de sorte. Innen risikostyring er det grå nesehornet til forveksling lik en sort elefant. Som Michele Wucker uttrykker det i sin bok om arten er det grå nesehornet elskovsbarnet til den sorte svanen og elefanten i rommet som ingen ser. Grå nesehorn er store og farlige som svaner og elefanter, men i motsetning til de dyrene er de meget sannsynlige og står i angrepsstilling rettet mot oss. Det positive er dog at vi har mulighet til å sette i gang mottiltak – gitt at vi handler i tide. Med andre ord er grå nesehorn 'kjente kjente' som vi er blinde for i motsetning til de hvite svaner, som vi ser.

Den hvite svanen

Egentlig er den hvite svanen lite omtalt innen risikostyring og kan trolig best defineres ved at den ikke er en sort svane. I Aberdeen bestiarium heter det «Olor autem dicitur quod sit totus albus plumis. Nullus enim meminit cignum nigrum» På norsk lyder det omtrent som følger: «Forresten kalles det for «olor» fordi alle fjærene er hvite. Ingen husker noen gang å ha sett en svart svane.» Skulle vi våge oss på en definisjon er en hvit svane en risiko som er kjent og tydelig for alle.

Den grå svanen

Enkelte risikoer har lav sannsynlighet for å inntreffe, men vil dog ha store konsekvenser (tenk f.eks cyberrisiko). Denne typer risikoer er 'kjente ukjente'. I naturens verden er en grå svane en ung svane som fortsatt ikke har skiftet farge til hvit. I risikostyringssammenheng forblir en grå svane ofte grå. Dog kan man noen ganger oppleve at bedre informasjonsgrunnlag bidrar til at beregning av sannsynligheten gjør at den også innen risikostyringen forvandler seg til en hvit svane.

SPERR OPP ØYNENE!

Jeg lurer på om vi vil se behov for andre dyr i vårt bestiarium for risikostyring, og om det grå nesehornet vil seire over den sorte elefanten. Vil vi klare å oppdage sorte svaner før det er for sent? Da må vi løfte blikket, sperre opp øynene, lytte og være årvåkne for alt som skjer rundt oss, tenke utenfor boksen og forsøke å forutse det som ingen andre ser. Kan hende lykkes vi, men det er ingen unnskyldning for ikke å varsle om de grå nesehornene som står klare til angrep. Her kommer vi langt med et objektivt og spørrende sinn samt vilje og mot til å tørre å fortelle keiseren at han ikke har klær på.

Risk culture beyond ticking boxes

SVETLOZAR KARANESHEV
MSc in Business Administration

Introduction

In a previous article published in SIRK 1/2018 I challenged whether internal audit is meeting the challenge of addressing appropriately the area of risk culture and I suggested the need for the organisation to start by developing a better understanding and a common language for risk culture. In this article I wish to demonstrate further how it is possible for an organisation to develop and change its culture and what tools are available to guide this process.

> The corporate culture is the most powerful control in any organization.
>
> *Jim Roth, author of Best Practices: Evaluating the Corporate Culture*

Risk culture is not something that is static. It is an evolving process that can be influenced and where changes can be managed. Organisations have therefore the ability to develop the risk culture that they wish for. To manage this, we need to look at risk culture through cultural lenses. Culture has many dimensions and we need to decide which of them are the most important to focus on. Assessing and managing risk culture should definitely not be a box ticking exercise.

The box ticking syndrome

In the corporate governance field, the box ticking syndrome defines a formal approach to the implementation of corporate governance principles – doing something just because there is a rule that says that you must do it[1,2]. Over the last few years, financial regulators (mainly in the banking and insurance sectors) are requiring companies to implement processes for the development and management of risk culture as part of the corporate governance framework. Can risk culture fall into the box ticking trap?

According to the European Banking Authority (EBA) «Institutions should develop an integrated and institution-wide risk culture» [3] as a tool for effective risk management and to enable good decision making. The minimum elements of strong risk culture according to EBA are:

(1) tone from the top – the management body should be responsible for setting and communicating the institution's core values;
(2) accountability – employees should know and understand the core values of the institution and must be held accountable for their actions;
(3) effective communication and challenge – a sound risk culture promotes open communication, and
(4) incentives – incentives should pay a key role in aligning risk taking with the institution's risk profile and long-term interest.

This framework was first presented in the Financial Stability Board's (FSB) Guidance on supervisory interaction with financial institutions on risk culture[4]. It draws on the experience and efforts of supervisory and regulatory authorities across the FSB membership and insights garnered from the market participants through roundtables and bilateral discussions[4]. The Guidance proposes a wide range of indicators of sound risk culture in accordance with the defined framework.

The clear framework and the large set of indicators may lead to the temptation

to develop a list to «diagnose» or «check» the level of risk culture in the organization and to prescribe actions to improve risk culture. Will it work? The use of the term «indicators» to refer to elements of risk culture could be misleading as it implies a linear relationship where the performance of each element can be manipulated individually. This is not the case as it is the totality and interaction of all the elements which makes the culture, and for this reason the checklist approach to measuring culture is wholly inappropriate[5]. If the supervisors and management of financial institutions want to assess culture and its influence on risk management, they need to consider the organisation's training and building of cultural experiences with a focus on behavioural analytics techniques. Culture is a complex issue and the temptation for boards and executives is to want to manage it in the same way as other business areas must be resisted.

Risk professionals (risk managers and internal auditors) need to dig below the surface and gain a deeper understanding of the true nature of the organizational and risk culture as the basis for understanding how culture can be both managed and changed.

Risk culture from the cultural perspective

If the appropriate definition of culture is not chosen then its application to the firm's management of risk opens up for many varied interpretations and may be subject to presumptions, misinterpretation and confusion[5]. Culture is the product of social learning by a group as it solves its problems of external integration and internal adaptation. As a product of learning from the interaction between the organization's members and their environment, the organizational culture evolves naturally (as organizations change) as well as by managed change (the leader may initiate change in an organizational culture when evolutionary processes are too slow or develop in the wrong direction)[6].

The definition of culture is important, but it is not sufficient in itself. We need to have a model or concept to support the definition. If we choose a model, we need to be sure that the selected model describes well enough the culture of the organization. Models are based on theoretical assumptions and empirical research and are developed to help us to simplify the process of the analysis and management of culture, but they have limitations[6]. We can dig deeper and discover the underlying concept of the management of culture by reviewing some of the widely used and well described approaches/models for the assessment and change of organizational culture e.g. by reference to Edgar H. Schein's[6,8] organizational culture model (box 1), The Competing Values Framework of Cameron and Quinn[9, 10] (box 2) and The Seven Levels Model of Richard Barrett[11, 12] (box 3) and identify the

Edgar Schein Organizational culture model

Schein's Organizational culture model divides organizational culture into three different levels:

1. Artefacts and symbols

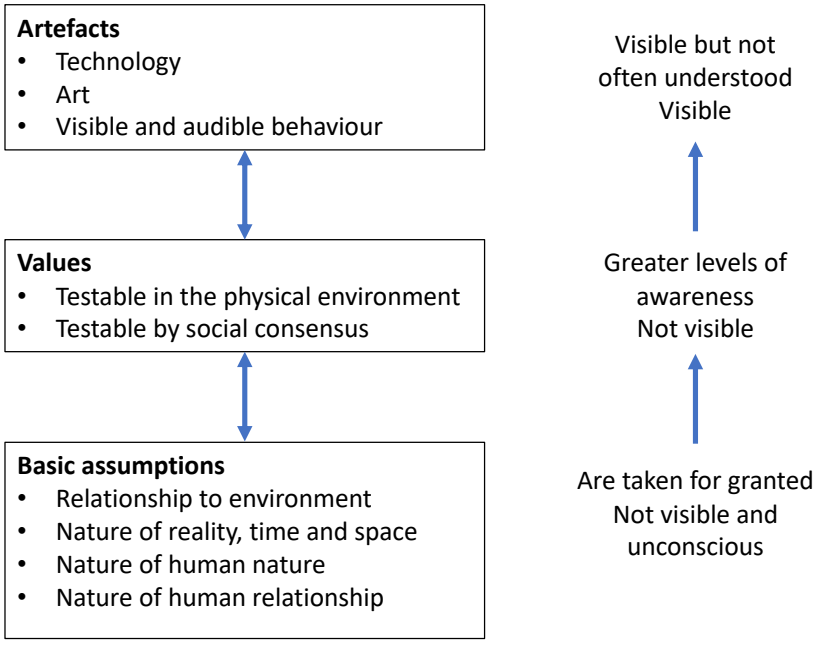
Artefacts mark the surface of the organization. They are the visible elements in the organization such as logos, architecture, structure, processes and corporate clothing. These are not only visible to the employees but also visible and recognizable for external parties.

2. Espoused Values

This concerns standards, values and rules of conduct. How does the organization express strategies, objectives and philosophies and how are these made public? Problems could arise when the ideas of managers are not in line with the basic assumptions of the organization.

Basic underlying assumptions

The basic underlying assumptions are deeply embedded in the organizational culture and are experienced as self-evident and unconscious behaviour. Assumptions are hard to recognize from within.



Box 1

common denominators in these approaches.

The first (and perhaps the most important) common thread is that managing culture is methodologically relatively similar to the process of managing change. The process used by the different approaches differs in the details, but is the same in general and can be defined as:

- Discovering the existing culture – there are two approaches to doing this: model based (Kim S. Cameron and Robert Quinn and Richard Barrett) and the "deciphering" approach of Edgar H. Schein. Both approaches use indepth interviews and discussions regarding existing culture and/or participatory approaches (like workshops). Model based approaches use, in addition, questionnaires and values inventories based on the models. As a result, a consensus view on the current organizational culture emerges.

  Values also play a key role in forming culture. Effecting change in behaviour and actions by changing values and beliefs is the essence of cultural transformation according to Richard Barrett. Behaviour is the manifestation of the culture (Kim S. Cameron and Robert Quinn). Change remains superficial and of short duration if it does not lead to an alteration of fundamental goals, values and expectations both of the organization and of the individual. Behaviour is an artefact according to Schein and it is driven by espoused values and shared tacit assumptions
- Designing the target culture – the same instruments and tools are used as in the discovering stage and some additional tools such as appreciative inquiry[13] (a change management approach that focuses on identifying what is working well, analysing why it is working well and then doing more of it), four whys[12, 14] (this tool helps individuals in a group to create their team vision and mission and to clarify the
- connection to an external vision and mission for example to that of their customers and society) and other tools[12] are applicable. As a result, a consensus view on the target organizational culture is defined.

The Competing Values Framework

From a list of thirty-nine indicators of effectiveness for organizations, Cameron and Quinn found two polarities by statistical analysis that make the difference when it comes to organizational effectiveness. Organizations have to choose whether they have:

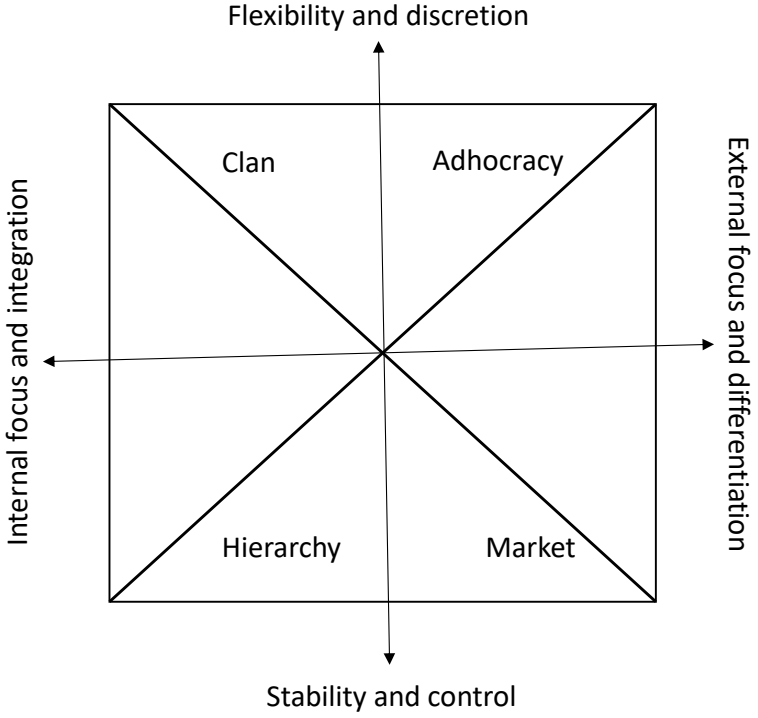
- Internal focus and integration - or - External focus and differentiation
- Stability and control - or - Flexibility and discretion

You can›t have both polarities at one hundred percent at the same time. Hence, they are competing values. By plotting those two dimensions in a matrix, the Competing Values Framework emerged. Its four quadrants correspond with four Organizational Culture Types that differ strongly on these two dimensions or four values: Clan Culture; Adhocracy Culture; Market Culture and Hierarchy Culture.

Box 2

To the left in the graph, the organization is internally focused: what is important for us, and how do we want it to work? To the right the organization is externally focused: what is important for the outside world, the clients, and the market? At the top of the graph, the organization desires flexibility and discretion, while at the bottom the organization values the opposite: stability and control.

https://www.ocai-online.com/about-the-Organizational-Culture-Assessment-Instrument-OCAI/Competing-Values-Framework
https://www.ocai-online.com/about-the-Organizational-Culture-Assessment-Instrument-OCAI/Organizational-Culture-Types/



- Delivering the necessary changes – this is effected by means of a change plan and the tools and the key performance indicators for culture change. The tools depend on the change management approach used and the cultural model chosen. Schein proposes two approaches:

(1) role models and behavioural examples or (2) stating clear behavioural goals and initiating a learning (trial and error) process. Richard Barrett uses personal alignment programs, group cohesion programs and value alignment programs. Kim S. Cameron and Robert Quinn combine organizational tools (stories, strategic action agenda, small wins, leadership implications, metrics and communication strategy) and personal development programs.

The role of leadership in the process of cultural change (management) is very important. According to Schein[6], culture and leadership are but two sides of the same coin and leaders are the ones who start the process of culture creation. The leaders of the group must drive the process of cultural change according to Richard Barrett[12]. Kim S. Cameron and Robert Quinn[10] state that leadership is an important factor of organizational culture and treat the ability to identify the most valued leadership attributes for the different types of culture as a separate cultural dimension. All this means that leaders are the main architects of culture and if elements of the culture become dysfunctional, leadership can and must drive culture change.

Practical implications for risk professionals

To avoid a box ticking approach and gain deeper understanding as to how culture works in our organization and how to manage it we need to:

Discover. Before trying to change our culture, we have to discover it "as is". As Richard Barrett says – you have to meet people where they are before you can take them where they want to go![12]. To discover our existing risk culture, we need to answer two important questions: [1] what are we doing when managing risk (what are the artefacts of risk culture)? and [2] why are we doing the things we are doing (what are our values and deep assumptions)? We can find the answers using models, that describe the culture (models are useful but must be deployed with care) or to use a culture deciphering approach.

Design. Culture has many dimensions and we need to decide which of them are most important and how they affect risk culture and risk management. Designing the target risk culture means to define what are the right behaviours when managing risks and what values and assumptions stay behind them.

Deliver. All work in risk culture management must be done with one simple concept in mind – managing culture is managing the change in the behaviour of people (Organizations don't transform! People do![12]). Change management can be done by using role models and behavioural examples or by employing a more sophisticated change management approach by using dedicated tools depending on the goals for example organizational tools (stories, strategic action agenda, small wins, leadership implications, metrics and communication strategy) and personal development programs.

Leaders play the most important role in this process – they are the main architects of culture and if elements of the culture become dysfunctional, leadership can and must drive culture change.

The Seven Levels Model of Richard Barrett

The Seven Levels Model describes the evolutionary development of human consciousness. There are two aspects to the model—the Seven Levels of Consciousness® Model and the Seven Stages of Psychological Development Model. People operate at levels of consciousness and grow in stages (of psychological development). The Seven Levels of Consciousness Model applies to all individuals and human group structures—organisations, communities, nations. The Seven Levels of Psychological Development Model applies to all individuals. The following diagram shows the correspondence between the Seven Levels of Consciousness and the Seven Stages of Psychological Development.

https://www.valuescentre.com/mapping-values/barrett-model

Box 3

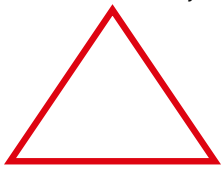
1. *D. Larkey, B. Tryan, Corporate Governance Matters; Pearson Education; 2011;*
2. *Ulrich Steger (Editor), Peter Lorange (Editor), Fred Neubauer (Editor), John L. Ward (Editor), Bill George (Editor), Mastering Global Corporate Governance; 2004; John Wiley & Sons*
3. *European Banking Authority, Guidelines on internal governance, 2018 https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance-revised-*
4. *The Financial Stability Board, (FSB), Guidance on supervisory interaction with financial institutions on risk culture, 2014 http://www.fsb.org/2014/04/140407/*
5. *Paradigm Risk Consulting, "To boldly supervise…", 2014 http://www.fsb.org/wp-content/uploads/c_140206rr.pdf*
6. *Edgar H. Schein, Organizational Culture and Leadership, 5th Edition (The Jossey-Bass Business & Management Series) 4th Edition, 2010*
7. *De Nederlandsche Bank, Supervision of Behaviour and Culture, 2015 https://www.dnb.nl/binaries/Supervision%20of%20Behaviour%20and%20Culture_tcm46-334417.pdf*
8. *Edgar H. Schein, The Corporate Culture Survival Guide, J-B Warren Bennis Series Book, 2009*
9. *The Competing Values Framework https://www.ocai-online.com/about-the-Organizational-Culture-Assessment-Instrument-OCAI/Competing-Values-Framework*
10. *Kim S. Cameron, Robert Quinn, Diagnosing and Changing Organizational Culture, Based on the Competing Values Framework Third Edition, Jossey-Bass, 2010*
11. *The Seven Levels Model https://www.valuescentre.com/mapping-values/barrett-model*
12. *Richard Barrett, Building a Values-Driven Organization: A Whole System Approach to Cultural Transformation, Butterworth-Heinemann, 2006*
13. *Dr David L Cooperrider, Diana Whitney, Appreciative Inquiry: A Positive Revolution in Change, Berrett-Koehler Publishers, 2005*
14. *Tor Eneroth and others, Get Connected https://www.valuescentre.com/resources/get-connected/get-connected-book#get-connected-english*

Krystallkulens plass i risikostyring

MARTIN STEVENS
Medlem av utvalget for risikostyring IIA Norge og internrevisor i Gjensidige forsikring

Om bruk av scenarioer i risikostyring

Det er mange ledere som kunne tenkt seg å ha en krystallkule for å kunne forberede virksomheten sin for fremtidens utfordringer. Med denne artikkelen ønsker jeg å oppmuntre til at bruk av scenarioanalyse kan være en virtuell krystallkule som Risk Manageren godt kan ha med seg i sin verktøykasse.



Ukjent fare

Om risikostyring og fremtiden

I bunn og grunn innebærer risikostyring arbeid med å styre i en usikker fremtid . Dagens fremtiden er et ukjent landskap som kun kan beskrives nøyaktig når det er blitt endret via nåtid til fortid. Derfor er det relevant å undersøke hvilke hjelpemiddel som finnes for bedre å kunne forstå hva vi kan forvente av fremtiden. Nedenfor vil jeg beskrive to ulike tilnærminger.

1) Den ene er å beskrive fremtiden ved hjelp av data fra nåtiden og forutsette at det også beskriver fremtiden på en god måte. Det vil si vi kan ekstrapolere utfra de historiske opplysninger vi besitter. Økonomifunksjoner bruker ofte denne metoden justert for kjente endringer i virksomheten (f.eks. nytt salgskontor) og omverdenen (f.eks. inflasjonssats) for å prognostisere for fremtiden. Den delen av en slik prognose nærmest i tid vil danne årets budsjett. Svakheten med slike analyser er at man ofte fastsetter et sett med tall som ignorerer de store usikkerheter knyttet til fremtiden. Dette gjelder særlig i vår tid der endringshastigheten i f.eks. markeder, produkter, politikk er relativt høy. Det er heller ikke vanlig at kommersielle virksomheter treffer særlig nøyaktig når poster i resultatoppgjøret sammenlignes med budsjettmål. Derfor kan det ved budsjettering være fornuftig å operere med et spenn av alternativer av typen «best case» og «worst case» prognoser. Dette vil også kunne bidra til fokusering på kritiske innsatsfaktorer, og til å kunne flagge tidsnok til å iverksette korrigerende tiltak der utviklingen går i feil retning.
2) I finansnæringen er det blitt vanlig å operere med risikostyringsmodeller som prognostiserer mulige utfall i fremtiden basert blant annet på dagens situasjon, foreløpige prognoser, historisk utvikling samt kjente samvariasjoner. I en slik tilnærming synliggjøres usikkerhet med hjelp av stokastiske metoder kombinert med simuleringer. Denne metoden gir også en utmerket mulighet til å analysere hvor følsomt det forventede resultatet er når de ulike parameterne (herunder også samvariasjon) endres. Ulempen med denne metodikken er at den ikke er så egnet til å fange opp effekten av større endringer i forretningsmønsteret fremover, som endringer i kompetansebehov, teknologisk utvikling eller endringer i markedet og samfunnet osv.

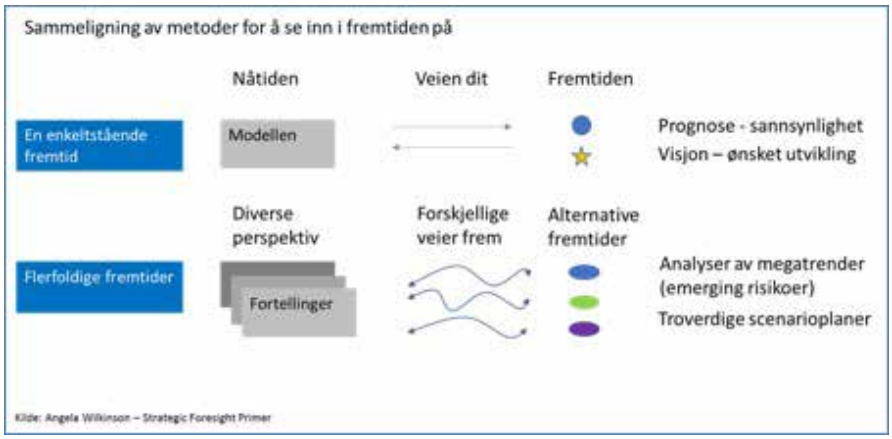
Om bruk av scenarioanalyse

I risikostyringsarbeid har det etter hvert blitt vanlig å identifisere nye risikoer (emerging risks) som risikoer som ennå ikke er kommet klart til syne, og derfor ennå ikke har hatt noen identifiserbar påvirkning på virksomhetens drift. Dersom det ikke foretas en videre analyse av de identifiserte risikoene kan det av ledelsen oppleves som å kjøre på en vei og se et rødt «ukjent fare» skilt foran seg. Bilføreren vil da normalt kjøre mer forsiktig, men det kan oppfattes noe frustrerende å ikke vite hva man skal akte seg for. Det vil hjelpe føreren betydelig om veimyndighetene lager trafikkskilt som gir bilister noen flere opplysninger, slik at de f.eks. vet om de skal redusere hastigheten, kjøre en omvei eller se opp for elger. Innen risikostyring vil dette bety at den som arbeider med risikostyring skal kunne kvantifisere effekten av «nye» risikoer, slik at disse risikoene får nødvendig oppmerksomhet hos ledelsen. Vi vet av erfaring at det som måles i kroner og ører vil få oppmerksomhet på en helt annen måte enn det en gul klassifisering klarer. Spørsmålet er om det i det hele tatt er mulig for risk manageren å kvantifisere effekten av slike nye risikoer. Svaret kan være at scenarioanalyse kan være et egnet verktøy.

Scenarioanalyse er et verktøy som tradisjonelt har vært anvendt av forretningsutviklere som arbeider med strategier, men medarbeidere innen risikostyring kan også ha glede av å ta verktøyet i bruk. Helt presist vil prognostisering bety å gå baklengs inn i fremtiden, mens med scenarioanalyser ønsker vi å øke vår forståelse om risikolandskapet lengre frem i tid. Forståelsen av alternative scenarier i fremtiden kan gjøre at vi bedre kan styre virksomhetens utvikling i dag, og ikke minst iverksette de tiltak som trengs for å legge om virksomhetens strategi før det er før sent. Ved å løsrive seg fra den historiske utviklingen, vil det også bli lettere å tenke «utenfor boksen».

Gjennom en scenarioanalyse får man mulighet til å vise et sett med flere mulige bilder av fremtiden (f.eks. 15 år frem i tid). For hver av disse bildene kan det lages en troverdig og logisk fortelling. Ut fra en slik fortelling kan risk manageren ha en rolle i å oversette et fremtidig scenario til resultatparametere og regnskapsmessige effekter.

I figur 1 sammenlignes billedlig de to måter å se inn i fremtiden på – prognostisering og scenarioanalyser.



Figur 1

1 ISO 31000 «risiko defineres som virkningen av usikkerhet knyttet til et mål»

2 Men for all del prognostisering har sin plass og jeg henviser til bokanmeldelsen i SIRK 2018/2 s. 36 «Superforecasting» om boken med samme navn der det fortelles om forskning på muligheten til å lære å være mer treffsikker i prognosearbeid

3 ECA Journal No. 10 https://www.eca.europa.eu/en/Pages/Journal.aspx

4 Strategic Foresight Primer av Angela Wilkinson utgitt av European Political Strategy Centre https://ec.europa.eu/epsc/publications/other-publications/strategic-foresight-primer_en

Konklusjon

De som arbeider med risikostyring forventes å være opptatt av hvordan fremtidige risikoer vil påvirke virksomheten. Noen ganger vil engen blomstre på grunn av de frøene vi sådde i fjor, mens andre ganger kan det være basert på hva fuglene og vinden bringer med seg. For å kunne få et innblikk i hva som kan få fremtidens eng til å blomstre eller visne, bør risikomedarbeidere utfordre seg selv og sin fagkompetanse gjennom å ta del i arbeidet med fremtidsscenarier.

Etterord

Artikkelforfatteren ble inspirert til å skrive denne artikkelen etter å ha lest en artikkel om dette temaet i fagbladet utgitt av European Court of Auditors i oktober 2018, med tittelen «Foresight – Exploring possible futures for better decisions today» . Derfra ble jeg ledet videre til et annet dokument som heter «Strategic Foresight Primer» som ga en god og praktisk innføring i temaet og en oversikt over scenariometoder. Illustrasjonen i figur 1 er hentet fra dette siste dokumentet.

What is the greatest risk, a medium risk or a medium risk?

The three steps of cyber risk management improvement

BY NIKLAS LARSSON
Transcendent Group https://transcendentgroup.com/consultant/niklas-larsson/

Photo: Shutterstock.com

If you search for best practices in cyber risk management you almost always end up with the green, yellow and red heatmap. You assign a number to the probability and consequence and multiply them, and you get a number you can put somewhere on the heatmap. You understand that the risk with a higher number is more important to put controls on but don't really understand how important. So, you add percentage ranges for the probability and monetary ranges for the consequence. Now you understand better the risk to the business. After adding some risks, you end up with bunch of risks in the same square on the heatmap, so you increase the size of the heatmap to prioritize easier. You are happy because now you know your risks, and in which order you should put controls. Then you get three questions: *What is our risk exposure? How much can we lose? If we spend 250 000 Swedish kronor (SEK), how much will the risk exposure decrease?*

You answer that we have 50 medium and 7 high risks and if we spend 250 000 SEK we will end up with 45 medium and 5 high. But is that really an answer? Is 45 medium and 5 high in line with the risk acceptance? How much money is really at stake for the organization and with what probability?

A better answer would be: *We have a probability of 5% of losing 1 000 000SEK or more within the next 12 months, this violates our risk acceptance (aka risk appetite). 250 000 SEK would get us down to 4% probability of losing 900 000SEK or more the next 12 months, which is in line with our risk acceptance.*

I know what you are thinking, it's impossible to know that. And you are right, it is impossible to know that. But is 100% certainty needed? What you need is estimations you can trust, that support decision making and prioritization without ambiguous language. You can never know if 4% really is 4%, as little as you can know a low is a low and not a medium. The biggest problem with the low is it can mean 1% probability to me and 15% to you, do we really see the risk in the same way then?

The heatmap has another limitation too. Every risk is managed separately, you can't get a business wide visualization of the risk exposure. A simple but not perfect solution is described in the book "How to measure anything in cyber security risk" by Douglas W. Hubbard. Instead of

assigning a score to the probability of a risk you set the probability in percent and for the consequence you assign a loss range you are 90% certain of (90% Confidence Interval, CI). You then add the risks to an excel sheet with monte carlo simulation. The result is presented as a loss exceedance curve (graph) expressing the risk exposure. Not perfect but a really good start in improving cyber risk management.

The loss exceedance curve visualizes three things at the same time which makes it easy to understand, the inherent, the residual risk and the accepted risk. On an organization wide scale. This enables understanding of the total risk exposure without the ambiguous language of low, medium, high or a score. As the Confidence Interval (CI) express uncertainty, a security measure can be to reduce the uncertainty by collecting and analyzing data, in other words, to understand the risk better. The new knowledge might have a great effect on the risk exposure, not everything is hard security measures like new technology or routines.

For example, we have assigned a risk a CI of 100 000 – 20 000 000 SEK. This express great uncertainty, we should probably assign resources to understand the risk better. After spending 20 hours in collecting and analyzing data we change the CI to 500 000 – 10 000 000 SEK, this uncertainty reduction will have an effect on the loss exceedance curve and by that our risk exposure. So instead of directly trying to put controls like creating a new routine or buying new equipment we affect the risk exposure just buy analyzing it more and reducing our uncertainty. Maybe the 20 hours spent have saved us some money.

This method also enables minor estimation of changes to the risk as we gain new knowledge. Moving a risk from red to yellow on the heatmap usually requires some major changes and feels like a daunting task. Changing a probability from 5% to 4,5% or CI from 100 000-400 000 to 120 000-380 000 requires less effort. Making small frequent changes is something Philip Tetlock in his research about forecasting found can increase the accuracy, he describes this in his book "Superforecasting". So, maybe we can get better risk estimation accuracy by including risk assessment in our daily work instead of having one large yearly risk workshop.

This brings us to improving the estimations given by subject matter experts and others. Richards J. Heuers Jr. writes something worth a thought in his book "Psychology of intelligence analysis":

"analysis is, above all, a mental process. Traditionally, analysts at all levels devote little attention to improving how they think."

Philip Tetlock writes the following in "Superforecasting" about the learnings from his forecasting research project:

"for it turns out that forecasting is not a "you have it or you don't" talent. It is a skill that can be cultivated"

This is why a good start to the cyber risk assessment is to begin with learning basic techniques in estimation and information analysis. Both the cyber risk framework FAIR and Hubbard advocate calibration which from my experience works well. Calibration is a way to practice estimation techniques and improve your skills in estimating your own uncertainty. This means that, if you are good at estimating your own uncertainty and answer 10 questions with 50% certainty you should have 5 correct answers (50%), if you are 80% certain you should have 8 correct answers. By measuring this we can understand how good the estimates given during the risk analysis are. We can never know if 4% probability really is 4% but we can know how good the person behind the number is at estimating. This brings us to a new learning from Philip Tetlock's research: measurement is essential to improve estimates. In Tetlock's research he found that experts are bad in forecasting and one reason may be that the accuracy of forecasts is never measured. He writes in his book Superforecasting[1] :

"The consumers of forecasting — governments, business, and the public — don't demand evidence of accuracy. So, there is no measurement. Which means no revision. And without revision, there can be no improvement"

When the calibration is done, the risk workshop can be held but the workshop should only identify risks. The analysis should be performed individually for let's say, two weeks. During these two weeks the persons giving estimates are encouraged to reduce his/her uncertainty by reading agreements and looking at old incidents or infrastructure maps. After this they assign their probability and CI. How much they want to reduce their uncertainty is up to them as uncertainty reduction comes at a cost (time is money). And the closer you get to absolute certainty the higher will the price be, the cost is exponential. Moving from 50% certainty to 60% is cheaper than from 97% to 99%. But with continuous small changes to the risk you will continue improving estimation skills and reduce uncertainty.

To conclude, you can divide the cyber risk management improvement into three steps, of which the first two have been covered in this article. The first step is to start using a method which removes ambiguous language and enables organization-wide aggregation and visualization of the total risk exposure. Step two is to avoid garbage-in, garbage-out by calibration, information analysis training and measurement. The more practice the better, but do not forget to measure improvement. As the last step a technical tool could help, the staff is trained in not putting garbage in, so the algorithms will not give garbage-out. But remember, analysis is above all a mental process.

This article is reprinted with permission from Transcendent Group transcendentgroup.com

[1] *Ref. book review «Superforecasting» in SIRK 2/2018*

Digital transformation - is cyber threat really the greatest risk of all?

BY OWE LIE-BJELLAND
Director GRC Solutions, Corporater

In a myriad of new risks, which is the number one most significant risk related to digital transformation?

Introduction

In the late 90's cyber and information security was in its infancy. So was I, I was in my mid-twenties and my aspiration was to leverage the new web technology to deliver enterprise-grade applications over the Internet. I was the technology guy and the co-founder of one of the first Software as a Service (SaaS) providers in Norway. As a SaaS provider handling some of the most business-critical information for the global oil & gas industry, information and cyber security were paramount to building our business due to the risk of negative reputation and legal consequences that obviously would have caused great loss and possibly bankruptcy for our boutique SaaS business. This is not to mention the ethical responsibility we took on to protecting our customer's data. I remember my partner once said, "if we get hacked, the financial consequences are so big we can just go home, and we don't even have to lock the door behind us". I started working on what would turn out to become a success, and what would give me great insight. It was hard work; however, my main challenges were not related to the complexity of establishing and maintaining an internal management system or keeping up with regulatory and legal requirements. My main challenges were firstly to make the board understand the potential loss and ROI for our negative and positive risks, resulting in dollars in my budget, and secondly to make the internal and external auditors understand our digital business.

History of risk assessment for information security management

In the early days of information and cyber risk, back in the era of ISO 27001:2005, risk assessments were conducted focusing on the infrastructure components and the deployed software. Consequence and probability were assessed using a qualified approach, also considering the component's vulnerability to calculate the risk level. This approach was good enough for the IT department to reduce the risk to a perceived acceptable level, however, it only got us so far. Problems arose when trying to enhance security further as we realized we painted ourselves into a corner. The work we produced was great for communicating internally among peers who understood the technical and security-related domain, however, it was not something we could easily share with top management to argue for doubling the security budget in the coming year.

With ISO 27001:2013 we saw a shift to align information security management more with enterprise risk management and the insistence on understanding the business context for correct implementation. This, along with digitization, led to a shift to place more emphasis on the assets i.e. actual information and information containers. The risk assessment methodology was enhanced to a semi-quantitative approach where intervals were used to decide the consequence. This was a step in the right direction, however, due to the nature of an interval scale, you cannot do any calculations when trying to aggregate and consolidate risks across departments and up the chain. This approach was still not optimal for communicating effectively outside an IT and security context. The challenges so far were very much related to digitization. However, when a company wants to disrupt its business model thru digital transformation, new risks are introduced.

Digital transformation comes with greater risk exposure

Digital transformation results in a merger of business context and digital context. The two worlds meet causing a reaction on bringing the new knowledge into the board room, blended with the expectation from the board that assurance and operations will add additional value to the business.

Where is the value?

Let's start with a common denominator; any business needs to properly manage its assets. With digital transformation comes the need to assess and manage a business' digital assets. These assets are the same assets security staff are protecting and anabling. However, assets are still very much out of sight or given less priority as initiatives, processes, infrastructure, cloud, and applications. Reading risk and assurance reports, I seldom see anybody focusing on assets. In a press release from 2017[1], Gartner says that "the value of an organization›s information generally cannot be found anywhere on the balance sheet". In the same press release, analyst

Photo: Shutterstock.com

Douglas Laney says that «anyone properly valuing a business in today›s increasingly digital world must make note of its data and analytics capabilities, including the volume, variety, and quality of its information assets». Further, Gartner predicts that "by 2022, organizations will be valued on their Information portfolios". If you think about it, how big a proportion of your company's assets are digital? You might be surprised to learn that they could easily add up to over 80%. With digital assets becoming a vital part of the business, it is a key figure when assessing the value of the business in an M&A setting, and it is increasingly important in an insurance context. The CFO office includes the current value of business-assets on the balance sheet, but what about the digital assets? Digital companies' M&A valuation is currently not reflected on their balance sheet[2], but this does not change the fact that a digital asset has a value. Have you ever stopped to consider the relationship between the inherent risk of a digital asset and the cyber insurance value? Surely, that's one good reason to keep track of the inherent risk.

Digital transformation comes with greater risk exposure and requires proper governance, management, and protection. Greater risk also means a greater risk of opportunities, not only the negative consequence of risk. A positive risk will potentially add value to your business – that is why we pursue the opportunity risk of digital transformation. Strategy, tactics, operation, and data must be seamlessly integrated and holistically governed to understand the real value of the business on its journey through digital transformation.

> Have you ever stopped to consider the relationship between the inherent risk of a digital asset and the cyber insurance value? Surely, that's one good reason to keep track of the inherent risk.

Brakes make a car go fast; great brakes even faster

In our boutique business, I quickly realized that risk management was the key to staying ahead of threats, making prioritizations, communicating with stakeholders, and aligning operations to our strategy. I have learned to think of risk management as an enabler for a business to perform better. To give you an analogy; the defensive way of thinking about the purpose of brakes is to make the car stop. Offensive thinking flips this around and emphasizes the benefits of having brakes – for the car to go fast. The better the brakes, the faster you can go. Keeping in mind that risk can be offensive, we're witnessing an unparalleled opportunity to

put digitalization on the board's agenda to stay ahead of the game – and I mean really put it on the agenda, not by checking in on the progress of digital transformation as the last item before lunch. Running a digital business requires a different mindset, different tools, different skills, and a different way of communicating. Businesses need to know that digital transformation is not about introducing tablets and providing board papers as PDFs – that is called digitization. It is a seismic shift in how to value your business, how to measure performance, and how to manage your risks. My personal statement is, "the greatest risk in digital transformation is the lack of effective communication between the board, executives, and managers". In a cyber context, the potential impact of this risk alone can be devastating to the company and individuals on the board.

Assurance might hold the key to remediation

A company's assurance function is experiencing challenges in adding value to its stakeholders. Executives seek greater value in the assurance function, especially when it comes to regulatory compliance, third-party relationships, cybersecurity, business continuity, emerging markets, and IT governance. The internal auditors in many companies are stuck between a rock and a hard place due to this communication gap. How do you effectively audit a company in digital transformation where security staff and business are not aligned? If there's a misalignment internally, how can we effectively assure that 3rd parties are aligned with the business context – after all, they might be managing or accessing some of our digital assets?

The assurance function has a great opportunity to add value to their stakeholders by advising on how to remedy this communication gap, running scenario-based threat assessments, assessing the processes and technologies exploiting the digital assets, aligning protection efforts with asset value, reducing compliance cost by holistically assessing compliance across multiple business domains and regions, working more effectively by getting insight into holistic and integrated risk & compliance data, leveraging RegTech, AI and analytics to streamline audits, and prioritizing the assets that matter the most. The 2018 Global Chief Audit Executive Research Survey Results states that: "failure to act will see risk and change outpace internal Audit"[3].

> the greatest risk in digital transformation is the lack of effective communication between the board, executives, and managers

From ignorance to fear

In human psychology, if you don't understand the consequence of a probable event, if you're not able to apply the impact to your own life or to another's life, you will enter the state of ignorance. However, after witnessing somebody in your immediate proximity getting impacted, or if you experience it yourself, you will find you enter the state of fear. Security managers have seen the threat exposure to digital assets for years, however, some have not been able to speak the language of executives, and some have not seen the potential business impact. The executives on their side have been in a state of ignorance, some have not understood the potential ramification for the business, their customers, the market, and even the economy.

With the recent incidents highlighted in the news impacting companies all around the globe with regards to data privacy, ransomware, information leakage, breaches and more, businesses have entered the state of fear. Cybersecurity vendors are aware of this, and they drive a lot of the news, emphasizing areas of fear where their products are specifically targeted. Their objective is to influence executive conversations in corporations about cybersecurity, using the executives state of fear and the lack of a realistic risk profile. The cybersecurity vendor marketplace is growing so crowded that some companies are even lying about security emergencies and threatening to expose insignificant breaches to the media. If the company's risk profile cannot be understood and trusted, it is very hard for managers, and not to mention executives and the board, to relate to the current trend.

At the top, performance goals and strategic initiatives are very often quantified. Anything executives believe can impact their objectives will get their attention. However, the more red/super-high risks on a heat map, the more frustrated they become. Semi-quantitative heat maps/risk cubes are not effectively communicating a realistic risk profile. They might even resent the idea of dealing with the risk. At this point, both parties are in a state of fear. The security managers are afraid of not conveying the message, and the executives are afraid they will not understand how to make the right decisions. This easily leads to frustration, stress, and conflicts. To move on from the state of fear to a state of awareness and eventually into confidence, executives must drive effective communication as part of their digital transformation.

From fear to FAIR

How do we get from a state of fear to a state of awareness? We need a way of communicating risk effectively. Executives are seeking a way of quantifying their cyber risks, similar to their traditional enterprise risks, and, they are seeking to understand cyber and the risk it poses to the business to make better and faster decisions to perform and conform. Managers, on the other hand, seek to understand the business context and successfully communicate the risk profile to executives to get their support for mitigating and pursuing the risks. Effective communication around risk management and digital asset management can be achieved by introducing a couple of tools:

The first tool is to have a uniform way

of quantifying risks; An example of a method used for establishing a uniform communication for cyber risk is Factor Analysis of Information Risk (FAIR)[4]. FAIR has emerged as the standard Value at Risk (VaR) framework for cybersecurity and operational risk. The result of a FAIR approach is easily understood by the board and executives. FAIR will also educate security staff to align their thinking to the business context. As you will estimate the value at risk, you need to identify the value for e.g. your digital assets.

The second tool is to integrate a siloed risk space; In 2017, Gartner introduced the concept of Integrated Risk Management (IRM). This can be leveraged to bridge the communication gap in combination with FAIR to establish the fundamental structure needed.

From FAIR to awareness

Directors need to ask the right questions to bridge the communication gap, and security managers need to be able to answer what they might perceive as irrelevant and very difficult questions.

- How secure are we as a company?
- What are the residual risk values compared to the inherent values for our digital assets?
- What's our current threat level?
- Are we spending the right amount of money?
- What is the ROI for cyber risk reduction (CR3OI) initiatives?
- What's the expected loss for a ransomware attack scenario?
- How do we compare to our peers?
- What are our options for mitigating the risks?

Thinking of risk in an integrated, holistic and quantitative manner will enable security staff to answer the above questions.

Speaking the same language – where to start?

Important actions to take are:

1. Ensure leadership commitment (yes, they are ready for it)
2. Identify the correct best practices for the cyber and information security management or overall GRC needs in your industry and market
3. Have an effective strategy and visualization of performance goals, objectives, and risks across the organization
4. Work on awareness and have everybody speak the same language when interfacing different groups in meetings using a quantitative language
5. Evaluate your existing risk tool's ROI
6. Agree on how to measure the effectiveness of a holistic GRC program
7. Establish a baseline of Inherent risk for your digital assets
8. Determine how much cyber insurance you need?

You can't manage what you can't measure

The current situation in many organizations is a siloed operation in digital coexistence, often lacking a unified tactical approach to risk management, which in turn drives performance, regulatory and organizational compliance management, legal management, audit management, third party risk management, digital risk management, and business continuity management. Peter Drucker's famous quote "you can't manage what you can't measure" is a key to solving this situation. However, the CEO of Corporater, Tor Inge Vasshus, once said "you can't manage what you can't describe" to help executives complement their metrics and get to a deeper understanding of their business. To bridge the communication gap for cyber risk, you must start describing your digital assets, assigning responsibilities, valuing them, and then risk assess them using a VaR approach. Here are a few examples of metrics you should consider monitoring holistically:

> You can't manage what you can't describe"
> *Tor Inge Vasshus*

- The ability to recover from a cyber attack expressed as cyber resilience[5] in a BCM context
- The value of your assets
- Risk exposure
- Effectiveness for risk and compliance management
- Effectiveness for assurance

Conclusion

In conclusion, to answer the question in the title to this article, in my opinion the greatest risk of all is in fact not cyber threat in itself but an inability to communicate internally in the organisation in a common language which allows meaningful decisions and actions to be taken, amongst these to reduce the cyber threat to an acceptable level.

[1] *https://www.gartner.com/en/newsroom/press-releases/2017-02-08-gartner-says-within-five-years-organizations-will-be-valued-on-their-information-portfolios*
[2] *https://hbr.org/2018/02/why-financial-statements-dont-work-for-digital-companies*
[3] *https://ic.globaliia.org/Documents/CS-3-9.pdf*
[4] *https://www.fairinstitute.org*
[5] *https://en.wikipedia.org/wiki/Cyber_resilience*

Styring av tredjepartsrisiko og krav til outsourcing i finansbransjen

EBA Guidelines on outsourcing arrangements

JANNE BRITT SALTKJEL
Director, KPMG Risk Consulting

INGVE RASMUSSEN
Associate, KPMG Risk Consulting

Stadig flere virksomheter engasjerer leverandører og tredjeparter for å få tilgang til nye tjenester, teknologi eller markeder. En annen motivasjon kan være å oppnå kostnadsgevinster gjennom kjøp fra leverandører som realiserer skalafordeler gjennom spesialisering og volum på sine kjerneområder. Dette skaper behov for å tilpasse virksomhetenes risikostyring til å også håndtere risiko forbundet med outsourcing og tredjeparter.

Fremfor å utvikle, investere i eller ansette en ønsket kompetanse eller funksjon, kan virksomheter i stedet knytte til seg leverandører eller tredjeparter som utfører de aktuelle oppgavene. Dette kan gjelde alt fra å engasjere en agent i et nytt land som virksomheten ønsker å satse på, til å sette ut kantinetjenester eller outsource drift av IT infrastruktur. På denne måten kan virksomheter sikre fleksibilitet samtidig som den oppnår lavere og mer forutsigbare kostnader enn ved å investere eller ansette selv, og slik redusere økonomisk risiko. Å sette ut

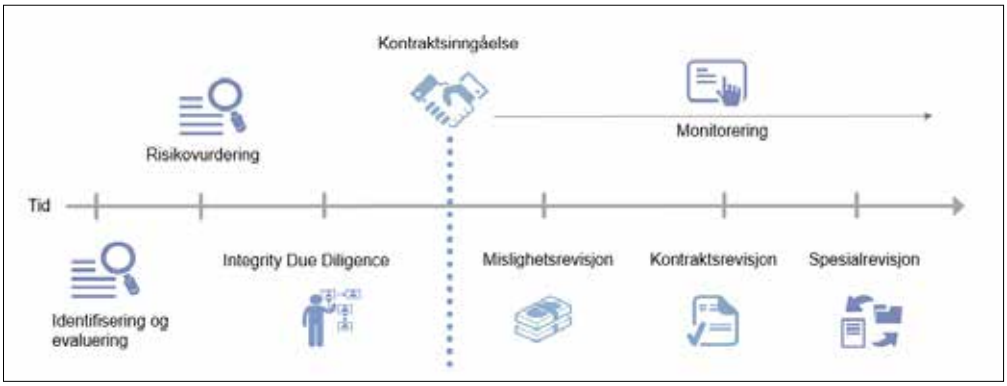
«Tredjeparter brukes i denne sammenheng om leverandører og underleverandører, agenter og partnere.»

en oppgave, betyr imidlertid ikke at ansvaret opphører – tvert imot vil bruk av tredjeparter eksponere virksomheten for nye risikoer og kreve nye rutiner for å sikre kontroll.

Operasjonell risiko og compliance

Når et foretak engasjeres for å utføre tjenester for en annen virksomhet, er dette med en iboende risiko for mangelfull innfrielse av oppgaven på grunn av utilfredsstillende kvalitet i egne eller underleverandørers prosesser eller operasjonelle svikt. I tillegg til kontraktbetingelsene, vil tredjeparten også måtte etterleve relevante lover og regler. Om tredjeparten bryter disse kravene i forbindelse med leveranse, for eksempel brudd på arbeidsmiljølov, personvern eller miljøkrav, kan oppdragsgiver stilles til ansvar. I verste fall kan brudd på straffeloven forekomme, for eksempel hvitvasking eller korrupsjon.

Det er naturlig nok langt mer krevende å ha kontroll over prosesser og ansatte når disse ligger i et annet foretak.



Figur 1 Prosess for håndtering av tredjeparter

Som et minimum er det derfor viktig å gjøre en evaluering av tredjepartens forutsetninger for å levere, risiko forbundet med outsourcing av den aktuelle tjenesten eller funksjonen, og integrity due diligence[1] i forkant av kontraktsinngåelse, og sikre seg mulighet til å overvåke tredjepartens prosesser, styring og kontroll (se figur1).

Samfunnsansvar

Kontroll og styring av leverandørkjeden er også et sentralt tema innen samfunnsansvar. Et foretak som tar samfunnsansvar på alvor, må sikre at også bruk av tredjeparter støtter oppunder og ikke er i konflikt med for eksempel virksomhetens bærekraftsmål og etiske anbefalinger. Dette kan innebære mer omfattende kontroll av tredjeparten og krav til tiltak som å samarbeide med selskapets leverandører om strategi og handlingsplaner innenfor samfunnsansvar og til å bidra til å skape kontinuerlig forbedring i leverandørenes utøvelse av samfunnsansvar. Dette gjelder både ved anskaffelser av innsatsfaktorer til egen produksjon og ved outsourcing av tjenester og funksjoner.

Styring av risiko forbundet med tredjeparter i finansbransjen

Økte kapitalkrav og press på kostnader har lenge skapt incentiv for bruk av tredjeparter i finansbransjen. I tillegg kommer teknologisk utvikling og endrede og internasjonalt harmoniserte regulatoriske rammebetingelser for betalingstjenester. Endrede «spilleregler» åpner opp for nye aktører og legger til rette for konkurranse og leveranser på tvers av landegrensene. Videre gir det ytterliggere motivasjon og muligheter for utkontraktering av aktiviteter eller funksjoner til tredjeparter.

«EBAs guidelines for outsourcing representerer anerkjent praksis og gode råd uansett bransje.»

Denne utviklingen påkaller naturlig nok tilsynsmyndighetenes oppmerksomhet. European Banking Authority›s (EBA) oppdaterte anbefalinger for virksomhetsstyring fra 2017[2] stadfester at styring og kontroll med outsourcing må være integrert i foretakenes øvrige virksomhetsstyring. 25. februar 2019 lanserte EBA egne anbefalinger[3] for outsourcingsordninger[4] som (med enkelte unntak) gjøres gjeldende fra 30. september 2019. Disse erstatter CEBS[5] sin veiledning for outsourcing for kredittforetak tilbake fra 2006 og EBAs egne anbefalinger for outsourcing av skybaserte tjenester. Anbefalingene fra EBA gjelder for kredittforetak, betalingsforetak, e-pengeforetak og tilsynsmyndigheter, og bygger på «følg eller forklar»-prinsippet; foretakene i EU må følge anbefalingene eller kunne forklare hvorfor de avviker fra dem.

EBAs nye anbefalinger for outsourcing innebærer mer detaljerte krav til foretakenes styring og kontroll av outsourcingsordninger. Fokuset rettes særlig mot outsourcing forbundet med betalingsformidling, IKT og skybaserte tjenester, som bekrefter de europeiske myndighetenes sterke fokus på IKT, sikkerhet og foretakenes generelle driftssikkerhet. Anbefalingene hensyntar også krav forbundet med GDPR (personverndirektivet).

Hva gjelder i Norge

Anbefalinger fra EBA blir gjeldende når Finanstilsynet bekrefter overfor EBA at de vil følges. Dette gjøres normalt noe tid etter at anbefalinger er EBA lansert. Det foreligger ikke enda slik bekreftelse for anbefalingene for outsourcing, men Finanstilsynet bekreftet i 2018 EBAs anbefalinger for bruk av skytjenesteleverandør, som nå er tatt opp i dette settet med anbefalinger og det vil derfor ikke være uventet at Finanstilsynet også bekrefter disse anbefalingene. Uansett utgjør prinsippene i EBAs anbefalinger ledende praksis for risikostyring forbundet med utkontraktering.

Overordnet vurdering av outsourcingsordninger

Anbefalingene er delt inn i fire bolker; virkeområde og forholdsmessighet, overordnet vurdering av outsourcingsordninger, rammeverk for styring og kontroll av tredjepartsrisiko, og selve outsourcingsprosessen.

EBA definerer outsourcing som en funksjon eller sett av aktiviteter som vanligvis utføres av virksomheten, og som isteden leveres av en ekstern tjenesteyter - en tredjepart. Anbefalingene fra EBA peker på at dette gjelder selv om foretaket ikke på noe tidspunkt har utført disse oppgavene selv og heller ikke er i stand til å utføre dem. Videre legger EBA til grunn at leveransen må være gjentakende og foregå over en periode. Anbefalingene gir flere eksempler på anskaffelser som ikke er å betrakte som outsourcing i henhold til deres anbefalinger, bl.a. enkeltstående kjøp av varer eller software lisenser.

Kritiske eller viktige funksjoner

Anbefalingene er dessuten rettet mot outsourcing relatert til kritiske eller viktige funksjoner. I hovedtrekk anses en funksjon som viktig eller kritisk dersom svikt i leveransen kan påføre virksomheten vesentlige økonomiske tap, driftsbrudd og problemer med å innfri foretakets forpliktelser overfor egne kunder, eller føre til manglende etterlevelse av regulatoriske krav[6]. EBA angir nærmere evakueringskriterier som skal legges til grunn. Dersom aktiviteten krever konsesjon fra myndighetene eller er vesentlig for foretakets internkontroll, vil dette også tilsi at funksjonen kan være kritisk eller viktig.

Rammeverk for styring og kontroll av risiko forbundet med tredjeparter

Å sette ut en tjeneste til en tredjepart, fritar ikke ledelse og styret for ansvar. Det vil si at det fortsatt er foretakets ledelse og styre som har ansvar for fastsetting av strategi og risikoappetitt, intern organisering, oppfølging av den daglige driften inkludert aktivitetene som leveres av tredjeparter, håndtering av risikoer og interessekonflikter og at foretaket etterlever de kravene som settes for å få og beholde konsesjon. Dette igjen setter en rekke krav til kontroll, monitorerings- og rapporteringsrutiner samt til avtalene med tredjeparter, slik at ledelse og styret kan ta informerte beslutninger i tide og har et handlingsrom i forhold til avtalemotpartene. Hovedkomponentene i et rammeverk for risikostyring forbundet med outsourcing i henhold til EBAs anbefalinger, er illustrert i figur 2.

En overordnet forutsetning, er at styring av tredjepartsrisiko skal være integrert i virksomhetens rammeverk for

«Man kan sette ut en oppgave, men man kan ikke sette ut ansvaret.»

helhetlig risikostyring. Foretakene må forankre dette i en egen policy som definerer prinsippene for alle faser ved en outsourcing, inkludert prinsipper for håndtering av interessekonflikter forbundet med å sette ut funksjoner eller oppgaver til tredjeparter. EBA setter også krav til at finansforetakene må rigge – og teste - sine beredskapsplaner slik at de kan implementere disse selv ved svikt i leveranse fra tredjeparter.

Outsourcingsprosessen

Selve outsourcingsprosessen omfatter foranalyse og kontraktsinngåelse. Det er i denne fasen foretakene kan legge fundamentet for adekvat styring og kontroll. Anbefalingene fra EBA anfører konkrete punkter som må dekkes, fra gjennomgang av konsesjonskrav, til vurdering av risikoer forbundet med utkontrakteringen og due diligence av tredjeparter. Den endelige kontrakten må regulere en rekke forhold, som for eksempel tredjeparters underleverandører, krav til data- og systemsikkerhet, informasjonstilgang, kundens rett til å gjennomføre revisjoner og til å terminere avtalen.

Dokumentasjon og oversikt

I tillegg til robuste prosesser for risikovurdering og –styring forbundet med den enkelte outsourcingsavtalen, kreves en samlet oversikt for å sikre helhetlig risikostyring. De færreste foretak har eller har hatt en samlet oversikt over alle outsourcingsavtaler. I praksis vil avtaler være inngått av ulike miljøer, og i den grad Innkjøp har vært involvert, har det vært forbundet med å sikre konkurransedyktige betingelser og kontrakter som ivaretar foretakets juridiske interesser og rettigheter. EBAs krav til dokumentasjon og oversikt over alle outsourcingsforhold krever derfor etablering av en sentralisert prosess for forvaltning av slike avtaler.

Figur 2 Hovedkomponentene i et risikostyringsrammeverk for outsourcing

Exit-strategier

I tillegg til terminerings-klausuler i kontrakter med tredjeparter, krever EBAs anbefalinger at foretaket også etablerer exit-strategier, som skal praktisk muliggjøre en terminering ved for eksempel svikt i leveranse eller ved implementering av en beredskapsplan. Utvikling av en exit-strategi tar utgangspunkt i en målsetting for exit-strategi, konsekvensanalyse, fordeling av roller, ansvar og ressursallokering ved utøvelse av exit-strategi og overføring av funksjoner og aktiviteter.

Oppsummering

EBAs anbefalinger for outsourcingsordninger vil tre i kraft ved inngåelse av nye avtaler i EU fra 30. september, mens eksisterende avtaler må utfases og erstattes med avtaler som møter kravene innen 31. desember 2021.

EBAs anbefalinger for outsourcing er imidlertid i tråd og har således gyldighet og relevans også for andre bransjer. Utvikling av et helhetlig rammeverk for styring av tredjepartsrisiko må speile virksomhetens aktivitet og særskilte risikobilde og ikke begrenses til tredjeparter forbundet med outsourcing. Også leverandører ved anskaffelse av innsatsfaktorer til virksomheters produksjon, infrastruktur, maskiner, utstyr og konsulentbistand til avtaler med partnere, agenter og sponsorer bør vurderes dekket av rammeverk for styring av tredjepartsrisiko.

Link til EBA´s anbefalinger for outsourcing:
https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements

[1] *Integrity Due Diligence er undersøkelse av tredjeparten, dets eieres og nøkkelpersoners integritet, dvs omdømme og historikk mht forretningsetisk atferd*
[2] *GL 11 - Guidelines on internal governance*
[3] *Finanstilsynet anvender «anbefalinger» ved oversettelse av EBAs «guidelines»*
[4] *EBA Final Report on EBA Guidelines on outsourcing arrangements EBA/GL/19/02*
[5] *Committee of European Banking Supervisors*
[6] *Spesifikt nevnt er kapitalkravregelverket / CRD IV og CRR, MiFID II, revidert betalingstjenestedirektiv / PSD2 og direktiv for e-pengedirektivet*

Tanker rundt risikoappetitt

IIA Norge var så heldige å få Paul Sobel på besøk 16. mai og vi benyttet muligheten til å høste litt av hans tanker rundt det store begrepet «risikoappetitt».

AV ELLEN BRATAAS
generalsekretær

One organization – one risk appetite? Any smart thoughts on how to break the appetite down?

– I think, because of certain financial services regulations around the world, there is a misunderstanding that risk appetite is a "statement" developed by a company. I believe it's really the discussion that should occur during strategic planning about the nature and amount of risk an organization desires to take, or avoid, in its pursuit of strategy. This discussion may be documented in a formal "statement", but I believe a good risk appetite discussion may result in many statements. For example, with each strategy chosen the board/executives should discuss what nature and amount of risk they are willing to accept in pursuit of that strategy and what they would prefer to avoid. If done comprehensively in connection with the strategic planning process, an organization may end up with several statements applicable to each of the individual strategies, as opposed to a single statement encompassing all strategies. So to summarize, risk appetite discussions should relate to individual strategies rather than a blanket statement applicable to all strategies.

The Board is ultimately responsible for setting the risk appetite, but do they in general have enough knowledge about the business and emerging risks?

– The board is ultimately responsible as part of their oversight role, but they must rely heavily on executive management who has the detailed knowledge about the business, as well as individual and emerging risks. Board members should leverage their overall business experience to challenge management on whether the risk appetite being recommended to the board makes sense given the mission, vision and core values of the organization.

Any suggestions on how to engage board discussions on risk appetite and how to translate risk language into understandable terms?

– We went through an exercise with the IIA Board similar to what I described above. That is, for every goal that was part of the IIA strategic plan, a few of us brainstormed possible statements about what we thought the board would want to accept in pursuit of that goal and what they would prefer to avoid. You will notice that we didn't say "not accept" because risk events sometimes are unavoidable so "prefer to avoid" better captured the direction to CEO Richard Chambers and his management team. I use this as an example because it illustrates a discussion with the board, using the language of the organization (IIA in that case) and specific words included in the goals. At the completion, when the board approved it, CEO

I 2018 ble Paul Sobel utpekt som styreleder for Committee of Sponsoring Organizations of the Treadway Commission (COSO), foreningen som er kjent for sine rammeverk for internkontroll og risikostyring. Paul Sobel innehar vervet i tre år. Han har lang erfaring som leder av internrevisjon i flere virksomheter, men gikk over i rollen som Chief Risk Officer at Georgia-Pacific LLC omtrent på samme tid som han ble styreleder i COSO. Sobel har hatt mange verv i globale IIA og var også den globale foreningens styreleder i perioden 2013 – 2014.

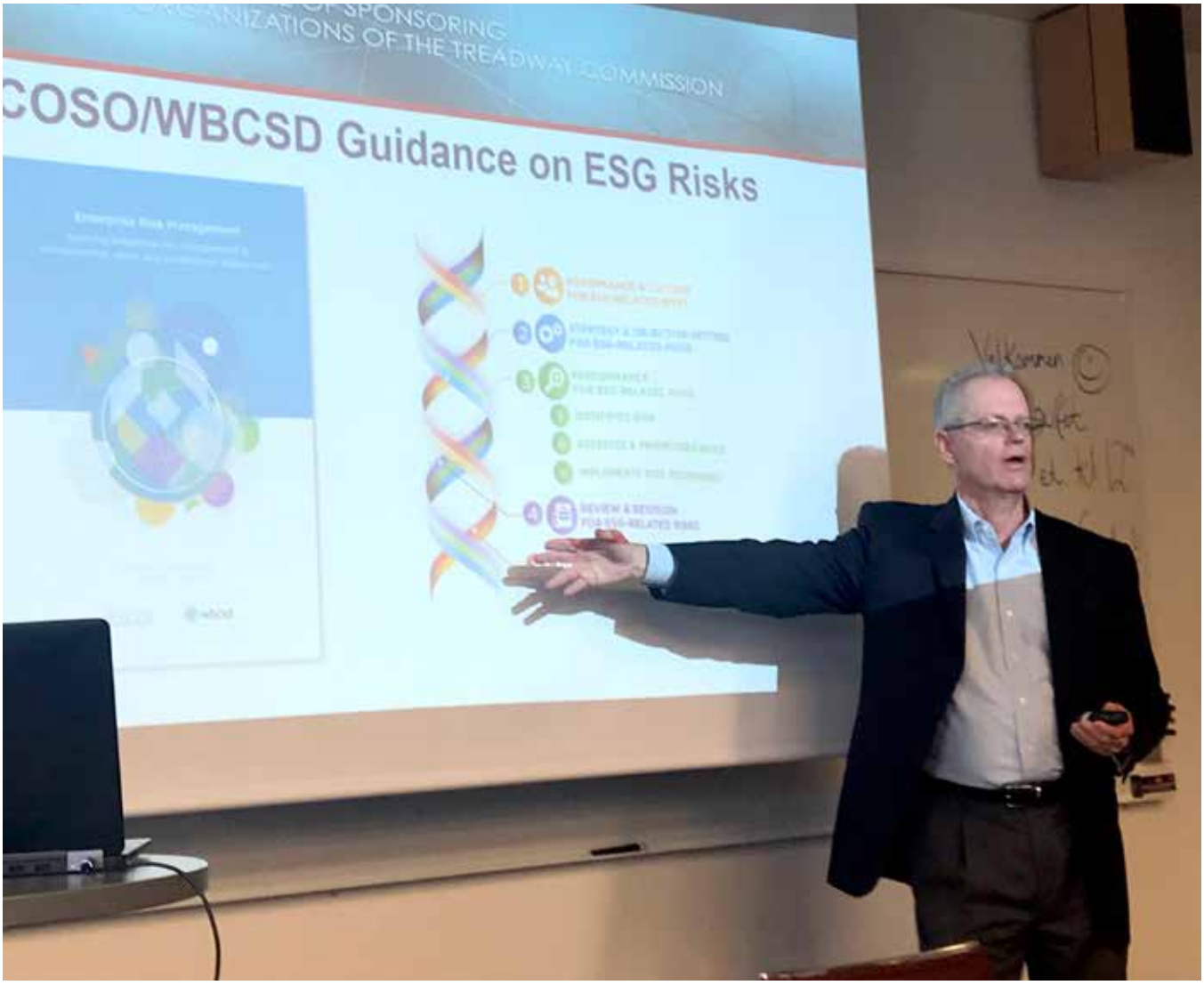


Foto: Privat

Richard Chambers and his team had a much clearer idea of what risk the board would accept and what information he would need to timely communicate to the board if unavoidable risk events occurred.

The same applies to any organization. Management should come to the board to discuss the selected strategies as well as the nature and amount of risk they believe the company must accept or should try to avoid in pursuit of those strategies. That discussion should use the language used in strategic planning and discuss real-life scenarios to help the board calibrate their agreement with management's risk appetite recommendations. Risk appetite is more of a strategic planning discussion than a risk management discussion.

In your role as a Chief Risk Officer, do you see a shift in what is considered risk types; such as compliance risk, financial risk, operational risk, strategic risk and new risks such as cyber, environmental etc. and will this affect the way risk appetite is defined?

I haven't really seen a change in the risk categorizations, such as you mentioned (strategic, operational, compliance and financial). Those categories seem to still work, even in today's rapidly changing environment. However, there occasionally needs to be discussion about where emerging risks fall in those categories. For example, would digital disruption be considered a strategic risk or an operational risk? The answer could be either, depending on how it impacts an organization.

In the end, the important thing is to have the discussion with the board about the new and emerging risks, and less about how they're categorized. The same then applies to risk appetite discussions. Even if there are no new strategies, management and the board need to discuss how emerging risk areas may impact their ability to achieve chosen strategies, and whether those emerging risks would change their perspective on risk appetite. Given the accelerated pace of change, these discussions should be held as often as necessary, as opposed to making it a once a year agenda item.

GRC-verktøy - hvor modne er vi i Norge?

Hvor god kontroll har vi på risikoen vi er eksponert for? Denne artikkelen baserer seg på en undersøkelse utført av Deloitte og gir innsikt i hvor modent det norske markedet er for bruk av GRC-verktøy.

KINE KJAERNET
Director – Risk Advisory
Deloitte AS

SEBASTIAN WELHAVEN
Consultant – Risk Advisory
Deloitte AS

SIGURD BERSTAD
Consultant – Risk Advisory
Deloitte AS

Funnene fra undersøkelsen er interessante: 64,7 prosent av respondentene i undersøkelsen benytter verktøy (inkl. Excel) for styring og kontroll. De største selskapene (målt i omsetning) og selskaper innenfor finans er lenger fremme når det gjelder bruk av verktøy, men de er ikke nødvendigvis bedre rustet for å håndtere risikolandskapet de er eksponert for enn de mellomstore og mindre selskapene. Svært få, uavhengig av om de har tatt i bruk verktøy eller ikke, mener selv at de har effektive prosesser for styring og kontroll.

Vi spår at dagens bruk av GRC-verktøy, som i dag er dominert av Excel, i fremtiden forsvinner og at risikostyring og internkontroll i sanntid vil bli en realitet. Å komme dit vil imidlertid ta tid og kreve ressurser, og det vil samtidig kreve at mennesker og verktøy jobber sammen på en helt ny måte.

GRC-verktøy – hva er det egentlig?

GRC i seg selv er et helhetlig konsept om et integrert og helhetlig styringssystem som omfatter eierstyring og selskapsledelse, risikostyring og internkontroll, samt etterlevelse av lover og regler, både gjennom compliance arbeid i andre linje og internrevisjon. Et helhetlig styring- og kontrollsystem bidrar til at selskaper opptrer etisk korrekt og i samsvar med selskapets risikoappetitt, eksterne lover og reguleringer, samt interne policyer og prosedyrer. I tillegg vil et slikt system bidra til at dette gjøres samlet gjennom strategi, prosesser, medarbeidere og økende bruk av teknologi.

Et av hovedformålet med GRC-verktøy er å skape en 'single source of the truth' ved å automatisere prosessene knyttet til dokumentering og rapportering innenfor styring og kontroll, og å automatisere aktiviteter relatert til etterlevelse som er tettest knyttet til virksomhetsstyring og målene til selskapet.

De primære brukerne av GRC-verktøy er risiko-, internkontroll- og compliance medarbeidere, samt ledere, internrevisjonsfunksjonen, primære sluttbrukere og endelige mottakere av rapportering for bruk i beslutningsstøtte. Rapporteringsmottakerne kan være internrevisjonen, revisjonsutvalget, ansvarlige ledere, ledelsen og styret i selskapet.

Nøkkelfunksjonene til et GRC-verktøy dekker flere områder og behov innen styring og kontroll og kan omfatte flere brukere og sluttbrukere:

- **Dokumentasjonshåndtering av styringspolicyer** inkluderer en spesialisert form for dokumentasjonshåndtering som muliggjør en livssyklus for policy og prosedyrer, fra etablering til gjennomgang, endring, vedlikehold og arkivering av styrende dokumenter. Dette kan innebære kartlegging av alt fra mandater, strategiske mål og forretningsprosesser, til risiko og kontroller, i tillegg til distribusjon til-, og attestasjon av ansatte som eier henholdsvis policy, prosedyre, risiko og kontroller.
- **Risikostyring** som en støtte til både første og andre linje med dokumentasjon for vurdering og håndtering av risiko, samt automatisering av arbeidsflyt og rapportering. Dette inkluderer aggregering og visualisering av risiko. Risikostyring komponentene fokuserer vanligvis på oppfølging av risikoer, hendelser og tiltak, men kan også benyttes for å samle inn data fra andre verktøy som brukes til risikoanalyse (kredittrisiko, markedsrisiko osv.) for å gi et helhetlig bilde av risikoene. Enkelte verktøy kan kombinere flere kilder til risikodata for å sikre konsekvent måling av selskapets risikofaktorer, slik at det kan gis rask og

enhetlig informasjon til selskapet som grunnlag for beslutninger.

- **Compliance og kontroll** som støtter både første og andre linje med dokumentasjon, arbeidsflyt, rapportering og visualisering av kontrollmål, kontroller og tilknyttede risikoer, undersøkelser, egenvurderinger og testing og utbedringer. Verktøyet innenfor etterlevelse inkluderer ikke kun finansiell rapportering (f.eks. SOX-etterlevelse), men støtter andre former for etterlevelse, eksempelvis bransjespesifikke forskrifter (Lov om offentlige anskaffelser) og etterlevelse av interne retningslinjer, eksempelvis etterlevelse av GDPR policy, Code of Conduct eller antikorrupsjonspolicy. Verktøy bør samordne kontrollaktivitetene på tvers av alle forsvarslinjene for å øke effektiviteten. Et godt utformet og integrert verktøy kan redusere kontrollkostnadene og kontrollbelastningen for virksomheten, samtidig som det gir høyere kvalitet på kontrollarbeidet og øker ledelsens innsikt i risikostyringsaktivitetene. De nyeste og mest avanserte verktøyene kan koble på databaser med lover og reguleringer og skaper til enhver tid oversikt over gjeldende lover og regelverk.
- **Revisjonsegenskaper** som støtter andrelinje og tredjelinjes internrevisjon i utarbeidelse av revisjonsplan og program, håndtere arbeidspapirer og revisjonsrapport, håndtere funn og jobbe aktiv med oppfølging av aksjoner.

Enkelte verktøy på markedet kan håndtere alle områdene nevnt over og ved å skaffe seg en helhetlig oversikt over styring og kontroll i eget selskap – et integrert perspektiv som dekker hele økosystemet for styring og kontroll – vil styret og ledelsen få bedre forståelse for hele risikolandskapet, hvilken innvirkning dette potensielt kan ha på organisasjonen og hvordan risiko er håndtert.

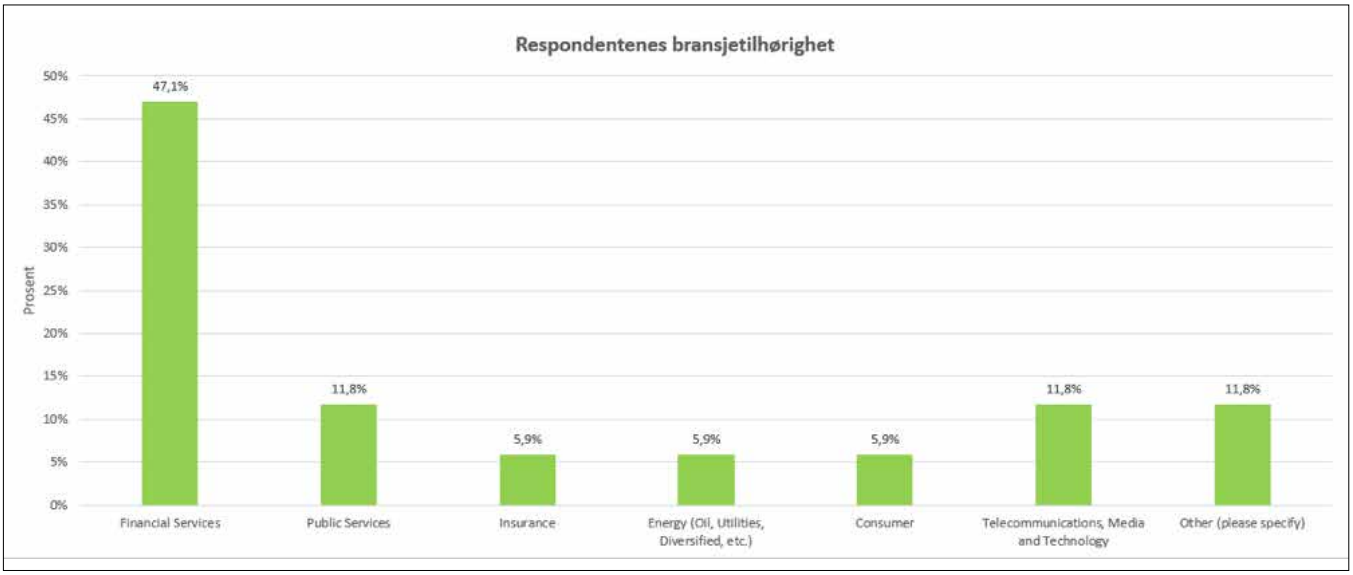
Metode og datagrunnlag

Til å begynne med ønsker vi å takke alle som deltok i undersøkelsen. Vi sendte undersøkelsen målrettet til enkelte klienter, samtidig som vi inviterte norske selskaper til å delta gjennom deling av undersøkelsen gjennom IIA Norge. Vi mottok et begrenset antall besvarelser fra store, mellomstore og mindre virksomheter (målt i omsetning) innen privat og offentlig sektor. Dette utgjør ikke et statistisk signifikant utvalg, men vi mener det gir en pekepinn på trender og en indikasjon på områder der norske virksomheter kan utnytte et større potensiale ved å oppgradere eller investere i et GRC-verktøy for å ivareta og overvåke styring og kontroll i eget selskap.

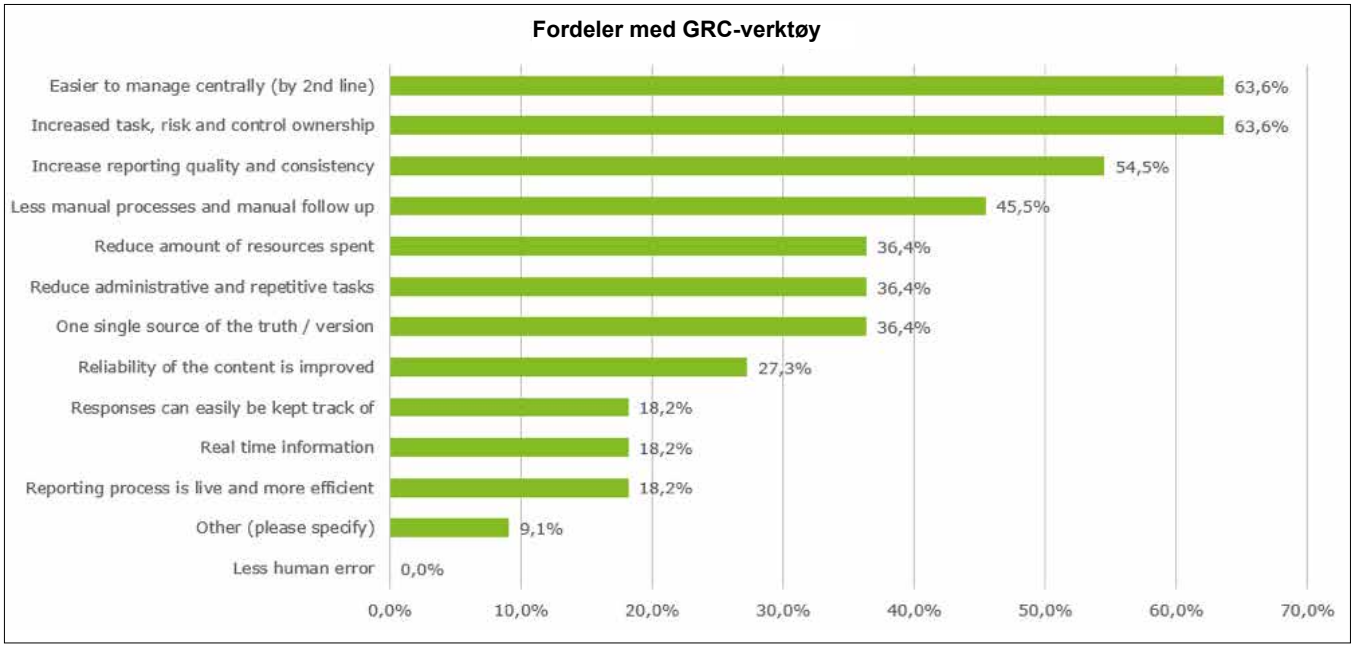
Totalt sett kan det virke som norske selskap er middels fornøyd med sine prosesser knyttet til styring og kontroll. På en skala fra 1-5, der 5 er best, får overordnet styring og kontroll en gjennomsnittscore på 3,08. Bryter vi tallet ned, ser vi at spredningen er relativt liten innenfor de ulike områdene av styring og kontroll. Compliance (2,94) scorer lavest og styring (3,18) scorer høyest. Basert på resultatene tegner det seg et bilde av at de fleste virksomheter er klar over at måten de identifiserer, håndterer og rapporterer risiko på ikke er tilfredsstillende og at det i stor grad er på tide med en oppgradering av både verktøy og måten å jobbe på, spesielt med fokus på å automatisere prosesser og å sikre et bedre datagrunnlag. Behov og ønske om å benytte et GRC-verktøy er til stede, spørsmålet er hvilket verktøy og hvilke områder verktøyet skal ivareta.

Selskapene som har besvart undersøkelsen representerer en rekke ulike bransjer i Norge. 47,1 prosent av selskapene som har besvart er i finansielle tjenester, 5,9 prosent i forsikring og 11,1 prosent i offentlig sektor. Resterende respondenter er spredt mellom energi, handel, Telecom, media og teknologi og andre bransjer.

11,8 prosent av respondentene innehar rollen som CFO i sitt selskap. De andre respondentene jobber med risikostyring (11,8 prosent), internkontroll (11,8 prosent), compliance (29,8 prosent) og



Figur 1: Respondentenes bransjetilhørighet



Figur 2: Fordeler ved GRC-verktøy

internrevisjon (23,5 prosent), mens de resterende 11,8 prosentene har andre ansvarsområder i selskapet. 47,1 prosent av respondentene jobber i selskaper med under 3 mrd i omsetning, 29,4 prosent i selskaper med en omsetning mellom 3 og 15 mrd og 23,5 prosent i bedrifter med over 15 mrd i omsetning (norske kroner).

Bruk av GRC-verktøy – benyttes til ulike behov

64,7 prosent av respondentene, svarer at de bruker et GRC-verktøy (inkl. Excel) for å dekke prosessen med styring, risiko, kontroll, compliance og internrevisjon. Flest (90,9 prosent) selskaper oppgir at de bruker verktøyet til fagområdet risikostyring, mens 81,8 prosent bruker det til fagområdet internkontroll. Deretter følger hendelsesstyring og compliance som benyttes av 63,6 prosent av respondentene. Et interessant funn er altså at flere selskaper har investert i et verktøy, men at svært få har valgt et verktøy på tvers av fagområdene. Hvorfor er det slik at ikke alle fagområder dekkes for å skaffe et helhetlig bilde av styring og kontroll?

Av selskapene som har GRC-verktøy implementert, bruker 81,8 prosent verktøyet i første linje, 100 prosent bruker det i andre linje, mens 45,5 prosent bruker det i tredje linje (internrevisjonen). Dette tyder på at kunnskap innenfor GRC-verktøy i økende grad også blir viktig for potensielle eksterne involvert i internrevisjon i tillegg til bedriftene som har GRC-verktøyene implementert.

Alle respondentene bruker GRC-verktøyet til rapportering. Andre bruksområder som benyttes er aggregering av risiko og oppfølging (63,6 prosent). Det færrest bruker GRC-verktøy til er å automatisere arbeidsprosesser (9.1 prosent) og å lage flytkart (18.2 prosent). Det som kunne vært interessant å vite mer om, er om det er verdien av å automatisere GRC prosessene eller manglendekunnskap om at det faktisk er mulig å automatisere prosessene i et GRC-verktøy?

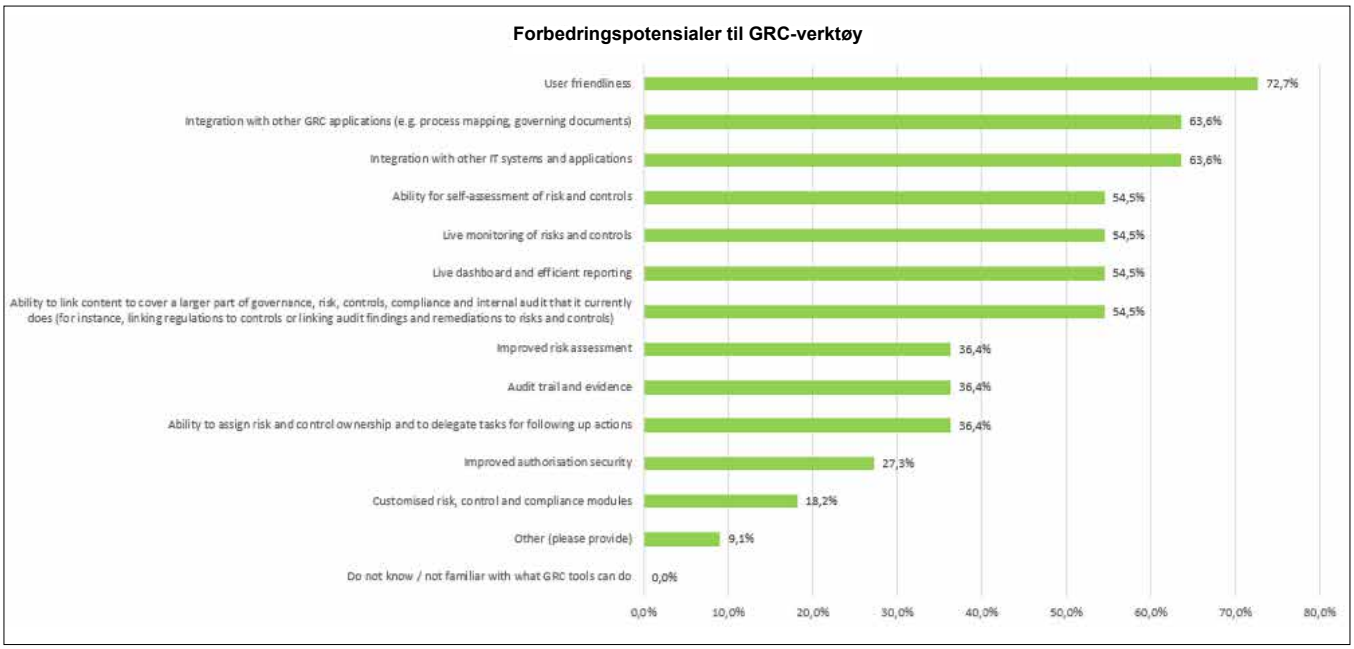
Av de som har svart at de har et verktøy, svarer 18,2 prosent at de implementerte det for under ett år siden, 36,4 prosent mellom ett til tre år siden, 36,4 prosent fire til seks år siden og 9,1 prosent for mer enn seks år siden. Dette tyder på at flere har eldre verktøy som potensielt kan være utdatert grunnet rask teknologisk utvikling og bør vurdere å oppgradere eller investere i ett nytt verktøy.

Flest respondenter (63,6 prosent) opplyser at verktøyet har gitt dem økt oppgave-, risiko- og kontrolleierskap, og at verktøyet har gjort det lettere å administrere sentralt (for andre linje). 54,4 prosent svarer også at verktøyet gir bedre rapporteringskvalitet og kontinuitet. I den andre enden av skalaen observerer vi at det ikke er noen som svarer at det fører til færre menneskelige feil. Dette kan tyde på at menneskelige feil ikke skjer i prosessene som GRC-verktøy dekker, og/eller at nye menneskelige feil oppstår som en følge av feil input i systemet på grunn av for eksempel dårlig brukervennlighet i verktøyet.

Respondentene opplyser at de er middels fornøyd (score 3.00 på en skala fra 1-5, hvor 5 er meget fornøyd) med brukervennligheten til deres nåværende verktøy. Samtidig opplyser flest respondenter (72,7%) at verktøyet kunne hatt bedre brukervennlighet. 63,6 prosent svarer at verktøyet kunne vært bedre integrert med andre IT-systemer og applikasjoner, og at det kunne vært integrert bedre med andre GRC applikasjoner.

Utbredt bruk av Excel for styring og kontroll

Av de som allerede benytter et verktøy for å dekke prosessen med styring, risiko, kontroll, compliance og internrevisjon, så svarer 63,6 % at de bruker Excel/Word/PowerPoint. Totalt sett bruker 41,15 prosent av selskapene Excel/Word/PowerPoint som verktøy for å dekke prosessen



Figur 3: Forbedringspotensialer til GRC-verktøy

med styring, risiko, kontroll, compliance og internrevisjon. Av bedrifter som benytter Excel/Word/PowerPoint, bruker flest (85,7 prosent) det til rapportering.

Av de som ikke planlegger å anskaffe et nytt verktøy de neste 12 månedene, opplyser flest (42,9 prosent) at størrelsen på bedriften og intern motstand er de viktigste årsakene til manglende utskifting. Kun 14,3 prosent opplyser at de er fornøyd med det nåværende GRC-verktøyet, og derfor ikke ønsker å investere i et nytt verktøy de neste 12 månedene. Respondentene som planlegger å investere i et verktøy de neste 12 månedene, ønsker først og fremst å digitalisere internkontroll og hendelseshåndtering.

Trender

Utviklingen innenfor GRC-verktøy er at de i større grad skal kunne justeres og tilpasses til selskapers behov, størrelse, bruksområde og samhandle bedre med andre IT-systemer. Dette har resultert i forbedrede API (Application Programming Interface)-løsninger som tillater GRC-verktøyene å koble seg til andre IT-systemer.

Det er også en utvikling i integrering av GRC-løsningene blant leverandørene, noe som er en konsekvens av behovet for større investeringer i komplekse risikoanalyser for å møte ulike problemstillinger innenfor «big data». Denne integreringen fører til at selskapet kan få bedre kontroll og et mer presist beslutningsgrunnlag. Det er også et økt fokus på effektiv og intuitiv visualisering av data, slik at brukeren enkelt kan forstå og tolke resultatene.

Vurderer du å ta i bruk et verktøy for styring og kontroll? Dette bør du tenke på

For å maksimere utbyttet av ressursene som investeres, anbefales en evalueringsprosess for de ulike mulighetene som et GRC-verktøy gir. Dette gjør det mulig å ta beslutninger om verktøy basert på en enkel vurdering. I en slik vurdering bør følgende temaer analyseres:

• Scope og omfang

Selskapet må avgjøre hvilke fagområder som skal omfattes av verktøyet, eksempelvis: helhetlig risikostyring og internkontroll, internkontroll i forbindelse med finansiell rapportering, internkontrollregister og mulighet for å teste kontroller, cyberrisiko, operasjonell risiko, compliance, IT risiko, hendelseshåndtering eller internrevisjon, eller alle komponentene i ett og samme verktøy.

Når selskapet skal definere scope og omfang er det viktig å se på selskapets behov og ambisjon. Vi anbefaler også å skaffe en god oversikt over det nåværende IT-miljøet til bedriften i forbindelse med at scopet skal defineres for å sikre riktig integrering av data.

• Rammeverksbibliotek

Selskapet må så definere strukturen og innholdet i rammeverksbiblioteket som skal være på tvers av alle områdene i scopet. Dette innebærer policyer, prosedyrer, prosesskart, prosessinndeling, risiko taxonomi, risikoregister, kontrollregister, selskapsstruktur og fullmakter, for å nevne noen.

• Risikovurdering

Metode som skal benyttes for risikovurdering må defineres og besluttes, dette inkluderer blant annet: Iboende og/eller gjenværende risikovurdering, en sannsynlighetsvurdering og definisjon av dimensjonene av denne, en konsekvensvurdering og en definisjon av konsekvensene i denne (eks. finansiell, omdømme, regulatorisk) samt årsaker og hendelse kategorier.

• Kontrollvurdering

Metoden som benyttes for kontrollvurdering må defineres og besluttes, dette inkluderer: Behovet for å evaluere effekti-

viteten av designet og/eller kontrollutførelse og/eller operasjonell effektivitet. For både risiko og kontrollvurdering må det defineres hyppigheten av dette og hvem som skal utføre handlingene og i hvilken grad eiere og utfører skal ha tilgang til å gjennomføre og dokumentere i verktøyet, samt ha anledning til å laste opp dokumentasjon for sporbarhet.

Vurderingen vil bidra til å avgjøre om den beste løsningen innebærer å utarbeide et nytt verktøy internt, å kjøpe en pakkeløsning, investere i en løsning som i stor grad er skreddersydd eller å gå for en «best-of-breed». Når det er tydelig hvilket behov selskapet har, identifiser så de beste løsningene i markedet. Det finnes en stor mengde tilgjengelige verktøy. Ved hjelp av kjerneområder for vurdering vil det være mulig å velge en liste av potensielle kandidater for en live demo, slik enkelte leverandører kan tilby.

Hva er neste steg / Konklusjon

Teknologi, reguleringer og sikkerhetstrusler utvikler seg konstant. Dermed blir håndtering av styring, risiko, compliance og sikkerhet en vedvarende og økende utfordring for de fleste organisasjoner. Med økende krav til etterlevelse, søker organisasjoner å redusere kostnadene og øke verdiskapningen fra investeringene i kontrollprosesser, mennesker og teknologi. For å håndtere disse truslene bør ledelsen benytte en rekke integrerte verktøy og metoder for å identifisere og styre risikofaktorene på en hensiktsmessig nivå.

GRC-verktøy tilbyr betydelige fordeler i form av reduserte kostnader, økt effektivitet gjennom automatisering og minimering av feil som resulterer i økt etterlevelse. Til tross for at det er brukt enorme ressurser på styring og kontroll det siste tiåret, viser vår undersøkelse at det fortsatt er mange selskaper som bruker kun Excel/Word/PowerPoint for å håndtere styring og kontroll. Selv om Excel kan fungere godt for enkelte selskaper, og kan benyttes for enkelte områder innen risikostyring, så har vi fortsatt til gode å se Excel integrert godt på tvers av de ulike fagområdene. Selskaper som har tatt i bruk teknologi og som utnytter data, får et mer helhetlig bilde av styring og kontroll i selskapet, og har derfor et stort fortrinn. Med en integrert løsning kan selskapene i større grad la ressurser jobbe med verdiskapning i selskapet enn rapportering og oppfølging.

Resultatene av vår studie viser at en del norske selskaper har gjort et godt stykke arbeid med å innføre GRC-verktøy, men at flere fortsatt henger etter i forhold til sine globale partnere og konkurrenter. Vi ser at en del selskaper bruker GRC-verktøy, og at det er en økning i bruk og funksjonalitet. Basert på funnene som viser at det finnes et forbedringspotensial rundt brukervennlighet i verktøyene til respondentene, og at verktøyet kun brukes til en begrenset mengde fagområder, er det liten tvil om at det finnes et uutnyttet potensiale for mer effektiv bruk av verktøyene. Ettersom teknologien utvikles må selskapene sørge for at verktøyene fortsetter å håndtere risiko tilstrekkelig. Dette inkluderer blant annet å sørge for at verktøyene integreres for å oppdage og beskytte mot Cybertrusler.

En beslutning om å automatisere og samle selskapets arbeid med styring og kontroll kan være nødvendig – og skulle kanskje til og med vært tatt for en stund siden? Det er virksomhetens stabilitet, omdømme og verdier som står på spill.

6 TIPS TIL HVA DERE MÅ TENKE GJENNOM FØR DERE VURDERER Å TA I BRUK ET VERKTØY FOR STYRING OG KONTROLL

1 Scope og omfang, hvilke fagområder skal verktøyet dekke?
Er det er ønske å lage en felles plattform for styring og kontroll, eller skal det kun benyttes til enkelte fagområder, eksempelvis kun risikostyring?

2 Brukere, hvem skal bruke verktøyet?
For å få med organisasjonen bør det sikres at alle ansatte som har en rolle knyttet til det fagområdet verktøyet skal dekke ha tilstrekkelig tilgang. Eksempelvis bør en risikoeier i første linjen ha tilgang for å legge inn og endre risiko, mens andre linje må ha tilgang for oversiktsbilde.

3 Rammeverk.
Hvilke rammeverk skal legges til grunn og er det mulig at verktøyet kan tilpasses til deres behov? Eksempelvis ISO eller COSO.

4 Linket innhold.
Er det mulighet for å linke innhold? Eksempelvis å ha flytkartet og samtidig ha en link som tar deg rett inn i strategiske mål, som igjen tar deg videre til risiko og til tiltak? Eller for eksempel mulighet for å integrere regulering og endringer direkte inn til policy og prosedyrer med krav og føringer for å til enhver tid ha oversikt over hvordan selskapet håndterer endringer i reguleringer.

5 Aggregering av risiko.
Mulighet for å aggregere risiko fra prosessnivå og helt opp til strategiske risikoer? Mulighet for å få opp risikobilder for enheter, funksjoner og enkeltselskap?

6 Rapportering, dashboard og visualisering.
Mulighet for å presentere den informasjonen du ønsker og muligheten for å tilpasse rapportering i henhold til ønske fra styre og ledelsen?

The Chicken KPI: Be Careful What You Measure

All organizations have one or a few metrics that they focus on and talk about all the time. It doesn't take long for employees to figure out what's important based on what gets asked for and talked about the most. Sure, executives talk about metrics addressing customers, employees, culture, and other factors, but what gets reviewed in daily or weekly reports is what really matters.

BLOG BY MARK GRAHAM BROWN
Corporate Advisory Board, Corporater
– 18th February 2019

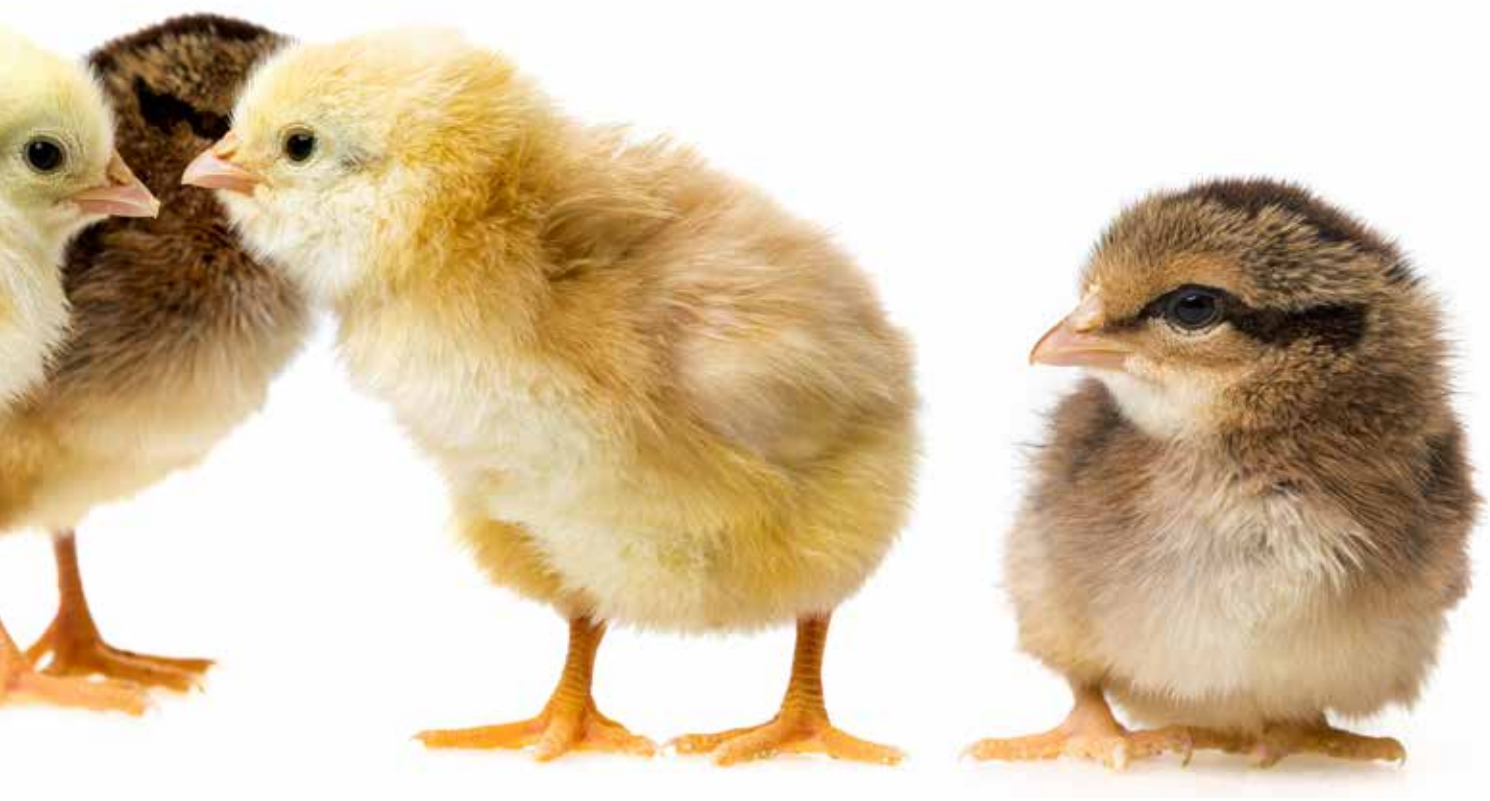
Focusing on a single metric tends to either lead to poor performance on other metrics or may resort to cheating in order to make performance look good on this single metric.

The best example of the danger of focusing on a single measure came when I first started my own consulting practice in California. My second client was in the fast food business and had a chain of fried chicken restaurants that was growing in both the U.S. and internationally. One of the challenges they faced was training new restaurant managers. They hired me to document those best practices by spending time in a number of their best run restaurants around the country. My report on best practices would then serve as the foundation for the new management training program.

The first place I visited was Alcoa, TN, which is outside of Knoxville. The manager's name was Roy and he was full of enthusiasm and energy. I told Roy that management had picked him for this study because he was one of the best managers in the USA. I let him know I would be observing him while he worked and then talk to him from time-to-time throughout the day. After watching the lunch crowd come and go, I had very little written down on anything Roy was doing differently. Around 2:30 we got a chance to sit down and talk and I started by asking him what he measured that management considered important: «Well the first thing I keep track of every day is the employee's errors» I replied that keeping track of mistakes sounded like an important metric. He replied: «I don't keep track of their mistakes, I keep track of their errs». Again, I repeated that errors were an important thing to track. He corrected me saying: «Errs like 8 errs in a day – how many errs people work per day». I realized the communication problem we were having and tried to listen more carefully to his Tennessee accent.

Roy went on: «The one metric that is really important to management is Chicken Efficiency. At the end of every day, I have to calculate my Chicken Efficiency score, and they make me mash these chicken stickers on a graph in the back room that is the size of a poster. Then I have to call in my Chicken Efficiency score to my boss every evening. This is the measure that all the managers talk about all the time.»

Looking at Roy's chart it looked like he was achieving 99-100% Chicken Efficiency every day that month that must be



good. However, I still didn't know what the measure entailed. Roy explained: «Chicken Efficiency is basically a scrap measure. You take how much chicken you cook and divide it by the number of pieces of chicken sold. If you sell all the chicken you get 100% chicken efficiency, which is the goal – no waste or scrap.»

When I asked Roy how he achieved near perfect Chicken Efficiency every day he answered: «I'm gonna let you in on a secret, but don't put my name in the report saying you heard this from me. My secret is I stop cooking chicken around 7:30 and only cook to order after that. That way none of the chicken sits under the lights for too long, everyone gets hot and fresh chicken, and I don't throw any of it away – 100% chicken efficiency.»

I asked, don't you get people coming in here all evening until the restaurant closes? Roy replied: «Oh yeah we get tons of kids coming in here after baseball or soccer practices or games, families, and lots of people. I tell them I'm going to make their chicken to order and it will take 15-20 minutes.»

I asked, do most of them wait? Roy answered: «Heck no, they file right out the door and head off someplace else, but management doesn't measure that. They do want to make sure I don't throw any chicken away every day, however. My buddie Leon taught me this trick – he got promoted to rung three». I went on to visit other restaurants and every one of them talked about the importance of Chicken Efficiency.

When I gave my report to management they were surprised and horrified that managers were purposely not cooking chicken, making customers mad and could not understand how this metric became so important. They explained that all they talked about was customer satisfaction and it is stressed in every meeting. However, customer satisfaction is only measured once a year with a survey done by Mystery Shoppers the third week of March each year. Restaurant Managers focused on good customer service for a couple of weeks in March each year and then knew they could slack off for the remainder of the year on this metric. However, Chicken Efficiency is measured and reported daily, and promotions are tied to this metric, as well as bonuses.

The lesson of this story is in spite of your efforts to tell people that all your KPIs/metrics are important, many organizations focus too much on one or two and too little on the others. The concept behind the Balanced Scorecard is that you can't judge the health of an enterprise by looking at a single metric. A healthy well-performing organization shows good performance on a suite of metrics addressing much more than just short-term financial results. Yet, it's rare for me to work with an organization that does not have a few Chicken Efficiencies, so you might want to take a hard look at what you measure and talk about all the time to avoid some of the unwanted side effects seen by the chicken restaurant.

This blog is reprinted with permission from Corporater/Denne blogg ble først utgitt på websiden til Corporater og er gjengitt med tillatelse. Link til den originale bloggen:
https://corporater.com/en/the-chicken-kpi-be-careful-of-what-you-measure/

Hva innebærer agil?

Agil er et begrep som går igjen i ulike fora. Men hva innebærer det egentlig å være agil? Agilitet handler om smidighet og fleksibilitet, og beskrivelsen av arbeidsmetodikken har sitt utspring i 12 prinsipper som en gruppe softwareutviklere i USA ble enige om i 2001.

MARIT TRODAL
Prosjektleder IIA Norge

Disse 12 prinsippene utgjør The Agile Manifesto. Kort oppsummert ønsket gruppen av radikale utviklere et felles grunnlag for fremgangsmetoder for utvikling av software:

"We are uncovering better ways of developing software by doing it and helping others do it. Through this work we have come to value:

- **Individuals and interactions over processes and tools**
- **Working software over comprehensive documentation**
- **Customer collaboration over contract negotiation**
- **Responding to change over following a plan**

That is, while there is value in the items on the right written in green, we value the items on the left written in red more."

Disse prinsippene ble ansett som radikale tilbake i 2001, men har siden fått internasjonal utbredelse. Sentralt for softwareutviklerne var ønsket om mer tilpasningsdyktighet, økt menneske- og kundefokus, samt en erkjennelse av at veien blir til mens man går. Store ressurser blir ofte brukt på utforming av prosjekter, estimering og utvikling av krav som til slutt blir endret eller forkastet etter test. Denne tilnærmingen kalles gjerne 'fossefallsmetoden.'

Å sluke en elefant

«Fossefallsmetoden» er betegnelsen på et prosjekt der kunden typisk presenterer en komplett kravspesifikasjon av typen: «Sånn ønsker vi at websiden vår skal se ut.» «Sånn skal den nye løsningen være.» Kostnader og tidsbruk blir estimert ut ifra dette, som om prosjektet har en begynnelse og en slutt - en lineær utforming. Utfordringen er at et it-prosjekt ikke har en naturlig avslutning. En ny webside er ikke et sluttprodukt, men et produkt i kontinuerlig utvikling og tilpasning. Man tar utgangpunkt i hvilke behov kunden har og tilpasser underveis.

Fossefallsmetoden tar ikke tilstrekkelig høyde for ukjente problemer og muligheter som oppdages underveis. Fungerte ikke denne løsningen etter intensjonen? Må vi skrape alt? Med fare for å sette en elefant i halsen bør man ikke sluke den hel, men dele kolossen opp i passe store biter – håndterbare deler og kortere leveranser med vurderinger og tilpasninger underveis.

Veien blir til mens man går

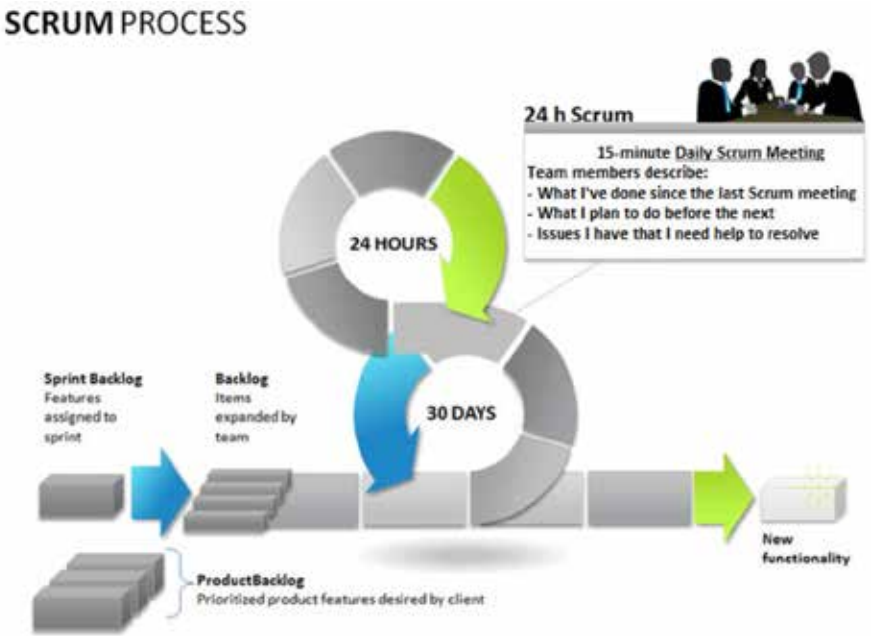
En agil tilnærming innebærer som nevnt at et prosjekt deles opp i mindre delmål og korte tidsintervaller – omtalt som 'sprinter.' (Se fremstilling av prosessen under.) Prosessen er iterativ og prosjektet leverer delmål ved avslutning av en sprint, teamet samarbeider tett med kunden og sjekker av før prosjektet går videre til neste sprint. Ble resultatet bra? Kan vi gjøre noe bedre? Hva må eventuelt tilpasses?

Scrum står sentralt innen agil metodikk. Se for deg at prosjektet og kunden har daglige møter på 15 minutter – 'scrums.'Ved effektiv bruk av disse teknikkene kan prosjektet justere kurs, redusere unødige oppgaver ('waste'), og jobbe fokusert mot neste delmål av sprinten. Målet er gode leveranser gjennom hele prosjektet og å redusere risiko for at man ikke leverer på kundens behov.

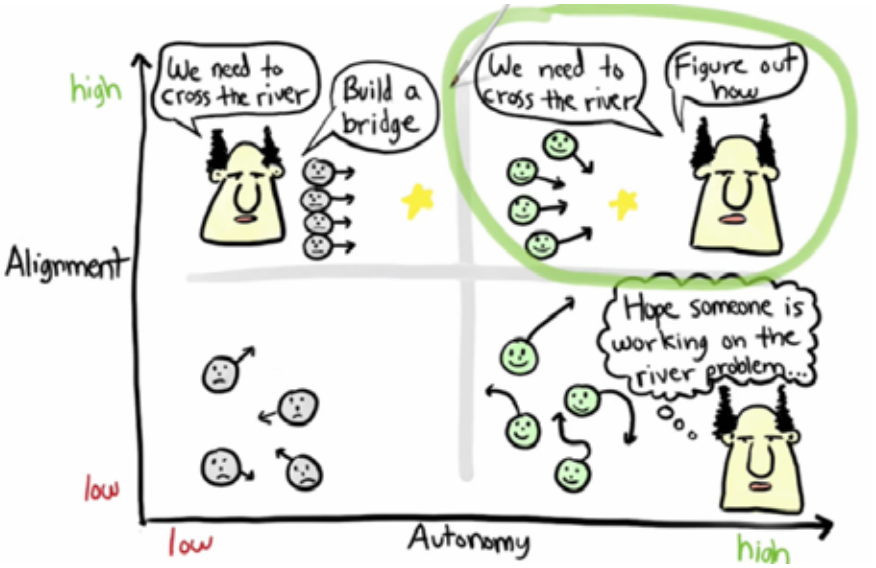
På tide å bevege seg mot agil?

PWC UK hevder i sin rapport'Agile Auditing: Mindset over Matter' (2018) som følger;

'Agile methodologies are often promoted as a cure-all for waste and inefficiencies in the audit process, but in the real world 'Agile Auditing' works better for some projects (e.g those adopting an agile approach) and in



https://www.cprime.com/resources/what-is-agile-what-is-scrum/



LEAN VERSUS AGILE

Lean architecture – just-in time delivery of functionality, just in time pouring material into the forms
Agile architecture – one that supports change, end-user interaction, discovery, and ease of comprehension (of functionality)

Kilde: Jim Coplien

I boken «Det agila företaget» av Lennart Francke og Göran Nilsson presenteres en modell som kort beskriver hvordan virksomheter som vil bevege seg til et agilt system må tenke:

- Fra eierorientert til kundeorientert
- Fra belønningssystem til indre motivasjon
- Fra kontroll til tillit
- Fra nøye planlegging til rask tilpasning

Kilder:
http://agilemanifesto.org/
https://lederne.no/2018/11/13/agilt-hva-vil-det-si-a-jobbe-agilt/
https://blog.soprasteria.no/blog/2010/05/24/lean-eller-agile/
https://www.iia.nl/SiteFiles/AgilePerformer_ia201712-dl%20(002).pdf
https://www.knowit.no/articles/move/fa-mer-ut-av-utviklingsbudsjettet-med-agile-metoder/
https://plan.io/blog/ultimate-guide-to-implementing-agile-project-management-and-scrum/

Bilder:
https://www.visual-paradigm.com/scrum/scrum-vs-waterfall-vs-agile-vs-lean-vs-kanban/
https://labs.spotify.com/2014/03/27/spotify-engineering-culture-part-1/

some businesses (e.g those that are more dynamic rather than traditional) more than others.'

Tradisjonelle strukturer og hierarkier kan være bremseklosser på reisen mot en dynamisk og agil kultur. I dag handler mye om innovasjon og produktivitet og om å eksperimentere og lære. Virksomheter som Spotify, Facebook, Microsoft er eksempler på agile foregangsvirksomheter. Figuren under er hentet fra beskrivelsen av Spotify Engineering culture (kilde: Henrik Kniberg) og illustrerer ønsket kultur og lederskap. Høy grad av autonomi kombinert med felles forståelse av formål betyr at ledere kan fokusere på hvilke utfordringer som må løses, men overlate til teamene å løse dem.

På IIAs årskonferanse 2019 deltok Ralph Daals, Group Chief Auditor i RSA Insurance. Han fortalte om internrevisjonens agile reise og hvordan de hadde hentet inspirasjon fra blant annet Spotify og Google. RSA Insurance har lagt vekt på å tiltrekke seg de beste talentene, bygge på deres styrker, gi dem frihet og mulighet til å skape et felles formål. Agilitet må være forankret i mindset, kulturen og verdiene til teamet, hevdet Daals. Det handler om å være dynamisk, fleksibel, med evne til å forutse, agere og kontinuerlig forbedre. En effektiv agil arbeidsmetodikk er betinget av teamets mindset.

Personvern i praksis

Riktig behandling av personopplysninger innebærer at enkeltpersoners interesser ivaretas på en god og trygg måte i henhold til lovverket. Et sentralt element ved behandlingen av personopplysninger er kravet om at enkeltpersoner skal ha informasjon om hvordan deres personopplysninger behandles.

ERLING GRIMSTAD
Advokatfirmaet Erling Grimstad AS
www.governance.no

I mer enn 15 år har jeg vært med på å gi råd og veiledning til kommuner, offentlige etater og private foretak om behandling av personopplysninger. Jeg har erfart at det behandles flere opplysninger enn nødvendig eller at behandling skjer i strid med formålet opplysningene er innhentet for. Jeg har også erfart kunnskapsmangel blant de som behandler personopplysninger. Mange ansatte i kommuner og private foretak mangler kunnskap om grunnleggende plikter og krav i personvernregelverket. Det er forståelig. Personvernregelverket er omfattende og komplisert. I forbindelse med rådgivning og kursvirksomhet har vi erfart at mange stiller de samme spørsmålene om personvernreglene, uavhengig av bransje eller om de arbeider i offentlig-/privat sektor eller i organisasjoner.

Etter å ha innehatt roller som rådgiver, personvernombud og foredragsholder, har jeg innsett at kunnskapsdeling om GDPR må skje på helt nye måter. Derfor fikk vi idéen om å utvikle Personvernrådgiveren som er en digital rådgiver i personvern. Personvernrådgiveren har gjort det mulig å dele kunnskap om typiske utfordringer ved etterlevelse av GDPR og besvare spørsmål som de fleste har om behandling av personopplysninger.

GDPR compliance

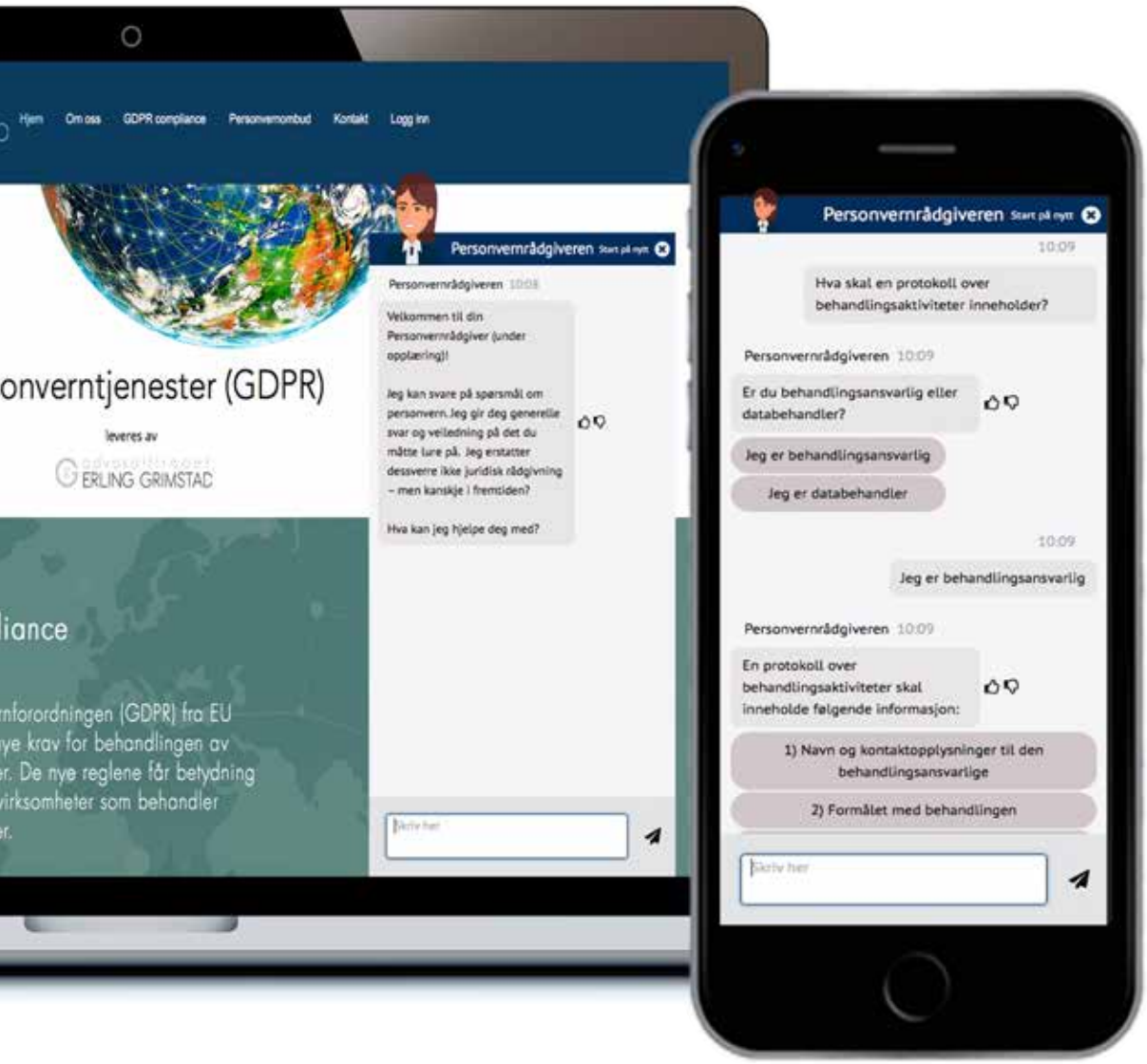
Utfordringene ved regeletterlevelse av personvernforordningen er først og fremst kunnskapsmangelen hos personer som behandler personopplysninger om egne ansatte, kunder, brukere, innbyggere og andre.

Det mangler fortsatt god veiledning og svar på mange av de konkrete utfordringer og problemstillinger som medarbeidere vil ha svar på for å sikre at de løser oppgavene på best mulig måte. Personvernforordningen er et rammeverk som nødvendigvis ikke har svar på alle de spørsmål som ansatte stiller om de krav som gjelder.

De grunnleggende personvernprinsippene er momenter som skal anvendes når spørsmålene skal besvares. Anvendelsen av prinsippene i praksis krever kunnskap om hvordan prinsippene skal vektes i forhold til hverandre og med bakgrunn i absolutte krav og tilsynsmyndighetenes veiledninger. Det er en rekke kollisjonstilfeller der en lovbestemmelse for eksempel stiller krav til oppbevaring av personopplysninger, mot der personvernhensyn tilsier sletting. Disse konfliktsituasjonene er virksomhetene avhengig av å gå opp og utarbeide retningslinjer for.

Jeg beskriver her ett eksempel på hvor krevende det kan være å forstå hvilke regler som gjelder. Behandling av opplysninger om kunder etter hvitvaskingsloven krever at de rapporteringspliktige skal innhente, dele og arkivere en rekke sensitive personopplysninger om sine kunder for å forhindre hvitvasking av utbytte fra straffbare handlinger. Denne form for behandling av personopplysninger løses ikke av personopplysningsloven, men av hvitvaskingsloven som tillater slik behandling.

Alle virksomheter som behandler personopplysninger må etablere sitt eget internkontrollsystem for å sikre etterlevelse av personvernforordningen. Kravene til dokumentasjon for å oppfylle personvernforordningen kan bli omfattende, avhengig av type virksomhet du arbeider i. Dette gjelder for eksempel rutiner, prosedyrer, slik som for avvik og for behandling, personvernerklæring, protokoll over behandlingsaktiviteter og lignende.



Det handler om kompetansekrav for ansatte

Riktig behandling av personopplysninger handler blant annet om kunnskap hos alle de ansatte i virksomheten som er satt til å behandle personopplysninger. De skal blant annet vite hvordan personopplysninger innhentes, deles, videresendes, arkiveres og slettes. Disse oppgavene kommer på toppen av andre presserende kjerneoppgaver for ansatte som allerede er presset på tid. Derfor må det tenkes nytt i måten kunnskapsformidlingen utføres på. Selvsagt vil kurs, møtepunkter der utfordringer kan løses, gode retningslinjer og god internkontroll fortsatt være sentrale deler av løsningen. Men det må noe mer til for at ansatte skal få den veiledningen de trenger, og når de trenger den.

Løsningen vi fant, var utvikling av Personvernrådgiveren. Dette er en chatbot som gir veiledning på de spørsmålene du har og besvarer de mange typiske utfordringene ansatte har i arbeidet med personvern. Formålet med tjenesten er at brukerne som nødvendigvis ikke har mange forkunnskaper skal kunne gjøre de riktige valgene om behandling av personopplysninger i arbeidssituasjonen.

Hvordan er Personvernrådgiveren utviklet?

Til sammen tre jurister, som alle har kompetanse innen personvern, har drevet opplæringen av chatboten. Personvernrådgiveren er matet med informasjon som begreper, definisjoner, krav og veiledninger. Fordi mange ikke har nødvendig kunnskap om hvilke spørsmål som bør stilles til personvernrådgiveren, gir chatboten veiledning i hvilke spørsmål som bør stilles. Dette gjelder for eksempel ved utarbeidelse av rutiner, databehandleravtaler og utarbeidelse av protokoll. Chatboten bistår også i beslutningsveier ved utøvelse av registrertes rettigheter, slik at den ansatte kan være sikker på at alle vilkår og hensyn er ivaretatt.

Et eksempel kan være hvor en registrert person (en person det behandles personopplysninger om) ber om innsyn i personopplysningene som behandles om vedkommende. Personvernrådgiveren kan i slike tilfeller bistå den ansatte med veiledning i hva det kan gis innsyn i. Et eksempel er hvilke personopplysninger det kan gis innsyn i, hvem som kan be om innsyn, om det kan kreves vederlag og hvilket format som kan benyttes ved utsendelse av informasjon. Ved bruk av Personvernrådgiveren kan den ansatte forsikre seg om at alle krav og hensyn er ivaretatt.

Personvernrådgiveren ble lansert i februar 2019 og er den første juridiske rådgiveren innen personvern i Norge. Personvernrådgiveren vil være din egen bedriftsadvokat eller «husadvokat» i personvernspørsmål. Du kan lese mer om tjenesten på personvernradgiveren.no.

How combined assurance can maximise the effectiveness of risk management

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

Weaknesses of the Lines of Defence model

Many firms have adopted the three lines of defence model (3LoD), which is expected to provide a simple and effective methodology for improving risk management by clarifying roles and responsibilities among different stakeholders of an organisation[1]. After the financial crisis in 2008, authorities in many countries have tried to strengthen governance mechanisms and have actually recommended the 3LoD model to embed risk management throughout financial companies. While this model is in use in many organisations, it has been argued that the 3LoD model may actually reduce the accountability and effectiveness of risk management due to its limitations[2].

The Institute of Internal Auditors announced in January 2019[23] that it will work to update the model of the Three Lines of Defence to meet the changes in stakeholder expectations and the increased complexity in organizations. One of the goals for updating the existing position paper, "Three Lines of Defence in Risk Management and Control", is to broaden the scope with emphasis on coordination and collaboration in the Three Lines model.

«If a company claims to have a 3LoD model, but can´t produce a comprehensive mapping of risks, then the effectiveness of that model is debatable[3]»

Companies that do not have a well-coordinated 3LoD model are, according to the findings of EY[4], likely to experience one or more of the following challenges:

- Siloed risk functions that work with different risk categorizations, terminologies, scales and technological solutions, which reduces value and increases cost
- Confusion, when management has one view of an organization's risk profile, and risk functions have a different view
- Layers of redundant controls - Not having a holistic understanding of controls in place to manage risks and a lack of clarification of responsibilities may lead to duplication in control activities and increased cost of control

Three distinct lines in the 3LoD model are not always sufficient to enable clarity of responsibilities for the management of risk in banks and financial institutions, according to Martin, Willman, Boukens and Rockley[5]. This will impact the management of risks in many ways:

- Inability to provide proper attestations or statements on the effectiveness of risk management, including the established controls
- Aggregate risk exposures at different organizational levels may not be given proper consideration, resulting in a lack of ability to track against risk appetite
- Limited ability to bring about behavioural changes that will over time lead to better risk culture in the organization
- Decisions can be made, and actions executed without full use of expert input and/ or senior approvals
- Lack of ability to report risks to stakeholders

The following weaknesses in the 3LoD model were identified by Arndorfer and Minto[6] after evaluating specific governance features of banks and insurance companies:

- Misaligned motives for risk-owners in the 1st line of defence
- Lack of skills, expertise and organizational independence of the control functions in the 2nd line of defence
- Inadequate and subjective risk assessment performed by the 3rd line of defence

Stockenstrand and Nilsson suggest that the 3LoD model is only a framework for assigning duties associated with risk and the concept as such is no benchmark. Therefore, it is necessary that organizations are able to design and use the lines of defence in a deliberate manner. Risk management actions must be tailored and apportioned to address meaningful risks.

Also, internal auditors should align with, and if viable rely on other co-assurance providers. In the same way, first- and second-line actions must be coordinated and aligned. This is the starting point of the combined-assurance framework[7]. Rather than a sequence of separate lines, as the 3LoD model might simply be considered, all lines must be intentionally designed to endlessly support and complement each other.

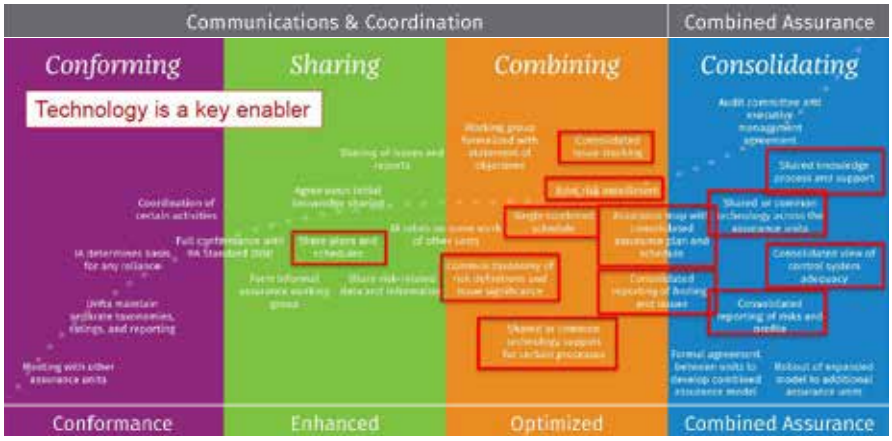


Figure 1: Coordination Maturity Benefit Curve by Grocholski and Gowell, IIA International Conference Dubai 2018, page 51

Combined assurance

Combined assurance[8] aims to provide holistic assurance to the board on the effectiveness of risk management and internal control systems by coordinating assurance activities for different sources of assurance.

It is argued that bringing assurance providers together will lead to immediate rationalization and efficiency benefits[9]. There are several other stakeholders that have described multiple gains that will come from assurance mapping and combined assurance (HM Treasury, 2012[10]; PwC, 2014[11]; European Commission, 2015[12]; Alexander, 2018[13]) but studies conducted by professional organisations[14] suggest that combined assurance implementations are rare because organisations have run into trouble with the execution.

According to the study by the Institute of Internal Auditors UK and Ireland[15], the reasons for failing to coordinate assurance activities include (in order of priority):

- The different taxonomies and methodologies among assurance providers (40 per cent)
- The immature Enterprise Risk Management (39 per cent)
- The difficulty of identifying the process coordinator (34 per cent)
- The selfishness/ egoism of assurance providers (27 per cent)
- The lack of an executive and board buy-in (26 per cent)
- The assurance providers' lack of competence and skills (21 per cent)

Why some fail to implement combined assurance? Because they haven't understood the benefits yet.

Associate Director, Group Internal Audit, an European bank with a turnover of USD 5.5 billion and 35 000 employees[16]

More recently, the presentation by Grocholski and Gowell[17] shows a Coordination Maturity Benefit Curve with four levels that internal audit can use to optimize its interactions with other assurance providers and a 4-Step Planning Framework; (1) Conformance, (2) Enhanced, (3) Optimized and (4) Combined Assurance; for developing an Assurance Action Plan. There are multiple benefits to implementing combined assurance[18], including:

- One taxonomy across all governing bodies and functions
- Efficiency in collecting and reporting information
- Common view of risks and issues across the organization
- More effective governance, risk and control oversight

Conclusion

As summarized by Huibers[19], combined assurance can help organizations by integrating and aligning assurance processes so that top management obtain a comprehensive, holistic view of the effectiveness of the organization's governance, risks and controls. Disappointingly, the 2015 CBOK[20] survey results show that knowledge of the combined assurance concept has still not achieved widespread acceptance. It is to be hoped that going forward combined assurance will be seen for the opportunity it represents for improved governance as the organization benefits from "one language, one voice, one view".

The foremost key success factor is that you have to believe in key benefits of combining assurance yourself and have the energy to embark on the journey.

Jenitha John, Chief Audit Executive, FirstRand[21], South Africa[22]

[1] *The Journal of Financial perspectives, EY, Global Financial Services Institute, November 2014, Volume 2 – Issue 3, Risk Management formations – an alternative approach to the 3 lines of defense model, page 2*
[2] *Howard Davies and Maria Zhivitskaya (2018), Three Lines of Defence: A robust Organising Framework, or Just Lines in the Sand?, https://doi.org/10.1111/1758-5899.12568, John & Wiley*
[3] *EY, Maximizing value for your lines of defence – A pragmatic approach to establishing and optimizing your LOD model, December 2013, page 5.*
[4] *Ibid, page 2*
[5] *The Journal of Financial perspectives, EY, Global Financial Services Institute, November 2014, Volume 2 – Issue 3, Risk Management formations – an alternative approach to the 3 lines of defense model, page 6.*
[6] *Arndorfer Isabella and Andrea Minto, Financial Stability Institute, Occasional Paper, No 11, The "four lines of defence model" for financial institutions, Bank for International Settlements, December 2015*
[7] *Stockenstrand Anna-Karin and Nilsson Fredrik (2017), Bank Regulation: Effects on Strategy, Financial Accounting, and Management Control, Routledge Publishing, New York*
[8] *Decaux Loic and Sarens Gerrit (2015), Implementing combined assurance: insights from multiple case studies, Managerial Auditing Journal, page 57*
[9] *Sarens Gerrit, Decaux Loic, and Lenz Rainer (2012), Combined Assurance, Case Studies on a Holistic Approach to Organizational Governance, The Institute of Internal Auditors Research Foundations*
[10] *HM Treasury, Assurance frameworks, December 2012*
[11] *PwC – Covering your bases – Implementing appropriate levels of combined assurance, January 2014*
[12] *European Commission, Public Internal Control Systems in the European Union, Assurance Maps, Ref. 2015-4*
[13] *Alexander David, Assurance Mapping, Chartered Institute of Internal Auditors & Daart Solutions, 2. February 2018*
[14] *Decaux Loic and Sarens Gerrit (2015), Implementing combined assurance: insights from multiple case studies, Managerial Auditing Journal, page 57*
[15] *IIA UK and Ireland, Professional Guidance for Internal Auditors: Coordination of Assurance Services, The Institute of Internal Auditors UK and Ireland, London, 2010.*
[16] *Decaux Loic and Sarens Gerrit (2015), Implementing combined assurance: insights from multiple case studies, Managerial Auditing Journal, page 67*
[17] *Grocholski Greg and Gowell Mike, IIA International Conference, Dubai 6-9 May 2018, Combined Assurance in Today's World of Audit – Aligning & Coordinating for Value*
[18] *Huibers Sam C.J., Combined Assurance: One Language, One Voice, One View; The Institute of Internal Auditors Research Foundation, 2015*
[19] *Ibid*
[20] *The Global Internal Audit - Common Body of Knowledge (CBOK)*
[21] *FirstRand is one of the largest financial institutions in South Africa with a net asset value of USD 8.8 billion and 46 000 employees*
[22] *Huibers Sam C.J., Combined Assurance: One Language, One Voice, One View; The Institute of Internal Auditors Research Foundation, 2015, page 3*
[23] *IIA Sets Exposure Period for 'Three Lines of Defense' Update, https://www.google.no/url?sa=t&rct=j&q=&esrc=s&source=-web&cd=1&ved=2ahUKEwjohMDl7_XhAhVikosKHeV7Dn-8QFjAAegQIBBAB&url=https%3A%2F%2Fglobal.theiia.org%2Fnews%2Fpress-releases%2FPages%2FIIA-Sets-Exposure-Period-for-Three-Lines-of-Defense-Update.aspx&usg=AOvVaw0Hnc5rn-SQVxlckyvp7EVn, 29. January 2019*

0-24 samarbeidet - felles innsats for utsatte barn og unge

0-24 programmet stakk av med Bedre stat-prisen for 2019 for sitt samarbeid for bedre samordnede tjenester for utsatte barn og unge mellom 0 og 24 år og deres familier.

MARTE WÆGE MYKLEBUST
Seniorrådgiver Direktoratet for økonomistyring.

OLA OTTERDAL
Seniorrådgiver internkontroll og risikostyring, Politidirektoratet

Barn og unge som har behov for hjelp fra flere tjenester får ofte ikke den hjelpen de trenger. Selv om tjenestene hver for seg kan være gode, fører dårlig samordning mellom dem til at innsatsen ofte settes inn for sent, og ikke blir god nok. Mye av ansvaret for å organisere hjelpen kan også bli liggende hos den enkelte eller familien.

Med dette utgangspunktet samarbeider Kunnskapsdepartementet, Arbeids- og sosialdepartementet, Helse- og omsorgsdepartementet og Barne- og likestillingsdepartementet og de fem direktoratene Integrerings- og mangfoldsdirektoratet, Arbeids- og velferdsdirektoratet, Barne-, ungdoms- og familiedirektoratet, Helsedirektoratet og Utdanningsdirektoratet om en rekke delprosjekter for å hjelpe utsatte barn og unge. Innsatsen er organisert i et program. Programmet har et sekretariat og en styringsgruppe med representanter fra alle de fem direktoratene[1].

Vi har snakket med sekretariatslederen for 0-24 samarbeidet, Birgit Leirvik.

> «Staten må i større grad samordne sine virkemidler og innsatser slik at de bedre understøtter og stimulerer samordnings- og utviklingsarbeid lokalt, og ta utgangspunkt i kommunenes og målgruppenes behov. På denne måten kan vi bedre legge til rette for at utsatte barn og unge og deres familier får den hjelpen de har behov for»
>
> *Fra Strategi for 0-24 samarbeidet*

Birgit Leirvik

1. Kan du fortelle litt om bakteppet for samarbeidet - hvorfor og hvordan det kom i gang?

Basert på tidligere erfaringer når det gjelder frafallsarbeid, for eksempel «Ny giv-samarbeidet», så man at tverrsektorielt samarbeid var nødvendig. I 2014 fikk vi i direktoratene et felles oppdrag fra departementene om å se nærmere på dette. Det ble satt ned en arbeidsgruppe med ledere fra de fem direktoratene, med et lite felles sekretariat. Det ble også satt ned flere arbeidsgrupper på tvers, på ulike fagområder (økonomi, regelverk, språk mv.)

Direktoratene leverte en felles rapport hvor vi skisserte en strategi og kom med forslag til en rekke konkrete tiltak. På bakgrunn av denne rapporten fra direktoratene kom et nytt oppdragsbrev våren 2015. Departementene var enige i hovedinnretning av arbeidet og hadde plukket ut cirka 25 av de foreslåtte tiltakene.

Direktoratene leverte også et forslag til felles oppdrag til Fylkesmennene, samt et stort felles satsningsforslag. Satsingsforslaget gikk i flere runder, men gikk aldri gjennom. Kanskje var det bra vi ikke fikk friske midler, det «tvang» oss til å forsøke å innrette eksisterende ressurser på en annen – og mer samordnet – måte? Vi har jobbet med mange og til dels nokså ulike prosjekter, både når det gjelder størrelse og temaområde. Men alt vi gjør handler i bunn og grunn om samordning knyttet til de sentrale virkemidlene våre; økonomiske, juridiske og pedagogiske.

Innsatser direktoratene iverksetter skal gi virkning i fylkeskommuner og kommuner. Men vi setter i gang mye hver for oss. Når vi begynner å se totaliteten i det vi til sammen setter i gang, så innser vi at det kan være for mye. Særlig for små kommuner kan det bli uoverkommelig å skulle forholde seg til alle de ulike satsingene og prosjektene fra direktoratene. Da vi satte i gang en kartlegging for å se nærmere på hvordan direktoratenes prosjekter og innsatser fungerte i Finnmark, innså vi at vi hadde behov for å skaffe oss oversikt over og samordne alle initiativene. 0-24 programmet ga midler til en prosjektleder hos Fylkesmannen i Finnmark, som fikk i oppdrag å skaffe en oversikt over ulike eksterne satsinger og prosjekter, rettet mot kommunene. Kommunene bruker mye ressurser på å rapportere til statlige aktører og man visste lite om hva man utsetter kommunene i Finnmark for. Dette var en vekker og vi har kanskje blitt mer forsiktig med å sette i gang nye satsinger[2].

2. Hvordan har dere brukt risikovurderinger i dette arbeidet?

Vi har jobbet med risikovurderinger hele veien, både internt (risiko for selve fremdriften av prosjektet) og ekstern risiko (måloppnåelse). Det rapporteres på risiko to ganger i året etter «vanlig mal» – rød, gul eller grønn risiko. Det er endel risikoer som har gått igjen hele veien: prioritering, oppslutning og eierskap/forankring. Andre ting som informasjonsflyt og kommunikasjon har vi fått bedre grep om underveis.

Måten vi har risikovurdert på kan ha en litt uheldig slagside ved at den hele tiden setter fokus på alt som er «vondt og vanskelig». Det gir lite fokus på styrker og hvilke muligheter vi burde utnytte. Sånn sett ville kanskje SWOT analyser el gi et mer balansert bilde og også bedre vise potensialet? Vi forsøker å løse et «gjenstridig problem». Dette er et komplekst arbeid som forvaltningen i utgangspunktet ikke er rigget for å løse. Det er mye risiko i dette arbeidet, og også vanskelig å vite hvor vi skal legge lista når det gjelder ambisjoner og vurdering av måloppnåelse.

[1] Se mer om hvordan programmet er organisert på 0-24 sine hjemmesider https://0-24-samarbeidet.no/om-oss/
[2] https://0-24-samarbeidet.no/prosjekt/0-24-prosjekt-i-finnmark/

Men risikostyring har selvsagt også en effekt ved at det holder oppmerksomheten på det som kan hindre at man leverer eller når målene.

Vi har hele tiden forsøkt å beholde en pragmatisk og praktisk tilnærming når det gjelder risikovurderinger, det skal fungere som et hjelpemiddel.

3. Det står i strategien at dere etablerte et felles utfordringsbilde - klarte dere også å etablere et nullpunkt å måle utviklingen opp mot?

Det er vanskelig å måle effektene av programmet på overordnet nivå, og vi har ikke egentlig definert et nullpunkt for hele satsingen. Det er lettere å måle resultatet av innsatsen internt i direktoratene (prosessmålene våre) og vi har definert et nullpunkt der. Det er også lettere å definere «nullpunkt» - altså si noe om nåsituasjonen – i de ulike delprosjektene. Vi kunne sikkert ha gjort en bedre jobb med målstrukturen innledningsvis. Vi jobber fortsatt med å forsøke å konkretisere målbildet ytterligere og synliggjøre bidragene fra de ulike delprosjektene for programmet som helhet bedre.

Det har vært nyttig å lære mer om programstyring/-ledelse, men endringsledelse er også sentral kompetanse i slikt arbeid. Vi kunne nok også hatt bedre prosesser og i større grad tatt inn over oss hvor viktig det er å involvere bredt og godt, og at folk kan møtes og snakke sammen. Når det er sagt så har vi virkelig hatt bruk for skriftlighet også. Det er viktig at vi dokumenterer beslutningsgrunnlag og beslutninger underveis. Vi er nøye med å holde orden i planer, fremdriftsplaner, avviksskjema, prosjektplaner og referater. Tverrsektorielt samarbeid gir mye rom for uklarheter og misforståelser. Det at vi formulerer skriftlig hva vi har blitt enige om og hvilke vesentlige beslutninger som er tatt underveis er helt avgjørende.

Det er også viktig å dokumentere og kommunisere læring og erfaringer. Det blir lett slik at det du har lært blir selvfølgelig og etter en stund så ser du ikke lenger at vi faktisk har kommet videre. Det å ha eksterne evaluatorer er viktig for dette, men vi har også lagt vekt på at kontinuerlig forsøke å lære av våre egne erfaringer underveis.

4. Har dere klart å sannsynliggjøre eller måle gjennom forskning eller på annen måte om arbeidet er begynt å bære frukter?

Deloitte evaluerer arbeidet vårt. De leverte en rapport våren 2018 – og kommer med en ny i vår. Hovedfunnene så langt er:

- Programmet har utviklet seg betydelig siden oppstarten.
- Det har vært utfordringer med forankring og organisering av programmet
- Det har vært utfordrende for direktoratene å samarbeide.

https://www.udir.no/tall-og-forskning/finn-forskning/rapporter/evaluering-av-0-24-programmet/

Ellers har Difi fulgt arbeidet i den første fasen og levert et læringsnotat https://www.difi.no/rapport/2017/01/laeringsnotat-2016-felles-problem-felles-losning-laerdommer-fra-0-24-samarbeidet

5. Det står i strategien deres at «Vi tar i bruk nye arbeidsformer der dette er hensiktsmessig, for eksempel digitalisering og tjenestedesign». Kan du si litt om hvordan brukerne har fått glede av det så langt?

Vi har hatt workshops med brukere, og jobbet med brukerinvolvering i ulike sammenhenger. Det var et godt virkemiddel også for å få fagfolk fra ulike sektorer til å samarbeide. Tjenestedesign og brukerfokus kan vri fokus bort fra egne kjepphester, og over på en felles innsats for å løse brukerutfordring.

Samtidig er det utfordrende at konsulentene (tjenestedesignerne) kan ha lite erfaring med tjenestedesign på direktoratsnivå. De foreslår gjerne sluttbrukertiltak (dette er gjerne på kommunalt nivå), mens direktoratene gjerne skal utvikle tiltak på statlig nivå. Å få til koblingen i mellom, er av og til utfordrende.

6. Har dere tatt utgangspunkt i erfaringer fra andre land eller andre tjenestekjeder i Norge?

Vi har lett etter tilsvarende innsats som vår andre steder, men ikke funnet så mye. Vi har et Nordisk 0-24 prosjekt initiert av Nordisk ministerråd etter inspirasjon fra det norske 0-24 samarbeidet. Alle de nordiske landene strever med de samme utfordringene knyttet til utsatte barn og unge, utenforskap og manglende samordning av innsatser og tjenester. Det gjennomføres en følgeevaluering av hele det nordiske 0-24 og det gjøres en vurdering eller evaluering av case i hvert enkelte land.

En beskrivelse av det nordiske samarbeidet og evaluering av det ligger også på 0 -24 nettsiden https://www.udir.no/tall-og-forskning/finn-forskning/rapporter/nordisk-0-24-samarbeid/)

I Sverige er det startet opp et 0-24 prosjekt, delvis etter modell av vårt[3]. De kommer og besøker oss rett etter sommeren.

7. Hvilke grep vil du trekke fram som mest vellykkede?

Tålmodighet har vært og er viktig. Det at vi gjorde et felles utredningsarbeid innledningsvis og fikk tid i en forprosjektperiode til å utvikle en felles problemforståelse tror jeg også var av stor betydning.

Videre er forankring på høyt nok ledernivå avgjørende, samt ledere som virkelig vil dette. Forankring på papiret er ingenting verdt alene, man trenger ledere som holder fanen høyt hele veien.

Vi har lært mye om kommunikasjon som virkemiddel. Dette arbeidet handler så mye om oppslutning, og om å skape ny forståelse og en kulturendring – og da er kommunikasjon et helt sentralt virkemiddel. Vi har blitt bedre på dette etter hvert, og ser hvor viktig dette virkemiddelet er.

[3] *https://www.skolverket.se/skolutveckling/leda-och-organisera-skolan/extra-stod-till-elever/tidiga-och-samordnade-insatser-for-barn-och-unga.*

Å krype til korset

Wells Fargo Business Standards Report

MARTIN STEVENS
Mediakomiteen og Gjensidige Forsikring

Det er tidligere i SIRK redegjort for utfall av uetisk adferd i USA sin fjerde største bank, Wells Fargo & Company. Det groveste eksempelet på uetisk adferd i denne saken er at det ble åpnet tusenvis av konti, og utstedt kredittkort i fleng, uten kundenes kjennskap og tillatelse. Praksisen gav bonus til de ansatte og bidro til at de også kunne beholde jobbene sine i et tøft KPI-regime. Nå har selskapet utgitt en egen rapport, som er offentlig tilgjengelig, og den har tittelen «Learning from the past, transforming for the future». Jeg mener det er unikt at rapporten ikke er skrevet på bakgrunnen av krav fra politikere eller myndighetene, men faktisk er utarbeidet som svar til et krav satt av bankens egne aksjonærer. De ønsket en redegjørelse fra selskapet rundt hva som er gjort for å sørge for at banken nå opptre på en bedre og mer etisk måte.

Rapporten redegjør for forbedringer som er gjort innenfor følgende områder:

- Kultur
- Ledelse og virksomhetsstyring
- Kundepleie
- Risikostyringsstruktur og -utførelse
- Forpliktelse til økt åpenhet.

For de som er mer interessert i detaljene anbefaler jeg at man kan laste ned rapporten her https://www.wellsfargo.com/about/corporate/governance/business-standards-report/

I denne lille artikkel vil jeg fokusere spesielt på den delen der det beskrives om hva man har gjort av forbedringer på risikostyringsområdet.

Det første som slo meg er at rapporten ikke bruker ordet «de ansatte», men alle blir omtalt som «teammedlemmer». Dette sier noe om den nye holdningen til de ansatte: i stedet for beinhard rovdrift, skal de inkluderes og tas med i utviklingen av banken. Det uttales videre i definisjonen av verdigrunnlaget i banken, at alle skal være ledere. De skal lede seg selv, lede teamet og lede forretningsutviklingen. Konseptet om at alle teammedlemmer er risikoledere er forsterket og det forventes dermed at alle tar ansvar for å unngå å ta unødvendig eller for høy risiko. Fokus fremover skal være på «Kontroll, lønnsomhet og vekst» i den rekkefølgen. Det understrekes at man skal fokusere på gode resultater i det lange løp og å skape verdier for aksjonærene på lang sikt. Samtidig har forbedringsarbeidet ført til en betydelig omdreining av fokus ved at belønning/bonus ikke skal baseres på kortsiktige leveransemål. For å måle kulturendringene sier de at de fokuserer nå på følgende varierte KPI'er:

1. Turnover
2. Ansiennitet
3. Feedback fra opplæring og høringsinitiativ
4. Mangfold og en inklusiv arbeidsplass
5. Input fra risikostyring, compliance og internrevisjon
6. Lukking av forbedringstiltak
7. Fremdrift i kulturforbedringstiltak.

I tillegg til fokus på kulturendring skal de ansatte motiveres til å bidra med gode innovative ideer som bruk av ny teknologi f.eks robotics.

Risikostyring er blitt styrket både gjennom nyansettelser og bedre fokus på helhetlig risikostyring, og ikke minst etablering av en Risikokomité.

I rapporten skrytes det av at kulturen er endret slik at man oppmuntrer til diskusjon og flagging av risikoer på alle nivåer og på tvers av forretningen. Det beskrives videre at dette betyr at ledere og kollegaer skal utfordres på en konstruktiv måte for å bygge opp et miljø som oppmuntrer til troverdig utfordring.

Organisasjonen skal etterleve de 3 forsvarslinjer. I definisjonen av hva som inngår som risikostyringens ansvar i 2. linjen nevnes å:

1. Utfordre forretningsbeslutninger og strategisk utvikling for å få god balanse mellom risiko og lønnsomhet.
2. Oppsummere et helhetlig risikobilde.
3. Utfordre risikoidentifikasjon og vurderinger gjort i 1. linjen samt deres risikoreduserende- og overvåkingstiltak.
4. Utføre uavhengige tester på hvordan gjennomføring av risikostyringsrammeverket er implementert.

I risikoreduserende øyemed skrytes det av et nytt regime for eskalering av saker der rask respons er viktigere enn millimeter nøyaktighet. Intensjonen er å unngå at hendelser som blir flagget gjennom kundetilbakemelding ikke tas tak i før etter 5 år og masing fra forbrukertilsynet.

Rapporten er interessant lesing og kanskje kan gi læring til oss alle uten at vi må i egen organisasjon begå de samme tabbene som Wells Fargo hadde gjort i sin.

JUST A SONG BEFORE I GO[1]

På tampen av en nesten femti år lang yrkeskarriere innenfor revisjon og revisjonsnære emner, skal jeg gi en liten oppsummering. Nå er jo slike tilbakeblikk oftest mer gøy for forfatteren selv enn for andre, så i håp om at flere av SIRKs lesere skal finne noe å glede seg over suppleres innlegget med et tonefølge av låter jeg setter pris på, med titler som antyder hva avsnittet dreier seg om.

TOR SOLBJØRG
Leder av IIA Norges fag- og metodekomité, tidligere revisjonssjef i Helse Nord RHF

WHEN I WAS YOUNG[2] – TAXMAN[3]

20 år gammel ble jeg ansatt som revisor-aspirant hos Skatteinspektøren i Nordland (senere Fylkesskattesjefen), og etter to skoleår i Oslo og to år med boketterssyn hos næringsdrivende i Nordland, var jeg utdannet skatterevisor. Jeg ble i etaten i fem år til, og kontrollerte alt fra kiosker til store industrivirksomheter. Jeg fikk møte mange flotte, dyktige og driftige mennesker, samt en og annen luring. Jeg lærte mye om skatt og avgift, kontrollteknikk, regnskap og rapportering, og utviklet vel en viss menneskekunnskap. Da jeg tidlig i karrieren opplevde at en næringsdrivende la armen faderlig rundt meg og erklærte seg som «Bodøs ærligste mann», tok det noen måneder før jeg skjønte at han burde puttet en «u» inn i det utsagnet! Jeg hadde oppdrag i minst halvparten av fylkets 45 kommuner, og det ble mange minneverdige opplevelser. En av disse var lastebileieren som under ettersynet jobbet på anlegg langt unna, og som ba meg dra innom moren hans og hente fakturamappa som sto i skapet i stua. Beklageligvis gikk hun i feil skap, hvor de fakturaene han hadde *holdt utenom* regnskapet sto. Mannen tok det med fatning, men gjorde det senere tindrende klart at det å legge feilaktig utleverte dokumenter til grunn for etterligning og avgiftsberegning, slik jeg gjorde, var et grovt brudd på grunnleggende prinsipper om fair play! Videre har jeg fortsatt ondt av oppfinneren/gründeren som under ettersynet innså at hans egentegnede plastbåt, støpt i garasjen i boligens underetasje, aldri ville bli sjøsatt – det var umulig å få den ut av bygget uten å rive hele veggen! Og jeg husker godt kollegaen min som gjennomførte alle ettersyn med voldsom entusiasme, i uttalt overbevisning om at «enhver næringsdrivende er en kjeltring, ikke bare inntil, men også etter at det motsatte er bevist!»

Crosby, Stills & Nash, Wikicommons

LIFE IN A NORTHERN TOWN[4] – BIGMOUTH STRIKES AGAIN[5]

Etterhvert tok jeg eksamen som registrert revisor og gikk over til privat revisjon i Noraudit i Bodø. Sjefen, Gunnar Pedersen, hadde enorm arbeidskapasitet, fenomenal analytisk teft og aversjon mot unødvendig bruk av stammespråk. Ett eksempel var da ledelsen i bedriften vi reviderte stolt presenterte grafer og tall som viste positiv utvikling i omsetning, resultat, markedsandel og ordrereserve. Gunnar lot seg ikke imponere, han spurte bare: Men har dere penger i kassen? (Jeg husker min egen umiddelbare reaksjon: Hva f.. slags spørsmål er det?). Når de svarte med nye tall og grafer som gjaldt alt annet enn likviditet, gjentok han bare spørsmålet, og slik fortsatte det inntil

svaret endelig kom: «Nei, akkurat der sliter vi for tiden…». Bedriften var i realiteten på konkursens rand!

I 1982 bar det til Bergen og Høyere Revisorstudium, med hustru og datter på slep. Bergensernes rykte som høylytte flåkjefter var velkjent, og på Aspmyra hadde «Heia Braaann»-skrålene ofte irritert meg kraftig. Men det ble et alle tiders år som vi tenker tilbake på med glede. En herlig by med masse flotte mennesker – og en og annen flåkjeft!

GOLD NUGGETS[6] – HOTEL ROOM[7]

Autorisasjonen og medfølgende partnerstatus i Noraudit betydde lange arbeidsdager fulle av utfordrende oppgaver. Kanskje hadde jeg også et håp om at denne karriereveien, i likhet med regnbuen, skulle lede til en kiste med gull. I så fall ble ikke forventningene innfridd, men jeg ble i alle fall rik på nyttige erfaringer – og du verden så mange gullkorn av både faglig og humoristisk art jeg bærer med meg fra samarbeidet med min kompanjong og mentor Gunnar Pedersen!

Baksiden av medaljen var drøyt 2.500 arbeidstimer i året og fryktelig mange reisedøgn. Jeg husker godt at en hyggelig julehilsen fra Torghatten Hotell i Brønnøysund avstedkom følgende melding fra madammen: Jeg skal pinadø sende deg julekort jeg også, for du sover jo nesten like mye her som på Torghatten!

I'M WAKING UP TO US[8] – SHE'S LOST CONTROL[9]

Jeg må ha sovet tungt i timen, når jeg ikke innså at så mye jobbing, reising og møtevirksomhet var uforenlig med et normalt familieliv med godt og nært forhold til ektefelle og barn. Heldigvis våknet jeg opp i tide – så vidt – og meldte overgang til Nordland fylkeskommune og jobben som fylkesrevisor. Den gangen, på 90-tallet, lå kommunal/offentlig revisjon langt bak privat revisjon rent faglig, så det ble naturlig å engasjere seg i kursing og utvikling av metodikk og standarder. Dermed fikk jeg gleden av, sammen med dyktige kolleger, å bidra til en solid faglig nivåheving i sektoren.

Det jeg husker best fra den tiden, er likevel saken med fylkeskommunens varaordfører. Hun hadde mangelfull kontroll på egen pengebruk, og løste problemet ved å tilegne seg midler fra arbeidsgiveren på utradisjonelt og kreativt vis. Jeg fikk ansvaret for å granske forholdene, og jeg ble hovedvitne i rettssaken som endte med dom for bedrageri og dokumentfalsk, samt fradømmelse av alle politiske verv. Også det var nyttig lærdom, og i ettertid ser jeg nok at jeg til tider beveget meg inn i grenseland for hva en revisor uten politimyndighet har anledning til å gjøre.

EN VELDIG HELDIG MANN[10]

Jeg hopper over gode minner fra årene i Norges Kommunerevisorforbund, Sivil-

Belle and Sebastian, Wikicommons

Terje Nilsen, Wikicommons

Halvdan Sivertsen, Wikicommons

[1] *Crosby Stills & Nash, 1977*
[2] *Eric Burden & The Animals, 1967*
[3] *Beatles, 1966*
[4] *The Dream Academy, 1985*
[5] *The Smiths, 1986*
[6] *Pavlov's Dog, 1976*
[7] *Edgar Broughton Band, 1971*
[8] *Belle & Sebastian, 2001*
[9] *Joy Division, 1979*
[10] *Terje Nilsen med Helge Jordal, 2016*

økonomutdanningen/Nord Universitet, KPMG og Nordlandsbanken – og nei, det var ikke min skyld at banken gikk under mens jeg var internrevisor der! – og kommer til jobben jeg har hatt siden 2005, som revisjonssjef i Helse Nord RHF. Her har jeg trivdes kjempegodt, ikke minst fordi vi internrevisorer får et detaljert innblikk i alle sider ved virksomheten, et innblikk som er få andre forunt. Godfølelsen skyldes nok likevel først og fremst at jeg på mange vis har vært svært heldig: Jeg har førsteklasses medarbeidere, samarbeidet med foretakets administrative ledelse har alltid vært utmerket – med et visst unntak for den aller første tiden, da de ikke var helt forberedt på hva internrevisjon faktisk innebærer – og ikke minst, styret og revisjonsutvalget, mine oppdragsgivere, er genuint interessert og engasjert i jobben vi gjør. Dét er motiverende!

KJERRINGØY[11] – FLYTT BODØ LENGER SØR[12]

Ett av mange gode minner fra denne tiden er NIRFs årskonferanse i 2013, som vi fikk gleden av å arrangere i Bodø. Noen av leserne husker kanskje utflukten til Kjerringøy i nydelig vær, hvor vi på returen ikke bare passerte flere velvoksne elger, men også en golfbane hvor spillet pågikk for fullt i lyset fra midnattssolen. I den forbindelse passer det også å nevne en pussig observasjon jeg har gjort ved flere anledninger: Det sitter atskillig lengre inne for kolleger fra Oslogryta å besøke Bodø, enn for oss å reise motsatt vei. Det må rett og slett være mye lengre å reise nordover enn sørover!

ALL OF MY FRIENDS WERE THERE[13] – A SONG FOR EUROPE[14]

Utviklingen går raskt på fagfeltene våre, og det er krevende å henge med. Kurser og øvrige tilbud fra faglige organisasjoner er derfor kjærkomne, og der syns jeg NIRF/IIA Norge har gjort en glimrende jobb. Ikke minst gjennom de årlige fagkonferansene hvor det alltid er gode foredrag om dagsaktuelle tema, samtidig som det sosiale aspektet er viktig. En internrevisors jobb er ofte ensom, så verdien av regelmessige møter med kolleger og likesinnede, som etter hvert også

Roxy Music, Wikicommons

blir venner, kan knapt overvurderes. Jeg vil også skryte av de europeiske konferansene arrangert av ECIIA, hvor jeg i årenes løp har plukket opp mange interessante nyheter og trender.

TEACH YOUR CHILDREN[15]

Jeg har, ikke minst i min tid i Helse Nord og IIA Norge, fått lov til å utvikle og holde atskillige kurs, foredrag og forelesninger, samt skrive artikler og lærebøker. Forhåpentligvis til glede for målgruppene, og definitivt til nytte for meg selv. Jeg tviler på om det fins mer effektive måter å tilegne seg dybdekunnskap og ny innsikt på, så jeg har et godt råd til dere som syns dette høres interessant ut, men hittil ikke har påtatt dere slike oppgaver: Gjør det nå!

HEY MAN, NOW YOU'RE REALLY LIVING[16] – TAKK TE DOKK[17]

En alternativ beskrivelse av formålet med internrevisjon lyder slik: «Å bidra til at virksomhetens styre og ledelse kan sove godt om natten». Min innsats som virksomhetens Jon Blund går nå raskt mot slutten, pensjonisttilværelsen venter. Den ser jeg fram til med svært blandede følelser, faktum er nok at jeg gruer meg litt. Men jeg prøver å tenke positivt og feste lit til det venner som har gått veien før meg hevder – at det er først nå man virkelig begynner å leve! Til dere lesere, venner og kolleger sier jeg lykke til med fortsatt

The Eels, Wikicommons

bidrag til andres gode nattesøvn, og tusen, tusen takk for den fine tiden jeg har fått ha sammen med dere!

Jeg runder av med et referat fra en familiesammenkomst nylig, hvor en av døtrene mine stilte følgende spørsmål: Hvordan i all verden har du holdt ut i noe så kjedelig som revisjon, gjennom hele yrkeslivet? Den videre samtalen forløp slik:

- Jo, skjønner dere, revisjon er noe mye mer enn bare et yrke eller en profesjon.

- Hva da – en lidenskap?

- Ja, kanskje, men egentlig mer enn det også…

- Jaha – et kall? (Tror faktisk en uforskammet svigersønn antydet «sykdom», og «besettelse».)

- Nei, det er … mens jeg fortvilet lette etter det forløsende begrepet, kom det tørt fra fruen:

- Jeg tror ordet du leter etter er «legning».

Kan hun ha vært inne på noe?

[10] *Terje Nilsen med Helge Jordal, 2016*
[11] *Halvdan Sivertsen, 1987*
[12] *Bare Egil Band, 2014*
[13] *Kinks, 1968*
[14] *Roxy Music, 1973*
[15] *Crosby Stills Nash & Young, 1970*
[16] *Eels, 2006*
[17] *Prudence, 1975*

CONFERENCE #ECIIA2019

Luxembourg, 18-20 September 2019

Embrace
Change and
Innovation in
Internal
Audit

· founded 1996 ·
institute
of internal
auditors
luxembourg

ECIIA

Internkontroll-prosjektet i Politiet – en løypemelding

OLA OTTERDAL
Seniorrådgiver internkontroll og risikostyring, Politidirektoratet

Denne artikkelen gir et innblikk i Politi- og lensmannsetatens arbeid med internkontroll de siste årene - de vurderinger man gjorde ved oppstart av internkontrollprosjektet og erfaringer underveis. Etaten jobber fortsatt med å lukke noen anmerkninger fra Riksrevisjonen, men det har nylig kommet positive signaler fra Stortingets kontrollorgan når det gjelder internkontroll på et viktig område. Det kan tyde på at det systematiske arbeidet begynner å gi effekt.

Politi- og lensmannsetaten (POD) er blant de aller største, mest komplekse, vesentlige og risikoutsatte statlige virksomhetene. Etaten er gjenstand for stor oppmerksomhet fra politikerne, media og publikum. Reformer og store endringer har satt sitt preg på etaten de siste årene. Selv om risiko er en ryggmargsrefleks hos politifolk og selv om Riksrevisjonen har gitt etaten anmerkninger på flere områder innenfor dens ansvar, så har internkontroll ikke stått høyt i kurs. Distrikter og særorganer har hatt stor grad av autonomi og det finnes store reelle forskjeller på situasjonsbildet til de ulike enhetene. Det er med andre ord utfordrende å få til enhetlig og helhetlig internkontroll. Ledelsen bestemte seg for å ta grep og mandatet for internkontrollprosjektet ble godkjent i 2016. At dette skjedde i en periode der 27 politidistrikter skulle bli til 12 og hvor det var gitt føringer om at styringen skulle sentraliseres og standardiseres ga noen ekstra utfordringer, men også noen unike muligheter.

Politidirektoratet har også vært gjennom en omorganisering og ny organisasjon ble iverksatt fra 1. januar 2019. Det er Styringsavdelingen som har fagansvaret for virksomhetsstyring, risikostyring og internkontroll og seksjonsleder i Økonomiseksjonen Trude Beate Sveen har vært prosjekteier for internkontrollprosjektet.

Trude Beate Sveen

Trude, kan du si litt om foranledningen til etableringen av internkontroll-prosjektet?

Vi besluttet i 2016 å etablere et prosjekt på grunn av vår og Riksrevisjonen sin bekymring over om vi hadde god nok kontroll på politiets regnskap. I mandatet for prosjektet fremkom at målet var å eta-

Illustrasjon til artikkelen: https://www.shutterstock.com/

blere et system for intern kontroll tilpasset risiko og vesentlighet som er innebygd i PODs interne styring. I løpet av 2018-2019 skulle et velfungerende styringssystem med innebygget internkontroll være på plass. På den tiden hadde vi etablert en felles hovedbok for hele politiet og vi skulle gradvis fase inn hovedboksdata fra de ulike politidistrikt, særorgan og øvrige underliggende enheter gjennom hele 2017 og 1. kvartal 2018. I den forbindelse så vi behovet for å kartlegge alle våre lønns- og regnskapsprosesser og se om vi hadde tilfredsstillende kontroller i alle ledd for å sikre et fullstendig regnskap. Vi identifiserte prosesser og kontroller og laget nye kontroller der kontrollene manglet. Vi hadde en «soft close» (myk årsavslutning) per 30. september 2017, hvor vi blant annet testet kontrollene vi hadde etablert og de som var der fra før.

Hva slags diagnose stilte dere før prosjektet ble startet?

Det var usikkert om Riksrevisjonen kunne godkjenne politiets regnskap for 2017. Samtidig stilte de spørsmål ved om vi hadde et helhetlig internkontrollsystem for lønn og regnskap. Vi visste at vi ikke hadde et slikt system i politiet. Det var også Justis- og beredskapsdepartementet (JD) klar over og i tildelingsbrevet for 2018 ble etaten bedt om å sende en plan for det videre utviklingsarbeidet knyttet til internkontroll.

Ble det definert noen ambisjon med arbeidet?

Målet for prosjektet for 2017 var å få et godkjent regnskap fra Riksrevisjonen. Videre var ambisjonen å få opp et helhetlig internkontrollsystem i politiet.

Hvordan har dere gått fram i prioriteringen av leveranser og fokusområder?
Fokus i 2017 var på å sikre riktig regnskap. Det var viktig i prosjektgjennomføringen å tilpasse fremdrift og leveranser til tidsløpet for når de enkelte politidistriktene og særorganene skulle overføre regnskapsprosessene til felles tjenestesenter og lønn til DFØ. Enhetene hadde derfor ulike tidsplaner. I 2018 ble fokus endret til å utvikle hovedelementene i et helhetlig rammeverk for internkontroll, og 2019 er prøveår for innføring av dette rammeverket. Rammeverket består blant annet av roller og ansvar, årshjulsprosesser, samt struktur for styrende dokumenter og ny fullmaktsstruktur.

Hvordan vil du beskrive kulturen for styring og kontroll i etaten? Har denne endret seg de siste årene?
Både rammebetingelsene og måten internkontroll utøves på har endret seg de siste årene. Det finnes store mengder instrukser, rutiner med mer. Det er også mange innarbeidede arbeidsmåter som ikke alltid er formalisert. Hver enhet har fortsatt stor grad av autonomi, men koordineringen og samordningen fra direktoratet har blitt sterkere. Ledere for Stab for virksomhetsstyring i distrikter og særorganer har fått en viktigere rolle som bindeledd mellom det lokale og sentrale. Begrepsmessig har man rapportert på administrative kontroller i noen år, men nå er begrepet internkontroll innført. Men det er fortsatt potensial for forbedring. Internkontroll må bli en del av virksomhetsstyringen i etaten og få mer fokus. Det mangler en totaloversikt over all internkontroll, hva som er bra og mindre bra. Etaten jobber fortsatt med å lukke riksrevisjonsmerknader på sentrale prosesser. I tillegg til dette har det kommet rapporter fra vår egen internrevisjon om manglende internkontroll på enkeltområder. I prøveåret 2019 er det særlig fokus på å forbedre internkontrollen på beslag, sivil våpenforvaltning, budsjettdisponeringsmyndighet og styrende dokumenter.

Hvordan har du som prosjekteier involvert toppledelsen i arbeidet?
I 2017 satt vår avdelingsdirektør i styringsgruppen for prosjektet. Videre har det skjedd forankring gjennom linjen – det er tidvis gitt informasjon i toppledergruppen og ledelsen har også behandlet og sendt risikovurderinger til departementet. Justisdepartementet har ønsket en risikobasert tilnærming for gjennomføring av etatsstyringsmøtene og dette har gitt føringer for involvering av toppledelsen.

Internkontroll knyttet til lønn og regnskap

Det er i dag Politiets fellestjeneste (PFT) som har det operative ansvaret for lønns- og regnskapsprosessene i etaten. Marit Reitan er leder for enheten Lønn og regnskap i PFT og har vært sentral i internkontrollarbeidet på disse områdene. Her er det lagt ned tusenvis av timer med prosesskartlegginger, risikovurderinger mv. I et brev fra Riksrevisjonen fra mars 2019 kunne man lese følgende: «Ut fra det vi har observert vurderer vi at internkontrollen hos PFT innenfor lønns- og regnskapsprosessene er god».

Marit, hva vil du si har vært avgjørende ved det arbeidet dere har gjort for å få et slikt skussmål fra Riksrevisjonen?
Det er vanskelig å peke på en spesiell ting. Det ble gjort en grundig kartlegging av prosessene på begge fagområdene. Dette var verdifullt som input til risikokartleggingen som lå til grunn for implementering av internkontrollen. Å ha god innsikt i og god visualisering av prosessene er en kritisk suksessfaktor for en god kartlegging av risiko. Hvis jeg skal trekke frem en enkelt faktor, er det kanskje dette at man dermed kan dokumentere at vi har en genuin risikobasert internkontroll.

Det har vært mye fokus på å formalisere prosessene, men hvordan har dere jobbet med kultur og med å sikre god etterlevelse?
Det er et viktig spørsmål! Å etablere en kultur er et langsiktig arbeid. Vi har heldigvis svært dyktige ansatte i enhetene og i PFT, som er profesjonelle på sine områder og derfor har forståelse for betydningen av internkontroll. Det er jo heller ikke slik at det ikke fantes internkontroll tidligere, tvert imot var det mye god internkontroll på lokal basis. Det nye er jo at vi har standardisert, sentralisert og dokumentert internkontrollen i hele etaten, og dermed gjort den tilgjengelig for våre eiere og andre interessenter som Riksrevisjonen o.l. Men jeg må også si at vi jobber kontinuerlig med å forbedre denne kulturen. Det skjer blant annet med løpende oppfølging, tilbud om veiledning, og ikke minst anerkjennelse til de som gjør jobben med å sikre god etterlevelse.


Marit Reitan. Foto: Privat

Hva er holdningen til internkontroll i etaten (på lønn og regnskap og ellers i etaten)?
Jeg opplever de ansatte i politiet som bevisste sitt samfunnsoppdrag, og det gjelder også på dette området. God internkontroll er et bevis på at vi bruker fellesskapets ressurser fornuftig og med god styring, og vi kan dokumentere det. Vårt ansvar som ledere er å bidra til at denne sammenhengen blir forstått på alle nivåer i organisasjonen og at vi prioriterer også dette området. Dette ansvaret må utøves hver dag og en slik anerkjennelse fra Riksrevisjonen er en god oppmuntring til å jobbe videre.

Lars G. Røe. Foto: Privat

Ekstern prosjektleder

På grunn av manglende kapasitet internt bestemte POD seg for å kjøpe ekstern hjelp i mai 2017. Lars G. Røe har vært innleid prosjektleder for internkontrollprosjektet i omtrent to år.

Lars, hvordan har du opplevd å ha rollen som prosjektleder?

Dette har vært et spennende og utfordrende prosjekt med høy kompleksitet. Internkontrollprosjektet har jobbet sammen med økonomi- og regnskapsfunksjonene i virksomheten, med stab virksomhetsstyring i alle enhetene, med fagmiljøene i POD så vel som inn mot ledelsen. Det har vært givende å bidra til videreutvikling av styring og kontroll i en slik virksomhet. Vi startet med internkontroll knyttet til økonomiprosessene i 2017, og å har senere jobbet bredt med roller og ansvar, årshjulsprosesser på tvers av prosessområder så vel som styrende dokumenter, fullmaktsstruktur med mer. Jeg er spesielt opptatt av at for å lykkes må virksomheten evne å se mål- og resultatstyring, prosesstyring, risikostyring og internkontroll i sammenheng – dette skal sammen sikre god styring og kontroll i virksomheten. Min erfaring er at mange virksomheter bygger siloer med ulike fagmiljøer og personer, og at man ikke utnytter synergiene mellom disse områdene. Eksempelvis er tydelige prosesser nødvendig for å tydeliggjøre eierskap og ansvar, noe som igjen muliggjør oppfølging av internkontroll.

Hva har vært viktig for å lykkes i gjennomføringen?

En kritisk faktor for prosjektstyringen i dette prosjektet har vært etablering av arbeidsgrupper med representanter fra ulike deler av virksomheten for god involvering og kvalitetssikring av løsninger underveis. Deltakerne i arbeidsgruppene har også fungert godt som ambassadører ut mot organisasjonen og vært viktig for å sikre forståelse for løsningene. Andre viktige faktorer har vært å ha god forståelse for hvordan roller og ansvar er fordelt i organisasjonen, klare leveranser og kontaktpersoner i alle enhetene, og tilstrekkelig kapasitet til å sikre en god gjennomføring.

Hva vil du beskrive som mest vellykket?

Jeg tror nok at mange var usikre på om det var gjennomførbart å kartlegge, identifisere behov og implementere en formalisert internkontrollstruktur i lønn- og regnskapsprosessene i hele politiet i løpet av drøye syv måneder fra slutten av mai 2017. Dette i en periode med stor omstilling. For egen del er jeg meget fornøyd med at vi klarte dette på en så god måte. Heldigvis viste det seg at mye av det grunnleggende var på plass, men det var en hektisk periode.

Hvis du skal sammenligne internkontrollarbeidet i POD med tilsvarende forbedringsarbeid i andre virksomheter du kjenner - hva er særlig utfordrende i POD?

Jeg opplever nok at internkontroll er et utfordrende tema å forholde seg til for mange når vi går utenfor økonomiprosessene og skal snakke om å sikre internkontroll inn i operasjonelle prosesser. I produksjonsvirksomheter er kvalitetssikring bygget inn i prosessene som del av kvalitetsstyringen, mens for politifolk som har i sitt DNA at de skal fange tyver blir internkontroll fort svevende. Dette er nok tilsvarende og gjenkjennbart for mange virksomheter - i hvert fall i offentlig sektor.

En utfordring i politiet er den store bredden i oppgaveporteføljen. Politiet driver med sivil våpenforvaltning, internasjonale forpliktelser, samfunnssikkerhet, pass og mye annet i tillegg til kriminalitetsbekjempelse. Det er derfor vanskelig å få oversikt over den internkontroll som praktiseres innenfor ulike fagområder for så å kunne vurdere om den er tilfredsstillende. Samtidig er det mye kompetanse på risikostyring og internkontroll innen enkelte fagmiljøer på direktoratsnivå, noe som gir et godt grunnlag for videre forbedringsarbeid.

Hvor moden er POD på internkontroll og risikostyring per i dag? Hva kan andre virksomheter lære av POD?

Politiet er nå kommet et godt stykke på vei med å tydeliggjøre hva som skal inngå i risikostyring og internkontroll og hvordan det skal følges opp på tvers av virksomheten. Min erfaring fra offentlig sektor er at politiet på dette området kanskje er kommet noe lengre enn mange i dette arbeidet, selv om de fortsatt er i en utviklingsfase. Jeg ser mange virksomheter der de har styrende dokumenter som fordeler ansvar, men uten å tydeliggjøre hva som forventes for å ivareta dette ansvaret. Hvilke konkrete aktiviteter bør mellomledere utføre for å ta sitt ansvar, hvor ofte, og hvilke støtteverktøy finnes for å hjelpe dem med dette? Her kan mange lære om behovet for årshjulsprosesser, metodikk, skjematikk og andre støtteverktøy. Kunsten er å finne smarte løsninger, slik at det blir gjennomførbart i virksomheten.

Internkontroll i storbykommunene

MAGNUS DIGERNES
Director, KPMG Risk Consulting

FLEMMING RUUD
professor BI

Internkontroll er under utvikling og skjer i praksis og teori, standarder og veiledere, virksomheters innretting av internkontroll og ikke minst i regelverkskrav, senest med ny kommende kommunelov.

Som et resultat av et felles FoU prosjekt for storbykommunene Oslo, Bergen, Trondheim, Stavanger og Kristiansand finansiert av KS Program for storbyrettet forskning, har KPMG på oppdrag fra Bergen kommune belyst følgende overordnede problemstilling:

> «Hvordan kan storbykommunene utvikle og implementere en risikobasert og dokumentert internkontroll som styrker kommunens interne styring?»

I rapporten blir innholdet til internkontroll belyst fra flere sider. Status for dagens internkontroll i storbynettverkets byer er kartlagt og analysert og har blitt vurdert mot anbefalinger i teori og litteratur. Denne analysen danner, sammen med god praksis i kommunene, grunnlaget for våre anbefalinger til en fremtidsrettet internkontroll.

Rapporten er utarbeidet av KPMG på oppdrag fra Bergen kommune som et resultat av et felles FoU prosjekt for storbykommunene Oslo, Bergen, Trondheim, Stavanger og Kristiansand, og finansiert av KS Program for storbyrettet forskning. Professor Flemming Ruud, BI og professor Per Lægreid, UiB, har vært konsultert i løpet av prosessen. Den metodiske tilnærming har bestått av intervjuer, spørreundersøkelse, fokusgrupper i kommunene, samt dokumentanalyse.

Kort om status på dagens internkontroll

Kommunene har en systematisk tilnærming til internkontroll og det foreligger rammeverk for internkontroll hvor blant annet fullmaktsstrukturer og krav til ledere er dokumentert. Alle kommunene har definert ledelsens ansvar for internkontroll og kommunene bruker risikovurderinger som en del av mål og resultatstyringen. Hva gjelder avviksrapportering og oppfølging av avvik, varierer det hvor systematisk dette håndteres og det er også variasjoner på tvers av sektorer i den enkelte kommune. Et fellestrekk i kommunene, er at helsesektoren i størst grad har en systematisk tilnærming til og oppfølging av avvik. I rapporten brukes kjennetegn fra helsesektoren som grunnlag for analyse og anbefaling knyttet til øvrige sektorene i kommunene.

Ved nærmere ettersyn av de ulike delelementene ved internkontroll er det forskjeller mellom kommunene. Felles for alle er at styringsprosessene ikke er detaljregulerte. I rapportens analyse- og anbefalingsdel vurderes hva som kan være hensiktsmessig detaljeringsnivå for storbyer.

I ny kommunelov fremgår det at internkontrollen blant annet skal tilpasses virksomhetens størrelse. Storbyene er størrelsesmessig komplekse, og Oslo er i særklasse hva gjelder antall ansatte og enheter. Gjennom kartleggingen observerer vi at Oslo har tilpasset internkontrollen til egenarten og de ulike byrådsavdelinger. Trondheim og Bergen har i større grad et felles sektorovergripende internkontrollrammeverk, og Stavanger er i ferd med å innføre det samme. Kristiansand har ikke utviklet en helhetlig internkontroll. Hva gjelder oppfølging av internkontrollen, har kommunene i varierende grad systemer og verktøy som sørger for at ledelsen får en systematisk rapportering på internkontrollstatus. Trondheim skiller seg her noe ut ved egenutviklede systemløsninger for sanntidsrapportering, i tillegg til å ha et eget styringsteam som bistår gjennom alle deler av internkontrollen.

Gjennom undersøkelsen, fokusgrupper og intervjuer er flere observasjoner knyttet til styrings- og kontrollmiljø, prosess, roller og ansvar og oppfølging av betydning som oppsummert i tabellen under.

Innholdet i en fremtidsrettet internkontroll i storbyene

En lærdom fra litteraturgjennomgangen er at det ikke finnes én form for internkontroll som passer for alle, men at den skal tilpasses de konkrete forholdene.

Dette innebærer også at det ikke kan hentes eller utvikles et felles oppsett og innhold for internkontroll som vil være likt for alle de fem storbykommunene.

I rapporten omtales særskilte storbyutfordringer. Dette er knyttet til områder og utfordringer som har størst relevans for befolkningsrike kommuner. Hva som er særlig storbyrelevant bygger i hovedsak på innhentet informasjon, og i mindre grad på forskningslitteratur. Kravene til internkontroll i ny kommunelov peker også på at internkontrollen må tilpasses størrelse, egenart, aktiviteter og risikoforhold, uten at det gis konkrete føringer på hvordan dette skal ivaretas.

For å kunne belyse krav og prinsipper til styring og ledelse i større virksomheter er ledelsesteori anvendt. Med bakgrunn i nye lovkrav, god praksis, samt teori og litteratur, er det noen prinsipper som trekkes frem i rapporten som viktige for en fremtidsrettet internkontroll i storbyene, herunder:

- Internkontroll som bygger opp under faglig autonomi, kompetanse og samhørighet oppleves å gi ansatte tillit og frihet.
- Styring og ledelse påvirker hvordan internkontrollen innrettes og følges opp. Målene og verdiene som kommunens styring og ledelse er fundert på, må operasjonaliseres.
- Detaljregulert internkontroll gjør det vanskelig å etablere tillitsbasert styring og ledelse.
- I storbykommuner er det ikke opplagt at en lærer på tvers av sektorer. Det observeres at etablerte nettverk knyttet til gitte internkontrolltema gir læring på tvers av sektorer, og felles kvalitetssystem gir bedre kommunikasjon på tvers av sektorer. Dette er erfaringer som vil kunne være særlig viktig for de aller største kommunene.
- Eksplisitte krav til internkontroll, herunder tiltak og aktiviteter innenfor internkontrollen, øker ansattes bevissthet i arbeidet med internkontroll.
- Tydelighet rundt ansvaret for å dokumentere internkontrollen og for å følge opp at kontrollaktiviteter gjennomføres som planlagt.
- Enkel rapportering på internkontroll til toppledelse og tydelighet rundt hva som skal rapporteres når til rådmann/byråd. Dette for å forhindre at all informasjon blir eskalert og rapportert til toppledelsen.

Område	Oppsummert observasjon
Styrings- og kontrollmiljø	- Tillitsbasert styring og ledelse er i et fåtall av kommunene operasjonalisert - Det er en sammenheng mellom tillitsbasert styring og ledelse og i hvilken grad internkontrollen er detaljregulert; detaljregulert internkontroll vanskeliggjør tillitsbasert styring og ledelse
Prosess	- Hensikten og formålet med gjennomføring av risikovurdering er alltid klart - Sektorspesifikke lovkrav til internkontroll har styrket internkontrollen - En virksomhets kompleksitet og kultur er vesentlig for etterlevelse av etablerte rutiner
Roller og ansvar	- «Linjeforsvaret» er i liten grad operasjonalisert og implementert i storbykommunene
Oppfølging	- Få av storbykommunene har etablert en felles systematisk tilnærming til oppfølging av avvik på tvers av sektorer - Hensiktsmessigheten av felles avvikssystem blir vurdert forskjellig i kommunene - Det er i liten grad etablert helhetlig rapportering på internkontroll som viser sammenheng mellom risiko og oppfølging innen de ulike forsvarslinjene - Felles kvalitetssystem oppleves å gi bedre kommunikasjon på tvers av sektorer intern i kommunene

Anbefalinger

Etabler felles overordnede styringsprinsipper for internkontroll

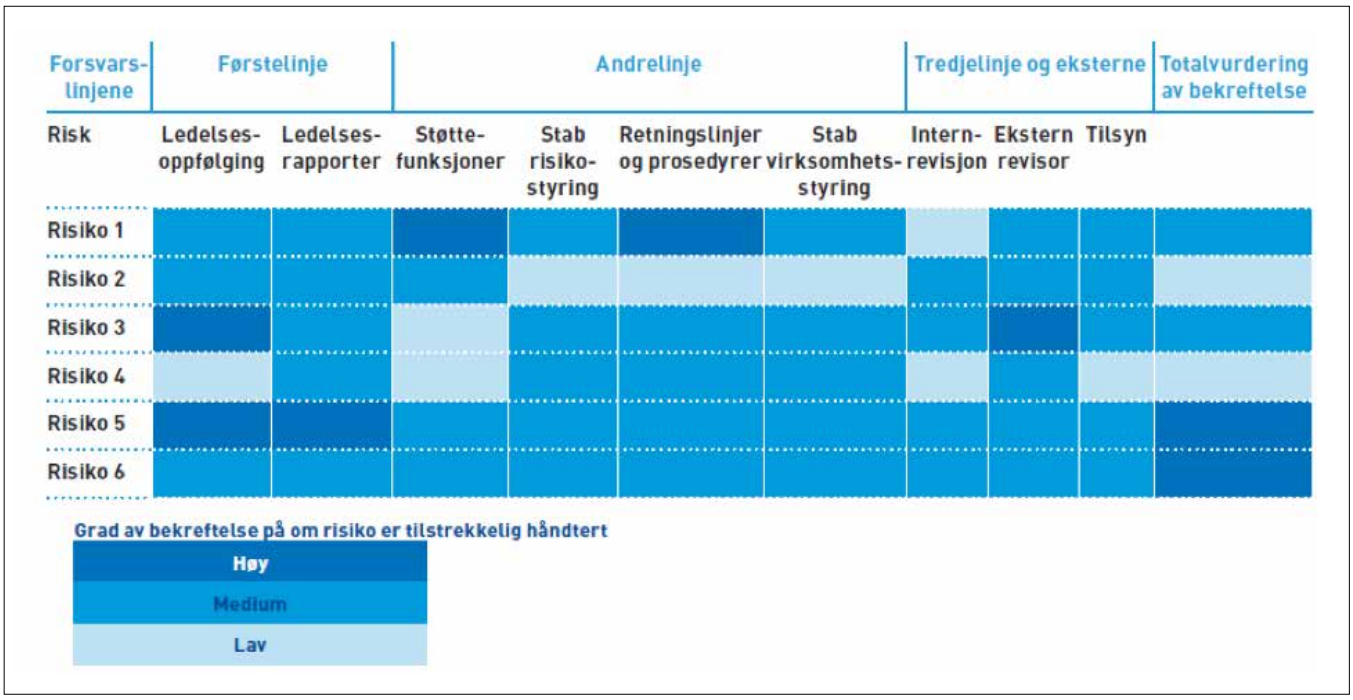
Flere av storbykommunene har eller er i ferd med å etablere prinsipper for tillitsbasert styring og ledelse, og jobber med forenkling. Litteraturgjennomgangen viser at tillitsbasert styring handler om å finne den rette balansen mellom styring og ledelse, kontroll og oppfølging, og ikke om fravær av kontroll.

Dette innebærer en tydeliggjøring av prinsipper på et overordnet nivå som skal gi føringer for prosesser og hvordan oppgaver utføres. I kartleggingen av kommunene kommer det fram at tillitsbasert styring ikke nødvendigvis betyr mindre kontroll. Det som er særlig viktig er at etablerte internkontrolltiltak skal gi mening og virke understøttende for kjerneoppgavene. På denne måten vil internkontrolltiltak bidra konstruktivt til oppgaveløsningen, og tydeliggjøre for medarbeiderne hvordan kontrollen bidrar til kjerneoppgavene. Tillitsbasert ledelse som gir rom for ansattes faglige autonomi og kompetanse for hvordan oppgaver utføres, oppfattes positivt.

Ansvar for, hyppighet av og hensikten med risikovurderinger bør tydeliggjøres

Det bør ikke være et mål at innholdet i internkontrollen skal være lik innad i kommunene, men at internkontrollen innordnes overordnede og felles føringer. Bruk av metodikk som pålegger enkelte felles aktiviteter, eksempelvis et årshjul kan være hensiktsmessig. Som en parallell til helsesektorens særlovkrav til internkontroll vil felles metodikk med tilhørende aktiviteter kunne være kommunens krav til internkontroll.

Felles, overordnede aktiviteter vil være utgangspunktet for sektor- og avdelingsvis oppfølging. I sektorer og avdelinger vil innholdet kunne være forskjellig, alt avhengig av den enkelte enhets særpreg.



Figuren illustrerer en helhetlig tilnærming til oppfølging av risiko.

Storbyer har stort mangfold og tilgang på fagkompetanse i egne avdelinger og kan legge til rette for internkontrollprosesser som tar høyde for autonomi, kompetanse og samhørighet.

Fra litteraturen fremgår det at risikovurderinger er sentrale i internkontrollarbeidet. Storbyer bør være særlig oppmerksom på å tydeliggjøre ansvaret for gjennomføringen av risikovurderinger, og hensikten med disse. Dette er forhold som bør forklares og tydeliggjøres i et felles rammeverk for internkontrollaktiviteter.

Definer og operasjonaliser ansvaret for internkontroll

I storbyene er det mange enheter i det som omtales som driftslinjen for kjernevirksomhet, og det er mange enheter innen stab- og støttefunksjoner. I rapporten plasseres ansvaret for internkontroll i driftslinjen. Samtidig vil ansvaret for internkontroll for gitte funksjoner ligge i stabsenheter, eksempelvis innenfor offentlige anskaffelser. I tillegg vil mange arbeidsprosesser involvere både drifts- og stabsavdelinger. Dette reiser svært ofte spørsmål om hvem som har ansvaret for at det er etablert internkontroll; både på enkeltoppgaver, på hele prosesser og innenfor særlige risikoforhold i prosesser.

For å fastsette "rammene" for internkontrollarbeidet kan det være hensiktsmessig for kommunen å starte med å fastsette organisering, roller og ansvar knyttet til internkontrollarbeidet. Roller og ansvar bør dokumenteres og følges opp. Det er særlig viktig at myndighetskart er tilstrekkelig konkret på hvilken stilling/leder som har hvilket ansvar på oppgaver og arbeidsprosesser, og at en slik oversikt tydelig skiller mellom driftsenheter og stabsenheter. Ansvaret for internkontroll blir utdypet i rapportens litteraturgjennomgang.

Etabler føringer for avvik og hendelser som skal rapporteres til hvilket nivå

Etablert internkontroll må følges opp og ledelsen i kommunen må påse at etablert internkontroll etterleves og fungerer som forutsatt og hvorvidt korrektive tiltak skal igangsettes samt hvordan disse i tilfelle skal følges opp. Oppfølging av internkontrollen er videre et viktig premiss for å utvikle en kultur for kontinuerlig forbedring. I den sammenheng er det viktig at det i kommunen skapes en kultur hvor det er rom for å kunne feile, men hvor registrering og håndtering av avvik verdsettes og anerkjennes som verdifullt for virksomhetens videre utvikling. Rapportering er det sentrale elementet i ledelsens oppfølging, og det trengs systematikk rundt hvilke forhold som skal rapporteres, hyppighet, og nivået rapportering skal stiles til.

Oppsummert anbefales at storbykommuner rapporterer til toppledelsen at virksomheter/avdelinger har etablert gode systemer og strukturer for internkontrollarbeidet. Dette omfatter etablering av et godt system for prosjekt- eller porteføljestyring. Rent praktisk vil dette innebære å rapportere avdelingsvis for hvordan internkontroll er planlagt, implementert og testet gjennom året, samt vurdere behov for forbedring. Dette kan gjøres gjennom en egenevaluering. Alle organisatoriske enheter bør rapportere, men rapportering til toppledelse kan aggregeres per virksomhetsområde eller liknende. Dette må avklares i rapporteringsrutinene.

Det var en gang

FOR 40 ÅR SIDEN

– Revisjon av årsoppgjøret og revisors valgbarhet

I Bankrevisoren 1 og 2 for 1979 er det to temaer som dominerer. Det ene er gjengivelse fra RVB (Revisjons Veiledning Bank) om revisjon av årsoppgjøret som gikk over til sammen 46 A-5 sider. Det andre store temaer som opptok 17 sider var om revisoren bør kunne bli valgt inn i styrende organer i forretnings- og sparebanker. Det var kommet i de to foregående år forskrifter fra Kredittilsynet (nå Finanstilsynet) der det ble slått fast at «ansatte som hører til revisjonspersonalet ikke var valgbare i bankers styrende organer». Her mente norsk bankfunksjonærenes forening (NBF) at skulle det være en slik ordning måtte det gjelde bare for ansvarlig revisor og eventuelt dennes stedfortreder. De forklarte at deres synspunkter bygget «bl.a. på impulser og meninger blant våre medlemmer i bankenes revisjonsavdelinger». Norsk bankrevisorforening gikk derimot sterkt ut og argumenterte for at ut fra både en uavhengighets og inhabilitets hensyn kunne dette ikke forsvares. Det ble også påpekt at revisjon beveger seg vekk fra å utføre rene bokholderioppgaver «i retning av større grad av kritiske kontroller og systemrevisjon». NBF forsvarte at revisjonsmedarbeiderne måtte få lov å ha tillitsverv i bankene ut fra at de også er ansatte i banken og bør kunne ta på seg å representere de ansattes interesse på lik linje med alle andre ansatte. NBF var også forutseende nok å komme med følgende uttalelse «Hvis man virkelig frykter en kollisjon mellom yrket og tillitsverv, så bør man kanskje overveie å flytte hele revisorfunksjonen og la ett frittstående firma overta dette. Denne løsningen er i bruk enkelte steder» men så føyde til at en slik løsning anbefaler de ikke.

Tidene har endret seg internrevisjon i bankene påtar seg ikke lenger ansvar for å revidere årsoppgjør. Det utføres utelukkende av eksterne revisjonsfirmaer. I dag mener jeg at IIAs etiske standarder som profesjonen følger utelukker helt temaet om at interne revisorer kan ta på seg tillitsverv i de selskapene der de er ansatt.

FOR 20 ÅR SIDEN

– «En ny definisjon av internrevisjon»

For 20 år siden utga IIA en oppdatert definisjon av internrevisjon som innebar at man skulle ha en konsulentrolle og blant annet revidere risikostyring. Dette brakte en del diskusjon med seg – ble uavhengigheten borte? – hva mentes med risikostyring?

I etterkant av internrevisjonskonferansen intervjuet Internrevisorbladet fire toppledere i internrevisjon; Vegard Østlien - Kreditkassen (nå Nordea), Einar Halse – Telenor, Oddbjørn Grinden – Forsvarssjefens internrevisjon og Kåre Thomsen – Statoil om hvordan de ser på utviklingen i faget vårt.

Det første temaet som ble drøftet var at den nye definisjonen av internrevisjon som hadde med seg en konsulentrolle. Å være konsulent mente man kunne lett føre til svekket uavhengighet. En internasjonal taler på årskonferansen hadde også uttalt at fokus på uavhengighet var avleggs, noe som Vegard Østlien mente var feil. Han ga uttrykk for at «uavhengighet er en viktig forutsetning for å kunne utføre eller bekle den rollen vi er tiltenkt i organisasjonen». Oddbjørn Grinden understreket at i hans organisasjon så ville de heller bruke tid til å snakke om «value added» enn uavhengighet. Andre påpekte at for dem var det viktigere å understreke objektivitet enn uavhengighet.

At Risikostyringsfunksjonen var ikke så gjennomført i norske virksomheter illustreres av følgende uttalelse fra Einar Halse som var kritisk til at den nye definisjon av internrevisjon nevner «risikostyring». Som han sier det «Bruk av begrepet risk management kan for ledelsen lett forbindes med forsikringsmessige spørsmål. Risk management er dessuten et operativt ansvar, slik jeg ser det».

Oddbjørn Grinden fortalte at internrevisjonsavdelingen hadde gjennomført en strategidebatt med det resultat at man definerte de produktene som skulle leveres i tillegg til de mer tradisjonelle revisjonsoppgavene. Han nevnte blant å utføre undervisning og rådgivning på fagområdet intern kontroll samt at de skal levere separate risikovurderinger når ledelsen ber om det.

Flere mente det var viktig å holde seg til kompetanseområdet som er styring og kontroll og ikke bevege seg ut på andre fagområder som f.eks strategi. Kåre Thomsen mente at spesialistkompetansen til internrevisjon ligger innenfor revisjon og revisjonsmetodikk. Han ga uttrykk for at «Ledelsen skal vite at vi arbeider systematisk med bakgrunn i et slik faglig fundament». Flere nevnte faktisk en utvikling til noe midt imellom konsulent og revisorrollen ved at revisjonsrapporter nå tok med seg også forslag til forbedringer.

Dette ble fulgt av en diskusjon om hvordan man sikrer spesialistkompetanse til revisjoner. Dette var man meget bevisst på at enten kunne man hente den internt fra i virksomheten eller fra eksterne konsulenter.

Intervjuet endte opp med en debatt rundt hvordan man skulle måle internrevisjonens kost/nytte. Alle var enige om at kost/nytten er noe som er vanskelig å bevise i kroner og øre men at man arbeider med å innhente kvalitativ tilbakemelding fra den reviderte enheten etter hver revisjon som er gjennomført. Einar Halse la også vekt på at opplevelsen til den reviderte enhetene ble adskillig bedre der det ble holdt en god dialog i et ansikt til ansikt avslutningsmøte.

Kåre Thomsen hadde det siste ordet i diskusjon da han kom med denne uttalelsen «Til spørsmålet om vi er ute av jobb om noen år, avhenger det helt av den jobben vi gjør i de kommende årene.»

Man bør merke seg at mye av den måten vi jobber på i internrevisjon i dag ble utformet i den tiden for 20 år siden. Siden den gang førte finanskrisen til et ytterligere fokus på revisjonsrollen og uavhengigheten i hvert fall i finansbransjen. Vi merker også at de vurderingene den gang stammer fra en tid før de 3 forsvarslinjer og at den 2. linjen skal i dag ivareta en del av denne konsulentrollen som den gangen lurte man på om og hvordan den skulle ivaretas av internrevisjonen.

Til slutt må vi vel ha gjort noe riktig i internrevisjonsmiljøet i Norge over de siste årene – still going strong!

Martin Stevens

Sekretariatet informerer

EXECUTIVE MASTER OF MANAGEMENT PROGRAMMET PÅ BI REVITALISERES

Programmet skal gi kandidater forståelse for sentrale elementer og prosesser som bidrar til god eier- og virksomhetsstyring (governance), og hvordan risikostyring, compliance og internrevisjon sammen med andre funksjoner bidrar til god governance og effektiv måloppnåelse. Programmet vil være interessant for kandidater som jobber med risikostyring, compliance, business controlling, så vel som internrevisjon. Man vil fortsatt kunne søke om tittelen Diplomert internrevisor etter endt studium hvis kravet til to års praksis er oppfylt. Det er rullerende inntak til studiet med oppstart av programmet september 2019.

IIA Norge har erfart at behovet for kompetanse om GRC er stort. Vi er derfor i ferd med å utvikle et modulbasert kurs innen GRC med oppstart høsten 2019. Formålet er å skape en større forståelse for Governance, Risikostyring, Compliance og Internrevisjon. Det blir satt av en dag til hver av de fire modulene og planen er at kurset avsluttes med Treffpunkt GRC i februar 2020. Modulene kan tas samlet eller også enkeltvis. Mer informasjon følger på IIA Norges webside.

NY NETTSIDE FOR IIA NORGE

Nettsider er ferskvare, og denne våren har tiden atter en gang gått med til prosjektering og utvikling av nye nettsider. Trender for bruk og design er i konstant endring og mulighetsbildet for nett og sosiale medier er i agil utvikling. Vi har en visjon om å gjøre nettsiden til selve 'hubben' for nyhetsdeling og informasjonsspredning, noe som krever et mye bedre redaksjonelt innhold enn i dag. Sammen med Mediakomiteen vurderer vi hvordan artikler i SIRK skal bidra inn i denne prosessen. I vår digitale tidsalder er det ikke sikkert at SIRK skal trykkes opp og distribueres i papirformat, men at artikler kontinuerlig legges ut når de er ferdigprodusert vil være mer tidsriktig. Som kjent er fremtiden nå, så kanskje er det siste trykte utgaven av SIRK du holder i hånden ...?

VI GRATULERER FØLGENDE MEDLEMMER

Diplomert internrevisor
Cecilie Stokke Clement, Grieg Investor
Rune Godtland, Zalaris ASA
Edit Anita Nordgaard, Barne-, ungdoms- og familiedirektoratet
Kenneth Hansen, Avinor
Hroar Haugsand, Kompetanse Norge

Certified Internal Auditor (CIA)
Merethe Nordling, Riksrevisjonen
Helena Holck Løchen, St. Helena Audit Service
Trond Brevik, Brevik Risk Management AS

Certification in Risk Management Assurance (CRMA)
Felipe Leandro Alves Pereira, National Oilwell Varco Norway AS

HVA GA MEDLEMSUNDERSØKELSEN AV SVAR?

I mars gjennomførte IIA Norge en medlemsundersøkelse for å få svar på hvor fornøyd medlemmer er med dagens tilbud, og hva foreningen bør jobbe mer med for å øke verdien av medlemskap. 27,3 % av medlemsmassen besvarte undersøkelsen og av disse kom 43,4 % fra offentlig sektor. Godt over halvparten av respondentene jobber med internrevisjon, mens resterende besvarelser fordeler seg likt på compliance og risikostyring.

Respondentene er i all hovedsak fornøyd med tilbudet fra foreningen, og det er kurs/seminarer, erfaringsutveksling og tilgang til relevant informasjon som gjør medlemskap verdifullt. Kurs og aktiviteter avholdes dessverre nesten alltid i Oslo, noe som gjør at medlemmer i andre deler av landet ikke får tilsvarende muligheter. Å kunne gjøre aktiviteter tilgjengelig gjennom webinar, skype og podcast vil være et skritt i riktig retning for å øke verdien av medlemskap for alle. Foreningen jobber med å visualisere et kompetansehus og ved å tilrettelegge for tydeligere opplæringsstruktur, vil det være enklere for virksomheter å planlegge kompetanseheving internt.

COSO CHAIR PAUL SOBEL I OSLO

Over førti medlemmer tok turen til Bjørvika 16. mai for å lære mer om COSO og ISO-rammeverkene, og hvordan Telenor og Yara arbeider med risikostyring i praksis. Det er ikke hver dag at IIA får besøk av styrelederen i COSO, ei heller at styrelederen åpner opp for innspill til fremtidige rammeverk og veiledninger.
COSOs styreleder velges for tre år av gangen og Paul Sobel var ganske trygg på at det ikke ville skje endringer i eksisterende rammeverk i perioden han er valgt for (2018 – 2021), men at han ville oppdatere eksisterende veiledninger og utgivelser av nye veiledninger til rammeverkene.

Potensielle oppdateringer til COSO-veiledninger:
- Monitoring Guidance
- Understanding and Communicating Risk Appetite
- Practical Approaches to Creating and Protecting Organizational Value
- COSO in the Cyber Age

Potensielle nye veiledninger:
- Using COSO ERM to Manage Compliance Risks
- Blockchain and its Impact on Internal Controls and Implications for ERM
- Psychology and Sociology of Fraud
- Assessment Tools for Risk
- Robotic Process Automation and Artificial Intelligence

Det er kun rammeverkene COSO tar betaling for. Øvrige veiledninger finnes det mange av og de kan lastes ned fra www.coso.org.

KONFERANSER VERDT Å MERKE SEG

IIAs International Conference, 7. – 10. juli 2019, California, USA

ECIIA, 18 – 20. september, Luxembourg

MODELL FOR RISIKOMODENHET FÅR INTERNASJONAL OPPMERKSOMHET

For to år siden utviklet Ayse Nordal og Ole Martin Kjørstad, medlemmer av risikonettverket i IIA Norge, en enkel modell med en ny tilnærming til å vurdere risikomodenhet. Dette verktøyet ble presentert i SIRK nr.1 2017 og ligger tilgjengelig på websiden til IIA Norge. Siden da har modenhetsmodellen blitt presentert i ulike fora, både ved GRC-dagarne i Sverige, IIA-konferanse i Bulgaria, i tillegg til andre fora i regi av IIA Norge. Modenhetsmodellen ser ut til å dekke et behov internasjonalt, og både vi i IIA Norge og Nordal og Kjørstad gleder oss veldig over at modellen blir benyttet av flere internasjonalt.

Et knippe eksempler viser at modellen er blant annet rangert blant de mest populære studiematerialene ved University av Virginia. Dokumentet siteres også av artikler av Robert J. Chapman i UK og i pensumlisten av UCL Summer School. I tillegg har et konsulentselskap i UK og Nato sin administrasjon i Brussel bedt om ytterligere detaljer om modellen. Siste henvendelsen kom fra New Zealand, hvor et helseforetak hadde plukket opp modellen og tok kontakt for mer informasjon og erfaringer rundt bruk. Å dra til New Zealand for å dele erfaringer er muligens litt i overkant, men å invitere interesserte brukere til Oslo for å høre mer om modellen og risikostyring generelt gjør våre to engasjerte medlemmer gjerne.

Tidlig i mars hadde Undervisningsbygg besøk fra Island. Undervisningsbygg utarbeidet et heldags program til representantene fra Finansdepartementet, Skole- og utdanningsdepartementet og ordføreren i Reykjavik kommunes kontor. Gjestene fikk en generell introduksjon av foretakets oppgaver og målsetninger av administrerende direktør. Ayse Nordal introduserte foretakets risikobegrep, rammeverk, risikostyringsprosess og verktøy samt risikorapporteringen til styret. I tillegg ble det gitt en kort innføring i hvordan foretaket arbeidet med å bygge opp en risikokultur. Nordal og Kjørstad presenterte også modenhetsmodellen – til stor interesse for deltakerne. Dette er fremskritt gjennom deling av kunnskap satt i praksis.

Takk til våre engasjerte medlemmer som virkelig går i bresjen for god risikostyring!

NYHETER FRA IIA, ECIIA OG ANDRE PARTNERE SISTE HALVÅRET:

The redraw of the Lines of Defense
In his blog post from 05.12 2018, IIA President and CEO Richard Chambers writes that the time has come to take a new look at the Three Lines of Defense and give this trusted instrument a 21st century makeover. With the support of governance experts in the

public and private sectors, academia, regulators, and Big Four accounting firms, The IIA has begun a project to refresh the model.

«This yearlong project is headed by a core working group of governance experts who will tap into the vast experiences of an additional 30-member advisory group. The project includes a comprehensive review of governance approaches from around the world, and it will seek out and incorporate public comments through a formal exposure process. Ultimately, the project will result in a new IIA position paper on the subject, expected in the second half of 2019.

From the outset, The IIA´s objective has been to explore how best to update the Three Lines of Defense model to reflect the changes in modern risk management and governance, while at the same time preserving its straight-forward and clear approach. In keeping with its original intent, the refresh will focus on roles not organizational structures. In response to critiques, the aim is make the model more flexible, suitable to all sectors, and responsive to both the challenges and opportunities that risks offer.»

The IIA will expose proposed enhancements to the Three Lines of Defense position paper for public comment. Planned for release in multiple languages, the exposure will provide insight needed to enhance The IIA's position on the Three Lines of Defense to meet modern quality standards and to be more broadly accepted and adopted by all stakeholders around the world.

Practice Guide: Auditing Capital Adequacy and Stress Testing for Banks

The Basel Committee on Banking Supervision (BCBS) strengthened capital adequacy guidelines following several global financial crises. If observed, banking institutions should be able to absorb the volatility of potential credit, market, and operational risks in the wake of another serious market shift.

This new practice guide, developed for financial services auditors but useful to any auditor working with statistical models and capital, focuses on how to provide assurance that an institution is well capitalized to meet the guidelines and prepared for cyclical business changes. This guide will help readers understand, measure, and assess the appropriateness and completeness of an institution's capital planning process.

Global Perspectives and Insights series: 5G and the 4th Industrial Revolution – Part I

Part of a two-part series explores the pros and cons of the next generation of wireless network connectivity that is being hailed as the quantum leap in the world of technology. The report looks at 5G's potential impact and breaks down what organizations need to know in order to prepare. It also highlights key issues from implementation challenges, legal issues, and regulatory tests to disruptive technologies, data management, and cybersecurity concerns, the report seeks to prepare organizations for the potential impacts of 5G so they can proactively address the issues. Internal auditors and risk managers must recognize that while 5G offers unprecedented connectivity, it will also open the door to new challenges and disruptions. It is vital for internal auditors to learn all they can about 5G and embrace existing data analytics technology before 5G arrives in order to provide uninterrupted advisory and assurance services to organizations when it arrives.

Position Paper: Assurance over fraud controls fundamental to success

Every year billions of dollars are lost to fraud and corruption resulting in inefficiencies, aborted projects, financial challenges, organizational failure, and, in extreme cases, humanitarian disaster. Often fraud occurs because of poorly designed controls and weak governance undermining the organization's processes. Organizations should have robust internal control procedures to limit the risk of fraud, and internal audit's role is to assess these Controls. These areas are addressed in the position paper you can download from www.globaliia.org.

New Implementation Guidance for Code of Ethics

Internal auditors are often considered the conscience of their organizations. To be viewed as trusted advisors, they must strive to be above reproach and to avoid ethical pitfalls. The IIA has released new guidance for implementing its Code of Ethics. Each of the four Code of Ethics principles – Integrity, Objectivity, Confidentiality, and Competency – are accompanied by specific rules of conduct. These four Implementation Guides explain what internal auditors need to know to implement each principle and rule of conduct, and how to show conformance as part of a quality assurance and improvement program.

Each guide has a section devoted to:

- Getting Started
- Considerations for Implementation
- Considerations for Demonstrating Conformance

Global Perspectives and Insight: Agility and Innovation

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

Slagkraftig, smidig og treffsikker.
Er dette karakteristikker som beskriver din funksjon?
Eller er tung i sessen mer treffende?

Fortvil ikke. Hvis en stor og tung panda kan få svart belte i kung fu og redde verden, så er det håp for noen og enhver. Hvilken panda snakker vi om her? Kung Fu Panda selvfølgelig – eller Po Ping. Po er en entusiastisk, klumsete panda som drømmer om å bli en smidig og slagkraftig kung fu master.

Med usannsynlig god hjelp av skjebnen (og Dreamworks' kreative team) ender han opp sammen med en kvintett av kung fu studenter som blir trent opp av Master Shifu, en klok, streng rød panda som tester Po til det ekstreme. Har han det som skal til? Po er ingen opplagt kung fu master, men han har trua, selv om det røyner på til tider. Og det er når det virkelig røyner på for Po at Master Shifu øser av sin visdom:

«Hvis du bare gjør det du kan vil du aldri bli noe mer enn det du er akkurat nå.»

Kjernen i dette budskapet er enkel: kom deg ut av komfort sonen! Det skjer ikke noe der inne annet enn det som alltid har skjedd. Skal vi vokse og lære må vi utforske og pløye ny mark. Så hva med deg? Har du og dere testet grensene i det siste? Prøvd noe nytt? Har vi – det være seg internrevisjoner, risikostyrings- eller compliancefunksjoner - samme uutnyttet potensiale som Po?

Å flytte på komfortsonen var et gjennomgangstema på IIA konferansen i slutten av mai. Vi må by litt på oss selv – og våre medlemmer. La oss begynne med å utfordre oss selv litt. IIA Norges medlemmer var overraskende positive da de ble utfordret til å bidra med sosiale innslag. Hvor forferdelig er det ikke å grue seg til å ta steget ut av komfort-sonen, men for en helt vanvittig deilig følelse det er etterpå; følelsen av mestring av bekreftelse på at «jeg både vil – og kan». Det gir mersmak.

IIA Norge lar oss inspirere! Det er blitt pløyd ny mark og tatt noen steg ut av komfort-sonen det siste året. Hvordan? I fjor sommer dro Ellen Brataas og Marit Trodal (IIAs sekre-tariat) i filmstudio og laget e-læringsprogrammet 'Introduksjon til Internrevisjon.' Å stå foran kamera og formidle et manus med innlevelse og overbevisning krevde sitt av begge to. Men hva gjør man ikke for å spre det glade budskap om IIAs etiske rammeverk? Det ble mange tagninger for hver sekvens inntil de ble noenlunde varme i trøya. MEN – resultatet ble veldig bra! IIA Norge er stolte av programmet og klare for både mer e-læring og andre verktøy som kan bidra til å gjøre oss både smidige, treffsikre og slagkraftige.

Hvis Po Ping kan – kan vi. Kiya!!!! ...eller Just do it!

Returadresse
IIA Norge
Postboks 1417 Vika
0115 Oslo