SIRK

Styring – Internrevisjon – Risiko – Kontroll

NORGES INTERNE REVISORERS FORENING

Nr 1 2016

Mot lys i skyggene?

MARTIN STEVENS

Panamabyens påvirkning på forståelse av internrevisjonsrollen i Norge

Forsiden av SIRK henviser denne gangen til saken om *Panama Papers*. En dokumentlekkasje fra Panama har ført til den største oppmerksomhet i norsk presse på internrevisjon i manns (og kvinnes) minne.

Kort fortalt ble det lekket et hav av dokumenter (mer enn 11,5 millioner) fra et advokatfirma Mossack Fonseca i byen Panama. Dokumentene dekker et tidsrom på 38 år, fra 1977 til 2015. Et arbeidsteam av journalister, inkludert journalister fra Aftenposten, har gransket disse dokumentene over 6 måneder. Dokumentene beskriver hvordan det har blitt opprettet anonyme selskaper i skatteparadiser. Juridiske konstruksjoner i disse selskapene har bidratt til å skjule formuer, noe som også kan ha gjort det mulig å skjule eiendeler og inntekter fra beskatning.

Saken har avslørt mulige skjulte formuer hos 21 statsledere, og blant de mest kjente tilfeller er den britiske statsministeren (som noe sent kom med forklaringer om hans eierandeler i farens investeringsselskap og når disse investeringene ble avviklet), statsministeren i Island som måtte ta sin hatt å gå og kretsen rundt Putin (som så langt har ført til kontrabeskyldninger om vestlig svartmaling). Her på berget var fokuset derimot festet på landets største bank, DNB, som ble beskyldt for bevisst å ha lagt til rette for at kunder gjennom sin datterbank i Luxembourg kunne opprette anonymt eide selskaper på Seychellene med god hjelp fra Mossack Fonseca i Panama. Det hele ble ekstra pinlig som følge av at det etter et NRK innslag fra 2007 ble gitt uttrykk for fra DNB at banken ikke skulle bidra i etablering av den type eierskapskonstruksjon. Saken blir heller ikke bedre av at staten har en eierandel på 34 % i DNB. Også statsministeren uttrykte seg om saken: «Men det at DNB skal ha tilrettelagt for investeringer i skatteparadiser, synes jeg er skuffende. Vi forventer at man tar hensyn til omdømmet når det gjelder etikk og moral, ikke bare hva som er bunnlinje, lov og regler. Vi stiller høyere etiske krav til disse store norske selskapene.» (Aftenposten, 08.April 2016.)

Næringsminister Monica Mæland fra Nærings- og fiskeridepartementet ba om en redegjørelse for DNBs rolle i forbindelse med etablering av selskaper på Seychellene. DNB kom med sitt svar i april, og svaret er offentliggjort på DNBs internettsider. I rapporten som er utarbeidet av den juridiske avdelingen i DNB konstateres det som faktum at «DNB Banks representanter i Luxembourgbankens styre mottok i den aktuelle perioden presentasjoner knyttet til Luxembourgbankens strategi- og forretningsplaner, hvor det blant annet fremgikk at Luxembourgbanken kunne legge til rette for at kunder etablerte selskaper hjemmehørende i lavskatteland.» Denne innrømmelsen ble deretter etterfulgt med en annen uttalelse: «I materialet som er gjennomgått, har vi ikke funnet spor av at informasjon om etablering av selskaper i lavskatteland har vært løftet opp til konsernsjef, konsernledermøter eller styremøter i DNB Bank eller DNB ASA.» Gjennom DNBs rapport og rapportens fremleggelse i pressen kan man få inntrykk av at DNB legger mye av «ansvaret» for at toppledelsen og styret ikke var informert om selskaper i skatteparadiser på internrevisjonen. I et eget avsnitt i rapporten, under tittelen «Revisjon», fremheves det at datterselskapets internrevisjon ikke var forsvarlig organisert fordi internrevisjonen rapporterte til den lokale ledelsen i Luxembourg og ikke til styret samt hadde blandet sine rolle ved å yte rådgivningsbistand. DNBs konsernrevisjon i Norge fikk også passet påskrevet av den juridiske avdelingen: «Den juridiske avdelingens undersøkelser viser at Konsernrevisjonen i Norge ved flere anledninger fikk dokumenter med informasjon om at etablering av selskaper i lavskatteland var en del av DNB Luxembourgs tjenestetilbud. Disse opplysningene foranlediget ikke nærmere undersøkelser fra Konsernrevisjonen.»

Pressens reaksjon på denne rapporten var at det luktet av å ha funnet en beleilig syndebukk. Næringsministeren Mæland har kommet med ytterligere spørsmål i saken som hun ønsker å få belyst og i skrivende stund skal DNB ha iverksatt en ekstern gjennomgang ved hjelp av Advokatfirmaet Hjort. Det er også kommet frem gjennom media at både den tidligere internrevisoren i Luxembourg og den tidligere konsernrevisjonssjefen i DNB, Harald Jægtnes, ønsker å uttale seg om saken, men de er foreløpig ikke frigjort av sin taushetsplikt.

Det finnes et uttrykk som sier «There is no such thing as bad publicity». Tiden vil vise om dette uttrykket er også gyldig for DNB. Uansett utfallet har profesjonen vår fått mye publisitet i media hvor det har vært vist interesse for rollen til internrevisjon. NIRF har benyttet anledningen til å komme med uttalelser som har blitt sitert videre i media. Til og med Den norske Revisorforening har uttalt seg om saken. Ett blogginnlegg fra vår generalsekretær gjengis i dette nummeret av SIRK. Hensikten er å informere om rollen til internrevisjon og ledelsen, samt å gi innspill til etiske vurderinger i sin alminnelighet.

Siste ord er definitivt ikke sagt i saken om «Panama Papers» og for oss internrevisorer blir det interessant å følge med på ytterligere diskusjoner om ledelsens kontroll- og oppfølgingsansvar. Det kan også tenkes at ikke alle har forstått modellen med tre forsvarslinjer og derfor må vi internrevisorer benytte muligheten og gjøre den mer kjent. Dersom saken rundt «Panama Papers» utvikler seg videre etter nye avsløringer, vil vi i medieutvalget følge opp saken i fremtidige SIRK og på NIRFs blogg

PRESIDENTEN HAR ORDET

INGUNN VALVATNE
PRESIDENT
NIRF

Medieoppslag i kjølvannet av Panamaavsløringene har gitt vår profesjon en lenge etterlengtet oppmerksomhet, dog ikke på den måten vi ønsket oss. Slik er det jo ofte med oppmerksomhet. NIRF skal avstå for å ha meninger om den aktuelle saken, det er opp til andre å vurdere de ulike aktørers håndtering. Vår utfordring blir heller å bruke anledningen som er skapt til være tindrende klare på rollen vår og på hvilke bidrag vi kan gi til god styring og kontroll i norske virksomheter.

Mediedekningen kan tyde på at vi ikke har klart dette godt nok. Det er også krevende ettersom det ikke finnes én måte å innrette en internrevisjon på. Innretning og oppgaver vil stor grad avhenge av hvilke andre forsvarsmekanismer virksomheten har på plass. Nå som de første bølgene i saken har lagt seg er det naturlig å studere hendelsene i et større perspektiv. Hvor høy er egentlig bevisstheten rundt internrevisjonens roller i norske virksomheter. Og hvor godt forankret er vi gjennom lovverk og retningslinjer for virksomhetsstyring?

Finansvirksomheter av en viss størrelse har lenge hatt et krav om etablering av internrevisjon gjennom forskrift om risikostyring og internkontroll. Forskriftens veiledning utdyper rollen ganske klart: «*Internrevisjonen er et viktig ledd i styrets overvåking av risikostyringen og internkontrollen. Funksjonen er særlig aktuell i store og kompliserte organisasjoner, men også i mindre foretak med høy operasjonell risiko. Internrevisjon innebærer en styrking av internkontrollen og kan være aktuelt å vurdere også i foretak som ikke er pålagt å ha internrevisjon.*». Tilsvarende har Finansdepartementet fastsatt krav om at statlige virksomheter med inntekter eller utgifter over 300 millioner skal vurdere hvorvidt de bør bruke internrevisjon.

Til tross for økt fokus ser vi at de norske kravene om internrevisjon har en svakere forankring enn i land det er naturlig å sammenligne seg med. OECD, som legger viktige føringer for virksomhetsstyring i global kontekst, fremhever i en rapport fra 2014 det uvanlige i at kun 90 % av norske noterte selskaper har etablert en internrevisjon. NIRF vil i 2016 vektlegge dialog med forskjellige interessenter for å skape en bred og felles forståelse for rollen vår.

Det er likevel ikke nok at vi selv synes vi gir viktige bidrag. Det er gjennom gode leveranser og systematisk arbeid at våre bidrag blir synlig for andre. Det er for eksempel på sin plass å minne om at internrevisjonen i flere virksomheter har hatt en sentral rolle i å avdekke og håndtere korrupsjonssaker.

Kompetanseutvikling, erfaringsutveksling og nettverk er nøkkelord. Også her skal NIRF spille en viktig rolle gjennom kursvirksomhet, og tilbud om arenaer for videreutvikling av profesjonen vår. Årskonferansen som skal foregå i Oslo i juni vil ta for seg våre interessenters forventninger til oss. Vi håper flest mulig vil la seg inspirere av det spennende programmet og ta del i diskusjonene.

MEDIEKOMITEEN

Martin Stevens
Internrevisor,
Gjensidige Forsikring

Reidar Døli
Internrevisor,
Oslo Børs VPS

Esa Leporanta
Systems Audit Manager,
Nets Norway Branch

Lene Bollestad
Internrevisjonen
Norges Bank

Magnus Digernes
Senior Manager
KPMG

Neste utgivelse er desember 2016

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 NIRFs syn.

Grafisk produksjon:
Merkur Grafisk AS

Forsidebilde:
Foto: Shutterstock.com

INNHOLD

7

15

30

12

16

ISO/IEC 27001:2013

- En snarvei til bedre forståelse innen informasjonssikkerhet?

Av
ESA LEPORANTA
Systems Audit Manager,
Nets Branch Norway

De fleste av oss som arbeider innen internrevisjon eller andre beslektede fagområder er godt kjent med begrepene konfidensialitet[1], integritet[2] og tilgjengelighet[3], som beskriver de mest grunnleggende elementene innen informasjonssikkerhet (IS). Samtidig vil ulike sosiale og teknologiske krefter som endrer samfunnet vårt i dag medføre at det kan være behov for å tilegne seg noe bredere forståelse i emnet.

Noen få søk på Internett avslører at flere velkjente og profilerte virksomheter[4] har hatt betydelige utfordringer med å beskytte seg effektivt mot kybertrusler. Ifølge EY[5] er mangelen på kompetente ressurser en av de viktigste årsakene til at virksomhetene ikke klarer å respondere godt nok på informasjonssikkerhetstrusler.

ISO 27001 er en internasjonal standard for informasjonssikkerhetsledelse som kan anvendes for å øke vår forståelse om dette fagområdet. ISO 27001 anvender et begrep som heter *styringssystem for informasjonssikkerhet*[6]*(SSIS)* for å beskrive de prosesser og fortegnelser som trengs for hensiktsmessig informasjonssikkerhetsledelse i enhver organisasjon.

SSIS er en systematisk prosess for å etablere, implementere, drifte, overvåke, evaluere, vedlikeholde og forbedre organisasjonens informasjonssikkerhet for å kunne oppnå virksomhetens mål. Prosessen skal basere seg på virksomhetens egen risikovurdering. Det sikrer en mest mulig hensiktsmessig håndtering av organisasjonens informasjonssikkerhetsrisikoer.

Selve ISO 27001[7] - standarden er delt i ti kapitler. For virksomheter som ønsker å bli sertifisert mot ISO 27001, vil de krav som presenteres i kapitlene 4-10 være obligatoriske. Disse kapitlene viser en syklisk modell som begynner med etableringen og implementeringen av IS prosesser som deretter skal vedlikeholdes og forbedres ved behov.

Direktoratet for forvaltning og IKT (DIFI) har skrevet en fyldig rapport[8] som gjengir og vurderer erfaringer fra statlige virksomheter som har etablert et slikt styringssystem og brukt denne standarden. ISO 27001 ble oppdatert i 2013. Forrige versjon var fra 2005. I og med at forskjellene mellom de to ulike standardversjonene har blitt grundig beskrevet i en egen DIFI veileder[9], henvises det til denne rapporten for flere opplysninger.

Vedlegget til ISO 27001 standarden, Annex A, viser et rammeverk på informasjonssikkerhet på 12 sider og inkluderer 114 ulike kontroller på totalt 14 områder.

Standarden viser til ledende praksis og kan anvendes for å få en grunnleggende forståelse for hvilke minimumskrav det eksisterer innen informasjonssikkerhet. Standarden kan også brukes som et oppslagsverk i sikkerhetsarbeid og ved revisjoner.

Ved å ta dette rammeverket i bruk kan virksomhetens ledelse raskt øke organisasjonens kompetanse innen informasjonssikkerhet. Risikoen for at deres organisasjon blir nevnt blant de som i fremtiden har blitt utsatt for kyberangrep blir redusert.

[1] Informasjon ikke er tilgjengelig uten autorisasjon
[2] Informasjon ikke endres eller ødelegges uautorisert
[3] Informasjon er tilstede og anvendelig for autoriserte medarbeidere slik at pålagte oppgaver kan utføres
[4] Apple, CitiGroup, Ebay, JP Morgan Chase, Orange, Sony Pictures, Staples, Target, Wal-Mart
[5] EY Global Information Security Survey 2015 - http://www.ey.com/GL/en/Services/Advisory/ey-global-information-security-survey-2015-1
[6] ISMS = Information Security Management System
[7] ISO/IEC 27001:2013 - Information Technology - Security Techniques - ISMS - Requirements
[8] DIFI - Rapport 2012:15- Styringssystem for informasjonssikkerhet - ISSN 890-6583
[9] DIFI - Veileder for virksomheter som skal gå fra ISO/IEC 27001:2005 til ISO/IEC 27001:2013

Auditing #SocialMedia

Social media is used by billions of people across the world every day to communicate and stay in touch with friends and family. Businesses want to harness the power of social media to communicate with their customers and advertise their products, and corporate use of social media has grown organically over the last 10 years. Because of this, very few companies have the same level of rigour and governance around social media as they do for other business activities.

BY
PHIL MENNIE
PWC'S GLOBAL SOCIAL MEDIA RISK AND GOVERNANCE LEADER

Phil authored «Social Media Risk and Governance: Managing Enterprise Risk» (Kogan Page, 2015) and is a world-renowned expert, thought-leader and speaker on social media in the enterprise. Phil's expertise in social media stems for experience using web technology to better manage financial and operational data.

@philmennie

Many people and businesses have fallen foul of social media and have had their reputations tarnished as a result. The types of blunders include accidental posts from corporate accounts, cyber-attacks, data breaches, fines from regulators, harassment and even sad cases of suicide due to cyber bullying.

In 2016, social media risk is finally getting the attention it deserves. Many companies now list social media on their risk registers and are designing governance programmes around its use to safeguard from reputational damage. Internal auditors now face the challenge to audit how their business uses social media and assess whether the governance around it is appropriate and fit-for-purpose.

What is social media?

Social media means different things to different people. To some, social media only entails popular networks such as Facebook, Twitter and LinkedIn. I adopt a broader definition, and prefer to view social media as any digital platform that enables people to connect with each other. My definition, therefore, also includes photo-sharing apps such as Flickr and Instagram, messaging apps such as Whatsapp, and review and rating sites such as TripAdvisor and Yelp

These social media platforms are open to all, and many now rely on these technologies on a daily basis. Smartphones have crept into the bedroom and are often the first thing people look at in the morning and the last at night. The significant impact that social media has had on our lives is impossible to dispute. However, in addition to the networks we know so well, there is another suite of social media applications we don't hear about as often in the news: Enterprise Social Networks (ESNs). Enterprise social networks are internal platforms which businesses implement to help their own people connect and collaborate for work purposes. When used well they can increase employee productivity and improve communication.

What's at risk?

When evaluating the risks of social media it's natural for people to reflect on news articles or anecdotes. Many of these relate to reputational damage to individuals or companies, but as internal auditors we need to look deeper.

There are five categories of social media risk:

1. **Reputational risk:** This risk stems from people posting content online, either deliberately or by accident, which harms the reputation of an organization. A common mistake is when an employee who tweets on behalf of the organization mixes up his or her personal account with the organization's official account. It can be very embarrassing when a rude or inappropriate tweet is sent out from a company's official channel, but unfortunately there are many examples of this.

2. **Information security risk:** Social media has changed the way that we communicate, which has led to changes in what we share about ourselves online. Sometimes, careless employees can publish confidential information or intellectual property online by accident. Another risk relates to how a company manages access to its corporate social media

Internal auditors have a choice about the focus of their social media audits. They may focus their efforts on how their business uses social media in an official or corporate context, or the audit may focus more on how employees use social media, including the policies, training and guidance available to them.

accounts. For example, are login credentials being shared by users and are passwords secure and regularly updated?

3. **Financial risk:** Probably one of the most serious financial risks for larger companies is the negative effect social media can have on its share price. Yet, amazingly, many business executives just don't understand this. They understand that reputational issues or a bad article in the press or print media can impact their share price so I'm surprised that a disconnect to social media still endures. There are lots of examples of companies who have suffered declines in their share price following a blunder. Without appropriate processes in place to identify and respond to social media mishaps in a timely manner, a slip-up can quickly become viral and spread across the globe, and as a result investor confidence is lost.

4. **Operational risk:** Often, companies have a policy of blocking social media sites at work because they believe that employees will be wasting time on them when they should be working. But I would argue that employees can be motivated by being allowed to use social media for personal use, and there are business benefits too. Effective use of social media can help a company gain competitive advantage, recruit top people and even sell products and services. The main risk here is that if an organization doesn't embrace social media, it could lose its competitive advantage.

5. **Regulatory risk:** Regulation differs around the world, and the laws and rules which are applicable to your organization will depend on the country, or countries, in which you operate, as well as your industry. Many regulators include guidance and rules about how a business can and cannot use social media. For example, many countries publish advertising standards or rules around the archiving and retention of communications.

Internal auditors have a choice about the focus of their social media audits. They may focus their efforts on how their business uses social media in an official or corporate context, or the audit may focus more on how employees use social media, including the policies, training and guidance available to them. Alternatively, if your company has invested in an Enterprise Social Network, the audit may focus on how it is used and the governance around it. For example, an ESN may contain a wealth of sensitive personal data and intellectual property. Organizations need assurances that their networks do not have security holes through which data breaches could occur. Furthermore, the networks themselves are not cheap, so internal auditors may be asked to assess the value of the network vs. its cost.

The value of a social media audit

Unless you have experience auditing IT or emerging risks such as cyber security, the thought of conducting a social media audit can be daunting at first. But when you break it down, the purpose of a social media audit is to assess whether the company has the appropriate governance and control in place around its social media activities. This includes, for example:

Social media means different things to different people. To some, social media only entails popular networks such as Facebook, Twitter and LinkedIn.

- **Social media strategy:** It's important that businesses have a social media strategy. There are many reasons for adopting social media as a business, but without a clear strategy and direction from leadership, it's unlikely that a social media programme will achieve its goals. In fact, without a strategy it may be difficult to work out what the goals and objectives are in the first place! This makes it difficult for an internal auditor to assess whether or not the programme is making a return on investment or whether or not it is providing any benefit.

- **Ownership, roles and responsibilities:** Social media needs an overall owner who can provide the direction, and budget, for how the business will exploit social media. There will probably be a number of different teams and stakeholders involved in social media, so it's important that their roles and responsibilities are defined, and that the stakeholders have a way of collaborating and communicating about relevant social media issues. For example, updates to the social media policy may be discussed at regular working groups or committee meetings.

- **Policies and documentation:** A well-written social media policy is a must. The social media policy shouldn't be a long, boring document. Instead, it should be short and include practical advice and examples that encourage employees to use social media in an effective and controlled way which does not bring risk to the company.

- **Internal control:** Social media was originally designed as a communication medium, not as a business tool. Because of this, few social networks have adequate controls around, for example, user access to corporate accounts. Internal auditors will need to assess what tools are being used to manage access or to archive, monitor and moderate content before it is published.

Without a strategy it may be difficult to work out what the goals and objectives are in the first place!

Three top tips for internal auditors

1. **Be up-beat and positive**
   It's common for internal auditors to face friction when auditing social media as many people working in marketing or communications may be unfamiliar with the purpose and goals of an internal audit. They may never have experienced an audit before. Therefore, it's important to be up-beat and positive about how the business is capitalising on the opportunities that social media offers.

2. **Make your objectives very clear from the start**
   Internal auditors play an important role in helping their organizations achieve success in social media. They advise on how a business can improve its processes and documentation around the use of social media. It's important to explain to those running the accounts that adding more rigour will allow them to do more with the company's social media platforms, not less, and that potential issues will be able to be resolved more quickly and effectively.

3. **Arm yourself with examples**
   When you have completed your fieldwork and you move onto writing and presenting your findings, it's important to arm yourself with a number of real-world examples of previous social media blunders. For example, if you find that there is a lack of control around access to corporate social media channels, you need to use real world examples of how this has led to accounts being compromised, such as when The Associated Press Twitter account was hacked in 2013. The use of examples will help illustrate why your findings matter and emphasise the value of the audit.

The future of social media auditing

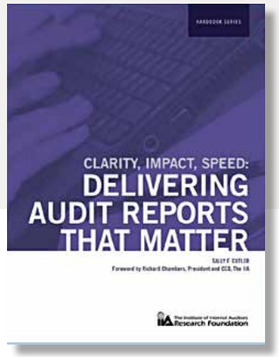
Perhaps you have already performed an audit of social media, or perhaps you've got it on the plan for this year and you're looking to understand what to include in your scope and work programme. Either way, it's important to remember that social media is a fast-changing environment, with new platforms and technologies continually appearing and existing platforms adding new functionality. These developments mean auditors need to ensure that they regularly revisit social media and incorporate new risks or platforms into their test plans. For example, live streaming is becoming popular with the rise of Periscope and the launch of live streaming within Facebook. These technologies introduce a new risk dynamic and one that's much faster and more difficult to control. I recently published a blog on LinkedIn about my experience using Periscope and it's clear to me that as auditors we will need to work hard to keep up with the new and emerging risks and ensure that our audits address those new risks as they develop.

It's important to remember that social media is a fast-changing environment, with new platforms and technologies continually appearing and existing platforms adding new functionality.

DELIVERING AUDIT REPORTS THAT MATTER

Av
ESA LEPORANTA
Systems Audit Manager,
Nets Norway Branch

Sally F. Cutler (2011):
Institute of Internal Auditors - IIA Research Foundation



Boken presenterer hvordan vi effektivt kan skrive relevante og tydelige revisjonsrapporter.

Cutler viser hvordan man effektivt kan utforme rapporter ved bruk av revisjonslogikk og ved å analysere både revisjonsmål og behov til de som skal lese rapporter. Boken er pedagogisk bygd opp, med mange eksempler og sjekklister for å vise sammenhengen mellom bokens ulike kapitler. Videre blir det synliggjort for leserne hvordan rapporteringen kan anvendes for å nå flere av revisjonens mål.

I boken anbefales det å innlede rapporteringsarbeidet med å avklare målene med rapporten, det vil si å identifisere om rapporten skal 1) overbevise 2) informere og/eller 3) dokumentere. Deretter bør det vurderes hvilken målgruppe rapporten skal skrives til. Målgruppene har normalt ulike informasjonsbehov. Kjennskap til den reviderte enheten og nivået i den tekniske forståelsen vil også variere mellom ulike målgrupper og bør tas i betraktning i utformingen av rapporten.

Heretter ble det henvist til fem komponenter (jfr. IIA's PA 2410-1: *Criteria, Conditions, Cause, Effects and Recommendations*) som kan anvendes for å bygge en logisk og overbevisende argumentasjon i en revisjonsrapport: 1) Kriterier, 2) Tilstand, 3) Årsak til avvik, 4) Konsekvens/ Risikonivå, 5) Anbefalinger.

I neste fase blir det anbefalt å ta stilling til rapportens struktur. Målet med denne fasen er å avklare hvilke av de fem komponenter som skal vektlegges i rapporten. Videre velges de delområder som gir høyest forventet rapporteringseffekt. Innen hvert delområde må oppbygningen avklares og det må bestemmes hvilke overskrifter som sikrer en god flyt gjennom revisjonsrapporten.

Ved fastsetting av rapportens delområder anses det som best praksis å følge denne rekkefølgen: 1) Overskrift, 2) Sammendrag med hensikt, omfang og konklusjoner, 3) Observasjoner med anbefalinger. Når rekkefølgen av delområder er avklart, bør det fastsettes hvilket format rapporten skal ha, noe som er eksemplifisert i boken med fire ulike maler.

Når det gjelder selve rapporteringsprosessen, var det anbefalt å benytte en innarbeidet rapporteringsstruktur som er godt kjent både av de som skriver og kvalitetssikrer revisjonsrapporter. Videre var det ansett som god praksis å lage preliminære diskusjonsnotater som kan anvendes for å presentere eventuelle revisjonsfunn på en tidlig fase i revisjonen. Disse notatene kan også anvendes for kvalitetssikring av internrevisorens arbeid i avdelingen.

Når det gjelder kvaliteten i skrevet tekst, vektlegges det på to elementer: 1) lengden av setninger. For eksempel ble det frarådet å skrive setninger med flere enn 20 ord. 2) valg av ord som er kjent av og tilpasset til leseren. For eksempel hvis målgruppen til rapporten din ikke er eksperter på det området rapporten din handler om, bør bruk av ekspertord unngås.

Boken har en gjennomtenkt struktur med tydelige eksempler. Det er ingen tvil om at flere virksomheter kunne ha effektivisert sin revisjonsrapportering ved systematisk bruk og dokumentasjon av sine logiske revisjonskomponenter. Ved å tilpasse og implementere de maler og den logikken som finnes i boken til Cutler, er det mulig få en ny «hverdag» - med en mer effektiv revisjonsrapportering.

Varsling – en viktig del av bedriftens compliance program

Et velfungerende varslingssystem gir bedriften mulighet til å korrigere avvik og rette opp i uønskede forhold. Det bør være et viktig element i bedriftens compliance system - som har som hovedformål å forebygge brudd på lover og regler. Men hva skal til for å lykkes, og hvilke utfordringer kan man møte? Med utgangspunkt i praktiske erfaringer fra større organisasjoner - inklusive internasjonale bedrifter, belyses dette i denne artikkelen.

Av
LENE SVENNE
Corporate Compliance Officer, KONGSBERG Gruppen ASA

Formålet med et varslingssystem

Arbeidsmiljøloven setter rammene for hva som må ivaretas i varslingssystemet i paragrafene 2-4, 2-5 og 3-6. De to første paragrafene omhandler varsling om kritikkverdige forhold i bedriften og vern av den som varsler, mens paragraf 3-6 omhandler arbeidsgivers plikt til å legge til rette for varsling. Varsling skal forebygge både konflikter på arbeidsplassen og økonomisk og annen kriminalitet. Med utgangspunkt i lovgivningen, kan man si at varslingssystemet skal legge til rette for at ansatte kan varsle om kritikkverdige forhold uten å oppleve å bli «straffet» for det. Videre at arbeidsgiver kan ta tak i avvik og uønskede forhold for å sette inn nødvendige tiltak; og ikke minst å komme tidsnok i inngrep for å unngå at forholdet det er varslet om utvikler seg til en konflikt som det kan bli vanskelig å løse.

Oppbygging av et varslingssystem

Et compliancesystem bør bygges opp på en systematisk måte, og det samme gjelder varslingssystemet som et av elementene i compliancesystemet. En måte å illustrere dette på vises nedenfor med kommentarer for de enkelte delene. Det finnes ikke en enkeltstående riktig måte å gjøre dette på; hver virksomhet må vurdere sin risikoprofil og ut i fra det bygge opp et system som passer for seg.

«Tone at the top»

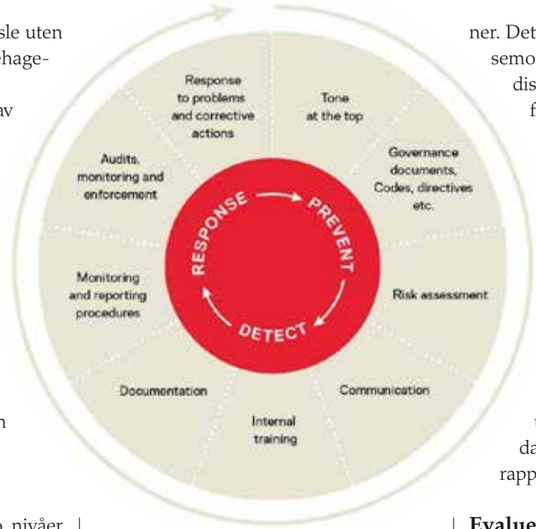
Det er helt avgjørende at ledelsen på alle nivåer er helt klare og tydelige på at varsling er viktig for bedriften. Både for å kunne ta tak i situasjoner og gjøre korrektive tiltak i tide før eventuelt ytterligere skade skjer, og for at ingen form for gjengjeldelse overfor en varsler skal forekomme. I alle virksomheter vil det fra tid til annen oppstå konflikter, faglige eller personalmessige. Disse skal normalt løses i «linjen»; det vil si i den daglige drift så nær problemet som mulig. Varslingssaker vil normalt være saker som krever en mer omfattende behandling. Uansett type sak må ledelsen gå foran med et godt eksempel og vise at den tar ansvar og ved det skape tillit hos de ansatte. Det er viktig å vise med handling at varslingssystemet fungerer i praksis og ikke bare er et papirsystem.

> «Å varsle er å si i fra om kritikkverdige forhold som foregår i virksomheten».

Interne retningslinjer

Rutiner for hva man skal og/eller bør varsle om, hvordan man skal varsle, hvordan og av hvem et varsel skal behandles, rapporteringslinjer og beslutningsnivåer bør beskrives så klart og tydelig som mulig i interne retningslinjer. Det kan ofte være vanskelig å avgjøre om en bekymring faller innenfor begrepet «kritikkverdige forhold» og for å gi veiledning til de ansatte vil eksempler være nyttige. Det er viktig at de ansatte tas med på råd ved utforming av retningslinjene for å skape eierskap og engasjement. Varsling fra en ansatt er en alvorlig og ansvarlig handling, og det er viktig at de ansatte er trygge på at de kan varsle uten å bli utsatt for represalier eller ubehageligheter.

I Norge er varsling regulert av arbeidsmiljølovens (AML) bestemmelser. Det er viktig å sette seg inn i lovbestemmelser for andre land hvor man har virksomhet. De interne rutinene bør være klare på om man legger de norske reglene til grunn for all virksomhet «world-wide», og eventuelle særbestemmelser og begrensninger man må ta hensyn til, f.eks begrensning i retten til anonym varsling i noen land.



Risikovurdering

Risikovurdering bør foregå på to nivåer når vi omhandler varslingssystemet. Først i forbindelse med risikovurdering av selve compliancesystemet; har bedriften et godt nok varslingssystem for å få inn og behandle relevante varsler, og er det en god kultur i bedriften som understøtter varsling. Videre må konkrete varsler underlegges en risikovurdering for å avgjøre hvordan de skal behandles. Varsler om svært alvorlige forhold kan kreve umiddelbare tiltak for å stoppe pågående ulovlig aktivitet, mens andre forhold kan være av en ikke tidskritisk karakter hvor relevante tiltak f.eks. kan være endring av rutiner.

Kommunikasjon

Informasjon om bedriftens varslingsrutiner kan, og bør, gis på mange måter. Naturlige media kan være bedriftens intranett og nettsider, informasjon i forbindelse med nyansettelser, bedriftsaviser mv. Informasjonen må gis på de ulike språk som bedriftens ansatte bruker. I selskapets årsrapport eller bærekraftrapport bør det også gis informasjon om varslingssaker.

Intern opplæring

Informasjon om varslingssystemet bør inngå i obligatoriske introduksjonskurs og etikkopplæring for alle ansatte, samt kurs for ledere på ulike nivåer og for tillitsvalgte. Temaet må gjøres lett forståelig og tilgjengelig, og gjentas ofte!

Dokumentasjon

Selve varselet kan komme i nær sagt alle former, og det er ikke krav om skriftlighet i AML. De interne rutinene bør beskrive hvordan saksbehandling skal dokumenteres, hvem som skal ha tilgang til saksdokumenter og hvordan det skal arkiveres. Det bør føres nøyaktige logger for all kontakt med varsler, og all dokumentasjon må oppbevares på en sikker måte og oppfylle krav til personvern.

Undersøkelser

Ved mottak av et varsel må det avgjøres hvem som skal ha ansvar for undersøkelser og hvordan man skal undersøke påstanden. Varselet kan gjelde alvorlige forhold, samtidig som det gir lite konkret informasjon, noe som kan gjøre det vanskelig å vite hvordan man skal angripe en sak. Det er viktig å tenke gjennom dette i forkant, og utarbeide prinsipielle rutiner for hvordan man skal behandle et varsel inklusive beslutningsnivåer og rapporteringsrutiner. Det kan også tenkes interne interessemotsetninger i konkrete saker, og disse kan forebygges ved at det finnes prinsipielle rutiner. I mange saker kan det være behov for bistand fra tredjeparter som har kompetanse innenfor granskning, og som også har mulighet til å gjøre undersøkelser i andre land. Oppdraget bør beskrives så spesifikt som mulig, både med hensyn til undersøkelsens omfang og kostnadsrammer, eventuelle trinn og faser i undersøkelsen, samt hva og hvordan man ønsker at resultatet skal rapporteres.

Evaluering og videreutvikling

Varslingssystemet bør som andre elementer i compliancesystemet være gjenstand for evaluering og en kontinuerlig videreutvikling. Dette kan gjøres i forbindelse med internrevisjon hvis virksomheten har det (forutsatt at internrevisjonen ikke har ansvar for varslingssystemet) eller ved eksterne evalueringer.

Reaksjoner på avvik, sanksjoner og korrigerende tiltak

Bedriften bør ha et enhetlig reaksjonsmønster for alvorlige brudd på eksterne lover og regler og interne retningslinjer. Disse bør være utformet på prinsipielt grunnlag og være retningsgivende for alle deler av virksomheten. Som eksempel kan nevnes interne regler om hvilke typer saker som skal anmeldes; det bør angis eventuelle beløpsgrenser for anmeldelse, og ikke minst hvilket beslutningsnivå som skal avgjøre slike saker for å forhindre forskjellsbehandling og at enkeltpersoner fatter feil beslutninger.

> Kritikkverdige forhold er forhold som er i strid med lover, regler eller etiske normer samt interne retningslinjer.

http://www.kongsberg.com/en/kog/sustainability/

Utfordringer og erfaringer

Å etablere et varslingssystem er overkommelig for de fleste virksomheter. Det er viktig å ta hensyn til egenart, størrelse og risiko når man planlegger og implementerer rutiner. Det finnes mye god veiledning i artikler og faglitteratur, og det er også god tilgang på konsulentbistand både for etablering og selve driften av varslingssystemer hvis man skulle ønske en ekstern part til å ivareta det.

En del utfordringer vil trolig være generelle enten man velger den ene eller andre løsningen, og nedenfor beskrives noen som bygger på praktiske erfaringer.

Kulturforskjeller

Varsling i Norge og vestlige land er godt etablert og kjent blant ansatte. Vår lederstil og bedriftsdemokrati, med høy grad av åpenhet og medbestemmelse, oppfatter varsling som et effektivt virkemiddel for en velfungerende organisasjon. I andre deler av verden, hvor lederstilen kan være mer autoritær og hierarkisk, og oppsigelsesvernet betydelig svakere, oppleves ikke alltid varsling som et virkemiddel de ansatte føler seg trygge på. Konkurransen mellom de ansatte for å fremme egen karriereutvikling kan også være betydelig «skarpere» enn hva vi er vant med. Varslingssystemet kan misforstås og/eller misbrukes for egen vinning, og dette kan gi utfordringer i vurderingen av innholdet i et varsel, spesielt når det er mer rettet mot person enn handling. Det kaller på en ekstra årvåkenhet og at man har fokus på de kritikkverdige forholdene og forsøker å skille det fra en eventuell personalkonflikt. Det er viktig at man er oppmerksom på at det kan være to parter som har krav på vern i en slik prosess; både den som varsler og den det varsles om.

Det kan også være kulturforskjeller i en og samme bedrift, som kan gjøre det ekstra utfordrende å utforme retningslinjer som både er prinsipielle og konkrete nok til å dekke behov i ulike deler av virksomheten.

Hva er et kritikkverdig forhold

Selv om de interne retningslinjene er forsøkt skrevet så konkret som mulig og eksempler er gitt, kan det likevel være vanskelig å avgjøre om et varsel gjelder et kritikkverdig forhold - og eventuelt avvise det. Det er viktig at man på prinsipielt grunnlag vurderer dette og f.eks. etablerer en fast gruppe som vurderer innkomne varsler, herunder hvem som skal saksbehandle varselet, og avgjør eventuelt avvisning av varselet. En avvisning bør alltid følges av en veiledning om en instans som vedkommende som har varslet kan henvende seg til. Hvis det f.eks. gjelder en personalkonflikt bør man få henvisning til HR avdelingen, verneombudet eller en tillitsvalgt.

En variant kan være hvis det forhold det varsles om i utgangspunktet kan være svært alvorlig, men er lite spesifikt, og varsleren enten er anonym eller ikke ønsker å utdype varselet. Et eksempel på et slikt varsel kan være en påstand om at virksomheten i et spesifikt land eller prosjekt er drevet på en «uetisk måte», uten nærmere beskrivelse. Det bringer oss over i neste utfordring:

Arbeidstilsynets veileder kan være en god start ved oppbyggingen av et varslingssystem og interne rutiner.

Undersøkelser av varsel – hva er «godt nok»

Med bakgrunn i eksemplet i forrige avsnitt kan en mulig tilnærming være at compliance avdelingen eller internrevisjonen gjennomfører en risikoanalyse av den omtalte virksomheten eller prosjektet. Man kan analysere verdikjeden og vurdere hvor det kan være risiko for korrupsjon eller andre alvorlige lovbrudd. Analysen kan bestå av intervjuer med ledelse, regnskapsgjennomgang med fokus på trender/avvik fra forventning, omfang av gaver/representasjon/sponsing, mediasøk for virksomheten, ledelsen og forretningspartnere, vurdering av bruk av konsulenter, agenter og lobbyister. Hvis ikke dette gir noen røde flagg, har man da gjort nok? Eventuelt hvor langt skal man gå hvis det dukker opp noen røde flagg? Og hvem skal bestemme om man har gjort nok? Det er ikke gitt et fasitsvar på slike utfordringer, og man bør tenke gjennom på forhånd hvordan man vil forholde seg til slike dilemmaer når man utformer rutiner for undersøkelser av varsler.

Oppsummert

Et velfungerende varslingssystem må bygge på tillitt og ansvarlighet - og de interne rutinene må være velfunderte og forankret både hos ledelse og de ansatte. Systemet må være godt planlagt og systematisk oppbygget utfra bedriftens egenart. Et godt tips er å tenke gjennom hvordan man vil behandle ulike saker som er kjent fra andre virksomheter og lage prinsipielle rutiner- før man står midt oppe i en sak i egen bedrift.

> «Compliance» er systemer og roller i virksomheten som påser at lover og regler etterleves av ansatte og andre som handler på vegne av virksomheten.

Kan vi lære noe av Panama-avsløringene?

Av
LENE BOLLESTAD
internrevisjonen, Norges bank

Vi har vel alle fått med oss Panama-avsløringene som nådde offentlighetens lys i starten av april 2016. Jeg skal la være å dvele ved sakens fakta, men det er ingen tvil om at skatteparadiser aldri har vært så omdiskutert som i dag. Men skatteparadiser omfatter mer enn bare Panama og denne ene konkrete saken. Andre velkjente skatteparadiser inkluderer blant annet Cayman Islands, British Virgin Islands, De forente arabiske emiratene, Singapore og en rekke til, som i ulik grad praktiserer fordelaktige skattesatser og beskyttelse av selskaps- og eierinformasjon. I kjølvannet av Panama-avsløringene har en rekke relevante spørsmål blitt satt på agendaen, og jeg vil sette søkelys på ett av dem; nemlig viktigheten av en skikkelig integrity due diligence.

I et tidligere innlegg publisert på NIRFs nettside, og forrige utgave av SIRK, «Ville du giftet deg med en fremmed?», satte jeg viktigheten av gjennomføringen av bakgrunnssjekker, eller såkalt integrity due diligence (IDD), på agendaen ved etablering av relasjon med tredjeparter. Selskapsinformasjon og reelle eiere og eierinteresser er blant de sentrale områdene man ønsker å kartlegge gjennom en slik prosess. I artikkelen sammenliknet jeg TV Norge-programmet «Gift ved første blikk» som går ut på at tre par skal gifte seg uten å vite noe om hverandre, og det faktum at det i forretningsverden gjennomføres dealer, transaksjoner og kontrakter uten at man nødvendigvis kjenner motparten. Konklusjonen var at alle tre par i sesong 2 – 100% - ble skilt, samtidig som at det finnes en rekke eksempler på dealer, transaksjoner og kontrakter som sannsynligvis aldri burde vært gjennomført.

Når selskaper etablerer seg i såkalte skatteparadiser er vanligvis det reelle eierskapet vanskelig å identifisere, nettopp fordi skatteparadiser ofte kjennetegnes ved at selskaps- og eieropplysninger holdes skult og som regel er utfordrende å få tilgang til. Med andre ord vil man kunne støte på store utfordringer og potensielle røde flagg ved gjennomføringen av IDD, med funn som sannsynligvis bør vurderes på ledelse- og/eller styrenivå, og undersøkes videre. Relevante områder kan omfatte selskapets reelle eierskap eller selskapets transaksjonsstrømmer.

Gjennomføringen av en skikkelig IDD prosess er derfor ett av læringspunktene jeg tror kan trekkes ut i kjølvannet av Panama-avsløringene: Har vi egentlig gjort tilstrekkelig bakgrunnsundersøkelser før etablering relasjoner med tredjeparter? Vet vi egentlig hvem motpartene våre er? Vet vi egentlig hvor pengene våre kommer fra eller flyter til? At gjennomføringen av IDD vil kunne avdekke alle «lik i bagasjen» er det er selvsagt ingen garanti for, men en skikkelig prosess bidrar til å sette røde flagg på agendaen og til at man tar stilling til den risikoen det eventuelt kan innebære.

Databehandleravtaler under kontinuerlig forbedring

Av
CHRISTINA AAR
Tjenesteansvarlig for personvern i Norden, EY Advisory/Risk

Det er få virksomheter som kan vise til en planmessig og systematisk oppfølging av kravene overfor databehandler i avtaleperioden.

Mange virksomheter bruker eksterne leverandører for ulike typer tjenester, typisk innen lønn og IKT-tjenester. Om tjenesten omfatter behandling av personopplysninger, er leverandør å anse som databehandler. Som behandlingsansvarlig virksomhet har man ansvar også for personopplysninger som behandles hos en databehandler på vegne av virksomheten. Jeg vil i denne artikkelen peke på flere av de utfordringer vi ser i praksis; alt fra mangel på oversikt over databehandlere virksomheten har, lite presist innhold i avtaler, manglende oppfølging i avtaleperioden til uklare rolle- og ansvarsforhold for slike avtaler innad i den behandlingsansvarlige virksomheten.

Modningsreise for både behandlingsansvarlige og databehandlere

Gjennom utførelse av internrevisjoner og vår rådgivningsvirksomhet innen personopplysningsloven, ser vi et bredt spekter av virksomheter fordelt på flere sektorer. Vi observerer at det stadig oftere foreligger en databehandleravtaler der det skal foreligge slik avtale. Dessverre er innholdet i avtalene ikke alltid like presist eller tilpasset de(n) aktuelle behandlingen(e) avtalen gjelder. Det er få virksomheter som kan vise til en planmessig og systematisk oppfølging av kravene overfor databehandler i avtaleperioden. Fortsatt svarer flere behandlingsansvarlige virksomheter at de forventer at leverandøren «tar ansvar for det hele». Litt for ofte svarer leverandører at kundene ikke har stilt noen særskilte krav og at de dermed ikke er kjent med noen begrensninger i behandlingen av personopplysninger eller hva kunden mener er nødvendig sikringsnivå for å oppnå tilfredsstillende informasjonssikkerhet.

Leverandører som vil overleve i markedet over tid, bør opptre som en profesjonell part og utfordre kundene på innhold i slike avtaler. Det er likevel den behandlingsansvarlige som sitter med ansvaret for at behandlingen av personopplysninger er i tråd med personopplysningslovens krav og tilstrekkelig sikret.

Om databehandleravtale

Hvis en virksomhet setter ut hele eller deler av behandlingen av personopplysninger til andre virksomheter, skal det inngås en databehandleravtale. Eksempler på slike situasjoner er bruk av eksterne skyløsninger for lagring av informasjon eller bruk av et eksternt firma som sørger for å makulere papir som kastes i en virksomhet.

Krav om og til en slik avtale fremkommer av personopplysningsloven § 15 jfr. § 13. Begge parter har uavhengig av avtalen et selvstendig ansvar for å sikre tilfredsstillende informasjonssikkerhet etter personopplysningslovens § 13, jf. personopplysningsforskriftens kapittel 2. En databehandleravtale kan være en frittstående avtale mellom partene, eller en integrert del av andre avtaler som f.eks. også omfatter de merkantile forhold.

Databehandleravtalen skal inngås før behandlingen av personopplysningene starter opp og en databehandler kan ikke behandle personopplysninger på en annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige.

Det er således avtalen som gir en databehandler rett til å behandle personopplysninger og innholdet i avtalen gir rammene for hva databehandler kan og skal gjøre med personopplysningene.

Utfordringen med Datatilsynets mal

Vi har sett flere eksempler på at virksomheter kun har utfylt første og siste side av Datatilsynets mal for databehandleravtaler. Det vil sjelden, om noen gang, være tilstrekkelig. Datatilsynet presiserer også i tilhørende veiledning at malene kun inneholder minimumskrav. En slik mal vil ikke kunne dekke alle typer av situasjoner der en ekstern leverandør utfører tjenester på vegne av en behandlingsansvarlig. Til det er virksomheter, sektorer og type behandlinger for forskjellig. Datatilsynets mal med veiledning viser på en god måte hvilke temaer som bør omfattes i en databehandleravtale. Det konkrete innholdet og de aktuelle føringene må den enkelte virksomhet selv sørge for, slik at avtalen gir de nødvendige rammene for den aktuelle behandlingen. Hvilke tiltak som er nødvendig skal være basert på en risikovurdering slik at tilstrekkelig beskyttelsesnivå oppnås for de aktuelle informasjonsverdiene som inngår i avtalen.

Tema som må dekkes er:

- Formålet med behandlingen
- Hvordan personopplysningene skal behandles av databehandler
  - o Konkrete rutiner for hvordan personopplysningene kan og skal brukes, herunder regler for eventuell utlevering.
  - o Eventuell arbeidsfordeling for ivaretakelse av registreres rettigheter (informasjon, innsynsbegjæringer, retting, sletting mv)
- Krav om tilfredsstillende informasjonssikkerhet ifht konfidensialitet, integritet og tilgjengelighet, som for eksempel:
  - o Sikre overholdelse av taushetsplikt
  - o Regulering av hvilket personell hos partene som skal ha tilgang til personopplysningene
  - o Tilgangskontroll og tilstrekkelige kontrollmekanismer f. eks. loggføring
  - o Fysiske sikringstiltak
  - o Hvordan rutiner mv skal dokumenteres
  - o Utførelse av sikkerhetsrevisjoner (hyppighet, omfang, dokumentasjon)
  - o Avvikshåndtering, herunder avklaring av hvem som har ansvaret for å melde avviket til Datatilsynet dersom avviket har ført til uautorisert utlevering av personopplysninger
- Eventuell bruk av underleverandør
- Avtalens varighet
- Hva som skal skje med opplysningene etter at avtalen er opphørt

Oppfølging i avtaleperioden

Vi ser dessverre litt for ofte at den behandlingsansvarlige virksomheten synes å være godt fornøyd med at avtalen foreligger. Det er ikke like ofte vi observerer at avtalens innhold og status i etterlevelse av databehandleravtalen faktisk følges opp underveis i avtaleperioden.

Den behandlingsansvarlige skal forsikre seg om at databehandleren har et tilstrekkelig sikkerhetsnivå og har plikt til å følge opp også underveis i avtaleperioden. Dette kan gjøres ved å:

- sette temaet på dagsorden i møtene som avholdes med leverandør,
- avkreve årlig statusrapport for etterlevelse av punkter som fremkommer av avtalen,
- be om innsyn i dokumentasjon av gjennomførte sikkerhetsrevisjoner,
- inspisere den konkret oppfølging av eventuelle avvik og tiltak som blir iverksatt for å forebygge samme avvik skjer på ny,
- be om innsyn i eventuelle egenkontroller, tredjepartsgjennomganger eller lignende som benyttes i virksomhetens egen ledelses gjennomgang.

Videre, ved terminering av avtalen er det viktig å sikre klar avtale om hva som skal skje med de personopplysningene leverandør har i hende på det tidspunktet. Skal disse slettes på forsvarlig vis eller tilbakeleveres til den behandlingsansvarlige? Det kan i denne forbindelse være lett å glemme at personinformasjon kan være lagret på flere lagringsmedier, som ulike mellomlagre og back-up servere mv.

Intern fordeling av roller og ansvar

Vi observerer relativt ofte at virksomheter mangler en samlet oversikt over databehandlere virksomheten har eller burde hatt databehandleravtale med. Dette skyldes som regel at det er uavklarte rolle- og ansvarsforhold både for den enkelte avtale i kombinasjon med mangelfull koordinering av inngåelse og forvaltning av slike avtaler. Mangel på oversikt gir risiko for at avtaler ikke foreligger eller

En virksomhet bør jo ha flere drivere for å sikre god etterlevelse av krav til personvern enn bare et ønske om å unngå bøter.

RÅD

- Påse at det er klare rolle- og ansvarsforhold internt for inngåelse, oppfølging og terminering av databehandleravtaler.
- Sørg for at det foreligger en oversikt over alle databehandlere som viser hvem som er ansvarlig, når avtalene utløper og hvor de er arkivert.
- Sikre at ajourhold og gjennomgang av oversikt og innhold i avtaler inngår som en del av internkontrollrutinene.

ikke har tilstrekkelig innhold. Mangel på tydelig plassert ansvar gir risiko for at alle tror at noen andre ivaretar ansvaret. Om ansvar for slike avtaler spres utover i virksomheten er det en fordel å legge til rette for ivaretakelse av personvern og informasjonssikkerhet gjennom å utarbeide virksomhetsspesifikke maler, angivelse av minimumskrav på ulike områder, samt fastsette obligatorisk kvalitetssikringsrutine e.l. for å sikre et harmonisert nivå på sammenlignbare avtaler.

Erfaringer fra global undersøkelse

EY gjennomfører årlig en survey innen informasjonssikkerhet og personvern. I 2015 deltok i alt 1755 virksomheter fra 67 land[1]. Ett av temaene som ble trukket frem av mange respondenter i resultatene fra 2015, var bekymringer knyttet til mangel på kontroll over hvordan leverandører faktisk benyttet personopplysninger som ble behandlet på vegne av virksomheten. Respondentene ga videre egen virksomhet forholdsvis lav modenhetsgrad ved spørsmål om hvor effektiv forvaltning av informasjonssikkerhet ved bruk av leverandører er i egen virksomhet.

Endringer med ny personvernforordning?

Ny personvernforordning (GDPR) er vedtatt og vil tre i kraft i EU i 2018. Det samme er planlagt å gjelde også for Norge, selv om det formelt sett skal på plass en beslutning om tilpasning av EØS-avtalen.

En av endringene som kommer med ny forordning er en mer eksplisitt regulering av databehandlers ansvar. Forordningen vil dermed fungere bedre som en støtte for de tiltak som er nødvendig å iverksette for å sikre tilfredsstillende ivaretakelse av personvern og informasjonssikkerhet. I tillegg nedfelles det direkte krav om at også en databehandler må demonstrere at kravene etterleves gjennom egen dokumentasjon, bruk av sertifiseringer, tredjepartsrapporter mv.

De stedlige Datatilsyn gis videre anledning til å gi bøter både til en behandlingsansvarlig og en databehandler opptil 20.000.000 EUR eller opptil 4% av global omsetning. Bøter i denne størrelsesorden er jo et språk som gir mer oppmerksomhet til tematikken også på øverste ledernivå. En behandlingsansvarlig vil om det avdekkes alvorlige mangler ikke kunne slippe unna med å peke på databehandler, om virksomheten ikke har stilt tydelige krav gjennom databehandleravtalen og ikke følger opp underveis i avtaleperioden.

En virksomhet bør jo ha flere drivere for å sikre god etterlevelse av krav til personvern enn bare et ønske om å unngå bøter. Ivaretakelse av omdømme overfor både eksisterende og potensielle kunder er en sentral faktor for de fleste virksomheter. Et solid grep om etterlevelse på dette området vil kunne være markedsdifferensierende. Det vil dessuten være effektivitetsgevinster å hente ved å ha velfungerende rutiner for å sikre etterlevelse av personvernhensyn i egen virksomhet. Det er som regel mer ressurskrevende å skulle reparere og justere både systemer og rutiner i etterkant om det avdekkes at det ikke er tatt tilstrekkelig hensyn til de rettslige føringene på dette området.

Begrepsforklaringer:

Behandling av personopplysninger	Er iht personopplysningslovens definisjon enhver bruk av personopplysninger, enten det er innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter, jf. Personopplysningslovens § 2 nr. 2.
Behandlingsansvarlig	Er iht personopplysningslovens definisjon den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jf. personopplysningslovens § 2 nr. 4. Dette er dermed den rollen som har ansvaret for at opplysninger behandles i henhold til de krav som personopplysningsloven oppstiller. Dette er typisk virksomhetens leder. Denne kan og er som regel avhengig av å delegere oppgaver for å sikre ivaretakelse i det daglig. Slik fordeling av roller og tilhørende skal være dokumentert i internkontrollsystemet.
Databehandler	Er iht personopplysningslovens definisjon den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. personopplysningslovens § 2 nr. 5. En databehandler har et selvstendig ansvar for å ha tilfredsstillende informasjonssikkerhet, for å verne personopplysningene som behandles på vegne av behandlingsansvarlige jf. personopplysningslovens § 13 og skal bare behandle personopplysninger i henhold til avtale med den behandlingsansvarlige.
Personopplysningsloven	Lov av 14. april 2000 nr. 31. Tilgjengelig via www.lovdata.no
General Data Protection Regulation (GDPR)	Ny personvernforordning, Datatilsynet har lagt ut mer informasjon via disse sidene: https://www.datatilsynet.no/Regelverk/EUs-personvernreform/personvernforordningen-vedtatt-i-eu/

[1] *Resultatene gis for alle respondenter, per land og per sektor. I tillegg får den enkelte deltaker sin benchmark mot resultatene. Se mer informasjon her: http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity*

Risikostyring og organisatorisk læring

Av
EYSTEIN BONNEVIE-SVENDSEN
Oberst/nestleder,
Forsvarsdepartementets internrevisjon

Innledning

Da jeg for et par år siden reviderte hvordan Forsvaret håndterer erfaringer slo det meg hvor like Forsvarets prosess for erfaringshåndtering og risikostyring basert på COSO ERM[1] er. Begge tar utgangspunkt i en målsetting, fokuserer på henholdsvis mulige og inntrufne hendelser, og tilstreber å lukke avvik. Dette gjøres ved å finne, implementere, og evaluere tiltak for å oppnå en kontinuerlig forbedring.

Dette inspirerte min prosjektoppgave på masterprogrammet i intern revisjon på BI 2014-2015, hvor jeg ønsket å belyse om risikostyring slik den ble gjennomført i Forsvaret også var et egnet verktøy for å ivareta organisatorisk læring.

En sentral konklusjon fra min undersøkelse er at kontinuerlig forbedring forutsetter en lærende organisasjon, og for at forbedring skal finne sted, må risikostyringen legge til rette for og bidra til organisatorisk læring. Denne artikkelen bygger på prosjektoppgaven og ser på om litteratur som beskriver organisatorisk læring kan gi nyttige bidrag til alle som er opptatt av å få risikostyring til å fungere best mulig.

Grunnleggende forutsetninger for læring i organisasjoner

Læring, kompetanseutveksling og bruk av kompetanse begynner og slutter[2] hos den enkelte medarbeider. Det er medarbeiderne som gjennom sin kompetanse bruker og utvikler prosesser og systemer, og disse prosessene og systemene kan igjen bidra til læring og ny kompetanse. En organisasjon disponerer bare den kompetansen som ligger hos de medarbeiderne den til enhver tid måtte ha.

Læring er en prosess der mennesker og organisasjoner tilegner seg ny kunnskap, og endrer sin adferd på grunnlag av denne kunnskapen[3]. En forutsetning for læring i organisasjoner er at individer i organisasjonen er i stand til å lære og at det som er lært av enkelte spres til andre i organisasjonen, såkalt kollektiv læring. Deretter må den kollektive kunnskapen omsettes i handling. Endrede handlinger medfører igjen ny læring hos individer og dermed etableres en læringssirkel (Figur 1).

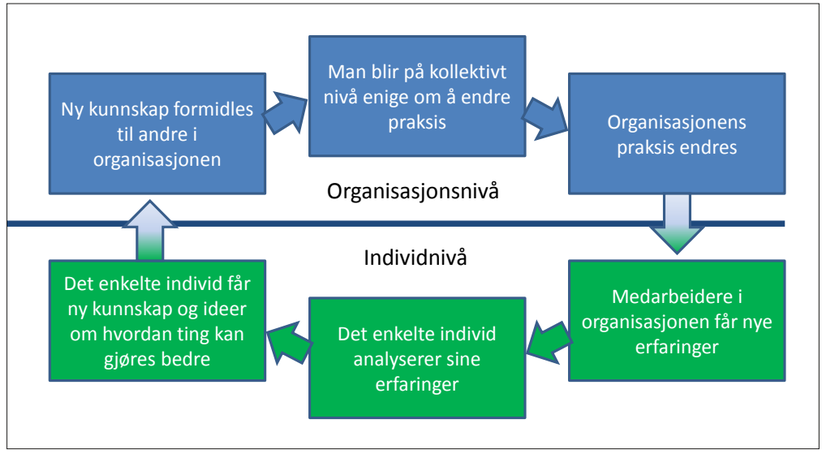
Læringsprosessen slik den er fremstilt i figur 1 starter med utgangspunkt i en personlig konkret erfaring. Å omsette erfaring til læring innebærer at vi basert på våre erfaringer er i stand til å handle på en mer korrekt og mer effektiv måte i nye situasjoner. Den enkelte reflekterer over disse erfaringene, analyserer, og ser på konsekvenser av det erfarte sett i forhold til tidligere erfaringer.

Denne analysen kan foregå på tre nivåer[4]: det første er enkelkretslæring (single loop learning) der eksisterende prosedyrer justeres basert på tilbakemelding (feedback) – gjør vi tingene riktig? Neste nivå er dobbelkretslæring (double loop learning); hvor grunnpremissene for jobben som utføres analyseres, noe som kan føre til at strategier endres og helt nye prosedyrer utvikles – gjør vi de riktige tingene? Tredje nivå er såkalt deuterolæring (deuterolearning) hvor selve læreprosessen analyseres og eventuelt gjøres mer hensiktsmessig. En lærende organisasjon må beherske all tre nivå[5].

Det er imidlertid viktig å merke seg at læringssirkelen bare kan virke[6] dersom mennesker deler ideer om nye mønstre, og organisasjonen har lagt til rette for kollektiv læring. Organisatorisk læring er helt avhengig av at den enkelte først er villig til å engasjere seg i refleksjon og analyse, og deretter villig til å dele sine refleksjoner med andre i organisasjonen, som vist i figur 1. En kultur preget av gjensidig tillit er en forutsetning for den enkeltes vilje til å dele. Det er særlig tre faktorer av betydning for om, og i hvilken grad, en medarbeider er villig til å bidra med sin kompetanse til kollektiv læring: subjektiv mestringstro, motivasjon, og personlige egenskaper og behov[7].

Alan Frost har[8] gjort rede for et antall faktorer som har ført til at kompetansestyring i mange tilfeller ikke har gitt ønsket effekt. En vurdering av disse årsaksfaktorene[9] (listet i venstre del av figur 2) viste igjen hvor viktig det er å ha riktig kompetanse i en virksomhet for at

[1] *Norges Interne Revisorers Forening (NIRF)(2005). Helhetlig risikostyring – et integrert rammeverk. Oslo: Norges Interne Revisorers Forening (NIRF)*
[2] *Lai, L. (2008) Strategisk kompetansestyring. 2. utgave. [Først utgitt 2004.] Bergen: Fagbokforlaget*
[3] *Jacobsen D.I. og K. Thorsvik (2007). Hvordan organisasjoner fungerer. 3. utgave. [Først utgitt 2002.] Bergen: Fagbokforlaget.*
[4] *Argyris og Schøn i Kaufmann G. og Kaufmann A.: Psykologi i Organisasjon og Ledelse: 3. utgave 2003, Fagbokforlaget, Bergen*
[5] *I følge Jacobsen og Thorsvik (2007) tyder empiri og teori på at det er krevende å balansere behovet for singelkrets og dobbelkretslæring; for mye vektlegging av det ene vil kunne bidra til å utelukke det andre.*
[6] *Heijden, Kees Van der: Scenarios - The art of strategic conversation: (Second Edition), Chichester, Wiley 2005.*
[7] *Lai 2008*
[8] *Frost, Alan (2014). A Synthesis of Knowledge Management Failure Factors. www.knowledge-mangement-tools.net*
[9] *Mangelfull ledelsesinvolvering - mangelfull kompetanse – mangelfull planlegging, koordinering og evaluering – uklare målsettinger og effekt av tiltak – svakheter ved organisasjonsstruktur – svakheter ved organisasjonskultur.*



risikostyring skal fungere optimalt. Vurderingen identifiserte også hvor nødvendig det er med grundig planlegging og hensiktsmessige evalueringer - sammenhengen mellom planlegging og evaluering er verdt å merke seg; Linda Lai har antydet[10] at evaluering blir skadelidende når planprosessen ikke fører til klare mål som kan danne grunnlag for systematisk evaluering og oppfølging. Å gjennomføre gode evalueringer kan være en utfordring siden mange leveranser, spesielt fra offentlig sektor, er vanskelige å kvantifisere. Flere forskere har imidlertid vist at det er fullt mulig å vurdere måloppnåelse også for offentlig virksomhet[11].

Utfordringer knyttet til deling av erfaringer

Organisasjonen må legge til rette for at deling av erfaringer og for at endringer kan finne sted. Imidlertid foregår mye av den kollektive læringen uformelt, så organisasjonen må tilstrebe at formelle prosesser samspiller med de uformelle prosessene som foregår medarbeiderne imellom[12].

Edgar H Schein[13] identifiserer menneskers og gruppers vilje eller engstelse til endring som det fremste hinderet for læringen. Jo mer omfattende en endring er, og jo flere grupper som påvirkes av den, desto sterkere kan man anta at motstanden mot endringen vil bli[14], , f.eks. kan sterke gruppenormer hindre en gruppe i å lære av sine handlinger. Endring kan omfatte en rekke forhold som alle innebærer at interne maktforhold og forholdet til omgivelsene endres[15]. Maktforhold er knyttet til kultur siden informasjon gir makt.

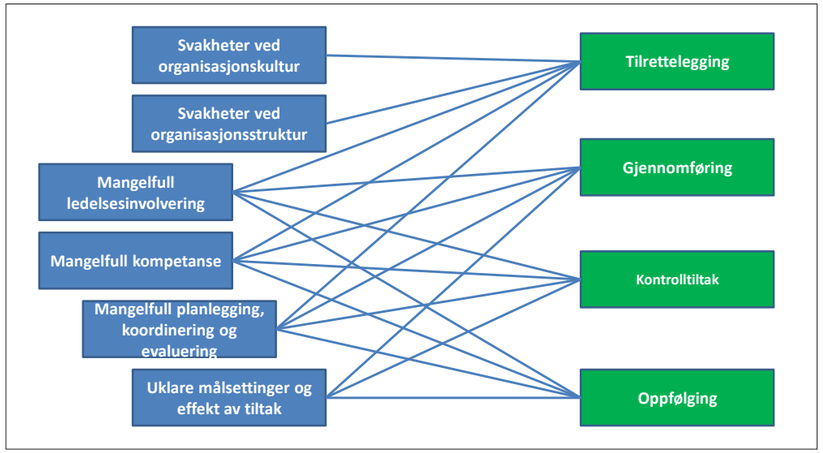
Vi mennesker er mer tilbøyelige til å endre adferd dersom det oppfattes som relevant for den enkelte. Forhold som kan virke inn på relevans er den enkeltes plassering i en organisasjon, grad av formalisering og type struktur, og kommunikasjon. En lærende organisasjon kjennetegnes av at det er etablert arenaer eller ordninger som fremmer sosial samhandling og kunnskapsoverføring, mangfold og evne til å tilegne seg ny kunnskap, og at den enkelte forstår helhet og sammenhenger i egen organisasjon[16]. Ledere har en viktig rolle i å tilrettelegge for læring.

Svært forenklet må to kriterier være oppfylt for at en medarbeider skal være motivert for endring. For det første må han eller hun oppleve et incentiv for å delta og en frykt (føle en forpliktelse) for ikke å delta i endringen. Denne opplevde forpliktelsen kan ofte være knyttet til intern kultur og gruppenormer. For det andre må det være rom for å feile uten at det får negative konsekvenser.

Læring i COSO ERM, DFØs veiledere[17] og bevilgningsreglementet[18]

COSO ERMs[19] beskrivelse av et internt miljø, samt informasjon og kommunikasjon som viktige elementer for god risikostyring, har mye til felles med et miljø tilrettelagt for organisatorisk læring. Imidlertid er ikke begreper forbundet med kontinuerlig forbedring eller organisatorisk læring anvendt i beskrivelsen av COSO ERM. Viktigheten av å satse på kompetanse blir nevnt, men i liten grad hvorfor og hvilke krav som bør stilles til denne. Det nevnes f.eks.

[10] Lai 2008
[11] Bl a Lai 2008, Hanson, Torbjørn (2010). Produktivitetsmålinger i Forsvaret – metode og anvendelsesområder, FFI-rapport 2010/01495, og Kvalvik, S. N., Mjelva, A. og Presterud, A. O. Håndbok i kontinuerlig forbedring og fornying i Forsvaret – hvordan identifisere og gjennomføre tiltak? FFI-rapport 2011/01294
[12] Argyris og Schøn i Kaufmann & Kaufmann 2003
[13] Schein, Edgar H (1999). The corporate culture survival guide: sense and nonsense about culture change. San Fransisco: Jossey-Bass.
[14] I modne organisasjoner handler læring om å avlære og erstatte etablerte antagelser og verdier like mye som å lære nye. Mange motsetter seg endringer fordi slik avlæring oppleves som ubehagelig og angstfremkallende.
[15] Jacobsen og Thorsvik 2007
[16] Jacobsen og Thorsvik 2007
[17] Senter for Statlig økonomistyring (2005). Risikostyring i staten - Håndtering av risiko i mål- og resultatstyringen. Senter for Statlig økonomistyring (2007). Hvordan få en god start på risikostyring i statlige virksomheter.
[18] Fellesbetegnelse for «Reglement for økonomistyring i Staten» (RØS) og «Bestemmelser om Økonomistyring i staten» (BØS)
[19] I oppgaven fordelte jeg komponentene i COSO ERM-rammeverket på 4 grupper for å unngå gjentagelser; tilrettelegging, gjennomføring, kontrollaktiviteter, og oppfølging.



ikke at kompetansen må være god nok til å ivareta organisasjonslæring på alle tre nivå (presentert ovenfor). Videre nevner COSO ERM heller ikke at resultatet av kontrollaktiviteter (ofte i form av anbefalinger) vil være viktige innspill til organisatorisk læring.

DFØ tilfører viktige bidrag til organisatorisk læring, som lederens betydning, rollen medarbeiderne må ta i forhold til medansvar og involvering, betydningen av uformell kommunikasjon, krav til klare mål og bevisste og godt formulerte kritiske suksessfaktorer, viktigheten av å utnytte muligheter, samt betydningen av dokumentasjon og handlingsplaner. Alt dette er elementer som også bidrar til organisatorisk læring. COSO ERM og DFØs veiledere beskriver i liten grad oppfølging, og ingen av dem nevner at selve læringen først og fremst er knyttet til denne prosessen[20].

I figur 2 har jeg forsøkt å illustrere forholdet mellom Frosts årsaksfaktorer og min egen gruppering av COSO ERM-kategoriene. Faktorene Ledelsesinvolvering og kompetanse påvirker hverandre gjensidig ved at ledelsen rekrutterer og utvikler kompetanse, mens kvaliteten på de rådene ledelsen får er avhengig av kompetansen til de som gir dem. Disse to faktorene påvirker alle de andre faktorene, og har konsekvenser for alle 4 grupper av kategorier. Dette understreker hvor viktig ledelsens engasjement og medarbeidernes kompetanse er for organisatorisk læring.

Avslutning

COSO ERM og DFØs tidligere veiledere i risikostyring synes ikke å være utarbeidet for organisatorisk læring. Begreper som «kontinuerlig forbedring» og «organisatorisk læring» er benyttet i svært liten grad, og beskrivelsen av oppfølgingsprosessen - det er først og fremst her læringen foregår – er ikke rettet mot hvordan læring i organisasjoner foregår. Imidlertid tilfører DFØs veiledere mange momenter som vil kunne bidra til en lærende organisasjon. Forskning og litteratur omkring organisatorisk læring gir mange nyttige perspektiver som kan få virksomheter til å få mest mulig utbytte av sin risikostyring.

Læring innebærer at mennesker og organisasjoner faktisk endrer sin adferd på grunnlag av tilegnet kunnskap. Risikostyringens implementering av tiltak innebærer også endring, og endringer blir sjelden vellykkede om det ikke tas hensyn til medarbeidernes motivasjon for endringen. Læringssirkelen i figur 1 må fungere i en lærende organisasjon, og er den viktigste forutsetningen for organisatorisk læring; nemlig at den enkelte medarbeider er villig til å dele sine erfaringer med andre. En annen forutsetning for en lærende organisasjon er at den har kompetanse som setter den i stand til å beherske både singel- og dobbeltkretslæring. Alle disse forholdene kan organisasjonen påvirke selv. Frosts 6 årsaksfaktorer vil kunne være et nyttig utgangspunkt for å forstå årsakene til eventuelle svakheter i risikostyringen i egen virksomhet. Perspektiver om organisatorisk læring er nyttig for alle som skal bidra til å få risikostyring til å fungere best mulig.

[20] DFØs veileder i internkontroll fra 2013 skriver i pkt 4.5.2 om å «Bruke informasjon fra oppfølgingen til styring, læring og forbedring» (av internkontrollen), og slår fast at systematisk oppfølging er (også) et avgjørende element i virksomhetens generelle lærings- og forbedringsarbeid.

Pro bono-programmer i bedrifter

Pro bono er det raskest voksende formen for frivillighet blant ansatte i bedrifter . I Norge doneres i økende grad kompetanse til etablerte pro bono- organisasjoner privat på eget initiativ, men også bedrifter benytter i større og større grad ansattes kompetanse til pro bono arbeid.

Av
ANNE AABY
Daglig leder i Prospera

Tradisjonelle former for frivillighet blant bedrifter er blant annet dugnadsarbeid på turisthytter, innsamling av penger og salg av produkter der inntektene går til et godt formål, mens ved å donere profesjonelle pro bono-tjenester benyttes ansattes *kjernekompetanse* for å skape verdi uten å ta betalt for tjenestene.

Tilbudet om profesjonelle pro bono-tjenester har sitt opphav i den juridiske verden. Idealet om at alle må ha tilgang til rettshjelp i en demokratisk rettsstat ble noen steder der staten ikke tilbyr økonomisk støtte til juridisk hjelp, løst i form av pro bono tjenester. I noen vestlige land er derfor advokatfirmaer påbudt å tilby en andel pro bono-tjenester for å kunne beholde advokatlisens.

I Norge merker vi størst interesse for kompetansebasert frivillighet blant konsulenter som privat og på eget *initiativ* melder seg for å donere sin kompetanse. Kompetansebasert frivillighet kan forstås som frivillig arbeid der fagkompetente mennesker donerer kompetanse gratis. I Norge er organisasjonen Prospera ledende innen dette området. Prospera har 260 pro bono-konsulenter lokalisert i Oslo, Bergen og Stavanger, og er i ferd med å kunne tilby tilsvarende tjenester også i andre store norske byer. Omfanget og verdien på leveranser fra Prospera øker for hvert år. Prospera ble opprettet i 2009 og har siden etablering bidratt med leveranser til sosiale entreprenører og ideelle organisasjoner med en verdi på over 5,5 MNOK. I 2014 var summen 1,1 MNOK, mens 2,5 MNOK ble donert i 2015.

Pro bono-organisasjoner, som Prospera, har etablert arenaer der profesjonelle kan finne en måte å donere sin kompetanse innenfor frivillighetens rammer. Pro bono-organisasjoner utviser også samfunnsansvar ved å lære sosiale entreprenører å bygge kapasitet og kompetanse. I Pro bono-prosjekter braser kompetanse, energi og engasjement sammen i møtet mellom non-profit og for-profit kultur. Nye geografier, nye markeder og nye økonomier representerer en spennende arena, der et ønske om å løse samfunnets utfordringer er grunnleggende drivkraft. Prosperas formål er å hjelpe sosiale entreprenører og ideelle organisasjoner i å lykkes med å løse en sosial utfordring. Men det vi *egentlig* gjør er å tilrettelegge for frivillighet på en ny måte slik at travle mennesker med høye faglige kvalifikasjoner kan bidra med sin frivillighet innenfor rammer som også skaper verdi for sosiale entreprenører.

Norske bedrifter ligger langt etter og mange har ennå ikke oppdaget gevinsten ved å donere bort kompetanse, mens amerikanskeide og franskeide selskaper i Norge i større grad har sett gevinsten, og har etablert sofistikerte og betydningsfulle pro bono-program. Dette engasjementet bør norske bedrifter koble seg på og bidra til, for her kan man faktisk hente ut konkrete gevinster i form av lokal tilknytning, samfunnsrelevant engasjement og synlighet, økt lojalitet blant ansatte og innovativ kompetanseheving, for å nevne noen.

> Kompetansebasert frivillighet kan forstås som frivillig arbeid der fagkompetente mennesker donerer kompetanse gratis.

Et godt pro bono program tar sikte på å engasjere ansatte, er basert på bedriftens kjernekompetanse, forretningsmål og verdisett. I tillegg bør det hensynta tilgang på ledig tid innenfor arbeidsplassens arbeidstid opp mot de ansattes engasjement på fritiden. Gevinstene bedrifter kan hente av å implementere et program for kompetansebasert frivillighet er blant annet:

1. En innovativ måte å utvikle sine medarbeidere på
2. Økt lojalitet blant ansatte
3. Økt lokal tilknytning ettersom pro bono-prosjektene ofte er hyperlokale
4. Bedret omdømme
5. Verdien av bedriftens kompetanse synliggjøres i samfunnet
6. En mulighet til å applisere kjerne-kompetanse på nye områder, ideer, økonomier og geografier

Vi ønsker å invitere norske bedrifter inn i denne raskt voksende bevegelsen.

1 CECP Giving in Numbers | 2015 Edition

Eksempel på virksomhet med Pro bono-arbeid: KPMG

HR direktør og leder for CSR i KPMG, Vivi Kristensen, forteller at en viktig del av KPMGs CSR arbeid er å tilby fagkunnskap vederlagsfritt til ideelle organisasjoner med begrenset budsjett og ugjorte oppgaver. KPMG donerer probono-arbeid tilsvarende en samlet kroneverdi på inntil kr 500 000 pr år, med utgangspunkt i timeprisen til ansatte som leverer tjenestene.

Samfunnsansvar står høyt på KPMGs agenda, og selskapet har mange engasjerte medarbeidere som setter pris på dette, sier Vivi. Noen ansatte har organisasjoner de brenner for, og søker KPMGs CSR-komité om probono-midler til å bistå disse. Andre ganger er det ideelle organisasjoner som henvender seg til KPMG og utfordringen går da videre til det aktuelle fagmiljøet internt. Det er rift om å få bruke fagkompetansen sin i et probono-team, forteller Vivi.

KPMG stiller krav til organisasjoner de skal bistå, blant annet i forhold til omdømme og gjennomføringsevne. Når det gjelder det enkelte prosjekt er det viktig at det gir nytteverdi og læringseffekt for medarbeiderne som bidrar. Vi ønsker at ansatte som gjennomfører probono-arbeid skal få nye og annerledes erfaringer å ta med seg videre, sier Vivi.

Det siste året har KPMG gjort flere pro bono-prosjekter for Leger Uten Grenser, i tillegg til oppdrag for Røde Kors, Kirkens Bymisjon, VIBRO og Reach for Change.

Leger Uten Grenser er KPMGs hovedsamarbeidspartner, og for deres ansatte har KPMG tidligere gjennomført et kompetanseprogram innen målrettet prosjektstyring. Utvikling av ledere er et annet område Leger Uten Grenser har uttrykt at de gjerne ønsket bistand til. Det var en utfordring KPMG ville ta, og hadde kompetanse til å levere. Basert på innspill fra organisasjonens HR-avdeling skreddersydde en av konsulentene i KPMG Advisory et opplegg spesielt for de aktuelle lederne. Nylig gjennomførte n større gruppe mellomledere et 2 dagers lederutviklingsprogram , hvor deltakerne fikk en bevissthet rundt rollen som leder, samt nyttig metodikk og verktøy for utøvelse av lederrollen.

Vivi forteller at den aktuelle konsulenten uttrykker det samme som mange andre KPMG›ere som har fått gjøre probono-prosjekter i arbeidstiden: Det er inspirerende å få jobbe med entusiastiske og idealistiske mennesker som brenner for det de jobber med, og det gir en ekstra dimensjon til jobben som KPMG-konsulent.

Vi opplever at probono skaper stolte og motiverte medarbeidere, det gir nye impulser og erfaringer for de som bidrar, og det gjør oss til en enda mer attraktiv arbeidsgiver for spesielt yngre jobbsøkere, avslutter Vivi.

> Samfunnsansvar står høyt på KPMGs agenda, og selskapet har mange engasjerte medarbeidere som setter pris på dette.

Rapportering på samfunnsansvar stadig viktigere

KPMGs globale undersøkelse[1] viser at Norge er blant landene med flest selskaper som rapporterer på samfunnsansvar og bærekraft. Rapporten viser imidlertid at det fortsatt er en vei å gå når det gjelder kvalitet.

Av
ANETTE RØNNOV
Senior Manager, KPMG

Globale trender

KPMG har for niende gang utført sin undersøkelse Global Corporate Responsibility Reporting. Undersøkelsen analyser hvordan de 100 største selskapene[2] i 45 land rapporterer på samfunnsansvar. I tillegg ble karbonrapporteringen til verdens 250 største selskaper analysert[3].

Norge har lovkrav som gjør det obligatorisk for store foretak å rapportere på samfunnsansvar, og havner derfor høyt på listen sammen med andre nasjoner med lignende forpliktelser. 9 av 10 store norske selskaper rapporterer derfor på samfunnsansvar. Over 80% av selskapene rapporterer på samfunnsansvar i årsberetningen, mens 4% har valgt å publisere enkeltstående samfunnsansvarsrapporter. Norge har den fjerde største økningen i rapportering av landene, etter India, Sør-Korea og Taiwan. Globalt har rapportering på samfunnsansvar økt de siste to årene, selv om det er en mer beskjeden vekst enn tidligere.

Generelt har kvaliteten i rapporteringen ikke forbedret seg i særlig grad siden vår forrige undersøkelse, dette på tross av økt fokus på rapporteringskvalitet. Dog har rapporteringen på muligheter, risiko og respons på risiko blitt styrket. Det er positivt da det gir innsyn i hvordan selskapene evaluerer sin egen posisjon og hvilken retning de beveger seg i. Slik informasjon er sentral informasjon for interessenter å få tilgang til.

Rapporteringsraten er fortsatt høyere blant verdens 250 største selskaper enn på «landnivå». For de store selskapene har ekstern verifikasjon også blitt standard. Det gjøres for å styrke troverdigheten til informasjonen som rapporteres, samt å forbedre rapporteringssystemet internt. Vi forventer at de 100 største selskapene på nasjonalt nivå vil følge verdens største selskaper i både rapporterings- og verifiseringsomfang.

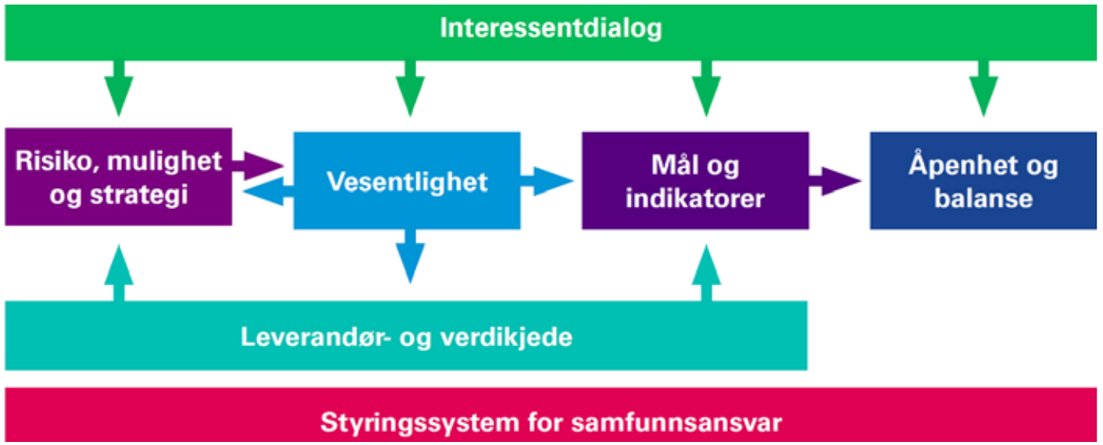
Vi ser også en stor fremvekst i rapportering på karbonutslipp. Med COP21[4] og den norske regjeringens ambisjoner som bakteppe, er det åpenbart at rammebetingelsene for norske bedrifter vil endres. Dette vil blant annet være i form av krav til utslippsreduksjoner og høyere klimakostnader, samt økte forventinger fra interessenter til rapportering på de finansielle følgene av klimaendringer. Halvparten av verdens 250 største selskaper rapporterer at deres arbeid med å redusere sine klimautslipp har hatt positive innvirkninger på selskapets drift. Positive innvirkninger innebærer reduserte kostnader, økt effektivitet og økt innovasjon i selskapet. Bilbransjen, logistikk og handel rapporterer oftest om fordelene, deretter følger olje- og gasselskapene.

God rapportering reflekterer god styring

Lovkrav er en av de sterkeste driverne for rapportering på bærekraft og samfunnsansvar. Men ved å heve ambisjonene utover myndighetskravene er selskapene bedre forberedt på fremtidige innstramminger i lovkrav og økte forventninger fra interessenter. At et selskap rapporterer, betyr ikke nødvendigvis at lovkravene og intensjonen bak disse innfris og at innholdet er relevant. Vår erfaring er at god rapportering er en konsekvens av god virksomhetsstyring. Vi opplever at selskapene som jobber strategisk og målrettet med samfunnsansvar og integrerer arbeidet i kjernevirksomheten, belønnes i form av redusert risiko, økt effektivitet og mer vellykket innovasjon. Slik skiller de ledende selskapene seg ut og skaper konkurransefordeler.

LISTE OVER SPØRSMÅL LEDELSEN (OG INTERNREVISJONEN) BØR STILLE SEG:

- I hvilken grad er virksomheten eksponert for fremtidige reguleringer, skatter og rapporteringskrav?
- Hvordan kan virksomheten vokse og samtidig redusere utslipp?
- Gjenspeiles styringen av selskapet i rapporteringen på bærekraft?
- Er vi ledende på bærekraft i vår bransje?



Figur 1: Syv suksesskriterier for god kvalitet i rapportering på bærekraft og samfunnsansvar[5].

Til tross for at flere selskaper rapporterer på sitt arbeid med samfunnsansvar og bærekraft, har ikke kvaliteten på informasjonen blitt merkbart bedre. God rapportering kjennetegnes ved at den får frem hvordan arbeidet med samfunnsansvar styrker øvrig drift, samt at informasjonen reflekterer arbeidet på en åpen og balansert måte. Syv suksesskriterier for god rapportering er illustrert i figuren under:

En god rapport bør forklare hvordan selskapet identifiserer sine nøkkelinteressenter og hvordan det forholder seg til disse. Det er spesielt viktig å vektlegge hvordan interessenter bidrar til å forbedre beslutningsgrunnlaget og hvordan deres innspill påvirker selskapets strategi.

Resultatene fra vesentlighetsanalysen bør fremgå i rapporteringen. Selskapet bør vise hvordan det kontinuerlig jobber med å identifisere hvilke aspekter som er kritiske for selskapets videre drift. Vi ser for eksempel at klimaendringer rapporteres oftere som vesentlig.

Det bør komme tydelig frem hvordan selskapet identifiserer muligheter og risiko og forklarer hvordan selskapet responderer strategisk. Globale trender viser et skifte i hvordan selskaper rapporterer på klimarisiko: I tillegg til å øke omfanget av rapporteringen ser vi tydeligere at selskaper rapporterer mulighetene som fremkommer av klimaendringer.

Ingen rapport på bærekraft og samfunnsansvar bør utgis uten forpliktelser i form av tidsbestemte og målbare ambisjoner. Beste praksis vil være å inkludere opprinnelig målsetting, evaluering av måloppnåelse og fremtidige ambisjoner. Selskapet får da gode styringsverktøy og det blir enkelt for interessenter å følge selskapets utvikling på området.

Troverdighet kan bare oppnås om det gis innsyn i utfordringer, ikke bare suksesshistoriene. Utfordringene, mål som ikke er nådd, begrunnelse og hvordan situasjonen skal håndteres bør være beskrevet i rapporten.

Behovet for åpenhet og håndtering av vesentlige aspekter inkluderer også arbeidet med underleverandører og verdikjedens påvirkning på kunder og sluttbrukere. En god rapport adresserer derfor miljømessige og sosiale forhold knyttet til leverandører og levering og bruk av produkter.

Rapporten bør inneholde en forklaring på hvordan hensynet til bærekraft og samfunnsansvar er ivaretatt i organisasjonsstrukturen. Det innebærer en forklaring av hvor ansvaret er plassert og hvilke incentiver og kontrollrutiner som er implementert.

Forventninger i fremtiden

Som følge av økte forventninger til bærekraft fra myndigheter og interessenter, forventer vi forsterket bærekraftsrapportering fremover. Hovedfokuset vil ligge på karbonfotavtrykk og aksjonærer vil forsikres om at risiko adresseres på en adekvat måte og at muligheter utnyttes. Dette innebærer også vektlegging av de finansielle følgene av klimarelatert risiko. Nylig har finansministrene i G20 landene nedsatt en arbeidsgruppe for å vurdere hvordan finansverdenen bør ta høyde for de finansielle følgene av klimarisikoer[6].

Strengere klimapolitikk og klimakostnader og høyere forventninger fra interessenter vil skape større muligheter og incentiver i lavkarbon-økonomien, og selskaper som i dag tjener på å være ledende innen bærekraft i sin bransje vil oppleve at konkurransekraften deres øker ytterligere: De som er forberedt på utviklingen vil se resultater i form av lavere kostnader, økt innovasjon og dermed økt aksjonærverdi. Ledelsen bør derfor spørre seg hvordan de kan vokse parallelt med fremtidige reguleringer, skatter, prising av utslipp og forventninger fra interessenter? Videre bør de synliggjøre verdiene de skaper og forringer for samfunnet, miljøet og aksjonærene gjennom god rapportering.

[1] *Currents of change, The KPMG Survey of Corporate Responsibility Reporting 2015.*
[2] *Listen over de 100 største norsk selskapene er basert på Dagens Næringslivs årlige liste med oversikt over inntjeningen til Norges største selskaper. Dataene ble hentet ut juni 2015.*
[3] *Listen over de 250 største globale selskapene er hentet fra Fortune Global 500 rangering for 2014.*
[4] *FNs 21. klimatoppmøte i Paris i november 2015.*
[5] *Bærekraft og samfunnsansvar – I hvilken retning beveger bedriftenes rapportering seg? KPMG, 2015*
[6] *Financial Stability Board: Task Force on Climate-related Financial Disclosures, 2016*

NYTT FRA NIRF

KURSAKTIVITETER 2016

PLANLEGG KURSKALENDEREN ALLEREDE NÅ OG SKAFF DEG VEDLIKEHOLDSPOENG (CPE) FOR ÅRET SOM KOMMER

CYBERSECURITY & SOCIAL MEDIA RISK: What every professional needs to know

13. juni 2016, 09.00 – 12.30

Social media is a dominant force in today's world of connectedness. Its use is still growing in all parts of the world, and with that, risk is growing exponentially. Within an organization, use of social media by different departments can compromise the reputation of the organization and staff. Changes in internet usage, such as the proliferation of mobile devices and the rising use of social media, have presented new challenges for cyber security.

As long as staff is connected and online, the risk of cyber-attacks is imminent. It is thought that the Sony hack in 2014 was the result of one staff member clicking on a malicious link in an email. This was confirmed as the reason hackers penetrated the New York Times in 2013. Neither of these actions could have been prevented by IT.

This session is designed for those responsible for governance and risk management to align strategies to adapt to the changing social media landscape.

- Discuss fallout from real life cases of cybersecurity breaches.
- Tips on cybersecurity strategies & social media policies.
- Discuss a pragmatic approach toward combating cyber threats.
- Corporate social media blunders
- What needs to be in the social media policy

You can also attend CYBERSECURITY & FRAUD: The basics of conducting online investigations, from 12.30 – 17.00 and get a discount. For both seminars NOK 3 800 for members and NOK 4 500 for non-members.

Lecturer:
Nejolla Korris

CYBERSECURITY & FRAUD: The basics of conducting online investigations

13. juni 2016, 12.30 – 17.00

This seminar focuses on the basics of online investigations for non-IT professionals. The internet is a valuable tool for gathering information and building investigation data. Learn how to use online search tools and databases efficiently and effectively. With the majority of the world's population on popular social media sites, people share more information online than ever before. Learn how social media and other online communities allow the investigator to gather evidence and other tools to bolster the investigation.
This interactive session will have course participants working with various case studies to illustrate how the internet can provide beneficial information to their investigation.
Learning outcomes:

- Expand your knowledge in the use of the internet for research and as an investigative tool
- Learn how to effectively use search engines to gather information
- Learn how to obtain information from social media sources.
- Access information from corporate and public record searches.

You can also attend CYBERSECURITY & SOSIAL MEDIA RISK: What every professional needs to know, from 09.00 – 12.30 and get a discount. For both seminars NOK 3 800 for members and NOK 4 500 for non-members

Lecturer:
Nejolla Korris, international expert in the field of Linguistic Lie Detection and she is a frequent presenter for The Institute of Internal Auditors, ISACA, the American Society for Industrial Security, the American Bar Association, the American National Safety Council, the American Institute of Certified Public Accountants and various fraud prevention groups. She was awarded the Queen's Diamond Jubilee Medal for her international work in linguistic lie detection.

Grunnkurs i Compliance

15. juni 2016, 09.00 – 17.00

Formålet med kurset er å gi deltakerne grunnleggende innføring i compliancefunksjonens organisering og rolle, samt se nærmere på hovedaktiviteter inn under funksjonens ansvarsområde. Innholdet i kurset er bransjeuavhengig, men det vil også bli gitt noen praktiske eksempler på lov og forskriftskrav, individuelle tilpasninger og egne erfaringer, i tillegg til diskusjoner og case. Kurset tar utgangspunkt i «beste praksis» og Veileder for compliancfunksjonen, utarbeidet av en arbeidsgruppe som selv jobber med compliance innen ulike bransjer.

Agenda

- Generelt om compliancefunksjonen og begrepsavklaringer
- De tre forsvarslinjer, hvem har ansvar for hva
- Etablering av compliancefunksjonen, herunder:
  - funksjonsbeskrivelse og ledelsesforankring
  - rapportering og uavhengighet
  - organisatorisk plassering og organisering
  - autoritet, informasjon, ressurser, kompetanse, avlønning
- Oppgaver, metode og hovedaktiviteter, herunder
  - risikotilnærming
  - rammeverk
  - compliancekultur; tonen på toppen, kommunikasjon og opplæring
  - avviksregistrering
  - varsling
  - monitorering
  - rapportering
  - integritetsundersøkelser (IDD)

Intervjuteknikk

23. - 24. august 2016, 09.00 – 16.00

Gjennom kombinasjon av teori, eksempler, analyser og flere praktiske øvelser fra deltakernes virkelighet, skal deltakerne få en forståelse for hva som skal til for å beherske intervjusituasjonen, forberede og ta kontroll over intervjuet og på den måten tilegne seg relevant viten på en effektiv og formålstjenlig måte i en revisjon. Det finnes ingen fasit på hvordan man gjennomfører et godt intervju, men kurset gir deltakerne innsikt i en utprøvd metodikk og hvordan den kan anvendes i praksis. Kurset tar for seg intervjuet som sjanger, hvordan en stiller de gode enkeltspørsmålene, hvordan en hindrer avsporinger eller ufrivillige sporskifter og hvordan en bestemmer mål og strategi for intervjuet.

Introduksjon til internrevisjon

14. september 2016, 09.00 – 17.00

På denne dagen vil vi gi en innføring i internrevisors roller og ansvar, begrepsavklaringer og definisjoner, samt hvilke etiske regler og hvilke krav som ligger i internrevisjonens standarder. Kurset gir deltagerne de nødvendige grunnkunnskaper i internrevisjon gjennom introduksjon til internrevisjonens rammeverk, spesielt rettet mot de obligatoriske delene. Innholdet i kurset er nødvendig basiskunnskap for kurset Praktisk Internrevisjon.

Slik skriver du rapporter som faktisk blir lest

15. september 2016, 09.00 – 17.00

Mye hardt arbeid nedlegges i å skrive rapporter, men rapportene får ikke alltid den gjennomslagskraften vi hadde håpet på. Gjennom denne dagen går vi igjennom basiskunnskapene og huskereglene du må kunne for å skrive godt og få egen stemme hørt.

- Hva bør en revisjonsrapport inneholde?
- Hvordan få frem det viktigste budskapet?
- Hvordan best kommunisere til de ulike interessentene?

Praktiske eksempler på rapporter på enkelt oppdrag, års- og kvartalsrapporter vil bli presentert med refleksjoner rundt struktur, innhold og format.

Praktisk internrevisjon

27. september - 29. september 2016, 09.00 – 16.00

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

- Planlegging
- Gjennomføring
- Rapportering
- Oppfølging
- Dokumentasjon
- Kvalitetssikring

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

Strategic thinking for internal audit

11. October 2016, 09.00 – 17.00

More and more organisations are teaching their key people to think strategically. This helps to anticipate issues, makes plans more effective and helps to ensure change is delivered more smoothly. This masterclass outlines a range of key techniques for effective strategic thinking and strategic influencing. The aim is to strengthen the ability of auditors to increase the impact of their work and anticipate and overcome disagreements.

Course programme

- Analysing your thought processes
- Balancing
- Detail with intuition
- Firmness with flexibility
- Reflection with consultation

KURSAKTIVITETER 2016

- Logic with feelings
- Balancing strategic thinking and tactical thinking
- Understanding the ways in which others think
- How this can aid negotiation and persuasion
- Understanding the ways others resist and the “hooks” to persuade them
- Learning to think Ahead
- One move ahead is not enough
- Envision the future
- Discover opportunities behind obstacles – explore patterns of behavior
- Action planning
- Concrete steps to enhance reporting
- Concrete steps to overcome resistance
- Actions to improve your reputation in the business

Presented by: James Paterson PIIA, Risk and Assurance Insights Ltd

Root cause analysis (RCA) and analysing audit themes

12. October 2016, 09.00 – 17.00

This master class is for experienced internal audit staff, managers and HIAs who want to look at best practices around analysing the root causes of their audit findings. Associated with this is the question of how to analyse themes from audit assignments in order to reveal key underlying problems in governance, risk and compliance that may need senior management or board attention.

Course programme

- What does the IIA say about Root cause analysis including the latest update from the IIA UK
- The origins of robust root cause analysis and why root cause analysis can be difficult
- Practical applications of 4 key root cause techniques
- 5 whys, Fishbone diagram, Pareto and Logic tree
- Examine the ways to ensure RCA work does not delay assignments
- Looking at the ways effective RCA can help deliver shorter, more impactful audit reports
- the importance of having appropriate RCA categories (beyond traditional risk categories) so that audit findings can be properly themed
- Understand how RCA and thematic analysis play a key role in understanding risk culture.

Presented by: James Paterson PIIA, Risk and Assurance Insights Ltd

Cybersecurity: for ikke-spesialister

19. oktober 2016, 09:00 - 16:30

Cybersecurity er et IT-tema som både er på styrenes og toppledernes agenda, og som rangerer høyt på de fleste internrevisorers risikokart. Cybersecurity har seilet opp som nr. 1 av topp ti risikoer i flere undersøkelser, bl.a IIAs CBOK «Navigating Technology’s Top 10 Risks, Internal Audit’s Role», COSOs «COSO in the cyber age» og KPMGs «Top 10 key risks in 2015». IIA og ISACA har også publisert «Cyber-security – what the Board of Directors needs to ask»
Hvordan skal internrevisor angripe dette ut i fra et ikke-spesialist perspektiv?
Kurset er under utvikling og et mer detaljert program publiseres siden. Rammen for kurset vil være:

- Cyber Security (CS) i et topplederperspektiv
- «Top ten questions to ask» – fra styret til toppledelsen og fra internrevisor til toppledelsen
- Hvordan revidere CS ut fra et modenhetsperspektiv
- Hvordan revidere CS ut fra et annet perspektiv enn modenhet

Kurset vil belyse hvilke risikoer som er mest aktuelle, og hvordan internrevisor kan planlegge og gjennomføre en internrevisjon uten å være ekspert.

Fra revisor til Fraud Wizard

1. november – 2. november 2016, 12.00 dag 1 til 12.00 dag 2

Selv om det kan være ulike meninger om i hvilken grad revisor har plikt til å finne misligheter eller ikke, er det bare de som leter som finner misligheter og korrupsjon. Dette gjelder både eksterne og interne revisorer, for så vel de som jobber med revisjon i kommunal og statlig sektor. Målet med kurset er å vise hvordan vi alle kan vi bli betydelig flinkere til å oppdage signalene på misligheter og korrupsjon.

Kurset går fra starter med lunsj klokken 12.00 tirsdag 1. november og avsluttes med lunsj onsdag 2. november.
I kursprisen inngår også hotellrom, da det vil bli case og diskusjoner med gjesteforeleser under middagen første kvelden. Deltakerne har mulighet til å velge mellom to spor (privat eller offentlig sektor) under deler av kurset. Ved bruk av case og realistiske dokumenter vil teknikker og metoder bli demonstrert gjennom en interaktiv og veiledende workshop.

Les mer om alle kursene og meld deg på via vår nettside www.iia.no.

Risk management og målstyring hånd i hånd

INTERVJU MED
EYVIND AVEN,
VICE PRESIDENT RISK MANAGEMENT, STATOIL

Eyvind Aven leder Statoils Enterprise Risk management enhet. Aven har vært en av nøkkelbidragsyterne til oppbyggingen av Statoil sin risikostyring på konsernnivå siden oppstarten på slutten av 90-tallet.

Av
MARTIN STEVENS
Internrevisor, Gjensidige

Historisk har det vært to forskjellige interne miljøer innen virksomhetsstyringen. På den ene siden er det et miljø med økonomisk bakgrunn som har hatt fokus på målstyring og Key Performance Indicators og på den andre siden et risikostyringsmiljø som har arbeidet med temaer som risikoappetitt og Key Risk Indicators. Statoil har arbeidet med å bygge en bro mellom disse to miljøer og jeg tok kontakt med Eyvind Aven, Vice president Risk management, Statoil for å høre nærmere om dette.

Risk management som egen profesjon er ung. Det er de færreste som jobber med risk management som har hatt dette som fag på ved skole/universitet. Hva er din bakgrunn og hva slags bakgrunn har de som arbeider i Risk Management hos dere ?
Min bakgrunn er som siviløkonom fra NHH med fokus på finansteori og bedriftsøkonomi. Jeg startet som bedriftsrådgiver i bank før jeg gikk over til Statoil i 1992. Der jobbet jeg med strategi og økonomisk analyse på konsernnivå og innenfor naturgass før jeg begynte fulltid med helhetlig risikostyring (ERM) i 1999 sammen med Petter Kapstad. Sammen utviklet vi Statoils ERM funksjon. Mye av læringen har vært å utfordre etablerte sannheter, diskutere med kollegaer i tilsvarende stillinger i andre industriselskaper og banker.

Ellers i enheten er det folk med utdannelse primært innenfor økonomifagfeltet, men som har erfaring fra ulike områder som gassmarkedsanalyse, gasskontrakter, forsikring, midoffice trading, trading support, styrende dokumentasjon og investeringsanalyser.

Meg bekjent finnes det ingen autoritativ definisjon av Risk. Hvordan definerer dere Risk i Statoil og hvorfor har dere valgt denne definisjonen?
Vår definisjon bygger på ISO31000, moderne risikostyringsteori og hva vi har sett er relevant innenfor ERM i bedrifter. ISO31000 sin generelle definisjon gjelder for enhver organisasjon og er koblet direkte mot måloppnåelse. Et viktig spørsmål her er hvilke mål er det snakk om? I ERM kontekst er det viktig at risikostyring understøtter bedriftens overordnede mål som er å skape verdier og unngå negative hendelser som f.eks. ulykker. Videre var det viktig at risikostyringen støtter opp om de overordnede målene og ikke bare handler om å øke sannsynligheten for å oppnå KPI-mål. Sistnevnte tilnærming kan lett føre til suboptimalitet og risikostyringen må utformes på en måte som reduserer faren for dette. I tillegg er ofte usikkerheten i analysene undervurdert. Moderne risikostyringsteori kobler risikostyring mot aktivitene i en bedrift uavhengig av mål og med denne bakgrunn definerte vi risiko som avvik i forhold til en referanseverdi med tilhørende usikkerhet. I 2015 kom for øvrig Petroleumstilsynet med ny definisjon for risiko som også var i samme gate: «Risiko er konsekvensene av virksomheten, med tilhørende usikkerhet».

Statoils definisjon av risiko

Avvik i forhold til en referanseverdi med tilhørende usikkerhet

Jeg regner med at dere har etablert ERM i Statoil, har dere en egen definisjon på dette? Føler du at det avviker fra andre selskapers definisjon?
Enterprise Risk Management (ERM) handler om å drive risikostyring på vegne av Statoil på en måte som støtter de overordnede målene for en bedrift som Statoil, dvs. verdiskaping og unngå uønskede hendelser. Risikoene oppstår som følge av våre aktiviteter i verdikjeden og konsekvensene for Statoil måles i nåverdi etter skatt for pengerisikoer og i forhold til en pre-definert skala for skade på mennesker og

integritetsrisikoer. Ofte er risikostyringen ikke klar på om en ser på konsekvensen for Statoil eller for en oppgave. For sistnevnte bruker vi begrepet Task Risk Management (TRM) med fokus på konsekvenser i forhold til oppgavens leveranse (dvs. kost, tid og kvalitet). ERM og TRM gir som regel samme prioritering, men

> I Statoil skiller vi mellom ERM (Enterprise Risk-Management) og TRM (Task Risk Management) med fokus på oppgavens leveranse (dvs. kost, tid og kvalitet).

ikke alltid. Vi har derfor beskrevet i våre styrende dokumenter at ERM skal ha fortrinnsrett overfor TRM dersom konflikter skulle oppstå.

Mitt inntrykk er at de fleste industriselskaper har samme intensjon med ERM, men at mange ikke har tatt innover seg hvordan målhierarkiet påvirker risikostyringen. Dermed kan det oppstå suboptimalitet, som ikke blir ordnet opp i.

Jeg forstår Statoil forsøker å koble sammen Risk Management med målstyringsarbeid. Tradisjonelt har disse to ledelsesprosesser hatt utspring i forskjellige miljøer risk management og controllermiljø. Hvorfor du mener det er viktig å kombinere disse to prosesser og hvordan dere jobber sammen?
Dette tror vi er et viktig steg i riktig retning for virksomhetsstyringen. En ledergruppe behøver å se sitt målstyringsarbeid og risikostyring samlet. Selv om vi mener prosessene er atskilte kan de koordineres på en måte som gavner helheten. F.eks. vil målstyringsarbeidet ha godt av å koble styringen tettere mot strategiske mål og risikoen knyttet til disse og ikke bare mot KPI mål. KPI'ene er indikatorer og skal vise om vi er på rett vei. Feil bruk av målstyring, dvs. primær fokus på mer eller mindre gode KPI mål og mindre på de strategiske målene kan lett medføre suboptimale beslutninger. En overforenklet risikostyring vil ikke kunne hindre dette og vi legger derfor opp til at risikostyringen kobles opp mot de strategiske målene. Disse må igjen være kalibrert mot de overordnede målene som er å skape verdi og unngå hendelser.

Det finnes utallige eksempler på risikostyring som støtter misforstått målstyring. Vi forsøker å finne en løsning der risikostyringen og målstyringsarbeidet sammen støtter oppnåelse av de strategiske målene.

Men er det slikt at dette har betydd en omdefinisjon av rollen til Risk Management? Har man overlatt deler av sine oppgaver til controllermiljø?
Jeg er vel heller av den oppfatning av at risikostyring alltid har vært en integrert del av ledelse, men at den ikke har fått nok oppmerksomhet etter hvert som verden rundt oss har blitt mer og mer komplisert. Risikostyringen er ikke blitt strukturert nok behandlet. Et sentralt spørsmål i risikostyring er risiko for hvem? Når dette ikke er avklart vet en ikke om risikostyringen støtter de overordnede målene til en bedrift.

En god controller vil også være opptatt av risiko i beslutninger, men har ofte hovedfokus på resultater, målstyring og performance i forhold til det samt beslutningsstøtte. Controller vil derfor sammen med spesifikk risikokompetanse gjennom Risk management-miljøet kunne bidra med et bedre beslutningsunderlag for ledelsen.

Alle gode ideer skal være win/win for begge parter? Hvordan ser du fordelene for begge parter med en nærmere integrering av risikostyring og controllervirksomhet? Det er forhåpentligvis slik at totalen blir større enn bare å legge sammen de to oppgavene?
Helt enig, en koordinert risikostyring og controllervirksomhet vil forbedre ledelsesprosessen, både på løpende oppfølging, men mest på beslutningsstøtte og strategiarbeid. Risk management handler ikke om å gå inn i controlleren sine oppgaver, men å utvide perspektivet i begrepet ledelse, sikre bedre beslutninger særlig i tilknytning til nye prosjekter og fremtidig risikoprofil. Risikostyring vil synliggjøres gjennom strategiske beslutninger og veivalg.

Hvor ser du utviklingen i Rrsikostyring som fag beveger seg? Er det å konsolidere dagens status eller er det nye utviklingsområder på horisonten?
Risikostyring som fag er ungt og de som tok utdanning før år 2000 hadde lite om dette. Innenfor økonomiske fag var det primært finansiell risikostyring og da relatert til aksjer osv. Nå snakker vi mer om å få risikostyring integrert med de andre ledesesprosessene og der i gjennom få en betydelig større påvirkningskraft i bedriftene. For fremtiden ser jeg at forholdet mellom risikostyring og styret eller representanter for styret kan få en viktigere betydning, særlig med utviklingen mot Chief Risk Officer som større banker etter hvert har fått.

> «Det finnes utallige eksempler på risikostyring som støtter misforstått målstyring. Vi forsøker å finne en løsning der risikostyringen og målstyringsarbeidet sammen støtter oppnåelse av de strategiske målene.

ANMELDELSE

Corruption the musical?

Av
MARTIN STEVENS
Internrevisor, Gjensidige

REIDAR DØLI
Internrevisor, Oslo Børs VPS

En musikal om korrupsjon? På et sted som heter «Ingensteds»? Dette gjorde sitt til at nysgjerrigheten ble pirret. Lokalene var fullsatt på premierekvelden og vi publikummere fikk servert en monolog ved manusforfatter og for anledningen skuespiller Nigel Krishna Iyer som var illustrert med sang og musikk.

Den innbitte korrupsjonsjeger grubler over hva som skal til for å åpne øynene for at korrupsjon begås av nordmenn i Norge. Dette er ikke et fenomen som opptrer kun ved fremmedfolk under fjerne himmelstrøk. Hans ide er at denne problematikken må det la seg gjøre å kommunisere gjennom å lage en musikal. Handlingen i en musikal må være engasjerende. Det er den utformingen av dette musikalmanuset som stykket handler om.

Musikken var skrevet av Sigrun Merete Mongstad. Hun stod også for deler av fremføringen. Musikken både myknet opp det ellers så tørre temaet og ga det et medmenneskelig perspektiv. Hun sang blant annet om hvordan ektefellen til en korrupsjonskurk opplever sin eksistens. Fra musikken kom også leitmotivet «nothing ever changes» som understrekte korrupsjonsjegerens opplevelse av at det er ingen vilje blant ledere og politikere til virkelig å ta tak i korrupsjonsbyllen.

Dette var underholdning men det var underholdning real life. Korrupsjon eksisterer og skjer blant oss. Høydepunktet for var i valg av avslutning til den tiltenkte musikalen. Kanskje løsningen er å drepe

den som fremmer budskapet slik at alt og alle kan fortsette som før.

For vår del er vi klar til å kjøpe billett til musikalen «Corruption» når den tiden kommer. Det store spørsmålet er om den vil få den nødvendige finansieringen, og hvis ikke, hvorfor ikke? Mens man venter på musikalen er et godt alternativ å se stykket om den. Men vær forberedt på at du kan miste troen på at vi opptrer så etisk forsvarlig her på berget som vi liker å tro.

Det er også verdt å nevne at Nigel Iyer sitt prosjekt fikk et solid etterspill i Dagens Næringsliv der stykket og de tema som ble tatt opp fikk flere siders spalteplass fredag 18. mars, med oppfølgingssaker både lørdag 19. mars og påfølgende mandag.

Det var en gang

Av
MARTIN STEVENS
Internrevisor, Gjensidige

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

I 2003 fusjonerte Norsk Finansrevisorforeningen inn i NIRF. Forening begynte sitt liv som Norsk Bankrevisorforening og ble grunnlaget i 1921. Medlemsbladet deres het først Bankrevisoren før det skiftet navn til Finansrevisoren.

For 20 år siden

Etter å dømme fra sommerutgaven av Internrevisoren for 1996 har vi med en aktiv forening å gjøre. Det fortelles om konferansen på Sundvolden hotell med rekordoppslutning av 118 deltagere. Blant temaene var CoCo modellen for internkontroll, Egenevaluering av internkontroll og Ledelsens forventninger til intern revisjon. Hvis man trodde at det siste er noe vi begynte å fokusere på i de siste årene tar man grundig feil. En viss ansatt fra Kredittilsynet var på hugget her, som man kan lese fra reportasjen:

Anne Merethe Bellamy, Kredittilsynet hadde første innlegget og stilte oss raskt to kritiske spørsmål: Hvor mange av de tilstedeværende mener å være en merverdi for organisasjonen? Og: Hvor mange oppfattes å være av merverdi til toppledelsen? Forsiktige armer gikk opp og ned og noen følte seg litt utrygge på morgenkvisten.

Internrevisjon er et yrke i forandring. Har vi gjort nok med kommunikasjon, vet vi hvem kundene våre er og hva er egentlig produktet vårt?.....I alt for lang tid har vårt yrke vært en forlengelse av økonomifunksjonen. Endringer i rammebetingelser, teknologi, større kompleksitet i prosessene og globalisering er noen av de utfordringer vi møter. Vi må frem i lyset. Vi må markedsføre oss. Vi må forbedre oss.

Nesten litt skremmende å tenke at de utfordringer som Anne Merethe ga uttrykk for er nesten like aktuelle i dag bortsett fra at det er de færreste som ser på oss i dag som en forlengelse av økonomifunksjonen, i hvert fall håper og tror jeg det!

Kloke ord fra Internrevisoren 1996:

«EDB er utmerket til å løse problemer som ikke ville ha oppstått hvis vi ikke hadde hatt EDB»

Prof. Knut Fægri i Naturen 1974.

Dataanalyse – en ny hverdag for internrevisjonen?

Av
MAGNUS DIGERNES
Senior Manager KPMG

Av
OLE WILLY FUNDINGSRUD
Director KPMG

Det sies at informasjon er det 21. århundres olje, og dataanalyse er motoren. Denne artikkelen tar for seg hva dataanalyse er og betyr for internrevisjonen, dagens status på bruk av dataanalyse i internrevisjonen og hvordan internrevisjonen bør bruke dataanalyse.

Hva betyr dataanalyse for internrevisjonen?

Den nylig utgitte boken «Dataanalytics – Elevating Internal Audit›s Value»[1] definerer dataanalyse som «prosess for å samle og analysere data for å bruke resultatene til bedre beslutninger». Boken har flere illustrative eksempler som kan anvendes for å forklare begrepet dataanalyse:

- Analyse av operasjonell, finansiell og andre data som kvantifiserer og belyser risiko og/eller muligheter
- Analyser på tvers av flere kilder
- Analyse av mønstre, trender og avvik gjennom automatiske og repeterbare prosesser

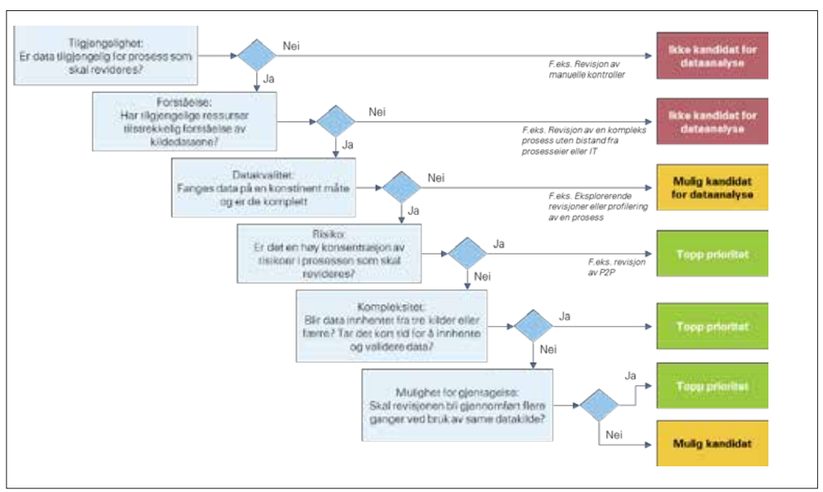
Boka definerer fire typer av dataanalyse; deskriptiv, diagnostisk, prediktiv og normativ. Den deskriptive datanalysen er den minst avanserte, men er den mest brukte. Eksempler på bruk av de ulike metodene i internrevisjonen beskrives i tabellen under

Status for bruk av dataanalyse i internrevisjon

I en nylig undersøkelse foretatt av KPMG og Forbes, hvor mer enn 400 CFOs og ledere i revisjonskomiteer ble forespurt, fremkommer det at 63% av internrevisjonene benytter seg av dataanalyse i isolerte eller spesifikke tilfeller[2]. Denne andelen forventes å synke innen de neste tre årene til fordel for en mer integrert bruk av dataanalyse.

KPMG Sør-Afrika foretok en undersøkelse blant internrevisjoner og konkluderte at 78% av internrevisorer oppfattet at dataanalyser gir dem merverdi.[3] Dette underbygges av IIA undersøkelsen «Data Analytics and Internal Audit Survey 2015» som viser at nesten 90% av alle respondentene mener at virksomheten vil benytte seg av dataanalyse i større grad i de neste 3-5 årene. Samtidig svarer 69% at de ønsker mer fokus på dataanalyse i virksomheten.

Et eksempel på en prosess som bør defineres er om dataanalyse bør inkluderes i et revisjonsprosjekt slik illustrert under[4]:



Type analyse	Forklaring	Eksempel
Deskriptiv	Rapportering på tidligere hendelser for å beskrive hva som har skjedd. Innebærer innhenting av en større datamengde brutt ned til mindre, mer meningsfulle biter av informasjon uten videre analyse.	Analyse av alle identifiserte utbetalinger på lørdager med størrelse over kr 10 000
Diagnostisk	Gir innsikt i hvorfor enkelte trender eller spesifikke hendelser oppstår. Inndeling av data I ulike måter, f.eks. pr. produkt, region eller kunder, gjør det enklere å forstå sammenhenger og årsaker.	Analyse av utbetalinger identifiserer Per Olsen, avdelingsleder som godkjente alle utbetalingen over kr 10 000 på lørdager
Prediktiv	Analyse som gjør det mulig å hente ut informasjon fra store datamengder, legge til forutsetninger og vurdere korrelasjoner for å kunne forutsi fremtidige resultater og trender	Analyse av utbetalinger på flere lokasjoner identifiserer alle utbetalinger på lørdager over kr 10 000 og definerer ulike attributter til hver hendelse, som f.eks. antall leverandører og periodisering i hver måned
Normativ	Normative analyser krever et store mengder data for først å vurdere fremtidige hendelser, og deretter vurdere tiltak som vil medføre beste resultat. Der prediktiv analyse besvarer «hva etterspørselen vil bli», besvarer normativ analyse «hvilke tiltak bør iverksettes for å maksimere profitt hvis etterspørselen er 100%?»	Analyser som bygger og tester scenarier rundt ulike rutiner for å vurdere hvilke tiltak som kan redusere antall utbetalinger på lørdager over kr 10 000

Hvordan kan internrevisjon i større grad integrere dataanalyser i sitt arbeid?

I boka «Dataanalytics – Elevating Internal Audit›s Value» fremstilles et rammeverk for å styrke tilnærmingen og bruk av dataanalyse i internrevisjonen. Dette rammeverket består av fire steg;

1. Utvikle en visjon for hvordan dataanalyse skal støtte internrevisjonen. Dette innebærer å definere fordelene ved å bruke dataanalyse og utvikle en strategisk plan for bruk av dataanalyse i internrevisjonen.
2. Evaluer dagens situasjon. I boka skisseres en modenhetsmodell hvor dimensjonene ressurser, prosesser og teknologi vurderes opp mot god praksis.
3. Utvikle og styrke ansattes kompetanse, prosesser og teknologi. Dette kan innebære strategiske initiativ som f.eks. samarbeid med andre miljøer i virksomheten, og vurdering av teknologiske løsninger.
4. Implementer, følg opp og videreutvikle. Implementering av et dataanalyse i internrevisjon er i stor grad endringsledelse, og forankring hos ledelsen er viktig. Videre er det sentralt å måle resultater underveis og være klar over at mulighetene innen dataanalyse er i stadig endring.

For å løse disse utfordringene er det nødvendig at internrevisjonen har tilstrekkelig med ressurser og kompetanse innen dataanalyse, prosesser for å utføre dataanalyse og rett teknologi.

Internrevisjoner har flere utfordringer når det gjelder å integrere dataanalyse i sitt arbeid. De største utfordringene fremkommer i IIAs undersøkelse «Data Analytics and Internal Audit Survey 2015» som viser:

- Vanskeligheter med å skaffe og/eller få tilgang til data
- Begrensinger på tid det tar å lage analytiske prosedyrer
- Manglende ressurser eller behov for å gi opplæring
- Manglende forståelse for dataanalyse
- Manglende forståelse fra ledelsen
- Manglende forståelse i tolkningen av resultatene

Konklusjon

Det er ingen tvil om at bruk av dataanalyse vil bli stadig mer viktig for alle virksomheter. Internrevisjonen er i en unik posisjon til å gripe denne muligheten ved å bruke dataanalyse strategisk, etablere strukturerte prosesser og bygge kompetanse. For at internrevisjonen skal utnytte dataanalyse på en best mulig måte og for å møte utfordringene dataanalyse byr på, bør et rammeverk etableres. Ved bruk av et slikt rammeverk kan internrevisjonen bl.a. vurdere dagens situasjon og hvilke strategiske grep som skal iverksettes.

[1] «Dataanalytics – elevating internal audit›s value» Warren W. Stippich Jr., og Bradley J. Preber, The Institute of Internal Auditors research foundation 2016
[2] KPMG International «Seeking value through internal Audit» Februar 2016
[3] KPMG Sør-Afrika «Data & Analytics-enabled Internal Audit» 2015 Survey.
[4] Illustrasjon fra «Data & Analytics Discussion» KPMG US 2015

Hvordan bruke blokkjedet i finansnæringen?

Av
ESA LEPORANTA
Systems Audit Manager,
Nets Branch Norway

Scott Rosenberg skrev i sin artikkel, *There is a blockchain for that*[1] , at «blokkjedet» representerer noe nytt som er litt vanskelig å forstå og anvende. For oss som ikke arbeider innen IT, virker det såpass fjernt at det heller ikke oppfattes som relevant. Samtidig er utviklerne ivrige til å utforske de muligheter teknologien tilbyr, og penger fra investorene strømmer inn. Ved en rask sammenligning kan dette ligne på det som skjedde da Web ble introdusert for 20 år siden.

Hva er egentlig blokkjede-teknologi?

I sin enkelhet er blokkjedet (på engelsk: blockchain) en teknologi som kan anvendes for å sende et digitalt budskap mellom to aktører, hvor begge kan stole på integriteten av budskapet uten engang å vite hvem den andre aktøren er. Det betyr at teknologien kan anvendes for å spore opp og gjennomføre transaksjoner online uten å bruke en klarert tredjepart, og forventes dermed å generere betydelige endringer i dagens kostnadsmodeller for finansiell transaksjonsprosessering.

I dagens samfunn er vi avhengige av at myndighetsorganer eller andre virksomheter bekrefter kildeautentisiteten. Det samme gjelder for øvrig for Internett hvor enkeltstående servere sikrer bruken av det eksisterende domenesystemet.

Noen av hjernene bak blokkjedet mener at teknologien kan anvendes til å redusere kostnader og øke konsumet. I tillegg gir det en mulighet til å moderere makten til banker og kreditkortgiganter. Andre er ute etter å sikre vår rett til privatliv og kommunikasjon ved å frigjøre oss fra aktører som FSA og Facebook. De mest radikale tror at vi faktisk kan klare oss uten dagens myndighetsorganer ved bruk av avansert matematikk som er kjernen i blokkjede-teknologien.

Blokkjede i banknæringen

Banker og andre relaterte næringer har etter hvert overkommet sin innledende mistenksomhet over blokkjede-teknologien, og ledende virksomheter arbeider i dag intensivt for å teste ulike løsninger for å effektivisere sine virksomheter. Ifølge en rapport laget av Santander, Oliver Wyman og Anthemis Group, skal det være mulig å redusere bankenes infrastrukturkostnader opptil $20 milliarder per år fra 2022[2].

> Blokkjedet forventes å generere betydelige endringer i dagens kostnadsmodeller for finansiell transaksjonsprosessering.

Det er spesielt innen to områder det forventes klare kostnadsfordeler: 1) Ved realisering av raskere prosesseringstider, og 2) ved redusering av kapitalmengden som bankene må stille i sikkerhet mot hver transaksjon.

Løpende utvikling innen blokkjede-teknologien

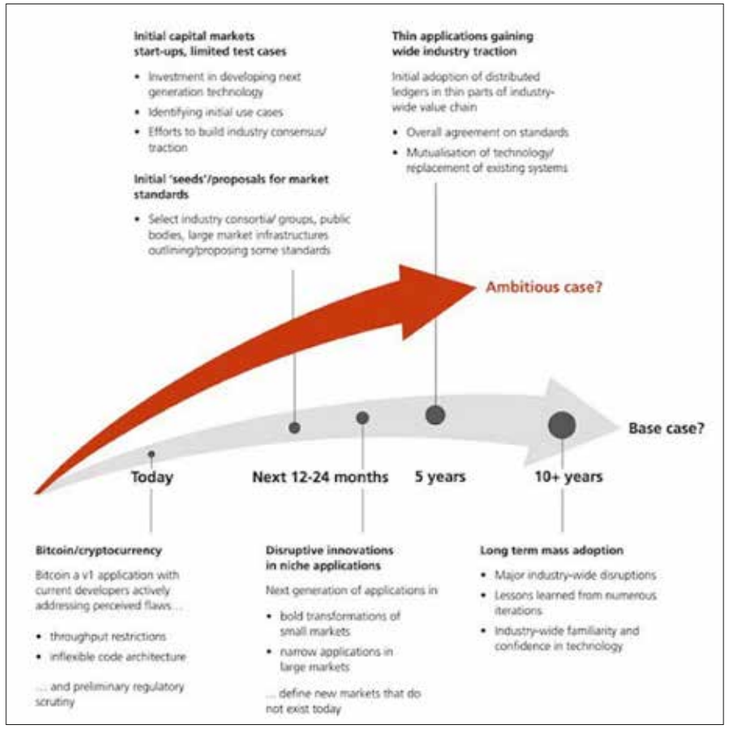
Før blokkjede-teknologien endelig kan tas i bruk gjenstår det en del arbeid, spesielt innen sikkerhet av teknologien som ikke har blitt løst tilfredsstillende i dag. Det gjelder blant annet desentralisert arkitektur hvor hver og en av aktørene skal ha like rettigheter. Det er heller ikke avklart hvordan teknologien kan skaleres opp for å innfri de volumkrav som finnes i den globale finansverden[3]. I slutten av 2015, ble det anslått at det skulle eksistere 12 millioner «Bitcoin wallets», uten at det er helt kjent hva som ble utfallet. Generelt, vil verdien av kryptovalutaer variere mer enn verdien av vanlige valutaer. Dette forklares med at det ikke finnes noen pengepolitikk som styrer størrelsen og vekst av pengemengden uten en sentralbank[4] som regulerer markedet.

Ettersom teknologien til blokkjedet gradvis har utviklet seg videre, har fokuset blitt flyttet vekk fra håndtering av kryptovalutaer til registering av fysiske dokumenter. Ved bruk av blokkjedet, kan brukeren i dette tilfellet lagre signaturen og tidsstemplet som er knyttet til dokumentet i blokkjedet. Eieren av den private nøkkelen til denne fortegnelsen vil samtidig bli registrert som en eier av eiendelen. Factom er et eksempel på et firma som tilbyr slike digitale applikasjoner ved bruk av blokkjedet.

Ethereum[5] er en annen aktør som har tatt konseptet med blokkjedet et steg videre gjennom å skape en modell for distribuert transaksjonsprosessering. Dette konseptet er et verktøy som kan anvendes for å implementere blokkjede-teknologien på helt nye bruksområder, og det uttalte målet er å kunne tilby løsninger hvor enkeltindivider kan kommunisere med hverandre globalt uten sentralisert koordinering.

> Banker og andre relaterte næringer har etter hvert overkommet sin innledende mistenksomhet over blokkjede-teknologien, og ledende virksomheter arbeider i dag intensivt for å teste ulike løsninger for å effektivisere sine virksomheter.

Bitcoin transaksjoner har blitt kritisert for at de blir bekreftet av anonyme deltagere som belønnes for sitt bidrag for fellesskapet. Dette har medført at noen av verdens største banker[6] har etablert en privat blokkjede gjennom et firma, R3CEV, som kun er åpen for inviterte medlemmer. Fordelen med dette er at alle deltagere har legale identiteter. Målet med dette nettverket er å etablere en bransjeomfattende plattform for å standardisere teknologien. Nettverket[7] består i dag av totalt 42 banker[8].



Bilde 1: Alternative utviklingsscenarier innen blokkjede-teknologien[15]

Blokkjede-teknologiens betydning for aksjemarkedene

The Securities and Exchange Commission (SEC) i USA har godkjent en plan fra selskapet Overstock.com til å utstede aksjer gjennom Internett ved bruk av en blokkjedebasert teknologi. I henhold til Patrick Byrne, administrerende direktør i Overstock.com, kan teknologien erstatte de systemer som brukes i dag av NewYork og NASDAQ børser. NASDAQ har også selv undersøkt hvilke fordeler denne teknologien kan tilby for å støtte transaksjoner mellom private virksomheter[9], ved bruk av sitt eget LINQ blokkjede, som utvikles i Estland[10]. Det er også forsket på hvordan denne teknologien kan anvendes for å øke kundeopplevelsen ved å effektivisere «kjenne din kunde»-prosessen[11], som skaper betydelige kostnader for banknæringen. Ved bruk av blokkjede-teknologien kan en serviceleverandør gjøre dette arbeidet på vegne av banken og lagre informasjonen digitalt i blokkjedet for fremtidig bruk[12].

Verdipapirsentralen i Australia, Australian Securities Exchange, presenterte i midten av februar i år sine planer for å flytte deres aksjeoppgjørssystem til

[1] *Scott Rosenberg, There's a blockchain for that, Backchannel, 13. Januar 2015 - https://backchannel.com/how-bitcoins-blockchain-could-power-an-alternate-internet-bb501855af67#.2xeajtr03*
[2] *http://santanderinnoventures.com/fintech2/*
[3] *Financial Times, Technology: Banks seek the key to blockchain, 01. November 2015*
[4] *EVRY, Whitepaper, Bank 2020 – Blockchain powering the internet of value.*
[5] *Capgemini, Blockchain: A Fundamental Shift for Financial Service Institutions.*
[6] *JPMorgan, UBS, Barclays, Bank of America, Credit Suisse, Deutsche Bank, Goldman Sachs, og Morgan Stanley, inklusive nordiske banker som Danske Bank, Nordea, OP Pohjola og SEB. Noter at listen ikke er uttømmende.*
[7] *Også kjent som Distributed Ledger Group eller DLG*
[8] *www.R3CEV.com, per 27. Februar 2016*
[9] *www.wired.com - SEC approves Plan to Issue Stock Via Bitcoin's Blockchain, 15. December 2015*
[10] *Financial Times, Australia is in the vanguard of blockchain's march to market, 17. Februar 2016*
[11] *Også kjent som «Know you Customer» eller KYC prosedyre*
[12] *M-Brain, Blockchain holds potential to transform the traditional banking industry, 29. Januar 2015*

blokkjedet i samarbeid med Digital Asset Holdings (DAH), som ledes av den tidligere JPMorgan bankieren Blythe Masters. Selv om DAH sies å ha en prototyp som fungerer, så er systemet ennå ikke ferdig til å tas i bruk. Ifølge en rapport laget av Oliver Wyman[13] og Euroclear[14], kan utviklingen av teknologien ta ytterligere ti år (se bilde 1 på side 37).

Samtidig har Bob Greifeld, administrerende direktør i NASDAQ, sagt at teknologien er den enkle delen av prosessen ved introduksjon av en blokkjede. Det som blir vanskelig er å få alle aktørene samlet og gå i takt. I tillegg er kompleksiteten i det amerikanske markedet betydelig større enn i Australia, som har brukt milliarder av dollar for å skape raskere clearingsystemer i løpet av de siste årene.

Hva har vi gjort i Norge?

I Norge har Bankenes Standardiseringskontor (BSK) satt temaet rundt digitale valutaer på agendaen gjennom å lage et diskusjonsnotat[16] som kort oppsummerer deres tanker om teknologien og hvilke steg det planlegges videre innen dette området.

Oppsummering

Forventninger til blokkjede-teknologien er enorme, selv om de teknologiske løsningene foreløpig ikke er ferdige. Samtidig tas det stadig nye skritt fremover og de store globale aktørene er i gang for lengst.

I slutten av februar 2016, ble det kjent at IBM har gitt ut 44.000 åpne kildekodelinjer med blokkjede-koder for å hjelpe utviklere innlemme teknologien i sitt arbeid.

Utenfor finansverdenen blir det utviklet blokkjede-programmer for eiendomsmegling, back office-systemer, streaming av musikk og kjøp av diamanter.

Gitt satsningen innen blokkjede-teknologien den siste tiden, er det delte meninger om hvilke begrensninger som finnes ved bruk av denne nye teknologien, og det blir interessant å følge med hva som vil skje fremover.

[13] Et globalt firma innen management consulting
[14] en europeisk verdipapirsentral
[15] http://uk.businessinsider.com/oliver-wyman-report-on-blockchain-adoption-in-capital-markets-2016-2?r=-DE&IR=T
[16] Terje Sletbak, Om digitale valutaer og bruk av Blockchain i finansnæringen, 2. November 2015.

Hvem har ansvar for at internkontrollen fungerer?

Av
STYRET I NIRF

I de siste dagers medieoppslag kan man få et feilaktig inntrykk av at internrevisjonen har ansvaret for at internkontrollen fungerer tilfredsstillende. Økt kompleksitet i mange typer virksomheter har de siste par tiår tydeliggjort betydning av god og effektiv eierstyring og selskapsledelse. Forventingene til oppfølging og kontroll fra styrer og ledelse er høye, og riktig bruk av internrevisjonen gir god støtte i dette arbeidet

Både lovgivning og internasjonal beste praksis slår fast at det er styret som på vegne av eierne har ansvaret for forsvarlig forvaltning. En viktig del av rolleutøvelsen skal skje gjennom å påse at virksomheten er godt styrt og kontrollert. Daglig ledelse har ansvaret for å gjennomføre styring og kontroll og sørge for at risikostyringen er organisert og gjennomføres på en betryggende måte. Det er også ledelsens ansvar å gi styret et dekkende bilde av risiko- og kontrollsituasjonen. Denne rolledelingen mellom styre og daglig ledelse er helt sentral i god eierstyring og virksomhetsledelse.

I større virksomheter har gjerne ledelsen sikret seg en ekstra trygghet for at styring og kontroll er tilfredsstillende ivaretatt gjennom bruk av kontrollfunksjoner for risikostyring og compliance. Disse funksjonene skal virke uavhengig av de ordinære forretningslinjene og bistå ledelsen i styring og kontroll. Tilsvarende kan styrene skaffe seg økt trygghet ved å etablere internrevisjon. Internrevisjon gir større sikkerhet for at styring og kontroll foregår forsvarlig. God praksis tilsier derfor at internrevisjonen skal rapportere direkte til styret og være uavhengig av toppledelsen.. Styret er ansvarlig for en god bruk av sin internrevisjon gjennom godkjenning av årsplan, ressurser og behandling av rapporter.

Internrevisjonen kan i tillegg på selvstendig grunnlag ta opp vesentlige forhold. Imidlertid kan internrevisjonen ikke stå ansvarlig for eller pålegge virksomheten å implementere tiltak i linjen.

NIRF synes det er positivt med oppmerksomhet om internrevisjonens viktige rolle. Vi oppfatter imidlertid at mediedekningen har skapt et inntrykk av at internrevisjon kan frita styrer og ledelse fra sitt viktige styringsansvar. I så fall ville internrevisjonen svekket styring og kontroll i norske virksomheter, noe som er stikk i strid med formålet.

Generalsekretæren informerer

AV ELLEN BRATAAS, GENERALSEKRTÆR

Internrevisjon har aldri vært den store kioskvelteren. For å være helt nøyaktig, har internrevisjon som tema i pressen vært mer eller mindre fraværende frem til denne våren. I forbindelse med Panama-papers og DNBs redegjørelse rundt etablering av kontoer i Luxemburg, sjokkerte Rune Bjerke en hel internrevisjonsnasjon med å legge store deler av ansvaret i Luxemburg på internrevisjonen. Styret i NIRF reagerte raskt med å publisere artikkelen «Hvem har ansvar for internkontrollen?» (artikkelen er gjengitt i sin helhet på side 38). Artikkelen ble referert til i Aftenposten, på vår nettside og i sosiale medier hvor den på LinkedIn blant annet er sett av 320 personer og delt videre av mange utenfor våre egen internrevisjonskrets.

NIRF håper at det søkelyset som har blitt satt internrevisjonens rolle og mandat, vil bidra til å skape større forståelse for internrevisjon som verktøy, samt klargjøre roller og ansvar for virksomheters systemer for internkontroll. I debattens hete har også temaer som governance-struktur i Norge, eierstyring, varslingskanaler, uavhengighet, korrupsjon og internrevisjonens kompetanse og ressurser også blitt løftet opp. Mange bra temaer som foreningen kan kaste seg på for å skape større forståelse for internrevisjon. Styret har bl.a sendt et innspill til kommende revisjon av anbefalingen til eierstyring og selskapsledelse, som NUES trolig vil oppdatere til høsten. Med et proaktivt innspill før revidert utkast foreligger, håper vi å få anbefalingen til i større grad å gjenspeile krav som stilles til virksomheter i store og viktige sektorer i Norge, samt anerkjent internasjonal praksis, ved minimum å inkludere at styrer bør vurdere etablere en internrevisjon.

Det har vært en spennende vår så langt og jeg har en følelse av at høsten ikke akkurat blir kjedelig den heller. Med tanke på at 80 statlige etater skal vurdere å etablere en internrevisjon denne våren, blir det interessant å se hvor mange som faktisk konkluderer på at de har behov for en. Med dette ønsker jeg alle medlemmer, tillitsvalgte og samarbeidspartnere en riktig god sommer, og ser frem til en utrolig spennende høst!

DIALOGFORUM FOR OFFENTLIG REVISJON

Riksrevisjonen har denne våren invitert Norges kommunerevisorforbund, Revisorforeningen og NIRF til et dialogforum for å utveksle informasjon om temaer knyttet til revisjon av offentlige virksomheter. En åpenbar harmonisering rundt internasjonale standarder og styringsprinsipper mellom privat og offentlig revisjon, og mellom ekstern og intern revisjon, tilsier at det kan være hensiktsmessig med en dialog mellom de forskjellige aktørene. Planen er å møtes to ganger i året, med oppstart i oktober.

MEDLEMSMØTE 14. JULI KLOKKEN 09.00 – 10.00:

WORDS DON'T LIE, ONLY PEOPLE DO

Nejolla Corris, anerkjent foredragsholder fra de internasjonale konferansene kommer til Norge for å snake om sitt spesialfelt: "Linguistic Lie Detection": Gathering truthful information is an integral part of any corporate environment. This overview presents how linguistic lie detection is used in business, audit, and investigative areas to help you become more effective in all your business relationships. Påmelding via www.iia.no.

GENERALFORSAMLING

Styret i Norges Interne Revisorers Forening (NIRF) har gleden av å invitere alle medlemmer til årets ordinære generalforsamling ONSDAG 8. JUNI FRA 09.00 – 10.00. Meld deg på via nettsiden.

MANGE SPENNENDE KURS OG SEMINARER FREMOVER

- Cybersecurity & Social Media Risk: What every professional needs to know, 13. juni
- Cybersecurity & Fraud: The basics of conducting online investigations, 13. juni
- Grunnkurs i Compliance, 15. juni
- Introduksjon til internrevisjon, 14. september
- Hvordan skrive revisjonsrapporter som blir lest, 15. september
- Praktisk internrevisjon, 27. – 29. september
- Strategic thinking for internal audit, 11. oktober
- Root cause analysis (RCA) and analysing audit themes, 12. oktober
- Cybersecurity for ikke-spesialister, 19. oktober
- Fra revisor til Fraud Wizard, 1. og 2 november

KONFERANSER VERDT Å MERKE SEG

IIAs International Conference (75-års jubileum), 17. – 20. juli 2016, New York, USA

ECIIA GRC-Conference, 6. – 7. oktober 2016, Stockholm, Sverige

Nasjonal fagkonferanse i offentlig revisjon, 25. – 26. oktober 2016, Gardermoen

VI GRATULERER FØLGENDE MEDLEMMER

Diplomert Intern Revisor (Dipl IR)
Ann Christin Flatland, Nets Norway
Unni Kristine Rognlien, Forsvarsdepartementet

Certified Internal Auditor (CIA)
Thomas B. Jacobsen, National Oilwell Varco Norway AS

Certification in Risk Management Assurance (CRMA)
Asif Iqbal, Telenor ASA

NYE VEILEDNINGER OG GUIDANCE FRA IIA

(alle kan lastes ned fra nettet)

THE GLOBAL INTERNAL AUDIT COMMON BODY OF KNOWLEDGE (CBOK)
Utgitt av: IIA Research Foundation

CBOK er en verdens største undersøkelse rundt internrevisjon som gjennomføres hvert 5 år. I CBOK 2015 deltok 14 518 respondenter fra 166 forskjellige land, 23 % av respondentene var fra Europa. Her er flere rapporter siden forrige SIRK, basert på dataene fra undersøkelsen. Du laster de ned i sin helhet på www.globaliia.org.

Relationships and Risk: Insights from Stakeholders in North America
How well are internal audit departments meeting the needs of the audit committee, and is the internal audit department receiving the proper support and oversight of the internal audit function? This report will help you understand the relationship and provide key insights on opportunities for improvement for the two groups.

Lifelong Learning for Internal Auditors: Certification and Training Levels Worldwide
By choosing to pursue a certification, internal auditors are taking a big step toward establishing a professional reputation that speaks loudly of integrity, dedication, and commitment to both the profession and his or her organization. This report reveals which certifications are most popular in different parts of the world.

The Top 7 Skills CAEs Want: Building the Right Mix of Talent for Your Organization
The evolution of the internal audit profession toward a more value-added risk assurance function continues to move forward. While technical skills are needed for day-to-day work, analytical/critical thinking and communication are personal skills that continue to be at the top of any chief audit executive's (CAE's) wish list. What other skills are most desired by internal audit managers for their staff? This report identifies the top 7 skills sought after by CAE and attributes that most CAEs are recruiting or building into their internal audit functions.

GREAT Ways to Motivate Your Staff: Shaping an Audit Team that Adds Value and Inspires Business Improvement
The most effective CAEs position their internal audit departments to add value and inspire business improvement by maximizing the productivity and contribution of their internal audit colleagues. But how do they set goals that inspire auditors to deliver insights that matter? Boost productivity with appropriate rewards? Address differences between generations?

This report provides GREAT insights on how CAEs and other audit leaders can improve their practices for evaluating and motivating internal auditors. You will learn strategies for goal setting, retaining talent, equipping employees, assessing performance, and treating success.

Interacting with Audit Committees: The Way Forward for Internal Audit
How well are internal audit departments meeting the needs of the audit committee, and is the internal audit department receiving the proper support and oversight of the internal audit function? The overall answer to these two questions is that both groups are doing better, but there are many opportunities for improvement.

Engaging Third Parties for Internal Audit Activities: Strategies for Successful Relationships
One of the biggest challenges CAEs face is having enough staff to meet demands and obtaining the right skills to complete their audit plans. To meet this challenge, many CAEs engage third parties for some of their internal audit activities. This report will help internal audit practitioners, managers, and audit committees to more effectively manage these relationships.

PRACTICE GUIDE: INTERNAL AUDIT AND THE SECOND LINE OF DEFENCE
Utgitt av: IIA global
Many organizations are restructuring responsibilities, ensuring governance and monitoring functions collaborate more closely to avoid duplication. With this change comes an additional weight for the chief audit executive; they may be asked to assume responsibilities for risk management, compliance, and other governance functions. Navigating through this process can be challenging; as a result, this guidance was developed to assist practitioners in making effective decisions regarding roles and responsibilities to assume related governance of risk management and controls.

Internal Audit and the Second Line of Defense offers guidance and recommendations for audit practitioners, especially chief audit executives, to ensure independence and objectivity are not compromised in situations where internal audit may be responsible for second line of defense activities.

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

Prinsessen som ingen kunne målbinde

En internrevisor kjennetegnes blant annet ved at han er nysgjerrig og evner å grave frem både nyttig og unyttig informasjon. Kanskje litt som Askeladden trollbandt prinsessen og fikk halve kongerike?

Det var engang en konge; han hadde en datter som var så vrien og vrang i ord at ingen kunne målbinde henne, og derfor lovte han ut at den som kunne gjøre det, skulle få prinsessen og halve kongeriket attpå.

Det var nok av dem som ville prøve seg, skal jeg tro, for det er ikke hver dag en kan få en kongsdatter og et halvt kongerike til givendes.

Så var det tre brødre også som hadde fått spurt om prinsessen, og da de ikke hadde det for rart hjemme, ville de ut og friste lykken, og se om de kunne vinne kongsdatteren og halve riket. De var venner og nokså vel forlikt, og derfor gikk de i følge alle tre. Da de hadde kommet et stykke på veien, fant Askeladden en Kundeavtale.

«Jeg fant, jeg fant!» ropte han.
«Hva fant du?» spurte brødrene.
«Jeg fant en kundeavtale,» sa han.
«Fy kast ‹n! Hva skal du med den?» sa de to, som alltid trodde at de var de klokeste.
«Å, jeg har slikt å gjøre, jeg har slikt å føre, jeg fører vel den,» sa Askeladden.
Da de hadde gått et stykke til, fant Askeladden et fullmaktssystem; den tok han opp.

«Jeg fant, jeg fant!» ropte han.
«Hva fant du nå?» sa brødrene.
«Jeg fant et fullmaktssystem,» svarte han.
«Pøh! Hva skal du med den? Kast ‹n!» sa de to.
«Jeg har slikt å gjøre, jeg har slikt å føre, jeg fører vel den,» sa Askeladden.
Da de hadde gått litt til, fant han en instruks som var utgått på dato; den tok han også opp.
«Gutter, jeg fant, jeg fant!» sa han.
«Nå, hva fant du nå?» spurte brødrene.
«En instruks som var utgått på dato,» sa han.
«Isj! Det var da også noe å dra på! Kast det!» sa de.
«Å, jeg har slikt å gjøre, jeg har slikt å føre, så fører jeg vel den,» svarte Askeladden.

Da de hadde kommet litt lenger, fant han hjemmesiden med informasjon om styrende dokumenter, og like etter fant han maken til det for datterselskapene.
«Jeg fant, jeg fant, gutter!» ropte han.
«Hva fant du nå da?» sa de andre.
«Hjemmesiden med informasjon om styrende dokumenter,,» svarte Askeladden.
«Isj! Kast dem! hva gjør du med dem?» sa de.
«Å, jeg har slikt å gjøre, jeg har slikt å føre, så jeg fører vel den, skal jeg vinne prinsessen og halve riket,» sa Askeladden.
«Ja, du ser ut til det du!» sa de to.
Så la de inn til kongsdatteren. De to eldste prøvde seg først, men ingen av dem klarte å målbinde kongsdatteren.

Så var turen kommet til Askeladden.
«God dag,» sa han.
«God dag igjen,» svarte hun og vrikket og vridde på seg.
«Det var da godt og varmt her,» sa Askeladden.
«Det blir heitere om vi får revisjon og de ikke er fornøyd med internkontrollsystemet,» svarte hun.
«Da har vi jo dette fullmaktssystemet å vise frem» sa Askeladden.
«Er det tilstrekkelig da?» sa prinsessen
«I tillegg har vi jo denne» sa gutten, og dro frem kundeavtalen.
«Du er så kroket i ord du,» sa prinsessen.
«Nei, jeg er ikke kroket, men dette er kroket,» svarte gutten, og viste hvor en kunne finne styrende dokumenter på intranettet.
«Nei! nå har jeg aldri sett maken!» ropte prinsessen.
«Her ser du maken,» sa gutten, og tok opp det andre eksemplet på hjemmesiden for datterselskapene.
«Jeg mener du er utgått for å målbinde meg, du?» sa hun.
«Nei, jeg er ikke utgått, men denne er utgått,» svarte gutten, og dro fram instruksen som var utgått på dato».
Så var prinsessen målbundet!
«Nå er du min,» sa Askeladden, og så fikk han henne og halve landet og riket attpå.

Returadresse
NIRF
Postboks 1417 Vika
0115 Oslo

Vi bryr oss om å skape de beste løsningene for deg

I BDO er vi opptatt av å kombinere internrevisjonserfaring med spesialistkompetanse innen de fagfeltene som preger risikobildet norske virksomheter står overfor i dag.

Gjennom tverrfaglige team bidrar vi til en løsningsorientert internrevisjon, med fokus på det som virkelig betyr noe for virksomheten. Enten vi ivaretar internrevisjonsfunksjonen eller bistår i gjennomføring av enkeltoppdrag, gir vi alltid våre kunder tilgang på spisskompetansen som behøves for å løse nettopp deres problemstillinger. Slik bidrar vi til å skape merverdi og trygge, gode løsninger for deg.

Virksomhetsstyring	Gransking og compliance	IT-revisjon og IT-risiko	Sikkerhet og beredskap	Transaksjons-rådgivning

For mer informasjon om våre tjenester og hva vi kan hjelpe deg med, se **www.bdo.no**

Revisjon | Skatt og avgift | Rådgivning | Regnskap

BDO