INFO

Foreningen af Interne Revisorer
Nummer 55 | December 2013 | 18. årgang

Ny revisionsbekendtgørelse:
Nu kommenteret af FSR

Intern revision i ikke-finansielle virksomheder

Sikkerhed & Revision 2013
Risici er blevet hverdag, men er virksomhederne klar til at håndtere dem ?

Operationel risikostyring
Kan rammeværkerne for risikostyring blive en risiko i sig selv ?

IFRS 4: Høringsudkast • COSO • Insurance Europe • ISA 610 Q & A

INFOs redaktion

Ansvarshavende redaktør

Koncernrevisionschef Poul-Erik Winther
Alm. Brand
☎ 35 47 78 97 ✉ abrpwe@almbrand.dk

Øvrig redaktion

Afdelingsdirektør Lars Geisler
Nykredit
☎ 44 55 93 08 ✉ lage@nykredit.dk

Head of Quality Assurance and Development
Lars Maagaard
Nordea
☎ 33 33 15 48 ✉ lars.maagaard@nordea.com

Revisionschef Louise Claudi Nørregaard
PensionDanmark
☎ 33 74 80 13 ✉ lcn@pension.dk

Senior Group Internal Auditor Dan Otzen
ISS World Services A/S
☎ 38 17 64 03 ✉ dan.otzen@group.issworld.com

Deputy Chief Audit Executive
Birgitte Rousing Svenningsen
Saxo Bank
☎ 39 77 41 30 ✉ bsv@saxobank.com

Specialkonsulent John Terp
Forsvarsministeriets Interne Revision
☎ 72 44 47 63 ✉ fir-ter@mil.dk

Næste nummer

INFO 56 udkommer i april 2014.
ISSN: 1903-7341 (Elektronisk version).

Indlæg til INFO

Artikler i INFO påskønnes med en vingave.

Forsidefoto

Ole Svenningsen

Redaktionens adresse

Alm. Brand A/S
Foreningen af Interne Revisorer (IIA)
Att: Koncernrevisionschef Poul-Erik Winther
Midtermolen 7
2100 København Ø.

Synspunkter, der kommer til udtryk i medlemsbladet, behøver ikke nødvendigvis at svare til bestyrelsens opfattelse eller være udtryk for foreningens officielle standpunkt.

Indhold

Besøg foreningens hjemmeside:

www.iia.dk

Leder

Senior Vice President Jesper Siddique Olsen, Danske Bank

Øgede forventninger til interne revisorer

Nu står vi endnu en gang midt i juletiden og som altid er dette en oplagt mulighed for at evaluere året der er gået men også en kærkommen lejlighed til at fokusere på 2014.

Trenden med nye regulatoriske krav for revisorer er fortsat i 2013, som eksempler kan nævnes bekendtgørelse om revisionens gennemførelse i finansielle virksomheder mv., opdateringen af ISA 610 samt Finanstilsynets certificeringsordning, hvor ekstern revisor skal have beskæftiget sig med ydelser til finansielle virksomheder i mindst 1.500 timer indenfor de seneste 5 år.

De regulatoriske tiltag er næsten udelukkende målrettet mod eksterne revisorer og om disse medfører ændringer for intern revision er ikke entydigt. Men dette betyder ikke at de ikke er relevante for interne revisorer, da disse er med til at øge forventningerne til vores profession. Når der ændres på kravene til de eksterne revisorer, er det som udgangspunkt altid fornuftigt at vurdere om kravene i mere eller mindre omfang skal implementeres i den interne revision.

Kvalitet har i 2013 igen været et nøgleord i debatten om fremtidens revisionspolitik. Forudsætningen for at kunne levere kvalitet er, at fagligheden er i orden. Derfor er det også relevant at se på de uddannelseskrav, der stilles til interne revisorer. Vi er som profession bevidste om vores ansvar og lovgivningsmæssige privilegier. Derfor har IIA været en positiv medspiller hele vejen igennem i den markante ændring af revisorbranchens reguleringsmæssige rammer, senest i relation til den opdaterede ISA 610.

Opdateringen af ISA 610 kan f.eks. være en kærkommen lejlighed til at se på den interne revisions organisatoriske opbygning mv. Intern revision skal kunne demonstrere, at den anvender anerkendt revisionsmetodik – revisionsstandarder, har implementeret en revisionsmetodik, har krav til rapportering af revisionen, at der er implementeret en tilstrækkelig og passende kvalitetssikring, at der er vedtaget etiske retningslinjer, at der er opstillet krav til de kvalifikationer medarbejderne skal have herunder efteruddannelse mv. Dette danner basis for et fagligt miljø, hvor de rette holdninger til revision understøttes – det understøtter intern revisions objektivitet og uafhængighed.

Finanstilsynets certificeringsordning er selvfølgelig ikke direkte relevant for interne revisorer i den finansielle sektor. Men kravene om højere og bedre kvalifikationer til revisorer er en konsekvens af stigende kompleksitet i virksomhedernes problemstillinger og derfor er kravene indirekte også relevant for interne revisorer.

Hvis intern revision skal tiltrække de bedst kvalificerede, kræver det, at man fortsat positionerer sig selv korrekt. Dette kan gøres ved at tiltrække arbejdskraft, som skal bidrage til mere kvalitet i revisionen af komplekse kerneområder, som afspejler de risici, virksomheden står over for nu og i fremtiden. Dette kan betyde, at man i fremtiden vil se flere ikke-revisorer være en del af intern revision og derved kan de skærpede krav bidrage til, at intern revision får en skarpere profil, som netop kan tiltrække kvalificeret arbejdskraft.

God jul, godt nytår og god læselyst.

Nyt fra bestyrelsen

Af koncernrevisionschef
Poul-Erik Winther, Alm. Brand

Bestyrelsesmødereferaterne lægges på foreningens hjemmeside kort efter mødernes afholdelse, og det er dermed muligt løbende at følge med i bestyrelsens arbejde. Referaterne indeholder bl.a. en status på de af bestyrelsen igangsatte aktiviteter.

IIA har samarbejdet med FSR Danske Revisorer om udarbejdelse af et notat om ISA 610. Notatet, samt en tilhørende Q&A, er færdiggjort i november og er offentliggjort på begge foreningers hjemmesider. Dette nummer af INFO indeholder tillige en omtale af notatet.

En af forudsætningerne for ekstern revisions anvendelse af intern revisions arbejde er, at den interne revision har et kvalitetsstyringsprogram. For at understøtte medlemmernes efterlevelse af dette krav, har foreningen nedsat et kvalitetsstyringsudvalg, og det er hensigten, at resultatet af udvalgets arbejde bliver præsenteret på en undervisningsformiddag i foråret 2014.

På uddannelsessiden sker der flere spændende ting. Tilrettelæggelse af årskonferencen 2014 er godt i gang. Endvidere arbejdes der med, at der i maj 2014 afholdes et forberedelseskursus til CIA-eksamen. Gå-hjem møderne vil fortsat blive optaget på video og lagt på hjemmesiden, således at de medlemmer, der ikke kan deltage på møderne, har mulighed for at se de enkelte indlæg efterfølgende.

Bestyrelsen har opdateret charters for de enkelte udvalg i IIA, og de opdaterede charters ligger på hjemmesiden. Dette gælde selvsagt også charter for INFO redaktionsudvalget, og som det fremgår heraf, skal udvalget bestå af medlemmer fra de enkelte sektorer i foreningen, således at der kan bringes artikler, der henvender sig til disse sektorer. Alle er meget velkomne til at rette henvendelse til redaktionen med idéer til emner, der kan bringes i kommende numre, og tilsvarende også meget velkomne til at skrive artikler til bladet.

Uddannelsesaktiviteter

Af Head of Quality Assurance and Development, Lars Maagaard, Nordea

Der er 36 medlemmer af IIA Danmark, der står registreret som havende en CIA (Certified Internal Auditor) certificering. Der kan være flere, som har en CIA certificering, ligesom der kan være medlemmer, der har taget CIA eksamen, men ikke har vedligeholdt den ved at opfylde det årlige krav til CPE point mv. Der er dog noget der kunne indikere, at vi i Danmark ikke har haft tilstrækkeligt fokus på CIA certificeringen. Uddannelsesudvalget har derfor valgt at tilbyde et kursus, der kan hjælpe dig på vej til certificeringen, jf. nedenstående.

Bliv certificeret intern revisor på et år!

Bestyrelsen har i sin strategi for IIA fastlagt en målsætning om, at foreningen skal medvirke til en høj faglig standard blandt interne revisionsafdelinger ved at gennemføre relevant, udviklingsorienteret og målrettet uddannelse. Et af de områder, som har høj prioritet, er ønsket om at øge antallet af certificerede interne revisorer blandt foreningens medlemmer. Det er derfor rigtig glædeligt, at det er lykkedes at lave en aftale med IIA Global i USA om et samarbejde, som betyder, at vi i foråret 2014 kan tilbyde det første forberedelseskursus til del 1 af CIA certificeringen i Danmark.

Tilbuddet består i et 3-dages kursus med en professionel instruktør, som tager udgangspunkt i CIA Learning System. Du får ved tilmelding til kurset mulighed for at købe læringssystemet til reduceret pris således, at du har mulighed for at forberede dig til eksamen både før og efter kurset. Der bliver naturligvis udstedt kursusbevis efter gennemført kursus, som giver 24 CPE. Hvis ikke du ønsker at gå til eksamen, vil der stadig være et stort udbytte af kurset, hvor du får en indføring i de vigtigste områder og begreber inden for:

- IIAs professionelle standarder
- Intern kontrol og risikostyring
- Intern revision - metode, teknik og værktøj

Når du har gennemført det første kursus, og måske også valgt at gå til eksamen på del 1 af CIA certificeringen, har du sikkert fået blod på tanden. Og godt begyndt er som bekendt halvt fuldendt. Så hvorfor stoppe her?

IIA planlægger at tilbyde forberedelseskurser til del 2 og 3 af CIA certificeringen i henholdsvis efteråret 2014 og foråret 2015, og du får dermed mulighed for at forberede dig til alle 3 eksamener inden for et år.

HVAD OMFATTER CIA EKSAMEN?

Der er tale om eksamener af 2 - 2½ times varighed, hvor man skal besvare 100 - 125 multiple choice spørgsmål inden for forskellige områder, jf. nedenstående oversigt.

PART 1 EXAM: INTERNAL AUDITING BASICS Duration: 2.5 hours Question Count: 125	PART 2 EXAM: INTERNAL AUDIT PRACTICE Duration: 2.0 hours Question Count: 100	PART 3 EXAM: INTERNAL AUDIT KNOWLEDGE ELEMENTS Duration: 2.0 hours Question Count: 100
TOPICAL FOCUS AREAS INCLUDE: • IIA Mandatory Guidance • Internal Control and Risk • Tools and Techniques for Conducting the Audit Engagement	TOPICAL FOCUS AREAS INCLUDE: • Managing the Internal Audit Function • Managing Individual Engagements • Fraud Risks and Controls	TOPICAL FOCUS AREAS INCLUDE: • Governance • Risk Management • Organizational Structure and Business Processes • Communication • Leadership • IT/Business Continuity • Financial Management • Global Business Environment

HVORDAN KVALIFICERER OG TILMELDER MAN SIG TIL CIA EKSAMEN?
For at kunne indstille sig til eksamen skal man kunne dokumentere, at man har bestået, hvad der svarer til en bachelorgrad. Herudover kræver certificering, at man har minimum 24 måneders erhvervserfaring som intern eller ekstern revisor. Man kan godt gå til CIA eksamen, selvom man endnu ikke har den krævede erhvervserfaring, men man opnår først status som Certified Internal Auditor, når man kan dokumentere de 24 måneders relevant erhvervserfaring.

Tilmeldingen til eksamenerne sker via IIA USAs hjemmeside (https://na.theiia.org/certification) hvor man indskriver sig i CIA-programmet i det såkaldte "Certification Candidate Management System" (CCMS). Her vil du også kunne finde IIA Certification Candidate Handbook, hvor du kan læse mere om CIA-eksamen. Selve eksamen foregår hos Global Knowledge ApS på Stamholmen 110, 2650 Hvidovre. Der er ingen faste eksamensdatoer, så man bestemmer selv, hvornår man vælger at gå til eksamen.

Proceduren vedrørende eksamenstilmelding og hjælp til samme, vil kunne tilbydes i forbindelse med forberedelseskurser, ligesom der vil blive mulighed for at danne læsegrupper, hvis det ønskes.

HVAD KOSTER KURSUS, MATERIALER OG EKSAMEN?
Forberedelseskurset foregår på engelsk og afholdes i København. Kursusgebyret bliver beregnet på omkostningsdækkende basis, og på grundlag af IIA Globals tilbud, forventes gebyret for forberedelseskurset til del 1 af CIA certificeringen at komme til at koste ca. 6.000 kr. ved minimum 25 deltagere (incl. forplejning, men ekskl. hotel). Hertil skal lægges prisen for CIA Learning System (dækker pensum til alle 3 eksamener), som forventes at ligge i størrelsesordenen 2.800 kr., og eksamensgebyret, som udgør ca. 1.400 kr.

HVORNÅR AFHOLDES KURSET?
Kurset afholdes i dagene 5.-7. maj 2014.

OG HVAD SÅ?
Hvis du er interesseret i dette tilbud, kan du tilmelde dig via IIAs hjemmeside.

Har du spørgsmål til kurset eller CIA-eksamen er du velkommen til at kontakte

Neil Jensen (neil.henrik.jensen@post.dk) eller Lars Maagaard (lars.maagaard@nordea.com).

Intern revision i ikke-finansielle virksomheder

Af Fagleder Kristian Koktvedgaard, Dansk Industri

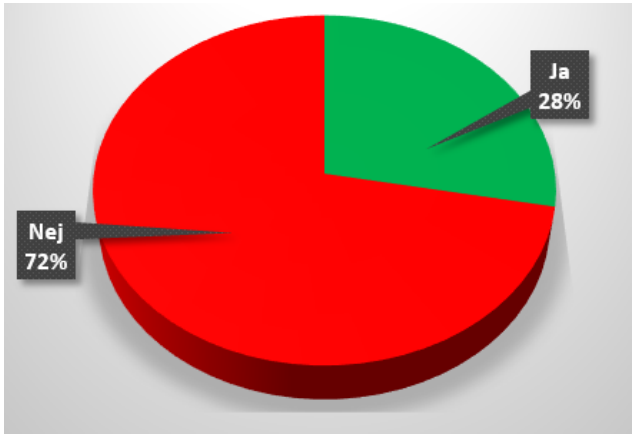
Udbredelsen af intern revision i ikke-finansielle virksomheder

Dansk Industri og FSR – danske revisorer uddelte i september 2012 Årets Regnskabspris for 1. gang. I den forbindelse uddeltes en specialpris baseret på oplysninger i ledelsesberetningen om interne kontroller i forbindelse med regnskabsaflæggelsesprocessen. Specialprisen lå i forlængelse af en tidligere publikation omkring implementeringen af Årsregnskabslovens § 107b, hvor en af hovedpointerne var vigtigheden af at gøre beskrivelsen virksomhedsspecifik. Til brug for denne artikel har jeg gennemgået de seneste årsregnskaber for de danskbaserede moderselskaber i C20 og Large-Cap indeksene på Nasdaq OMX med fokus på oplysningerne om intern revision i de ikke-finansielle virksomheder, herunder om oplysningerne er virksomhedsspecifikke.

Interne revisionsafdelinger har endnu ikke fundet almindelig udbredelse udenfor den finansielle sektor. Gennemgangen viser ikke overraskende, at de 5 finansielle virksomheder i stikprøven alle havde etableret intern revision i overensstemmelse med lov om finansiel virksomhed.

Ser man derimod på gruppen af ikke-finansielle virksomheder, så har alene 4 virksomheder ud af de 18 etableret en intern revisionsafdeling, mens ét selskab – Københavns Lufthavne - havde outsourcet opgaven til en ekstern leverandør. 13 ud af 18 – eller 72 procent – havde således ikke vurderet det nødvendigt at etablere en intern revision på nuværende tidspunkt (se figur 1).

Ud af de 4 virksomheder, der har etableret intern revision, finder vi de tre selskaber med den største markedsværdi (A.P. Møller – Mærsk, Carlsberg og Novo Nordisk). Der må således antages at være en sammenhæng mellem kompleksiteten og størrelsen af virksomheden og bestyrelsens vurdering af behovet for en intern revisionsafdeling.



Figur 1: Anvendelse af intern revision i ikke-finansielle virksomheder i C20 plus Large-Cap

At netop størrelse og kompleksitet sammen med økonomi har en betydning, fremgår tydeligt i Årsrapporten for Københavns Lufthavne. En velfungerende intern revision kræver udover en forankring med direkte reference til bestyrelsen /revisionskomiteen for at sikre den nødvendige uafhængighed - nødvendigvis også et fagligt miljø. Københavns Lufthavne har adresseret dette forhold i deres årsrapport med følgende beskrivelse:

"Revisions- og risikoudvalget vurderer hvert år behovet for en intern revision og kommer i den forbindelse med anbefalinger desangående. Revisions- og risikoudvalget er nået til den konklusion, at det under hensyn til selskabets forhold er mest hensigtsmæssigt at outsource de interne revisionsopgaver til et uafhængigt revisionsfirma med kompetencer indenfor dette område.
…
Bestyrelsen har på baggrund af indstilling fra Revisions- og risikoudvalget besluttet at få udført visse interne revisionsopgaver på outsourcing basis af et eksternt revisionsfirma.
Det er CPH's opfattelse, at behovet for at få udført interne revisionsopgaver, som følge af selskabets forhold, er af så begrænset karakter, at det er mest hensigtsmæssigt at få udført de pågældende opgaver på outsourcing basis.
Herved sikres også den nødvendige faglige kompetence til udførelsen af de pågældende opgaver."

Med dette valg kan Københavns Lufthavne opnå værdien af intern revision uden at skulle opbygge den faglige organisation, som en intern revision kræver.

Kommunikation af intern revisions arbejde overfor selskabets investorer.

Omfanget og fokus for intern revision er primært forankret indenfor to hovedområder:

- det interne kontrolmiljø incl. forretningsrisici samt
- forretningsetik og whistleblowersystemer.

Således fremhæves disse to hovedområder i alle beskrivelserne af den interne revisions arbejdsområder. Udover disse to hovedområder har intern revision i Novo Nordisk yderligere tre andre opgaver:

"Tre andre former for intern revision – kvalitetsrevision, organisationsrevision og revision af ledelsesværdier, kaldet faciliteringer – er med til at sikre, at virksomheden overholder høje kvalitetsstandarder og efterlever Novo Nordisk Way."

Den interne revisions involvering i disse faciliteringer fremgår dog ikke tydeligt i forbindelse med beskrivelser i Novo Nordisk's regnskab af eksempelvis kvalitetsauditeringer, og således er det svært for brugeren at se betydningen af intern revisions fingeraftryk på disse faciliteringer, herunder i hvilket omfang den interne revision har haft bemærkninger til disse faciliteringer. Dette kan naturligvis begrundes i hvordan virksomheden har valgt at strukturere sin ledelsesberetning m.m.

Generelt udgør rapportering omkring den interne revisors arbejde dog ikke en stor del af de gennemgåede årsrapporter. Således indgår i de fleste tilfælde alene kortere tekststykker i forbindelse med selskabernes afrapportering omkring corporate governance forhold, ligesom intern revision indgår grafisk i illustrationer omkring governancestrukturen hos eksempelvis Novo Nordisk og Lundbeck. På de ikke-finansielle virksomheder ses således ikke selvstændige erklæringer fra den interne revisor, således som det er tilfældet for nogle af de finansielle virksomheder. Henset til, at den interne revision rapporterer til Bestyrelsen/Revisionsudvalget giver dette også god mening. Skeler man til UK, der på dette område er meget langt fremme ikke mindst grundet arbejdet i deres "Financial Reporting Lab", indgår den interne revisors arbejde da også som en del af revisionsudvalgets rapportering i årsrapporten.

Et selskab – Carlsberg – skiller sig ud, idet Carlsberg i deres Corporate Governance rapport har valgt at prioritere en mere detaljeret beskrivelse af den interne revision og den interne revisions arbejde:

*"**Intern revision (Group Internal Audit)***
Intern revision sikrer en objektiv, uafhængig vurdering af tilstrækkeligheden, effektiviteten og kvaliteten af Gruppens interne kontroller. Lederen af Intern revision refererer til formanden for Revisionsudvalget. Revisionsudvalget skal godkende udnævnelse og eventuel afskedigelse af lederen af Intern revision. Intern revision arbejder i henhold til et charter og kommissorium, som godkendes af Revisionsudvalget.

Intern revision foretager årligt en vurdering af forretningsrisici. På baggrund heraf samt ved input fra bestyrelse, Revisionsudvalg, direktion og relevante ledende medarbejdere fastlægges en revisionsplan for året. Planen gennemgås og godkendes af Revisionsudvalget og bestyrelsen. Intern revision har ansvar for planlægning, udførelse og rapportering af den udførte revision. Rapporteringen indeholder observationer og konklusioner samt forslag til forbedringer af de interne kontroller på hvert revideret område.

Ved udførelse af en revision vurderer Intern revision, om den enhed eller funktion, der revideres, har en veletableret regnskabspraksis, skriftlige politikker og procedurer på alle væsentlige forretningsområder samt tilstrækkelige interne kontrolprocedurer. Herunder vurderes det, om kontroller omkring de væsentlige IT-systemer er tilfredsstillende, og om de følger IT-politikken.

Carlsberg-gruppen har et whistleblowersystem, som giver medarbejderne mulighed for at indberette forhold om mulig kriminel adfærd eller overtrædelse af Carlsberggruppens politikker og retningslinjer.

Whistleblowersystemet består af en hjemmeside og en telefonisk hotline drevet af en uafhængig tredjepart for at sikre det højeste sikkerheds- og fortrolighedsniveau. Indberetninger via whistleblowersystemet håndteres af en lille gruppe medarbejdere i Intern revision, som har ansvaret for at vurdere, om der er tale om overtrædelse. Intern revision rapporterer regelmæssigt – og mindst én gang i kvartalet – til Revisionsudvalget om forhold, der er indberettet via whistleblowersystemet, og eventuelle forholdsregler, der er truffet som følge heraf. I 2012 blev der foretaget 26 indberetninger via systemet. Siden lanceringen af whistleblowersystemet i april 2010 har nogle indberetninger og den efterfølgende undersøgelse ført til forskellige disciplinære sanktioner mod en eller flere medarbejdere, herunder afskedigelse som følge af overtrædelse af Gruppens politikker og i nogle tilfælde af straffeloven. De fleste af disse forhold har vedrørt enkeltstående tilfælde af svig begået af individuelle medarbejdere i Gruppen. Episoderne har ikke haft nogen væsentlig betydning for Gruppens eller det pågældende selskabs finansielle resultater."

I de andre selskaber findes oplysninger om den interne revisions aktiviteter i forhold til interne kontroller som delelementer i forbindelse med corporate governance rapporteringen, specielt i den lovpligtige redegørelse efter § 107b. Det særlige ved Carlsberg er dog især den detal-

jerede og åbne rapportering omkring Whistleblowersystemet, og Carlsberg skiller sig således ud ved at rapportere omkring de faktiske resultater af den interne revisions arbejde på dette punkt.

Unoterede selskaber er også aktive

Udenfor de primært udvalgte regnskaber er der også en række unoterede selskaber, hvor intern revision enten er etableret eller er under etablering. Således har ISS og Danfoss etableret interne revisionsafdelinger, mens DONG er ved at implementere en intern revision. Hos Danfoss afrapporteres den interne revisions arbejde således:

"Danfoss oprettede derudover en intern revisionsfunktion i 2011, som kan fremlægge sine konklusioner direkte for bestyrelsens revisionskomité. Den interne revision har til formål at yde uafhængig og objektiv revision for at sikre, at:

- *Koncernen har en god administrativ praksis*
- *Der er fyldestgørende interne kontrolprocedurer og forretningsgange på alle væsentlige aktivitetsområder*
- *Der er betryggende funktionsadskillelse i Danfoss' it-systemer*

Intern revision har i 2012 aflagt besøg hos en række koncernselskaber, udvalgt på baggrund af de risici og de koncernselskaber, der vægter mest i koncernens risikobillede. Revisionen har givet anledning til at indskærpe kontroller og procedurer i forskellige sammenhænge, men der er ikke konstateret forhold af væsentlig betydning for koncernens overordnede risikostyrings- og kontrolmiljø."

Danfoss har således som Carlsberg valgt i deres beskrivelse at være åbne omkring resultatet af den interne revisions arbejde ved at konstatere, at de har haft et behov for at indskærpe kontroller og procedurer, men at der ikke er konstateret forhold, der samlet set har haft en væsentlig betydning.

ISS har referencer til den interne revision i deres generelle beskrivelser omkring kontrolmiljøet, herunder beskrivelser omkring hvordan intern revision rapporterer til revisionsudvalget, men der er ikke specifikke referencer til resultatet af den interne revisions arbejde.

Konklusion

Min gennemgang af udvalgte regnskaber viser, at intern revision endnu ikke har fundet stor udbredelse i den ikke-finansielle sektor og at der er en klar sammenhæng mellem udbredelsen og størrelsen/kompleksiteten på virksomheden.

Gennemgangen viser også, at rapporteringen omkring intern revisions arbejde indgår som en del af corporate governance rapporteringen og ikke indgår med en selvstændig revisionspåtegning. Både Carlsbergs og Danfoss' regnskab viser dog, at den interne revisions fingeraftryk kan gives klart og tydeligt uden brug af en selvstændig revisionspåtegning ved at gøre beskrivelsen virksomhedsspecifik og konkret.

COSO - intern kontrol

Af Head of Quality Assurance and Development, Lars Maagaard, Nordea

Committee of Sponsoring Organizations of the Treadway Commission (COSO) har opdateret deres 'Internal Control – Integrated Framework (rammeværket)'. Rammeværket definerer et intern kontrol system og er noget de fleste i et eller andet omfang har stiftet bekendtskab med. IIA og ISA standarderne er bl.a. inspireret af rammeværket og bruges hos mange af vores kunder/auditees.

Rammeværket er i 2013 blevet opdateret i forhold til den oprindelige udgave, der daterer sig tilbage til 1992. Der er ikke mange ændringer i det opdaterede rammeværk og nærværende artikel kan da også opfattes som en kort genopfriskning af hovedlinjerne i rammeværket. Artiklen er kraftigt inspireret af 'Internal Control – Integrated Framework – Executive Summary' udgivet af COSO. Jeg kan kun anbefale, at læse dette dokument, da det på få sider giver et rigtig godt overblik over rammeværket.

Rammeværket indeholder måske ikke de store overraskelser når det læses, men jeg tror ikke, jeg siger for meget hvis jeg konkluderer, at det er langt nemmere at snakke om rammeværket end den praktiske implementering af det. Organisationer er typisk komplekse og i rammeværket lægges der bl.a. derfor også vægt på betydningen af ledelsens professionelle dømmekraft. Den bruges bl.a. i vurderingen af, hvad der er væsentlige risici og behovet for implementering af kontrolaktiviteter. Personer og ledelser er ikke ens og den professionelle dømmekraft influeres af personens erfaringer, risikoappetit mv. Et intern kontrolsystem udgøres i væsentligt omfang af mennesker, hvorfor der implicit i ethvert intern kontrol system er en iboende risiko for af de interne kontroller ikke fungerer efter hensigten. Et velfungerende intern kontrolsystem giver ikke fuld sikkerhed, men kan give begrundet/rimelig sikkerhed for ledelsen for at organisationens målsætning kan nås.

Nyhederne i det opdaterede rammeværk

Som sagt er ændringerne i forbindelse med opdateringen ikke store og indholdet fra 1992 er stadig fundamentet i COSO rammeværket. Ved opdateringen er der taget højde for de ændringer, der er sket de seneste 20 år, så rammeværket bedre reflekterer det nuværende forretningsmiljø. De 5 interne komponenter (kontrolmiljø, risikovurdering, kontrolaktiviteter, information og kommunikation og overvågning) er uforandrede, men i opdateringen er der implementeret 17 principper, der støtter disse komponenter. Målet for den finansielle rapportering er ligeledes udvidet til også at inkludere intern rapportering og ekstern ikke-finansiel rapportering.

Definitionen af intern kontrol

Definitionen af intern kontrol er uændret og er:

"Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."

Som det ses, er dette en bred definition, men inkluderer væsentlige begreber, der udgør fundamentet i et intern kontrol system, herunder hvordan en organisation designer, implementerer og udfører intern kontrol.

Definitionen inkluderer bl.a. det forhold, at intern kontrol langt fra kun er politikker og procedure, men i stort omfang omhandler mennesker og hvordan de agerer på de forskellige organisatoriske niveauer, når de udfører intern kontrol. Et andet væsentligt forhold er, at en intern kontrol proces vil være i konstant udvikling, da det løbende skal tilpasses organisationens og omgivelsernes forretningsmæssige forhold.

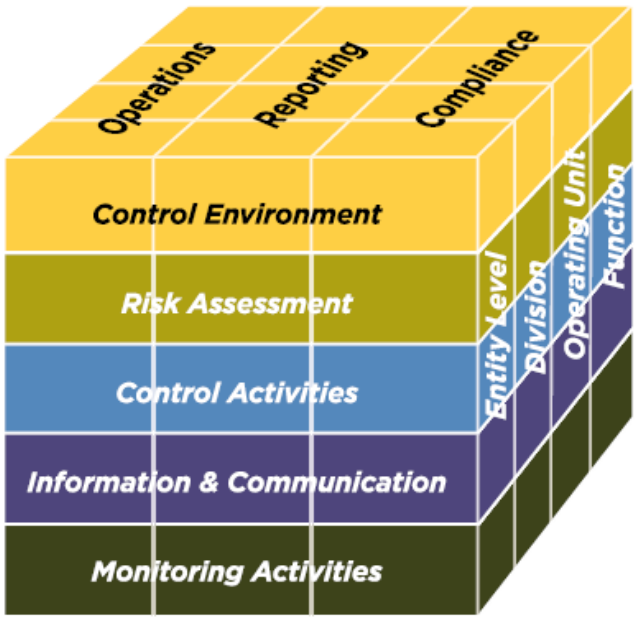
Rammeværket har defineret 3 kategorier for målsætninger:

- Operationelle målsætninger, der omhandler produktiviteten og effektiviteten i en organisations processer, herunder operationelle og finansielle målsætninger og sikring af aktiver mod tab.

- Rapporteringsmæssige målsætninger, der omhandler intern og ekstern finansiel og ikke-finansiel rapportering, der er underlagt krav om troværdighed, aktualitet og gennemsigtighed baseret på krav stillet af bl.a. myndigheder og organisationens politikker.

- Compliance målsætninger, der omhandler organisationens overholdelse af lovgivning, politikker mv.

COSO terningen fremgår af figur 1. Heraf fremgår samspillet mellem de 5 kontrol komponenter og målsætnin-



Figur 1: COSO Cube. Kilde: 'Internal Control – Integrated Framework – Executive Summary' af Committee of Sponsoring Organizations of the Treadway Commission

gerne for intern revision samt det forhold at det interne kontrol system kan fungere på flere forskellige organisatoriske niveauer.

Intern kontrol principper

I nedenstående fremgår de enkelte komponenter af intern kontrol og de principper, der understøtter den enkelte komponent. Principperne kan opfattes som en specificering af komponenten. Alle principperne relaterer sig til operationelle, rapporteringsmæssige og Compliance målsætninger.

Kontrolmiljø

Kontrolmiljøet er organisationen og ledelsens fokus på interne kontroller og understøttes af følgende principper:

P1: Organisationen udviser en forpligtigelse til at handle etiks og med høj integritet.

P2: Bestyrelsen er uafhængig i forhold til direktionen og overvåger udviklingen og udførelsen af organisationens interne kontrol.

P3: Direktionen etablerer en struktur, rapporteringslinjer og passende bemyndigelser og ansvar for at muliggøre opfyldelse af organisationens mål.

P4: Organisationen udviser evne til at tiltrække, udvikle og fastholde kompetente medarbejdere relevante for opfyldelse af organisationens mål.

P5: Organisationen holder den enkelte medarbejder ansvarlig for deres ansvar i relation til intern kontrol implementeret for at muliggøre opfyldelse af organisationens mål.

Risikovurdering

En organisations evne til at nå dets målsætninger forøges hvis den formår, at identificere de væsentlige risici, der er forbundet med målsætningen og evner at foretage en tilstrækkelig vurdering af omfanget disse risici. Risikovurderingen understøttes af følgende principper:

P6: Organisationen specificerer målsætningen tilpas klar, så det er muligt at identificere og vurdere de risici der relaterer sig til målsætningen.

P7: Organisationen identificerer risici for at organisationens mål ikke opnås og analyserer hvordan risiciene skal håndteres.

P8: Organisationen vurderer muligheden for besvigelser ved identifikation af risici for at organisationens mål ikke opnås.

P9: Organisationen identificerer og vurderer ændringer der væsentligt kan påvirke det interne kontrol system.

Kontrolaktiviteter

Kontrolaktiviteter er de faktiske handlinger, der foretages ved udførelsen af intern kontrol og omhandler følgende principper:

P10: Organisationen identificerer og udvikler kontrolaktiviteter, der begrænser de identificerede risici for at organisationen når dets mål til et acceptabelt niveau.

P11: Organisationen identificerer og udvikler generelle IT kontroller, der understøtter målopfyldelsen.

P12: Organisationen forankrer kontrolaktiviteterne gennem politikker, der definerer, hvad der er krævet og procedurer der omsætter politikkerne til handling.

Information og kommunikation

Effektiviteten af intern kontrol er i stort omfang afhængig af organisationens evne til at indsamle information og evnen til at kommunikere krav og forventninger mht. intern kontrol og understøttes af følgende principper:

P13: Organisationen indhenter eller genererer og bruger relevant information til at understøtte det interne kontrol system.

P14: Organisationen kommunikerer internt om bl.a. mål og ansvar for den interne kontrol i det omfang det er nødvendigt for at understøtte det interne kontrol system.

P15: Organisationen kommunikerer med eksterne parter om forhold, der påvirker det interne kontrol system.

Overvågning
Løbende overvågning medvirker til at sikre, at det interne kontrol system fungerer efter hensigten og understøttes af følgende principper:

P16: Organisationen identificerer, udvikler og udfører igangværende og/eller enkeltstående vurderinger af hvorvidt de enkelte komponenter af intern kontrol er til stede og fungerer.

P17: Organisationen vurderer og kommunikerer rettidigt mangler i den interne kontrol til dem, der er ansvarlige for at adressere manglerne, herunder direktionen og bestyrelsen når det er nødvendigt.

Effektiv intern kontrol

Et effektivt intern kontrol system giver en begrundet overbevisning/sikkerhed for opnåelse af enhedens mål. Intern kontrol medvirker til, at reducere risikoen for ikke at nå de opsatte mål for en, to eller alle tre kategorier af målsætninger. En effektiv intern kontrol kræver:

- At hvert af de fem komponenter og relevante principper er til stede og fungerer.

- De fem komponenter fungerer sammen på en integreret måde, hvorefter alle fem dele kollektivt reducerer risikoen for at organisationen ikke at nå et mål.

Hvis der opstår stor tvivl om tilstedeværelsen af de fungerende komponenter eller relevante principper, eller om komponenterne arbejder sammen på en integreret måde, kan den overordnede organisation ikke konkludere, at den har efterlevet kravene til et effektivt system af intern kontrol.

Vurderingen af effektiviteten af udformningen, implementeringen og udførelsen af intern kontrol er baseret på et skøn. Brugen af skøn inden for de begrænsninger som er fastsat via lovgivning, regler, regulativer og standarder forøger ledelsens mulighed for, at træffe en bedre beslutning omkring intern kontrol, men kan ikke garantere et perfekt resultat.

Selv om intern kontrol giver en begrundet overbevisning/sikkerhed for at opnå organisationens mål, er der stadig begrænsninger. Intern kontrol kan ikke forhindre dårlige skøn eller beslutninger, eller for den sags skyld eksterne begivenheder som kan være skyld i at organisationen fejler i at opnå de operationelle mål. Selv et effektivt system af intern kontrol kan fejle.

Operationel risikostyring

Af Ph.d. stud. Ulrik Christiansen,
Forsvarsministeriets Interne Revision

Introduktion

I dagligdagen hjælper søgemaskiner som Google med at finde de oplysninger, som er mest relevante for vores søgekriterier. I stedet for at vise en komplet og præcis søgning med alle oplysninger fra internettet, sikrer algoritmen, at resultatet af søgningen prioriteres, og den forsøger dermed kun at vise de mest relevante oplysninger afhængigt af vores valg af søgekriterier.

På samme måde er det ambitionen, at risikostyring skal give lederen information og viden om risiko. Derfor bruges der stadig flere rammeværker som eksempelvis COSO ERM til at tilpasse de organisatoriske processer og den operationelle praksis. Målet er her at få data fra driften, som kan rapportere på, hvilke risici der er (identificere), hvilken konsekvens de kan få (vurdering), og hvad der kan gøres ved det (respons/aktion). På den måde bidrager risikostyring til, at det bliver muligt for ledelsen at træffe hensigtsmæssige beslutninger på et faktuelt grundlag.

I forlængelse af ambitionen om at få styr på risici anvender flere organisationer diverse modeller og matrixer til at vurdere modenheden af deres risikostyring, niveauet af deres forsvarslinjer mod utilsigtede hændelser, og om de anvender den bedste praksis for de interne kontroller (eksempelvis Hamann og Andreasen artikel i INFO nummer 49 fra december 2011). Denne ambition er beundringsværdig, og har sikkert hjulpet mange organisationer i gang med en formaliseret og eksplicit måde at arbejde med risiko på.

Udfordringen er imidlertid, at ambitionen bygger på mindst to forudsætninger. For det første - at risiko kan defineres entydigt for organisations operation, og for det andet at risiko oversættes ens på tværs af de organisatoriske niveauer.

Dette har to umiddelbare indbyggede problemstillinger, som kan få alvorlige konsekvenser. For det første er en fuldkommen repræsentation af risiko umulig – der vil altid være sorte svaner, eller noget andet vi ikke kan indfange, når vi kategoriserer risiko (det viste Knight[1] allerede i 1921). For det andet, at de risici som rapporteres fra den operationelle frontlinje til direktionsgangen - hvor de typisk passerer et eller flere organisatoriske niveauer - vil blive tillagt forskellig betydning op gennem det organisatoriske hierarki.

Med andre ord kan vi ikke være sikre på, at de risici som blev identificeret i den organisatoriske frontlinje, også er de samme risici, som bliver reflekteret i de Pixi-bogs versioner, som bliver forelagt direktionen eller den øverste ledelse. Vi har derfor ikke en særlig god fornemmelse for, om de risici der præsenteres for den øverste ledelse, er de rigtige, eller om de er retvisende – det afgøres kun af fremtiden!

De to forudsætninger bygger på det faktum, at risici alt andet lige må være knyttet til en eller anden form for værdiskabelsesproces. Helt banalt afhænger vores opfattelse og forståelse af risiko af, hvad vi tillægger værdi. For entydigt at vurdere risici skal vi altså eksplicit kunne definere, hvor, hvad og hvordan værdi skabes eller forstås i vores organisation. Det er ikke så nemt, og det er nok baggrunden for, at de fleste organisationer har haft - og stadig har - så svært ved at håndtere de operationelle risici.

Denne artikel argumenterer derfor for, at rammeværkerne for risikostyring kan blive en risiko i sig selv. Vi bør derfor vurdere, hvad vi faktisk styrer på, når vi forsøger at styre risiko. Er det eksempelvis bestemte typer af interne kontroller? - de organisatoriske processer? - og i så fald hvilke? - eller er det begivenheder i alt almindelighed?

Afledt af denne vurdering bliver det efterfølgende muligt at overveje, hvordan denne styring konkret bidrager til den operationelle frontlinjes værdiskabelsesproces, samt håndteringen af de risici som opstår som en integreret del af denne proces.

Artiklen præsenterer først problemstillingerne med den operationelle definition af risiko. Artiklen giver derefter et kort praktisk eksempel på, hvordan usikkerhed omsættes til risiko, og derefter rapporteres fra den operationelle frontlinje til direktionsgangen. Afslutningsvis præsenterer artiklen eksempler på mulige løsninger, der kan afbøde

[1] Frank Hyneman Knight (1885–1972), amerikansk økonom og forfatter til bogen "Risk Uncertainty and Profit" fra 1921

konsekvenserne af de to indledende forudsætninger i det daglige arbejde med risikostyring.

At definere risiko i praksis

Begrænsningen i en praktisk definition af risiko er, at det kun indfanger, det vi umiddelbart kan opfatte (perception). COSO ERM har forsøgt at omgå dette ved kun indirekte at definere risiko, og i stedet definerer risikostyringsprocessen. COSO definitionen kommer nok tættest på målet, når den beskriver risiko som begivenheder med negativ indvirkning på værdiskabelsen eller muligheden for at nå fastsatte mål.

Definitionen giver en intuitiv fornemmelse af hvad risiko er, men er ikke tilstrækkelig. Den introducerer implicit en tids dimension – hvornår skal den negative indvirkning indtræffe? Samtidig er definitionen ikke eksplicit om, hvad der konkret menes med begivenhed, værdiskabelse og fastsatte mål.

På tværs af økonomi, psykologi og sociologi har man længe kendt til udfordringen om at definere risiko. Både Frank Knight, Harry Markowits, John Maynard Keynes, Daniel Kahneman og Ulrich Beck har alle forsøgt at indfange risiko i deres akademiske arbejde. Selvom flere af dem har modtaget nobelprisen i økonomi – herunder også psykologen Daniel Kahneman – er deres definitioner af risiko heller ikke tilstrækkelige, hvilket illustrerer udfordringen i at præcisere, hvad der konkret menes med usikkerhed, værdi eller eksponering, og det er næsten umuligt at omsætte det til noget praktisk, fordi det afhænger af det enkelte individ. Den mere teoretiske definition er derfor stadig et heftigt debatteret emne i flere akademiske tidsskrifter.

Hvis vi vender tilbage til Knights arbejde fra 1921, minder COSO definitionen mere om Knights definition af usikkerhed end om hans definition af risiko - måske er det derfor, at mange forskere fremhæver usikkerhedsmomenterne af det som praktikere kalder risikostyring. Usikkerhedsstyring lyder med rette helt forkert, men hvor er styringen i helt konkret risikostyring?

Styringen af det som praktikere kalder risiko, ligger i de konkrete værktøjer som anvendes til at håndtere usikkerhedsmomenter i hverdagen. Det er derfor mere hensigtsmæssigt, at definere et aspekt af hvordan vi opfatter risiko – eksempelvis hvordan en konkret risikomatrix bidrager til at omsætte usikkerhed til risiko og dermed gør det muligt at styre et aspekt af risiko. Dermed bliver det meningsløst at spørge til om en konkret risikomatrix indfanger risiko. Det er mere praktisk at spørge til, om den pågældende risikomatrix er brugbar for den daglige drift, og om det fremmer en adfærd, som den øverste ledelse finder ønskelig.

Et praktisk eksempel på operationel risikostyring

Jeg vil nu gennemgå et praktisk eksempel på risikostyring mellem tre organisatoriske niveauer. Eksemplet er taget fra mit forskningsprojekt, hvor jeg undersøger den operationelle risikostyring af de 4-6 mia. kr., som Forsvaret årligt investerer i materiel i en eller anden form (enten nyindkøb eller vedligeholdelse). Eksemplet er generelt, og illustrerer den velkendte proces, hvor information gradvist tilpasses for hvert organisatorisk niveau. For at gøre beskrivelsen så illustrativ som muligt, anvender jeg tre niveauer – operationelt, taktisk og strategisk niveau.

Forsvarets investeringer går ikke altid efter hensigten, og det sker, at de fra tid til anden ender som forside historier i diverse medier. Forsvarets ledere er hverken dovne, dumme eller ekstraordinært dristige, men risikostyringen har sin egen indbyggede logik der skaber visse udfordringer. Denne logik knytter sig til oversættelserne på de organisatoriske niveauer, hvor der bliver taget meget forskellige hensyn.

På det operationelle niveau identificeres opståede eller kommende begivenheder, som kan få indvirkning på tid, ressourcer eller kvaliteten af den pågældende investering. Hver måned vurderes alle identificerede risici og kategoriseres i en centralt defineret rapport. Derefter uploades rapporten på Forsvarets interne net. Helt overordnet sker der her en oversættelse af usikkerheden fra dagligdagen ind i de prædefinerede risikokategorier.

På det taktiske niveau vurderes de mulige strategiske konsekvenser af de rapporterede risici. De enkelte investeringer vurderes i forhold til andre investeringer og rangordnes i forhold til deres vurderede relative strategiske betydning. Derudover beskrives de iværksatte korrigerende handlinger, og endeligt beskrives en række forslag til yderligere respons og afbødende aktiviteter. Helt overordnet sker der her en oversættelse og prioritering af den samlede portefølje af investeringer, hvor kun de væsentligste investeringer rapporteres til det strategiske niveau.

På det strategiske niveau vurderes de rapporterede iværksatte aktiviteter og yderligere aktiviteter diskuteres. På baggrund af diskussionerne og risikorapporterne iværksættes der evt. yderligere analyse af problemstillingerne. De rapporterede risici vurderes her overordnet i forhold til forskellige interessenter. Helt overordnet sker der her en oversættelse af den politiske dagsorden, og af hvordan den øverste ledelses omdømme bedst sikres i forhold til de rapporterede risici.

Samlet set sker der for hvert organisatorisk niveau en reducering af informationen om risici. Den reduceres ved, i højere og højere grad at rubricere de samlede investeringer i fælles kategorier, der kan kvantificeres. Denne proces er helt klassik for alt ledelsesinformation, hvor informationen gøres gradvis mere ens, så den bliver sammenlignelig med anden information. Udfordringen er imidlertid, at jo mere kontekst der fjernes, og jo mere sammenlignelig informationen bliver, jo mere bliver det også muligt at koble informationen til abstrakte problemstillinger.

Eksemplet kan opsamles i følgende overordnede tendenser for det enkelte niveau:

- **Operationelt**: Fokus på begivenhedernes indvirkning på tid, kvalitet og ressourcer. (Projektstyring)
- **Taktisk**: Prioritering af de rapporterede risici i forhold til deres strategiske betydning. (Porteføljestyring)
- **Strategisk**: Vurdering af de rapporterede risici og de iværksatte handlinger i forhold til interessenter. (Interessent styring)

Fokus på de enkelte niveauer er meget forskellig, og informationen anvendes i forlængelse af dette fokus. Udover denne tendens sker oversættelse mellem de organisatoriske niveauer på baggrund af en informationsfiltrering, som foretages af de enkeltindivider, som arbejder med informationen.

Harvard forskeren Annette Mikes har her et godt bud, hvordan de enkelte individer behandler informationen. Mikes bruger en distinktion mellem to typer af oversættelse af risikoinformationen. Det hun kalder kvantitative skeptikere og kvantitative entusiaster. Kvantitative skeptikere tillægger kun risikoinformationen værdi som et input til deres overvejelser, hvor kvantitative entusiaster ser informationen som et spejl af virkeligheden, der reflekterer den nødvendige handling.

Samlet set er det derfor noget usikkert, om de rapporterede risici er retvisende, når de når til det strategiske niveau. Risikostyringen mindsker altså ikke usikkerheden, men reducerer flertydigheden, så den øverste ledelse kan overskue de samlede investeringer. Præcision er altså ofret for anvendelighed – graden af hvor anvendelig informationen er, bliver først bedømt engang i fremtiden.

Eksemplet er taget fra en offentlig kontekst, som ikke nødvendigvis kan generaliseres til private sektorer som banksektoren. Forsvaret har en meget stærk enhedskultur med en meget struktureret ledelsesuddannelse, man kan derfor argumentere for, at hvis det ikke er muligt at lave en stringent oversættelse mellem de organisatoriske niveauer i Forsvaret, så er det ikke nemmere i andre organisationer med en svagere enhedskultur.

Mulige løsninger

Jeg har i de foregående afsnit skitseret udfordringer med at definere risiko i praksis og med at rapportere risiko på tværs af organisationen. Jeg vil i dette afsluttende afsnit skitsere mulige løsninger på udfordringerne.

Vi styrer, på det vi kan opfatte som risiko (projektstyring, porteføljestyring, interessentstyring), og ikke på risiko i sig selv. På baggrund af den konkrete styring bruger vi også informationerne om risici forskelligt. Informationerne bør derfor i højere grad bruges som et input til en beslutningsproces frem for et endeligt billede på, hvad der skal gøres. Der er stor forskel på at tage ledelsesinformationen om risiko alvorligt eller bogstaveligt. Hvis vi tager dem bogstaveligt, og agerer på dem - som var de et billede af verden - øger vi muligheden for, at de bliver i en risiko i sig selv. Hvis vi derimod tager ledelsesinformation om risiko alvorligt, og samtidig er opmærksomme på den oversættelsesproces, der gør, at risiko bliver styrbar og muligt at rapportere, får vi mulighed for at imødegå noget af den usikkerhed, som stadig er en del af informationen.

Der bruges en del ressourcer på at indfange, rapportere og beregne risiko i sin fuldstædighed. Jeg er usikker på om ressourcerne vil gøre mere gavn, hvis de blev brugt på at understøtte den operationelle frontlinje i at håndtere usikkerhed. Måske skal risikostyring ikke bare anvendes til at topledelsen bliver informeret om diverse oversatte usikkerheder – men også bruges til at understøtte den operationelle frontlinjes mulighed for selv at håndtere og imødegå utilsigtede hændelser.

På tværs af en organisation har ledere forskellige perspektiver på, hvad der skaber værdi, og hvad der er en risiko. Jeg er usikker på om ambitionen med at definere risiko på tværs af organisationen er hensigtsmæssig, eller sagt på den anden måde, hvis alle havde den samme forståelse af værdi og tilgang til risici ,bliver det så ikke svært at skabe værdi!

Når vi googler information på nettet, skal vi til stadighed forholde os kritisk til informationen. Samtidig kan vi ikke sidde og google hele dagen, indtil vi har et fuldkomment svar – vi skal på et eller andet tidspunkt i gang med dagens opgaver, og nogle gange bliver vi nødt til at tisse på hegnet, for at vide om det giver stød!

Sikkerhed & Revision 2013

Af revisionschef, Bethina Hamann, Nationalbanken

Indledning

For jer der endnu ikke kender konferencen Sikkerhed & Revision kan jeg fortælle, at den blev afholdt for 12. gang på de sædvanlige dage – 1. torsdag og fredag i september - på Radisson SAS Royal Hotel.

Sikkerhed & Revision er udsprunget af 'græsrødderne' fra sikkerhedsfunktioner og it-revision og er i dag bygget op af en hoved stream og to daglige sessioner i streams der fordeles over 'Sikkerhed', 'Governance, Risk og Compliance (GRC)' og 'Revision'. I alt 21 sessioner á 45 minutter, med det formål at sikre opdateret viden om trends inden for it, trusler mod virksomhedernes it anvendelse og værktøjer til at imødegå truslerne samt hvorledes vi bør forholde os revisionsmæssigt hertil. Konferencen arrangeres af et uafhængigt konferenceudvalg bestående af repræsentanter fra de foreninger, hvis medlemmer er typiske deltagere. Det er ikke hensigten, at der skal tjenes penge på konferencen, men i høj grad hensigten, at der er et forum, hvor vi hvert år har mulighed for et par dages opdatering på et område i hastig udvikling. Konferenceudvalget for årets konference var:

- Bethina Hamann, IIA, formand for konferenceudvalget
- Ole Svenningsen, ISACA Denmark Chapter
- Lars Thomsen og Jens Lundsgaard, Foreningen af eksaminerende it-sikkerhedsledere
- Thomas Kühn og Lisbeth Kieme, FSR – danske revisorer

Forberedelse til konferencen

Da vi sidste år skulle i gang med at forberede dette års konference, satte vi os sammen og brainstormede på, hvad der kunne være af interesse det kommende år. Vi lader os typisk inspirere af, hvad der sker i samfundet omkring os, nye tiltag og ikke mindst deltageres input til, hvad der kan være interessant at få større indblik i. Noget udspringer således af konkrete interesser, andet af behov for information og ny viden og andet igen, kan være tendenser vi ser og tager op til overvejelse. Mange af de diskussioner vi havde undervejs, viste sig at kunne sammenfattes i nogle lidt større spørgsmål, nemlig:

Risici er blevet hverdag, men er virksomhederne klar til at håndtere dem? Er de vokset os over hovedet? Er det blevet for kompliceret? Mangler der kvalifikationer? Eller har vi bare fået større risikoappetit?

De fleste af os påvirkes dagligt af informationer om trusler, der efterhånden synes at kunne komme alle steder fra, og mod alle fronter. Så vores slut mål for årets konference skulle være at få perspektiveret trusselsbillederne og forhåbentlig derigennem sikre, at vi har fokus på det rigtige – nemlig det, der kan skade os mest, og som vi kan gøre noget ved. Vi tog udgangspunkt i de overordnede spørgsmål og herefter perspektivering ud fra samfundet, virksomhederne, virksomhedsledelsen og helt ned på specifikke ansvarsområder i virksomhederne. Alt sammen med en ambition om, at få udvidet horisonten og få noget praktisk anvendeligt med hjem.

Evaluering af konferencen

Med cirka 90 deltagere og gode evalueringer ser det ud til, at det lykkedes. Vi er glade for, at der var stor interesse for deltagelse, og at konferencen kunne leve op til det programmet stillede i udsigt. Det fulde program kan ses via dette link. I får her muligheden for at se eller gense nogle af de væsentlige budskaber fra konferencen, koncentreret om besvarelse af de overordnede spørgsmål, der må formodes at vedrøre os alle, og påvirker vores dagligdag.

Risici er blevet hverdag – kan og vil virksomhedsledelsen håndtere dem?

Årets åbningstaler, Stine Bosse, talte over vores store indledende spørgsmål. Det gjorde hun i sin egenskab af sin tidligere direktørstilling, nuværende bestyrelsesposter og som privatperson. Det var et rigtig godt indlæg fra en stor personlighed med gode, klare og brugbare budskaber.

Det fremgik tydeligt, at risikobilledet er ændret, og der er forventninger om, at de nye risici bliver bragt til ledelsens kendskab, og på en måde så de kan forstås. Stine fortalte meget levende om Tryg's situation før finanskrisen, hvor hun også blev introduceret til en række fancy finansprodukter, som finansfolk forsøgte at overbevise hende om, at Tryg skulle investere i. Stine fortalte, at hun blev ved med at spørge ind til sagen, da det var vigtigt for hende

at forstå, hvad produkterne indeholdt, og hvilke risici de medførte – men hun fik ikke svar hun kunne forstå, og valgte at sige nej tak. Stine er overbevist om, at folk gik ud af møderne og talte mindre pænt om, hvad den kvindelige direktør var i stand til at forstå, men ingen tvivl om, at Stines udgangspunkt er, at hvis man ikke kan komme til at forstå hvad der sker – så skal der siges nej.

Budskabet var det samme fra Jens Lund, CFO for DSV, der på sin egen måde gav lige så klart udtryk for, at hvis folk ikke kunne forklare ham, hvilke risici han sidder tilbage med, under og efter implementering af et givent projekt – så må folk hjem og tænke sig om en ekstra gang. Hans grundholdning er, at hvis det ikke kan forklares, vil det sandsynligvis ikke blive håndteret korrekt. Jens talte mere om det taktiske og operationelle i risikostyring, men udgangspunktet er det samme som Stines mere strategiske synsvinkel – nemlig at sikre bundlinjen. Jens' budskab er klart, at der kontinuerligt skal være styr på risici, fordi det giver bundline. Der ligger i øvrigt et planchesæt, der godt og inspirerende fortæller om DSV ledelsens sikkerhedsovervejelser.

Budskaberne er, at virksomhedsledelsen ønsker, på alle niveauer - strategisk, taktisk og operationelt, at få beskrevet risici og folk skal kunne forstå dem, før virksomheden kaster sig ud i nye tiltag. Så skal vi tro på Stine og Jens, skal vi ikke gå rundt og overbevise os selv om, at ledelsen ikke vil høre om risici, ej heller at ledelsen har opgivet at håndtere de risici vi udsættes for hver dag. Tværtimod – der er brug for, at risici kendes og håndteres til virksomhedens bedste. Stine er således overbevist om, at Tryg kom igennem krisen, fordi de tog strategiske beslutninger om at sige nej til finansprodukter, hun ikke kunne bringes til at forstå, mens Jens er overbevist om, at risikostyring skal være forankret på såvel taktisk som operationelt niveau, og det vigtigste er fælles forståelse og transparens. Begge ønsker en kultur, der sikrer håndtering af risici i tide.

Kulturen som bærer af ansvar for risici

Spørgsmålet er så, om vi har en sådan kultur rundt omkring i virksomhederne. Brian Christiansen, leder af Risk Assurance i PWC gik så langt som til at sige, at det fra bestyrelsernes side ser ud til, at de eksisterende processer ikke længere giver den sikkerhed, der er brug for til at afdække og sikre mod risici. Vi er simpelthen ikke opmærksomme nok. Brian brugte (på sine i øvrigt informative plancher) Alice (figur 1) som et eksempel.

Trusler mod it anvendelsen og håndteringen af dem

Truslerne 'udefra' blev perspektiveret af Thomas Kristmar fra Krisestyrings- og operationsafdelingen i Center for Cybersikkerhed under Forsvarets Efterretningstjeneste med indlægget 'Hvad lurer i cyberspace?'.

Det var tydeligt, at der var udfordringer i den danske infrastruktur. Som 'gammel' it revisor vil jeg end dog tillade mig at sige gammelkendte udfordringer. Nogle af de ting virksomhederne stadig ikke benytter sig af i tilstrækkelig grad, er eksempelvis sikring af redundans i kommunikation, firewall og forsyning, netværkssegmentering og beskyttelse mod DDOS angreb. Forhold jeg personligt tager for givet, at der er kontrol over, men det er åbenbart ikke det generelle billede. Det betyder også, at det er forhold, vi, som revisorer, stadig bør følge op på, ligesom Thomas fremhævede, at det stadig er vigtigt at sikre patchning, logning, administratorrettigheder, installering af programmer og overvågning af exe-filer, fordi det til stadighed er der de ser, at svagheder bliver udnyttet, og der sker brud på sikkerheden. Så bare bliv ved med at tage emnerne op – også selvom I måtte synes, at det er trivialiteter!

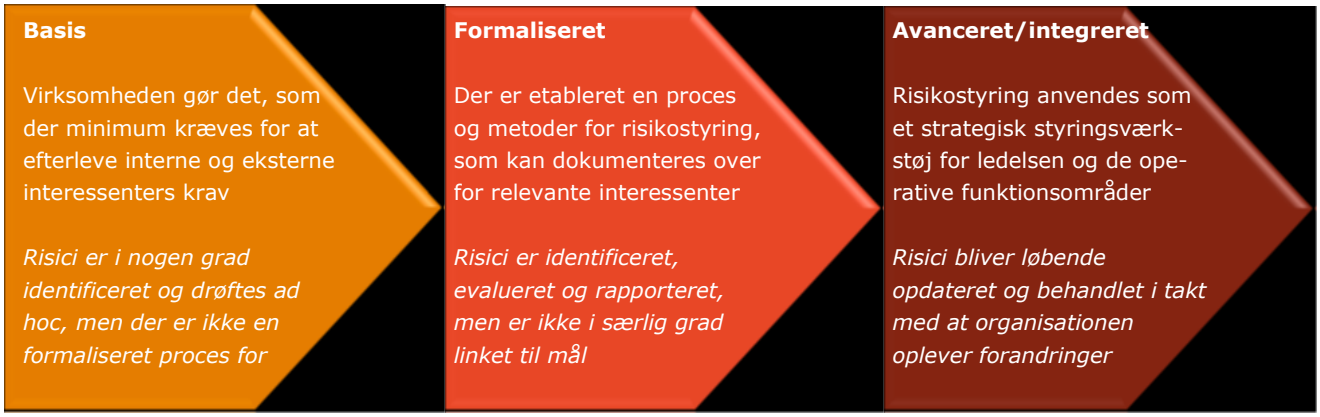
En anden vigtig pointe fra Thomas var, at det desværre ofte er tilfældet, at det er andre end den virksomhed med de svage kontroller der bliver ramt. Det kan ofte være

Figur 1.

"Alice var ved at blive træt af at sidde med hendes søster ved flodbredden, og af ikke at have noget at lave, da en hvid kanin med lyserøde øjne pludselig dukkede op tæt på. Det fandt Alice ikke specielt bemærkelsesværdigt, ej heller det, at kaninen sagde til sig selv: "Åh gud! Åh gud! Jeg kommer for sent!" gav anledning til undren hos Alice. Da hun tænkte det igennem efterfølgende, slog det hende dog at ***hun burde have undret sig*** *over dette, selvom det i situationen virkede ganske naturligt".*

Denne fortælling om – at du set i bakspejlet burde have undret dig – er hjertet i identificering og styring af nyopståede risici, som er det bestyrelserne pt. anvender tid på i deres risikostyring

Risikostyring (PWC plancher)



kunder eller andre samarbejdspartnere, og derfor er det ikke nødvendigvis virksomheden selv der rammes af deres egne dårligdomme. Det er en ikke uvæsentlig udfordring, hvorfor der kan være behov for regulering via lovgivningen. Som revisorer kan vi vel også være med til at gøre dette forhold klart for virksomhedsledelsen.

Håndtering af it truslerne ud fra et godt og simpelt perspektiv blev præsenteret af Raini Mihkelson, Head of IT Security, Danske Bank, Estonia Branch. Det var et godt praktisk eksempel på det, der ofte er meget vanskeligt at få etableret, men ikke mindre vigtigt af den grund, nemlig en samlet risikovurdering af de it services, der kører i virksomheden. Det var holdt simpelt i regneark, og afspejlede en stillingtagen til såvel it funktionens som forretningens risikovurderinger. Således en meget praktisk og derfor også anvendelig tilgang, der i det daglige sikrer håndtering af de risici, der måtte opstå i relation til afvikling af it driften. For de af jer der måtte være mere specifikt interesserede i dette, kan der helt sikkert formidles kontakt – til resten af jer – I skal bare vide, at det kan lade sig gøre! Selvfølgelig kræver det vilje, samarbejde og tid, men det behøver hverken være for kompliceret eller for uoverskueligt. Det vigtige er, at det sker.

> The Standard of Good Practice for Information Security:
> *"To enable individuals who are responsible for target environments to identify key information risks and determine the controls required to keep those risks within acceptable limits"* (ISF)

Rapportering af risici, mitigering og hændelser

Vi skal have rapporteret risici klart og tydeligt til ledelsen, som Stine Bosse og Jens Lund også fremhævede. Da ledelsesrapportering ofte er en af de sikkerhedsdiscipliner, der er vanskelig at håndtere, bliver den ofte forbigået. Revisionschef Thomas Gi Scharf fra KMD (som afløser for sikkerhedschef Rasmus Theede) kom med bud på, hvorledes de er i gang med at styrke deres rapportering, og hvor vigtigt det er med de rigtige data at rapportere på. For KMD er det rigtig vigtigt, at kunne redegøre for it-sikkerheden overfor kunderne, og derfor stiller bestyrelse og direktion også krav om et højt sikkerhedsniveau – og det sidste sted man ønsker at læse om KMD's svagheder er i avisen. Derfor er der et behov for rapportering, men det er uvant, og det kan være en stor udfordring at få rapporteringen målrettet en betydning for KMD's forretning. Indtil videre er det konstateret, at det er væsentligt med korte rapporter, der giver overblik, og fremhæver de væsentligste problemstillinger med angivelse af de tiltag, der imødegår de konstaterede risici. Det lyder som om, at en sådan tilgang vil opfylde de behov, der er givet udtryk for, fra virksomhedsledelsens synspunkt jf. de tidligere indlæg.

Beredskabsplaner og krisehåndtering

Når så uheldet er ude, er det væsentligt, at have planer at følge og kendskab til, hvad der skal gøres – og stadigvæk være klar over, at der vil være forhold, der ikke er taget højde for. Evne til at agere i et meget uforudsigeligt forløb er også vigtigt.

Stig Haudahl er security manager for DSS i Norge, der er primær leverandør af it til statslige enheder i Norge. Han fortalte om, hvordan der i 2006 blev startet et projekt om centralisering af statens it, og i 2008 skulle alle migreres over på den nye platform. Som i mange andre it projekter skete det, mens man stadig befandt sig i en udviklingsfase, uden tilstrækkelige test og med eneste prioritet at få tilgængelighed og stabile leverancer på plads. I de efterfølgende år drejede det sig så om, at holde kunderne tilfredse. Desværre blev sikkerhed først blev noget, der kom fokus på efter manglerne på samme havde været på forsiden af aviserne. I løbet af en

weekend var der sendt store mængder af data ud fra regeringens ubeskyttede netværk, og ingen vidste, hvem det var, eller hvilke data det drejede sig om. Desværre er det ofte de store sager, der skal til for at flytte fokus hos virksomhedsledelsen, men det gode var, at der i de efterfølgende år blev gjort mange tiltag mod at sikre overholdelse af sikkerhedsstandarder og etablering af beredskab.

Planerne og beredskabet kom på plads – og de virkede også, for de blev testet af under katastrofen i Oslo i 2011, hvor der skete markant skade på statens it – men de var (selvfølgelig) ikke fuldstændige, og det var vanskeligt at få bragt tingene tilbage til normalen på trods af gode og testede beredskabsplaner. Der vil altid være noget der ikke er taget højde for, bl.a. fordi vi ikke undrer os ligesom i eksemplet med Alice. Stig kunne vise, at der lå risikovurderinger på en ulykke af samme type som den bombe, der blev udløst, det var endda omtalt i aviserne, men alligevel var det ikke fundet relevant nok at tage højde for en så omfattende skade. Stigs budskab var dog på ingen måde, at man så kan lade være med at lave beredskabsplaner – tværtimod. Det er vigtigt, at der er noget at gå frem efter, så ikke alt er kaos, og det man skal tage stilling til i krisesituationen kan begrænses.

En anden der også har oplevet, at skulle håndtere en krise tæt på, er Per Gullestrup fra Clipper Group, der var ansvarlig leder, da Clipper blev udsat for en kapring af et af deres skibe tilbage i 2008.

Shipping er en branche, der er stærkt reguleret af lovgivning, så der er reelt set taget højde for mange ting (jf. også Thomas Kristmars ønske om mere regulering på cybersikkerhedsområdet). Så her var der planer og vejledninger for, hvilke tiltag der skulle ske, hvilket efter Pers opfattelse er meget vigtigt for at kunne håndtere en så vanskelig situation, hvor man ikke bare kan følge sine medmenneskelige følelser og første indskydelser.

Ingen tvivl om, at Pers første indskydelse var at betale, hvad der forlangtes og få sat gidslerne fri. Det er bare ikke sådan det foregår, for siges der ja, viser erfaringerne, at kravet øges, og det i øvrigt bare giver større incitament til at foretage yderligere kapringer. Så for at sikre mod fremtidige kapringer er man også nødt til at følge den proces en sådan situation tilskriver, hvor et meget væsentligt element er, at vente og ikke følge sine indskydelser. Det gør det om muligt endnu mere vigtigt, at der foreligger gennemtestede planer, som man har forholdt sig til mange gange. Hos Clipper har de også sikret, at beredskabsplanerne indeholder mange menneskelige aspekter, så virksomheden hele tiden handler med samvittighed. Dette omfatter blandt andet en hurtig kontakt til og sikring af de pårørende til mandskabet på det kaprede skib.

Pirateri kan synes 'langt væk' fra vores dagligdag, men det er værd at overveje, hvor godt vi er 'klædt på' i de forskellige virksomheder, når vi kigger på et stadigt mere voldeligt trusselsbillede, og når det kommer til trusler mod virksomhedernes aktiver gennem trusler mod mennesker. En perspektivering i retning af sikring mod kidnapning der kan anvendes som middel i et røveri, samt voldelige røverier i det hele taget bør iagttages. Herunder også, hvorvidt beredskabsplaner sikrer mod alle de trusler, der dukker op i krisen, eksempelvis kontakt til pårørende etc. så også virksomhedens samvittighed og image sikres bedst muligt i situationen.

Pers fremstilling bærer tydeligt præg af, at man skal have rigtig gode planer for håndtering af kriser, man skal have arbejdet så meget med dem, at man tror på, at de tager højde for det, man som virksomhed ønsker de skal tage højde for – og når det uforudsigelige så sker, såvel i form af problemer som muligheder, er man langt bedre klædt på til at håndtere dem.

Hvad kan vi selv gøre?

Set i et lidt større perspektiv er en beredskabsplan ikke bare en beredskabsplan. Det er et strategisk syn på, hvorledes virksomheden ønsker at fremstå og være klædt på til at håndtere risici på taktisk og operationelt niveau. Således kom vi fra det meget operationelle niveau, tilbage til den store betydning det har for det strategiske. Med et risikobillede i stadig forandring, og virksomhedsledelser, der forventer, at risici håndteres på alle niveauer i virksomheden, som en del af virksomhedens DNA, er det værd at notere sig, at vi alle bør være beredt. Sikkerhedsovervejelser skal 'implementeres' i den enkelte medarbejder – og det kan starte med dig! Det er vigtigt, at vi alle sikrer kontinuerlig opdatering af det operativsystem, der sidder mellem ørene på os, så vi er opmærksomme og klar til at håndtere det der måtte komme.

Håber I føler jer opdateret – som skrevet er I velkomne til at kigge de forskellige plancher igennem på www.fsr.dk/sikkerhed2013, der ligger meget mere end det, der er omtalt her – og I er selvfølgelig også meget velkomne på næste års konference, den 4.-5. september

Nye IFRS-regler om forsikringskontrakter

Af Partner, Statsautoriseret revisor, Lars T. Skovsende, Deloitte

1. Indledning

Formålet med IFRS 4, fase II-projektet, er at forbedre regnskabsaflæggelsen for forsikringskontrakter ved at udvikle én samlet global regnskabsstandard af høj kvalitet, som giver ensartet regnskabsmæssig behandling af disse kontrakter. IASB har gennem de forgangne år forsøgt at opnå størst mulig overensstemmelse mellem de internationale revisionsstandarder og de amerikanske regnskabsstandarder (udstedt af FASB). IFRS 4, fase II er udviklet i samarbejde med FASB og er derfor i vid udstrækning i overensstemmelse med den amerikanske standard med nogle enkelte undtagelser.

2. De 7 spørgsmål fra IASB

Efter udsendelse af høringsudkast til IFRS 4, fase II i 2010 modtog IASB et omfattende antal høringssvar med en lang række kritikpunkter af den foreslåede standard. IASB har i det nye høringsudkast indarbejdet en række ændringer, som var af så væsentlig karakter, at det var vurderet nødvendigt at spørge brugerne endnu engang ved at genudsende høringsudkastet til en fornyet høringsrunde. I forhold til denne høringsrunde har IASB alene bedt om tilbagemeldinger på 7 konkrete emner, hvoraf de væsentligste er; løbende regulering af servicemargen, anvendelse af anden totalindkomst, indregningskriterier for kontrakter med ret til bonus, overgangsbestemmelser samt præsentation.

3. Centrale begreber i høringsudkastet

I det følgende beskrives en række centrale begreber i høringsudkastet.

3.1 Definition af en forsikringskontrakt

Definitionen af en forsikringskontrakt er **uændret** i forhold til den nugældende IFRS 4.

En forsikringskontrakt defineres som

"en kontrakt, hvori den ene part (udstederen af forsikringskontrakten) påtager sig betydelig forsikringsrisiko for den anden part (forsikringstageren) ved at indvillige i at yde erstatning til forsikringstageren, hvis en bestemt usikker fremtidig begivenhed (den forsikrede begivenhed) påvirker forsikringstageren negativt."

3.2 Afgrænsninger til finansielle instrumenter mv.

Sondringen mellem forsikringskontrakter og finansielle instrumenter er fortsat afgørende for den regnskabsmæssige behandling af den enkelte kontrakt. IFRS 4, fase II, ændrer ikke væsentligt ved klassifikation af forsikringskontrakter (IFRS 4), finansielle instrumenter (IFRS 9) og andre kontrakter. Finansielle garantier (herunder kreditforsikring), hvor forsikringstageren er eksponeret for et tab, kan nu behandles som forsikringskontrakter, hvis forsikringsvirksomheden tidligere har behandlet disse kontrakter som forsikringskontrakter.

Opdeling i forsikringskontrakt og opsparingsdel

En række forsikringskontrakter indeholder et betydeligt opsparingselement, som – hvis det var en særskilt kontrakt – skulle behandles som et finansielt aktiv eller en finansiel forpligtelse efter IAS 39/ IFRS 9.

Der skal kun ske opdeling (*unbundling*) i en forsikringskontrakt og en opsparingsdel, hvis delene ikke er nært forbundet (*closely related*). Et opdelt element af opsparing skal behandles som et finansielt aktiv eller en finansiel forpligtelse ifølge IFRS 9.

Opdeling i forsikringskontrakt og opsparingsdel/ låneforhold

Samlet betyder det, at en forsikringsvirksomhed skal behandle disse kontrakter som følger:

(a) Hvis delene er nært forbundet (*closely related*), skal IFRS 4, fase II, anvendes på hele kontrakten.

(b) Hvis delene ikke er nært forbundet (*not closely related*), skal IFRS 4, fase II, anvendes på forsikringsdelen, og IFRS 9 skal anvendes på opsparingsdelen.

Tilbagekøbsoptionen (*surrender option*) for traditionelle livs- og pensionsforsikringer værdiansættes på baggrund af forventninger til forsikringstagernes anvendelse af optionen med en justering for risikoen for, at den faktiske adfærd afviger fra den forventede.

Indbyggede afledte finansielle instrumenter

Høringsudkastet foreskriver, at afledte finansielle instrumenter, der er indbygget i en forsikringskontrakt

(*embedded derivatives*), skal udskilles og måles særskilt efter reglerne i IFRS 9, medmindre det afledte finansielle instrument opfylder definitionen på en forsikringskontrakt for sig selv. Dette betyder, at de eksisterende regler fra IFRS 9 videreføres i høringsudkastet.

I henhold til høringsudkastet skal et indbygget, afledt finansielt instrument udelukkende adskilles fra hovedkontrakten og regnskabsmæssigt behandles som et afledt finansielt instrument efter IFRS 9, hvis følgende to betingelser begge er opfyldt:

a. De økonomiske karakteristika og risici, der er forbundet med det indbyggede, afledte finansielle instrument, er ikke nært forbundet (*closely related*) med hovedkontraktens økonomiske karakteristika og risici
b. Et særskilt instrument med samme betingelser som det indbyggede, afledte finansielle instrument opfylder definitionen på et afledt finansielt instrument og er omfattet af IAS 39/IFRS 9.

3.3 Måling til indfrielsesværdi
Formålet med indregning og måling af forsikringskontrakter er primært at måle de aktiver og forpligtelser, som opstår ifølge forsikringskontrakter i forhold til indfrielse af forpligtelsen.

Indregning og grænser
En forsikringsvirksomhed skal indregne de rettigheder og forpligtelser, der opstår som følge af en forsikringskontrakt, når forsikringsvirksomheden er forpligtet af kontrakten. Indregningstidspunktet sker ved det tidligst tidspunkt af følgende begivenheder:

- Begyndelsen af dækningsperioden
- Forfaldstidspunktet for forsikringstagernes første betaling
- Ved tegningstidspunktet, hvis kontrakten er tabsgivende

I høringsudkastet betragtes forsikringskontrakten som en samling af rettigheder og forpligtelser, inklusive muligheden for, at forsikringstageren opsiger eller fornyer kontrakten (*embedded options*). IASB mener, at disse forhold er en integreret del af forsikringskontrakten, og modellen skal omfatte indvirkningen heraf ved måling af den første byggeklods.

Måling heraf foretages inden for en tidsramme, som i høringsudkastet defineres som forsikringskontraktens tidsramme (*contract boundary*). Dermed redegøres for det økonomiske indhold af forsikringskontrakten. Det vil kræve en nøje vurdering af behandlingen heraf for at sikre, at fremtidige præmier kun medregnes, i det omfang præmierne vedrører eksisterende kontrakter (*within the contract boundary*).

Med tidsrammen menes et tidspunkt i fremtiden, hvor forsikringsvirksomheden enten kan vælge ikke længere at tilbyde forsikringstageren dækning eller nægte forsikringstageren dækningen, eller hvor forsikringsvirksomheden har ret til eller reel mulighed for at vurdere den risiko, der er forbundet med forsikringstageren, og efterfølgende fastsætte en ny pris, der afspejler risikoen.

Måling
Forsikringsforpligtelser skal som udgangspunkt måles til **indfrielsesværdien** med tillæg af en servicemargen, der eliminerer gevinst ved tegning.

Definition af indfrielsesværdien (present value of the fulfilment cash flows)
Udkastet definerer indfrielsesværdien som *"den forventede nutidsværdi af de fremtidige udbetalinger, fratrukket de fremtidige indbetalinger, der vil opstå, i takt med at forsikringsvirksomheden opfylder forsikringskontrakten, justeret for effekterne af usikkerhed vedrørende beløbet og timingen af disse fremtidige pengestrømme."*

For at opfylde disse kriterier skal udstedere af forsikringskontrakter, som udgangspunkt, måle forsikringsforpligtelser efter følgende **fire grundlæggende byggeklodser**:

Servicemargen	Udtryk for den indtjening, som virksomheden forventer at tjene, når alle skader og omkostninger er betalt og efter risikotillæg.
Risikotillæg	Reflekterer at præmie og erstatning ikke er sikre, men udtrykker bedste skøn. Det er en buffer til afdækning af en eventuel negativ udvikling i skøn og estimater. Frigivelse heraf er indtjening.
Diskontering	Afspejler nutidsværdien.
Forventede pengestrømme (statistisk middelværdi)	Omfattende alle ind- og udbetalinger i form af præmie, udgifter til erstatninger og omkostninger, herunder erhvervelsesomkostninger.

3.4 Forventede fremtidige pengestrømme
Den første byggeklods er et estimat over de fremtidige pengestrømme, der opstår på baggrund af kontrakten. Formålet er ikke at udarbejde ét bedste skøn, men i princippet at identificere de nødvendige antal relevante scenarier og udarbejde et neutralt skøn over sandsynligheden for hvert enkelt scenarie.

Forsikringsvirksomheden skal ved målingen af forsikringsforpligtelser udarbejde estimater over forventede fremtidige pengestrømme, der er:

a. **eksplicitte**, dvs. beregnet med reference til forventede pengestrømme, der troværdigt afspejler træk på forsikringsvirksomhedens ressourcer.
b. **set fra virksomhedens perspektiv, dog konsistente med observerbare markedspriser**. Det er ikke i henhold til udkastet krævet, at en forsikringsvirksomhed skal søge efter markedspriser på alle variable, bortset fra visse markedsvariable, hvor der er aktuelle og direkte observerbare markedspriser såsom f.eks. rentesatser og noterede børskurser.
c. **neutrale** og baseret på al tilgængelig information om størrelse, timing og usikkerhed i alle pengestrømme, der stammer fra kontraktlige forsikringsforpligtelser.
d. **aktuelle**, dvs. at de svarer til forholdene ved regnskabsperiodens udløb
e. **fra eksisterende kontrakter**, altså indenfor de eksisterende kontrakters grænser.

Enhed for måling af fremtidige pengestrømme (level of measurement)
Ved måling af forsikringskontrakter arbejdes der med en porteføljebetragtning af ensartede forsikringskontrakter med samme risikoprofil. Dette skyldes også, at det ikke vil være muligt at foretage en pålidelig måling af størrelsen af den fremtidige udbetaling kontrakt for kontrakt. Det vil derimod være muligt ud fra en portefølje af forsikringskontrakter at sandsynliggøre de fremtidige forventede pengestrømme og at opgøre størrelsen af disse pålideligt.

Erhvervelsesomkostninger
En forsikringsvirksomhed skal modregne de direkte og indirekte erhvervelsesomkostninger i opgørelse af de forsikringsmæssige hensættelser. Vurderingen skal foretages på porteføljeniveau. I målingen af erhvervelsesomkostninger kan der således indgå omkostninger fra såvel realiserede salg som ikke-realiserede salg.

3.5 Diskontering
Diskonteringen skal baseres på aktuelle markedsbaserede diskonteringssatser, som justerer de estimerede pengestrømme til aktuelle beløb. Diskonteringssatsen skal være konsistent med de observerbare aktuelle markedspriser for pengestrømmene fra forsikringsforpligtelsen med hensyn til eksempelvis timing, valuta og likviditet. Det betyder, at diskonteringssatsen typisk vil tage udgangspunkt i en risikofri rente før skat, hvortil der tillægges en faktor for illikviditet, hvis relevant.

Diskonteringssatsen kan bestemmes ud fra et top-down eller bottom-up tilgang, hvilket fra et teoretisk perspektiv vil resultere i samme diskonteringsrente. Såfremt der anvendes en top-down tilgang tages der udgangspunkt i investeringsaktiver, som tilhører forsikringsforpligtelser, hvorefter der korrigeres faktorer, som ikke er relevante i forhold pengestrømme, som tilknytter sig forsikringsforpligtelserne.

3.6 Risikotillæg

Hensættelsen til forsikringskontrakter indeholder et risikotillæg, som er udtryk for den kompensation forsikringsvirksomheden vil kræve for at påtage sig risikoen ved at opfylde og indfri forsikringskontrakten.

Der er metodefrihed for opgørelsen af risikotillægget, men virksomheden skal i noter oplyse om, hvilket metoder og overvejelser, som har dannet grundlag herfor. Virksomheden skal definere, hvilket konfidensinterval risikotillægget afspejler.

Risikotillægget skal måles ved første indregning og justeres ved hver balancedato ved at vurdere, hvor meget risiko, der resterer i forpligtelserne, og reduceres dermed over tid, i takt med at forsikringsvirksomheden fritages for risiko.

Risikotillægget skal opgøres pr. portefølje af forsikringskontrakter, der har ensartede risici, og som styres som én samlet portefølje. Der må tages hensyn til diversifikation mellem porteføljer eller negativ korrelation mellem virksomhedens porteføljer, således at diversifikationen afspejler den risikoprofil, som virksomheden normalt tager i betragtning, når virksomhedens risici vurderes.

3.7 Servicemargenen

Servicemargenen er et udtryk for det kontraktmæssige overskud, der skal indregnes systematisk over forsikringskontraktens dækningsperiode.

Servicemargenen opstår ved første indregning af forsikringsforpligtelser, hvis de forventede udbetalinger er mindre end de forventede indbetalinger. Servicemargen sættes ved første indregning til et beløb, der svarer til, at

forsikringsvirksomheden ikke indregner en indtægt på tegningstidspunktet. Servicemargenen kan ikke være negativ; altså hvor fremadrettede indbetalinger er mindre end fremadrettede udbetalinger. Det vil sige, at ved tabsgivende kontrakter skal tabet straksindregnes på indregningstidspunktet.

Servicemargenen indregnes systematisk i resultatopgørelsen over dækningsperioden således, at det afspejler den service, som virksomheden leverer til forsikringstager.

Servicemargenen skal opgøres på kohorte niveau; altså for ensartede forsikringskontrakter inden for en portefølje opdelt efter tegningstidspunkt og dækningsperiode.

Servicemargenen skal justeres på hver balancedato – men alene i forhold til ændringer i skøn relateret til fremtidig dækning eller Fremrykning eller forsinkelse i tilbagebetaling af investeringskomponent, såfremt dette er relateret til fremtidig dækning. Servicemargen må derimod ikke reguleres ved ændring i estimater for allerede indtrufne begivenheder (afløbstab/gevinst) eller ved ændring i risikotillæg. Disse reguleringer skal derimod føres direkte over resultatopgørelsen.

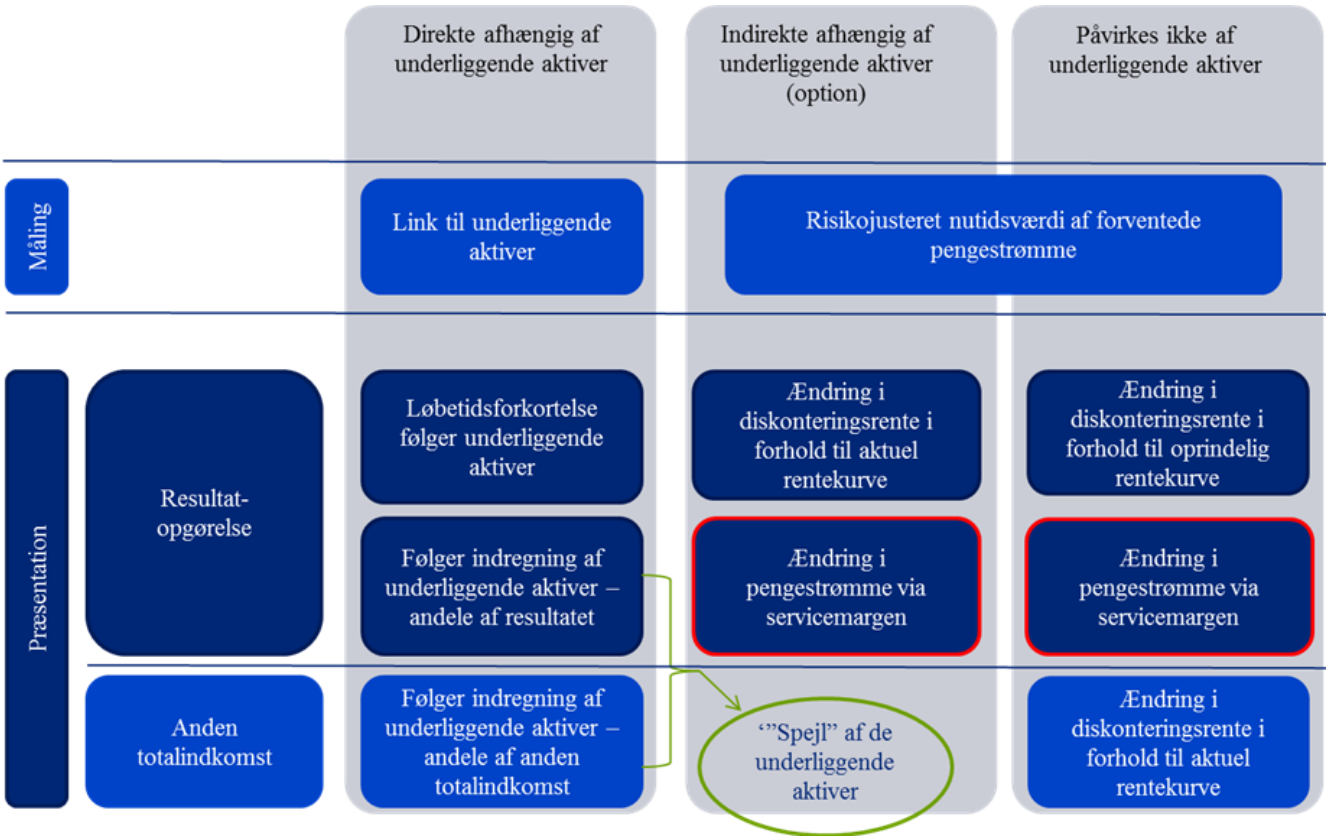
3.8 Undtagelser for anvendelse af byggeklodsmodellen

Forsikringskontrakter med kort dækningsperiode
Forsikringskontrakter med en dækningsperiode på ca. 12 måneder eller derunder kan i dækningsperioden måles til en tilnærmet indfrielsesværdi (*"premium allocation model"*) svarende til de nuværende præmiehensættelser. Præmiehensættelsen (*pre-claims liabilities*) beregnes ved første indregning, som de forventede præmier eventuelt fratrukket direkte henførbare erhvervelsesomkostninger. I skadebehandlingsperioden skal forsikringsvirksomheden opgøre erstatningshensættelserne efter byggeklodsmodellen – dog skal erstatningshensættelsen ikke diskonteres, såfremt denne forventes udbetalt indenfor 12 måneder.

Det vil være valgfrit om forsikringsvirksomheden modregner erhvervelsesomkostninger i præmiehensættelsen.

Kontrakter med ret til bonus
Såfremt forsikringskontrakten er linket til de underliggende aktiviteter enten i form af specifikke aktiver, en

Samlet overblik over indregningsmodeller for kontrakter med og uden ret til bonus



porteføljе af kontrakter eller i forhold til alle aktiver og forpligtelser i virksomheden som helhed, skal forsikringskontrakten måles i henhold til de underliggende aktiviteter – altså som et spejl af de underliggende aktiviteter (*mirroring approach*). Byggeklodsmodellen skal således ikke anvendes for disse kontrakter.

3.9 Præsentation af forsikringskontrakter i resultatopgørelse

Præsentation og indregning i resultatopgørelsen følger overordnet set et formål om at præsentere en omsætning eller et volume-mål for den leverede service i regnskabsperioden. Høringsudkastet arbejder med en omsætning *"Insurance contract revenue",* som udtrykker den leverede service i perioden. Omsætningen – naturlig præmie – udtrykker dermed summen af *a) forventede skader i perioden, b) amortisering af erhvervelsesomkostninger, c) frigivelse af servicemargen og d) frigivelse af risikotillæg.* Den indtjente præmie har således ikke nogen kobling til den faktiske indbetalte præmie. Det direkte opsparingselement af den indbetalte præmie vil ikke på noget tidspunkt indgå i den naturlig præmie eller indtrufne skader og vil dermed ikke på noget tidspunkt ramme resultatopgørelsen, men vil være en ren balancepostering.

Anden totalindkomst

Hovedreglen i forhold til indregning af ændring af diskontering af pengestrømme er, at løbetidsforkortelsen i forhold til den oprindelige rente på indregningstidspunktet indregnes i resultatopgørelsen under investeringsresultat, mens ændringer i den aktuelle rentekurven i forhold til sidste regnskabsperiode indregnes under anden totalindkomst (*Other comprehensive income*).

Anvendelsen af anden totalindkomst til kursregulering af rentekurven nødvendiggør, at det er nødvendigt at definere en række aktiver, hvor værdireguleringen i henhold til IFRS 9 også sker via anden totalindkomst til at afdække forsikringsforpligtelserne med henblik på at undgå accounting mismatch.

3.10 Overgangsregler og ikrafttrædelsestidspunkt

Som omtalt i indledningen vil IFRS 4, fase II formentlig træde i kraft 1. januar 2017 eller 2018, idet IASB har besluttet, at der som minimum skal gives en treårig implementeringsperiode.

Ved implementering af standarden skal der for igangværende forsikringskontrakter opgøres og indregnes den resterende del af servicemargen. Det vil sige, at der for alle forsikringskontrakter, der er i kraft på implementeringstidspunkt, skal servicemargen opgøres på det oprindelige indregningstidspunkt og fordeles over dækningsperioden for at kunne opgøre den resterende del på implementeringstidspunktet. Dette skal som minimum gøres 3 år bagudrettet, mens der for perioder før dette kan anvendes nogle simplifikationer til en mere pragmatisk opgørelse.

De øvrige elementer i byggeklodsmodellen opgøres i forhold til den fremadrettede dæknings-/afviklingsperiode baseret på nutidsværdien af de fremadrettede pengestrømme til dækning af den resterende dækningsperiode.

Insurance Europe - talerør for den europæiske forsikringsbranche

Af policy advisor David Luyckx og policy advisor Mette Baden, Insurance Europe

Insurance Europe er den europæiske forsikrings- og pensionsbranches fællesorganisation. Organisationen blev grundlagt i Paris i 1953 som Comité Européen des Assurances (CEA), for at repræsentere de europæiske forsikringsselskabers interesser ved The Organisation for Economic Co-operation and Development (OECD). Med etableringen af det Europæiske Fællesskab og den efterfølgende udvikling af den Europæiske Union, skiftede CEA gradvist sit fokus og flyttede sine aktiviteter fra Paris til Bruxelles.

> Insurance Europe repræsenterer over 5.000 selskaber, der samlet tegner sig for ca. 95% af alle præmieindtægter i Europa.

Organisationen etablerede sin afdeling i Bruxelles i 1987. I 2007 blev alle aktiviteter flyttet til den europæiske hovedstad. Hermed kunne sammenslutningen både effektivt repræsentere de europæiske forsikrings- og genforsikringsselskaber i EU og i internationalt regi, og opnå anerkendelse som forsikringsbranchens definitive talerør. Insurance Europe flyttede til deres nuværende lokaler i marts 2012, beliggende rundt om hjørnet fra Parlamentet og midt imellem Kommissions områdekontorer.

Insurance Europe har i øjeblikket 32 medlemmer. De nationale brancheorganisationer fra de 27 EU lande og fem brancheorganisationer fra ikke-EU medlemmer (Island, Lichtenstein, Norge, Schweiz og Tyrkiet) – derudover har to lande observatørstatus (San Marino og Serbien).

De danske interesser hos Insurance Europe varetages af Forsikring og Pension. Gennem de nationale brancheorganisationer repræsenterer Insurance Europe mere end 5.000 virksomheder, der tegner sig for ca. 95% af alle præmieindtægter i Europa. De omfatter alle former for genforsikringsselskaber, paneuropæiske selskaber, monoliners, gensidige samt små og mellemstore selskaber. Tilsammen genererer de præmieindtægter for € 1.100 milliarder, beskæftiger mere end en million ansatte og investerer i nærheden af € 8.400 milliarder i den europæiske økonomi.

Organisationsstruktur

Insurance Europes nuværende præsident, Sergio Balbinot, har 30 års erfaring fra forsikringsbranchen og sidder i en stilling som Chief Insurance Officer og vicedirektør for Generali koncernen i Italien, Europas tredjestørste forsikringsselskab.

Insurance Europes sekretariat arbejder tæt sammen med medlemmerne for at samle de europæiske forsikringsselskabers holdninger og skabe én fælles stemme for den europæiske forsikringsbranche. Sekretariatet administrerer ni komiteer, syv styregrupper og 20 arbejdsgrupper, hvor medlemmerne består af nationale eksperter, der analyserer og diskuterer problemstilligner og lovforslag – på såvel europæisk som internationalt plan - som kan have en indvirkning på forsikringsbranchen. Formændene for de forskellige komiteer og arbejdsgrupper er repræsentanter fra den europæiske forsikringsbranche.

De tre ledende instanser i den europæiske brancheorganisation er generalforsamlingen, ledelsen og den strategiske bestyrelse. Generalforsamlingen er den ledende instans og består af alle de nationale brancheorganisationer der i fællesskab udgør sammenslutningen Insurance Europe. Ledelsen har en administrativ og en beslutningstagende rolle og består af de administrerende direktører fra alle brancheorganisationerne der er medlemmer af Insurance Europe. Den strategiske bestyrelse leverer strategisk vejledning og består af 10 repræsentanter fra de nationale brancheorganisationer og fem repræsentanter CFO Forum, CRO Forum, the Pan European Insurance Forum (PEIF), Reinsurance Advisory Bord (RAB) og the Association of Mutual Insurers and Insurance Co-operatives in Europe (AMICE).

Insurance Europes virke

Insurance Europes virke er firfoldigt.

Først og fremmest skaber organisationen et forum for udveksling af viden og best-practice mellem medlemsorganisationerne og bistår med information, som vedrører den europæiske forsikringsbranche.

Dernæst bestræber de sig på at levere konstruktive og pålidelige bidrag til institutionerne, politikere og de national tilsynsmyndigheder, samt skabe opmærksomhed omkring strategisk interessante emner for de europæi-

ske forsikrings- og genforsikringsselskaber, samtidig med at fremme et åbent og konkurrencedygtigt marked til gavn for de europæiske forbrugere.

Insurance Europe organiserer arrangementer, der bringer politiske beslutningstagere sammen med forsikringsbranchen for at øge bevidstheden om forsikrings- og genforsikringsselskabernes rolle i samfundet og deres bidrag til den økonomiske vækst og udvikling. Målet er at fremme det positive billede af branchen og styrke forbrugernes tillid og tryghed.

Endelig er det Insurance Europes mål at være det første kontaktpunkt for de, der søger oplysning om den europæiske forsikringsbranche.

Publikationer

Insurance Europes sekretariat forfatter ofte publikationer, der er frit tilgængelige både på tryk og online på www.insuranceeurope.eu og som omhandler en bred vifte af emner inden for forsikring. Publikationerne skaber indsigt i branchens prioriteter og ekspertise og er rettet mod enten forbrugere eller eksperter.

"How insurance works" er en af de mest læste udgivelser, da den belyser de grundlæggende aspekter af forsikring, dets værdi og vigtigheden af bæredygtige og konforme lovgivningsrammer. De nyeste udgivelser omfatter blandt andet folderen "Funding the future". Denne udgivelse beskriver detaljeret forsikringsbranchens rolle som ideelle investorer i langsigtede investeringer, som de politiske beslutningstagere forventer vil fremme den økonomiske vækst i Europa. Folderen forklarer, hvorfor en tilpasset regulering er grundlæggende for at sikre, forsikringsselskabernes evne til at opretholde langsigtet finansiering af økonomien og stabilisering af de finansielle markeder.

Udover ad-hoc publikationer, udgiver Insurance Europe også en årlig rapport der opsummere deres involvering i europæiske beslutningstiltag. Endvidere udgives de årlige statistiske analyser "European Insurance in Figures" og "Key Facts", som oplyser om præmier og skadesanmeldelser, investeringer, forsikringsselskaber og distributionskanaler relateret til hver enkelt forsikringssektor.

En betroet samarbejdspartner

Insurance Europe varetager og formidler branchens interesser over for de vigtigste europæiske og internationale institutioner samt i medierne. På europæisk plan har de oparbejdet et stærkt samarbejde med – blandt andre – Kommissionen, nøglemedlemmer af Parlamentet, EIOPA og European Systemic Risk Board (ESRB). Organisationen er også medlem af European Financial Reporting Advisory Group (EFRAG), som bidrager til de internationale regnskabsstandarder, der udarbejdes af IASB og stiller teknisk ekspertise og rådgivning om regnskabsmæssige forhold til rådighed for Kommissionen.

Insurance Europe driver sekretariatet for den nye globale forsikringsorganisation, GFIA[1], som blev grundlagt i oktober 2012. Gennem GFIA koordinerer Insurance Europe samarbejdet med 36 andre internationale forsikringsorganisationer. Formålet er, at tale med én fælles stemme på globalt plan og sikre indflydelse på fremtidig regulering ved at virke som kontrapart til de politiske beslutningstagere og standardsættere såsom OECD, IAIS, IASB, FSB[2] og G-20 landene.

Nøgleområder i Insurance Europes arbejde

Udfordringerne for den europæiske og globale forsikringsbranche er større end nogensinde, da internationale politikere og lovgivere er fast besluttede på at adressere finansielle risici og fremskynde lovreformer for at fremme den finansielle stabilitet og forbrugertilliden. Der er således et tiltagende behov for at Insurance Europe fremhæver forsikringsselskabernes positive og vigtige rolle, for at sikre, at ny regulering for forsikringsselskaberne er passende og ikke forårsager utilsigtede restriktioner i måden hvorpå forsikringsbranchen opererer. Endvidere overvåger og forholder de sig til de forsikringsmæssige spørgsmål, der opstår på den tætpakkede europæiske og globale dagsorden for finansiel stabilitet – ofte med meget korte deadlines. Det ses ofte, at medarbejdere flyver ud af døren for at mødes med repræsentanter fra Kommissionen eller assistenter for rapporteurs fra Parlamentet, der har behov for at få besvaret forsikringstekniske spørgsmål i en frokostpause, mellem møder eller lige inden forhandlinger skal i gang.

I kølvandet på den finansielle krise, har politikere verden over søgt at forny og styrke regulerings-og tilsynsmæssige foranstaltninger for at undgå systemiske risici i den finansielle sektor grundet indbyrdes afhængighed. Insurance Europe arbejder blandt andet hårdt på at begrunde, hvorfor forretningsmodellen for forsikringsselskaber og udformningen af forsikringsmarkedet udgør langt færre systemiske risici end for eksempel banksektoren.

Med støtte fra G-20 landende og FSB, er IAIS ved at udvikle en fælles tilsynsstruktur for internationale forsikringskoncerner (ComFrame). Formålet er at øge samarbejdet mellem de nationale tilsynsmyndigheder samt luk-

[1] Global Federation of Insurance Associations - http://www.gfiainsurance.org/en/
[2] Financial Stability Board

ke ethvert hul i lovgivningen, der kan hindre et betryggende tilsyn. Ydermere planlægger IAIS at udvikle et globalt kapitalkrav for forsikringsselskaber der skal pålægges global systemisk vigtige selskaber (G-SIIs[3]) inden for en meget ambitiøs tidsramme. Det såkaldte backstop kapitalkrav for G-SIIs skal være færdigudviklet og anerkendt af G-20 landende inden udgangen af 2014 og det globale kapitalkrav skal være færdigudviklet inden udgangen af 2016. Insurance Europe og GFIA deltager i diskussionerne omkring udviklingen af disse krav for at sikre, at de globale kapitalkrav der udvikles af IAIS ikke pålægger de europæiske forsikringsselskaber endnu et rapporteringskrav – især taget i betragtning at risikobaserede kapitalkrav vil blive introduceret under det kommende Solvens II regime i EU.

Insurance Europe har ligeledes haft fuld fokus på Solvens II og har været involveret i både de politiske og tekniske drøftelser for at sikre, at resultaterne af drøftelserne også er noget der kan anvendes i praksis. I 2012 var Insurance Europe involveret i udviklingen af rapporteringsskabelonerne fra EIOPA med vedvarende feedback og løbende møder, hvilket førte til væsentlige forbedringer i både skabelonerne og tidsrammen for at implementere dem nationalt.

Andre arbejdsgrupper i organisationen beskæftiger sig blandt andet med udviklingen af de sammenhængende internationale regnskabsstandarder IFRS 4 fase II (til forsikringskontrakter) og IFRS 9 (for finansielle instrumenter), Kommissionens foreslåede ændringer til EUs forordning om databeskyttelse. Forskellige skattemæssige spørgsmål er også et fokusområde, som omfatter såvel eventuel indførelse af en afgift på finansielle transaktioner i 11 medlemsstater, som compliance med det nye amerikanske regelsæt for at forebygge skatteunddragelse for finansielle virksomheder kaldet Foreign Account Tax Compliance Act (FATCA), samt den foreslåede genindførelse af en tilknyttet genforsikringsskat i USA, som kan pålægge ekstra omkostninger på europæiske forsikrings- og genforsikringsselskaber.

Insurance Europe leverer blandt andet også jævnligt teknisk input til EU debatter om for eksempel bæredygtig tilpasning til klimaændringer og forsikringsdækning. De deltager i diskussioner omkring emner som clearingforpligtelsen for forsikringsselskaber under EMIR, sikring af bedre forbrugerbeskyttelse, konkurrenceretslige emner og europæisk kontraktret. Kort sagt, Insurance Europe dækker alle områder der berører forsikringsbranchen.

For mere information og adgang til publikationer se vores hjemmeside http://www.insuranceeurope.eu/

[3] http://www.iaisweb.org/Financial-Stability-Macroprudential-Policy-Surveillance-988

ISA 610 - Anvendelse af interne revisorers arbejde

Af koncernrevisionschef
Poul-Erik Winther, Alm. Brand

ISA 610 Using the Work of Internal Auditors er blevet ajourført af IAASB og er blevet oversat til dansk under navnet "Anvendelse af interne revisorers arbejde". Som et resultat af ajourføringen af ISA 610 er ISA 315 "Identifikation og vurdering af risici for væsentlig fejlinformation igennem forståelse af virksomheden og dens omgivelser" ligeledes blevet tilpasset med henblik på at redegøre for, hvordan en intern revisionsfunktion kan benyttes til ekstern revisors risikovurdering.

De ajourførte standarder træder i kraft for revision af regnskaber med perioder, der slutter 15. december 2013 eller senere, og er dermed også gældende for 2013 for virksomheder, der anvender kalenderåret som regnskabsår. Afsnittet, der omfatter direkte assistance, træder imidlertid først i kraft for perioder, der slutter 15. december 2014 eller senere.

Med henblik på at give vejledning om fortolkning af standardens bestemmelser har foreningen FSR – danske revisorers Finansielle Udvalg (FINU) og Foreningen af Interne Revisorer IIA nedsat en fælles arbejdsgruppe, der har set nærmere på, hvilke problemstillinger de ajourførte standarder rejser.

Arbejdsgruppen var sammensat således:

Fra FSR - danske revisorer:
Henrik Barner Christiansen, KPMG
Benny Voss, PwC
Kasper Bruhn Udam, Deloitte
Per Lindholt, Beierholm
Jakob Dedenroth Bernhoft, sekretariatet

Fra IIA:
Kim Stormly Hansen, Nykredit
Carsten Allerslev Olsen, Danske Bank
Jesper Siddique Olsen, Danske Bank
Poul-Erik Winther, Alm. Brand

Arbejdsgruppens medlemmer består alle af personer, der arbejder inden for/med den finansielle sektor, og arbejdsgruppens kommissorium har således alene været at belyse anvendelsen af standarderne i forhold til finansielle virksomheder med intern revision omfattet af bekendtgørelse om revisionens gennemførelse i finansielle virksomheder mv. samt finansielle koncerner – i daglig tale kaldet "revisionsbekendtgørelsen".

Arbejdsgruppens arbejde er mundet ud i et notat, der beskriver de væsentligste ændringer i de reviderede standarder samt arbejdsgruppens praktiske fortolkningsbidrag til anvendelse af standarderne, for herunder at sikre en optimal anvendelse af intern revisions arbejde i forhold til standardernes krav.
Notatet er således ikke en generel gennemgang af ISA 610 og de problemstillinger, som denne standard giver anledning til.

Samtidig er det vigtigt at understrege, at alle fortolkninger og synspunkter, som fremgår, er arbejdsgruppens og ikke nødvendigvis et udtryk for hverken FSR-danske revisorers eller IIA's holdninger som sådan ligesom ændringer til de forhold der behandles eller de holdninger, der tilkendegives, efterfølgende kan vise sig nødvendige.

Arbejdsgruppens arbejde er afsluttet den 15. november 2013 og FSR - danske revisorer vil, med udgangspunkt i notatet, efterfølgende tage en generel drøftelse med Revisortilsynet med henblik på en fælles forståelse af god revisionsskik ved tilrettelæggelse og gennemførelse af revisioner, hvor ekstern revision anvender interne revisorers arbejde.

Notatet er tilgængeligt på såvel IIA's som FSR - danske revisorers hjemmeside.

Ud over notatet har arbejdsgruppen også udarbejdet en Q&A, der ligeledes er tilgængelig på foreningernes hjemmesider. Den er gengivet på de næste sider:

Q & A – ISA 610 (ajourført)

Vurdering af den interne revisionsfunktion

1.	Q:	Hvad menes med, at den interne revisionsfunktion skal anvende en systematisk og disciplineret metode?
	A:	Med en systematisk og disciplineret metode menes, at der eksisterer en hensigtsmæssig og dokumenteret revisionsmetodik der tager afsæt i ISA'erne, og som omfatter risikovurderinger, arbejdsprogrammer, dokumentation og rapportering. Art og omfang skal stå i rimeligt forhold til virksomhedens størrelse og kompleksitet. Det er arbejdsgruppens holdning, at konceptet bør beskrives uanset den interne revisionsfunktions størrelse.
2.	Q:	Hvad skal et kvalitetsstyringssystem indeholde?
	A:	Et kvalitetsstyringssystem skal indeholde passende politikker og procedurer, som er relevante for en intern revisionsfunktion, jf. eksempelvis den internationale standard om kvalitetsstyring ISQC 1 eller krav til kvalitetsstyring i standarder, der er fastlagt af relevante professionelle organisationer for interne revisorer. Sådanne organisationer kan også fastlægge andre relevante krav som f.eks. udførelse af periodisk, ekstern kvalitetskontrol.
3.	Q:	Er det muligt at opfylde kravet til kvalitetsstyring i en intern revisionsfunktion, hvor der kun er en medarbejder, en revisionschef?
	A:	Ja, det er arbejdsgruppens holdning, at dette er muligt, såfremt der er etableret et kvalitetsstyringsprogram, og kvalitetskontrolopgaven er outsourcet.

Fastlæggelse af arten og omfanget af den interne revisionsfunktions arbejde, som kan anvendes

4.	Q:	Hvad omfatter betydelige vurderinger ?
	A:	Betydelige vurderinger omfatter i henhold til standarden i det mindste følgende: • vurdering af risiciene for væsentlig fejlinformation • vurdering af tilstrækkeligheden af udførte test • vurdering af hensigtsmæssigheden af ledelsens anvendelse af forudsætningen om fortsat drift • vurdering af betydelige regnskabsmæssige skøn, og • vurdering af hensigtsmæssigheden af oplysningerne i regnskabet og andre forhold, som påvirker revisors erklæring.
5.	Q:	Hvad ligger der i, at ekstern revision skal foretage alle betydelige vurderinger?
	A:	Ekstern revisor skal selvstændigt foretage de betydelige vurderinger og må således have opnået tilstrækkeligt grundlag for at kunne foretage vurderingerne. Dette grundlag kan delvist bygge på informationer indsamlet af intern revision. Intern revision kan således fortsat foretage planlægning, risikovurdering og udførelse, men ekstern revision kan på de væsentlige og risikofyldte områder – områder hvor der udøves betydelige vurderinger - ikke udelukkende basere sig herpå, men skal på disse områder selvstændigt dokumentere egne vurderinger og supplerende handlinger.
6.	Q:	Betyder de nye krav, at ekstern og intern revision ikke længere kan udarbejde et fælles planlægningsdokument?
	A:	Nej. Det er arbejdsgruppens holdning, at der fortsat kan udarbejdes ét fælles planlægningsdokument, som kommunikeres samlet til bestyrelsen. Det fælles planlægningsdokument skal tillige beskrive, hvordan den eksterne revisor planlægger at anvende den interne revisionsfunktion. Den eksterne revision skal udføre og dokumentere egen revisionsplanlægning og sikre, at det fælles planlægningsdokument er i overensstemmelse med denne.

Identifikation af væsentlige og risikofyldte områder

7.	Q:	Ekstern revision skal selvstændigt foretage alle betydelige vurderinger. Betydelige vurderinger vil efter arbejdsgruppens holdning alt overvejende knytte sig til væsentlige og risikofyldte områder. Hvordan defineres væsentlige og risikofyldte områder?
	A:	Definitionen af "væsentlige og risikofyldte" områder er ikke ændret i forhold til øvrige ISA'er. Som eksempler på områder, der typisk vil være væsentlige og risikofyldte i finansielle institutter, kan nævnes områderne it, going concern, herunder solvens, skat og evt. skatteaktiv, immaterielle aktiver, eksempelvis goodwill, ejendomme, unoterede værdipapirer, afledte finansielle instrumenter og eventualforpligtelser. For kreditinstitutter vurderes endvidere eksempelvis udlån og garantier (nedskrivninger/hensæt-telser) og likviditet at indebære betydelige vurderinger, mens det for forsikrings-virk-somheder herudover bl.a. omfatter forsikringsmæssige hensættelser (liv og erstatning), illikvide investeringsaktiver mv. Eksemplerne er selvsagt ikke udtømmende, og identifikation beror på en konkret vurdering, der er helt afhængig af den enkelte virksomheds forhold.

Anvendelse af den interne revisionsfunktions arbejde

8.	Q:	Må genudførelse foretages tidsmæssigt samtidigt med, at intern revision udfører revision på området? Eller skal det være en separat proces?
	A:	Ekstern revisions genudførelse skal ske uafhængigt af intern revisions revision, men det er arbejdsgruppens holdning, at det af hensyn til en effektiv tilrettelæggelse af revisionen at dette med fordel kan ske i umiddelbar tilknytning hertil, eksempelvis som led i et fælles revisionsbesøg.
9.	Q:	Hvor meget af intern revisions arbejde skal der udføres genudførelse på?
	A:	Fastlæggelse af omfang skal ske på baggrund af en individuel og professionel vurdering fra virksomhed til virksomhed afhængigt af kompleksitet, risikovurdering, den foretagne vurdering af den interne revisionsfunktion mv. Ifølge standardens punkt A30 vil den eksterne revisor sandsynligvis koncentrere sin genudførelse på revisionsområder/-mål, hvor den interne revision har udøvet væsentlig vurdering ved planlægning, udførelse og konklusion, samt på områder med højere risiko for væsentlig fejlinformation.
10.	Q:	Hvor selvstændig skal genudførelse være? Må ekstern revision anvende den af intern revision indhentede dokumentation som grundlag for sin genudførelse, eller skal alle data genindhentes fra grundsystemer?
	A:	Det er arbejdsgruppens holdning, at den af intern revision fremskaffede dokumentation som udgangspunkt kan anvendes, men det er afgørende, at ekstern revision selvstændigt planlægger, udfører og konkluderer på revisionen.
11.	Q:	Gør det forhold, at der udføres genudførelse, at gennemgangen af det af intern revision udførte arbejde i øvrigt kan reduceres?
	A:	Ifølge standardens punkt A28 kan de handlinger, som ekstern revision udfører for at validere intern revisions arbejde, ud over genudførelse også omfatte forespørgsler, observation af IR's revisions-handlinger og gennemgang af arbejdspapirer. Ifølge punkt A30 tilvejebringer genudførelse større revisionsbevis end de øvrige 3 arter, hvorfor behovet for disse i visse tilfælde kan reduceres.

12.	Q:	Af standardens punkt A16 fremgår nogle eksempler på arbejde udført af den interne revisionsfunktion, som kan anvendes af den eksterne revision, herunder test af kontrollers funktionalitet og substanshandlinger, der involverer begrænset vurdering. Hvordan skal dette punkt fortolkes?
	A:	Det er arbejdsgruppens holdning, at listen over områder under punkt A16 hverken er udtømmende for, hvad ekstern revision kan anvende af intern revisions arbejde, eller begrænsende for, hvad intern revision må udføre. Den interne revisionsfunktion kan således fortsat udføre arbejdet, dog således at den eksterne revisor inddrages i hele revisionsprocessen, når der skal foretages en betydelig vurdering på revisions-målsniveau i forhold til den pågældende regnskabspost. Jo mere vurdering der er nødvendig ved planlægning og udførelse af revisionshandlingerne samt stillingta-gen til revisionsbeviset, desto flere handlinger vil den eksterne revisor skulle udføre selv, fordi anvendelsen af den interne revisionsfunktions arbejde ikke alene vil give den eksterne revisor tilstrækkeligt og egnet revisionsbevis.

Dokumentation - Aftaledokumenter

13.	Q:	Hvilken betydning har den nye standard for de ifølge revisionsbekendtgørelsen krævede aftaledokumenter (revisionsaftale og funktionsbeskrivelse)?
	A:	Det er arbejdsgruppens holdning, at ISA 610 kun påvirker de eksisterende aftaledokumenter i mindre om-fang. Der er givet forslag til korrektioner af revisionsaftale og funktionsbeskrivelse i det af arbejdsgruppen udarbejdede notat.

Direkte assistance

14.	Q:	Hvori adskiller direkte assistance sig fra anvendelse af intern revisions arbejde i øvrigt?
	A:	Direkte assistance er anvendelse af intern revision til udførelse af revisionshandlinger under direkte instruk-tion, overvågning og review af den eksterne revision. Ved anvendelse af intern revision som direkte assi-stance stilles krav til aftalegrundlag med den finansielle virksomheds ledelse og mellem intern og ekstern revision. I de tilfælde, hvor intern revision ikke i tilstrækkelig grad lever op til kravene i ISA 610 til, at eks-tern revision kan basere sig på intern revisions arbejde, kan direkte assistance overvejes.

Revisionsbekendtgørelsen - nu kommenteret af FSR

Af afdelingsdirektør Peer Højlund, Nykredit

I september 2013 bragte INFO artiklen "Ny bekendtgørelse om revisionens gennemførelse i finansielle virksomheder mv.", hvor ændringer og tilføjelser til bekendtgørelsen, set fra intern revisions synsvinkel, kort blev gennemgået.

Efterfølgende har FSR's Finansielle Udvalg (FINU) afsluttet et lignende arbejde, som er offentliggjort på FSR's hjemmeside den 6. november 2013, www.fsr.dk/ Faglige_informationer, vælg faneblad "Revision og erklæringsopgaver" og herefter linket "Den nye revisionsbekendtgørelse for finansielle virksomheder – notat og arbejdspapirer fra FINU".

FINU's notat består af et sammenfattende dokument med konklusionen på konsekvenserne af den nye bekendtgørelse samt 4 tilhørende bilag, herunder et bilag hvor ændringer i revisionsbekendtgørelsen gennemgås i detail og yderligere 3 bilag med konkrete arbejdseksempler på henholdsvis materialeliste, arbejdsinstruks og ledelseserklæring.

Udvidelse af arbejdet?

FINU argumenterer for, at der på visse områder vil blive tale om en udvidelse af det arbejde, der skal udføres, for at afgive de krævede konklusioner og oplysninger efter bekendtgørelsen. Som eksempler på sådanne områder nævnes bestemmelsen i §11, hvor revisor skal konkludere om, hvorvidt virksomhedens admini-strative og regnskabsmæssige praksis på væsentlige områder er tilrettelagt og fungerer på betryggende vis, samt §31 vedrørende gennemgang af kapitalforhold i tilknytning til going-concern vurderingen, herunder virksomhedens opgørelse af individuelt solvensbehov.

Omfanget af denne "udvidelse" kan diskuteres, og vil under alle omstændigheder være forskellig fra institut til institut. I artiklens bilag 1 har FINU foretaget en sammenholdelse af hidtidig og kommende praksis, for hvert af de punkter der fremgår af revisions-bekendtgørelsens bilag 2. Ved nærmere læsning bliver det dog klart, at udvidelsen af arbejdet ikke nødvendigvis er helt så omfattende som FINU's notat lægger op til. Eksempelvis er der for punkterne 10-17 anført, at gennemgang af politikker og retningslinjer, gennemgang af direktionens redegørelse vedr. virksomhedens risici mv., stikprøvevis efterprøvning af indre sammenhæng mellem praksis, forretningsgange og kontrolprocedurer er opgaver, der medfører en udvidelse af arbejdsopgaven. Disse arbejdsopgaver må dog forventes i vid udstrækning at være en del af det arbejde, der allerede i dag udføres af intern revision, hvorfor udvidelsen af arbejdet primært består i strukturering og dokumentation af arbejdet, et arbejde der selvsagt vil være størst i år 1.

For så vidt angår going-concern vurderingen har Finanstilsynet i revisionsbekendtgørelsens bilag 2 anført, at revisors arbejdshandlinger også omfatter en gennemgang af opgørelsen af solvensbehovet. Gennemgang af solvensbehov vil i et vist omfang betyde udvidelse af arbejdet, om end omfanget kan diskuteres, idet solvensbehovet må forventes også hidtil at have indgået i revisors going-concern vurdering.

Kommentarer til øvrige bilag

Som en service til FSR's medlemmer, har FINU i notatets bilag 2, 3 og 4 givet en række gennemarbejdede eksempler på henholdsvis materialeliste, arbejdsinstruks og ledelseserklæring, som også interne revisorer med fordel kan drage inspiration af, i arbejdet med at sikre en hensigtsmæssig proces.

Bilag 2 er et eksempel på en liste, der tænkes fremsendt til virksomheden, over det materiale der skal leveres, som grundlag for revisors konklusioner og oplysninger. Materialelisten, som naturligvis skal til-pas-ses den enkelte virksomhed, er dermed også nyttig information for intern revision. Det er min vurdering, at oversigten er en god og overskuelig metode i arbejdet med at sikre, at revisor kan dokumentere fuld-stæn-digheden af sit arbejde som led i afgivelse af de krævede oplysninger og konklusioner i revisions-bekendt-gørelsen.

Bilag 3 er et tætskrevet og omfattende værk, der i struktureret form oplister krav i revisionsbekendt-gørelsen og de hertil knyttede arbejdshandlinger i revisionsbekendtgørelsens bilag 2. Omfanget kan umiddelbart virke skræmmende, men da der er tale om en fuldstændig liste, for alle typer af finansielle virksomheder, vil mange nok umiddelbart kunne skære en del af listen fra. I bila-

gets yderste højre kolonne har FINU anført forslag til "arbejdsinstruks", altså de konkrete handlinger der efter FINU's vurdering skal udføres, for at revisor har levet op til Finanstilsynets krav til arbejdshandlinger. Det er en rigtig god og overskuelig måde at omsætte lovtekst og kravene i revisionsbekendt-gørelsens bilag 2 til konkrete arbejdshandlinger, som intern revision med fordel kan lade sig inspirere af, eksempelvis hvis revisor er i tvivl om, hvordan arbejdshandlingerne formuleret af Finanstilsynet skal forstås.

Endelig er bilag 4 FINU's bud på kommende ledelseserklæringer. FINU lægger op til, at der skal være to ledelseserklæringer ved årsafslutningen. Den ene ledelseserklæring, som er eksemplificeret i bilag 4, skal indhentes som grundlag for de oplysninger og konklusioner der kræves ifølge revisionsbekendtgørelsen, og herudover skal der indhentes erklæring som grundlag for påtegning af regnskabet. Igen vil det være relevant med tilpasning til den enkelte virksomheds særlige forhold og praksis, og i nogle tilfælde vil det være hensigtsmæssigt at samskrive indhold til én ledelseserklæring.

God læse- og arbejdslyst.

Nye medlemmer

Nye medlemmer i IIA fra 5.09.2013 – 6.12.2013

ATP
Katrine Hulgaard Jensen

Coop Danmark
Ulla Vig

Danfoss
Martin Boller

Danske Bank
Christian Lund
Henrik Ahm
Niels Felstedt

Den Jyske Sparekasse
Hans Jørgen Winther

DONG Energy Oil & Gas
Jens Helskov Varder
Christina Maria Davidsen
Jacob Bjærg
Martin S. Petersen
Ulrik Kjersgaard Friis
Thomas Nordestgaard Sørensen

DSB
Claus Bo Jensen
Lisbeth Hygom
Marianne Berg Larsen

Finansministeriet
Rubia Malik

ISS World Services
Michael Gad

KMD
Thomas Gi Scharf

KPMG
Anne Tønsberg

Novo Nordisk
Nicolas Gomez Iglesias

Nykredit
Karina Thougaard Thomsen
Bjørn Sebastian Olesen

PenSam
Jens-Peder Vinkler

PwC
Jesper Hyveled

Rockwool
Allan Ømand Ungstrup

Skatteministeriet
Aliriza Ozden
Klaus Myssen
Mogens Tengstedt

Solar
Maj-Britt Lykke Viskum

Spar Nord
Carina Rubæk Gade

"Bagsmækken"

Foreningens adresse

Foreningen af Interne Revisorer (IIA)
c/o Regional Chief Auditor Dorthe Tolborg
Group Internal Audit
Codan A/S
Gammel Kongevej 60
1790 København V

CVR nr. 73954215

Indmeldelse i foreningen

Indmeldelse i foreningen foretages på www.iia.dk eller til:

Chefsekretær Dorte Dreiøe
Nykredit
☎ 44 55 93 07 ✉ ddh@nykredit.dk

Jobannoncer

Jobannoncer for medlemmer kan bringes på foreningens hjemmeside og/eller i INFO.

Annoncer bringes kun i INFO, såfremt der er plads hertil. Annonceudkast sendes til redaktionens adresse jf. side 1.

Certificeringer

Nærmere oplysninger om CIA-, CGAP-, CCSA- og CFSA-certificeringer kan fås på IIA´s internationale hjemmeside:
www.globaliia.org eller ved kontakt til:

Lars Maagaard, Nordea
☎ 33 33 15 48 ✉ lars.maagaard@nordea.com

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

Formand
Regional Chief Auditor Dorthe Tolborg
Codan
☎ 33 55 34 59 ✉ dtg@codan.dk

Næstformand
Vicerevisionschef Kim Stormly Hansen
Nykredit
☎ 44 55 93 17 ✉ ksh@nykredit.dk

Kasserer
Revisionschef Peter Jochimsen
ATP
☎ 48 20 37 28 ✉ pjo@atp.dk

Sekretær
Revisionschef Ole Kirkbak
Sydbank
☎ 74 36 31 00 ✉ ole.kirkbak@sydbank.dk

Bestyrelsesmedlemmer
Vicekoncernrevisionschef Neil Jensen
Post Danmark
☎ 33 61 50 15 ✉ neil.henrik.jensen@post.dk

Vice President Vibeke Aggerholm
Carlsberg Breweries
☎ 33 27 12 26 ✉ vibeke.aggerholm@carlsberg.com

Senior Audit Manager, CIA,
Afdelingsdirektør Anette Kauffmann Laursen
Nordea
☎ 33 33 41 33 ✉ anette.laursen@nordea.com

Koncernrevisionschef Pia Sønderlund Nielsen
Finansministeriet
☎ 33 92 26 77 ✉ pnn@fm.dk

Senior Vice President Jesper Siddique Olsen
Danske Bank
☎ 45 12 76 58 ✉ jol@danskebank.dk

Koncernrevisionschef Poul-Erik Winther,
Alm. Brand
☎ 45 47 78 97 ✉ abrpwe@almbrand.dk