INFO

Foreningen af Interne Revisorer
Nummer 60 | September 2015 | 20. årgang

Minitema

- *2nd Line funktioner*

Den nye IIA begrebsramme

Overblik over ændringerne til International Professional Practices Framework (IPPF)

Årskonferencen 2015

Højdepunkter fra årskonferencen 2015 på Hotel Nyborg Strand

Besøg af Anton van Wyk, Global Chairman of IIA

INFOs redaktion

Ansvarshavende redaktør
Revisionschef, CMA, CIA, CISA
Birgitte Rousing Svenningsen
Europæiske Rejseforsikring
☎ 33 27 84 82 ✉ brs@europaeiske.dk

Øvrig redaktion
Koncernrevisionschef, CIA
Morten Bendtsen
PFA Pension
☎ 39 17 60 12 ✉ mob@pfa.dk

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

Partner
Lars Maagaard
KPMG P/S
☎ 61 62 18 90 ✉ lmaagaard@kpmg.com

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

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

Senior Internal Auditor, CIA
Tobias Zorde
Nordea
☎ 55 47 33 27 ✉ tobias.zorde@nordea.com

Næste nummer

INFO 61 udkommer i december 2015.
ISSN: 1903-7341 (Elektronisk version).

Indlæg til INFO

Artikler i INFO påskønnes med en vingave.

Forsidefoto

Ole Svenningsen

Redaktionens adresse

Foreningen af Interne Revisorer (IIA)
Att.: Seniorspecialist Glenn Thunø
Intern revision
Nykredit
Anker Heegaards Gade 4-6
1780 København V

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

Indhold

Leder 3
Nyt fra redaktionen 5
Nye CIA certificeringer 5
Besøg af Anton van Wyk, Global Chairman of IIA 6
"Gå-hjem" møder om ny revisionsbekendtgørelse og operationel revision 7
Højdepunkter fra Årskonferencen 2015 10
Den nye udbyggede IIA begrebsramme 14

Minitema: 2nd line funktioner
Har intern revision en udfordring i relation til 2nd line of defense? 17
Revision af Compliance 23

Nye medlemmer 25
Uddannelsesaktiviteter 25
Bagsmækken 26

Besøg foreningens hjemmeside:

www.iia.dk

Leder

Anette Kauffmann Laursen, Senior Audit Manager, CIA, Afdelingsdirektør, Nordea

Sommeren er nu definitivt ovre både vejrmæssigt og kalendermæssigt, og det er tid til at fordybe sig i revisionsmæssige emner.

Operationel revision har længe været en del af arbejdet for mange af foreningens medlemmer. Men hen over foråret blev definitionen af, hvad operationel revision er for en størrelse accentueret af den ny Revisionsbekendtgørelses krav om operationel revision i finansielle institutter.

Her i INFO var operationel revision et minitema i sidste nummer, herunder Finanstilsynets ikke helt klare definition af, hvad intern revisions opgaver i forhold til operationel revision er/skal være. Desuden besluttede bestyrelsen, at afholde "Gå- hjem" møder, hvor revisionscheferne i den finansielle sektor kunne få lejlighed til at diskutere Revisionsbekendtgørelsen, herunder kravet om operationel revision. Du kan læse mere herom i artiklen "Gå-hjem møder om ny revisionsbekendtgørelse og operationel revision". En af konklusioner var, at der bør arbejdes på, at Finanstilsynet ensretter definitionerne af operationel revision i Revisionsbekendtgørelsen.

På Årskonferencen 2015 var operationel revision også et tema, bl.a. i Finanstilsynets indlæg "Operationel revision – hvad er meningen?" ved Jan Parner. Jan Parner udtrykte, "at operationel revision ikke er et kanonisk begreb", og "at området vil være under fortsat modning, både fra lovgiver og fra sektoren".

At området er under modning ses bl.a. i, at Revisionsbekendtgørelsen hen over sommeren har været drøftet i Finanstilsynets rådgivende revisionsudvalg. Resultatet heraf er, at en ny/opdateret Revisionsbekendtgørelse er på trapperne, hvilket betyder, at især definitionen og indholdet af operationel revision vil fremstå klarere. Vi har så stadig til gode at få indarbejdet (en ensartet) praksis i institutterne, og høre Finanstilsynets syn herpå.

Et andet spændende tema, der har været drøftet og fortsat vil blive drøftet, er 3rd line of defense contra 2nd line of defense: Hvordan forholder intern revision sig til disse funktioner, og hvordan skal de revideres. Nogle gode bud herpå med vægt på compliancefunktionen finder du i artiklerne "Har intern revision en udfordring i relation til 2nd line of defense?" og "Revision af Compliance".

Artiklen "Har intern revision en udfordring i relation til 2nd line of defense" er primært baseret på erfaringer fra den finansielle branche. Men der trækkes også paralleller til de påbud, Finanstilsynet har givet og offentliggjort i forbindelse med deres temaundersøgelse i foråret 2015.

I artiklen "Revision af Compliance" behandles krav og forventninger til revision af compliancefunktionen, samt hvilke komponenter revision af en virksomheds compliance-program skal omfatte.

Der er for mig ingen tvivl om, at intern revisions brug af 2nd line of defense arbejde og revision af 2nd line of defense vil være et tema og diskussionsemne, indtil vi ser en klarere praksis på området, og vi har en tydeligere tilbagemelding om, hvad der forventes fra lovgiver. Et første skridt i den retning vil være på Temadagen for den finansielle sektor den 5. november 2015.

God læselyst!

Nyt fra bestyrelsen

Referater fra bestyrelsesmøder lægges på foreningens hjemmeside umiddelbart efter mødernes afholdelse.

Du kan her løbende holde dig opdateret på bestyrelsens arbejde på hjemmesiden under "Nyheder" .

Nordea

Senior Internal Auditor

Er DU vores nye IT revisor, som har lyst til at arbejde i et internationalt, foranderligt og komplekst miljø?

Om jobbet

Group Internal Audit er en uafhængig afdeling, som rapporterer til bestyrelsen i Nordea Group. Fokus er på at udføre risikobaseret operationel revision.

Som Senior Internal Auditor vil du skulle lede og deltage i revision af IT infrastruktur og forretningsapplikationer.

Du vil være en del af IT revisionsteamet med arbejdssted i Storkøbenhavn. Nogen rejseaktivitet må forventes, men det tilstræbes at minimere dette ved brug af online-møder mv.

Generelt vil en Senior Internal Auditor:

- Lede eller deltage i 6-10 revisionsprojekter om året
- Være involveret i planlægning
- Indgå i dialog med relevante interessenter
- Assistere med at vedligeholde standarder og værktøjer
- Være sparringspartner for forretningsrevisorer

Dine kvalifikationer

Du har en relevant bachelor eller master uddannelse og er formentlig CISA certificeret. Du har 3-8 års erfaring med IT revision, herunder erfaring med IT sikkerhed, IT risk management, ITGC eller revision af forretningsapplikationer.

Andre vigtige kompetencer:

- Interesse for IT
- Behersker et eller flere programmeringssprog
- Har let ved at sammenstille og analysere data
- Engelsk på højt niveau skriftligt og mundtligt
- Arbejder systematisk og trives med at undersøge ting, som du ikke forstår

Det falder dig desuden naturligt at styre og drive møder, du er en stærk kommunikator, og så har du ikke mindst humor og kan lide at gøre en forskel.

Yderligere information og ansøgning

Vil du høre mere om jobbet, er du velkommen til at kontakte Senior Audit Manager Ole Svenningsen på +45 2516 1424.

Send venligst din ansøgning på engelsk senest den 25. september. Se mere her:

Nyt fra redaktionen

Birgitte Rousing Svenningsen, Revisionschef, CMA, CIA, CISA, Europæiske Rejseforsikring

Tak til John Terp

I sommerens løb har vi i redaktionen sagt farvel til John Terp fra Forsvarets Interne Revision. John har været et aktivt medlem af redaktionen og glimrende repræsentant for de interne revisorer i den offentlige sektor de seneste tre år. På grund af andre opgaver har John valgt at trække sig fra redaktionen. Der skal her til John lyde en rigtig stor tak for en fantastisk arbejdsindsats.

Bliv medlem af redaktionen

Som nævnt har vi sagt farvel til John Terp. Det betyder, at hovedparten af redaktionens medlemmer er ansat i den finansielle sektor, og at vi ingen medlemmer har fra den offentlige sektor. Det betyder selvfølgelig også, at det er en udfordring for os at sikre, at bladets artikler også er relevante for interne revisorer i den offentlige sektor eller i industrien. Vi leder derfor efter redaktionsmedlemmer, som har tilknytning til den offentlige sektor eller til industrien. Så har du det, og er du interesseret i at påvirke indholdet af bladet, hører jeg gerne fra dig. Du finder mine kontaktinformationer forrest i bladet. Har du ikke selv mod herpå, men synes du, at en af dine kollegaer vil være ideel, så opfordre kollegaen til at kontakte mig.

Læsertilfredshedsundersøgelse

På redaktionens vegne vil jeg også takke mange gange for de mange besvarelser, vi har fået på vores læsertilfredshedsundersøgelse i juni måned.

Generelt viser undersøgelsen stort tilfredshed med bladets format og udgivelsesfrekvens. Der er enighed om, at bladet er anvendeligt og giver værdi. Der er stor tilfredshed med, at bladet belyser emner fra forskellige vinkler i såkaldte mini-temaer. Svarene giver endvidere adskillige inspirerende input til artikler, hvilket er en stor hjælp til redaktionens fremtidige arbejde. Vi vil benytte efteråret til nærmere at studere undersøgelsens resultater og til at drage konklusioner herpå.

I forbindelse med undersøgelsen udlovede vi et par præmier, og det er mig en ære at kunne offentliggøre, at vinderne er:

1. præmie (2 biografbilletter + 3 flasker vin)
Ragna Kr. Jóhannsdottir
ATP

2. præmie (3 flasker vin)
Steen Scherfeldt
Sparekassen Kronjylland

3. præmie (3 flasker vin)
Lars Vestergård Cramer
Sparekassen Vendsyssel

Stort tillykke til vinderne.

Nye CIA certificeringer

Suzzie Frantzen, ATP
Heino Hansen, Nordea
Ole Klitgård, Codan
Rune Nielsen, DONG Energy Oil & Gas A/S
Jacob Reifling, Thorngaard Reifling A/S
Heinrich Ringsgart, Nordea
Carsten Sivertsen, Danske Bank
Marcin Winiarczyk, Danske Bank

Et stort tillykke med certificeringen !!!!

Besøg af Anton van Wyk, Global Chairman of IIA

Peer Højlund, Chefspecialist, Nykredit

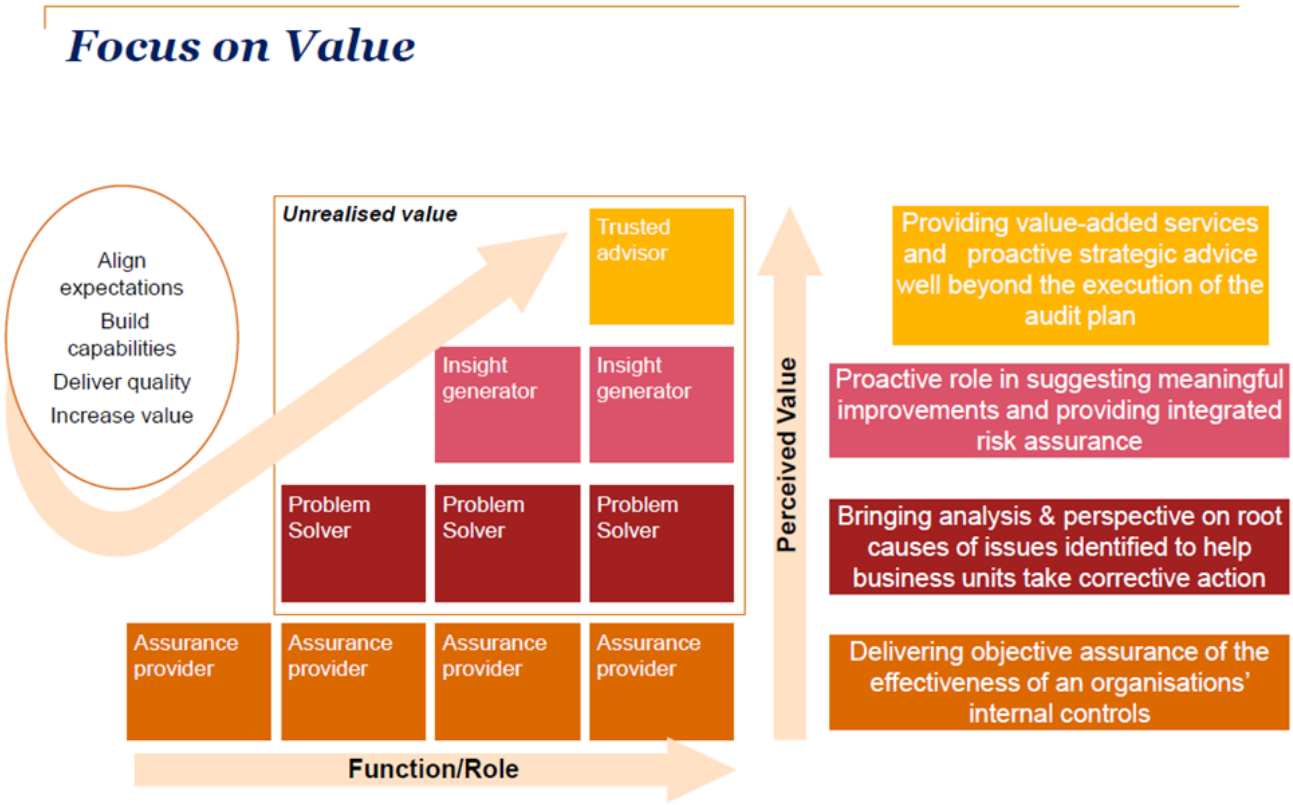
Den 8. juni 2015 var der fint besøg fra det store udland, da Anton van Wyk (AvW), Global Chairman of the Board of The Institute of Internal Auditors, slog vejen forbi Danmark. AvW var i den forbindelse inviteret til at afholde et indlæg på et gå-hjem møde for medlemmer af IIA's danske afdeling.

AvW er fra Sydafrika og arbejder til daglig som ekstern revisor, nærmere bestemt PwC, hvor han er partner. AvW har været medlem af IIA siden 1987 og blev i 2014 formand for IIA for en etårig periode, frem til sommerens globale konference i Vancouver, hvor formandskabet gik videre til Larry Harrington fra USA.

AvW indledte med en længere redegørelse for arbejdet som global chairman, og gav et indblik i en travl og hektisk formandsperiode, som omfattede en nærmest endeløs rejseaktivitet rundt til et stort antal lande med afholdelse af foredrag ved kurser og konferencer samt drøftelser af aktuelle temaer og trends i den interne revisionsbranche med lokale IIA afdelinger.

AvW fortsatte herefter med sit indlæg under overskriften "Mind the gap – Assuring Stakeholders of Internal Audits Value", hvor han bl.a. betonede vigtigheden af, at vi som interne revisorer forstår vores interessenters behov og forventninger til os, og med det udgangspunkt kom med en række nyttige og inspirerende input til hvordan vi kan tackle udfordringer i arbejdet med at udvikle intern revision fra at være "Assurance provider" til at blive "Problem Solver", "Insight Generator" og endelig "Trusted advisor" for vores stakeholders, jf. nedenstående figur.

Du kan finde AvW's plancher på IIA's hjemmeside under menupunktet "Uddannelse", "Kursuskatalog" og fanebladet "Afholdte møder", og herefter gå-hjem mødet med dato den 8. juni 2015.



"Gå-hjem" møder om ny revisionsbekendtgørelse og operationel revision

Morten Bendtsen, Koncernrevisionschef, PFA Pension

Indledning

Bestyrelsen i IIA besluttede i foråret, at afholde to "gå-hjem" møder for revisionschefer m.fl. hvor vi debatterede den ny revisionsbekendtgørelse herunder kravet om operationel revision.

Møderne blev afholdt i København og Randers.

Debatten blev bygget op omkring et indlæg af Kim Stormly Hansen, Poul-Erik Winther og undertegnede.

Artiklen skal give jer indblik i hvilke emner, der blev debatteret og i givet fald om debatten førte til afklaringer og konklusioner.

Agenda

- *Baggrund for de nye krav*
- *Definition af operationel revision*
- *Ny erklæring*
- *Outsourcing*
- *Væsentlighed og omfang*
- *Påvirkning af Intern Revision*
- *Afsluttende bemærkninger m.v.*

Baggrund for de nye krav

I høringsbrevet til den nye revisionsbekendtgørelse fremgår:

"Baggrunden for forslaget er, at Den Internationale Monetære Fond (IMF) ved sin undersøgelse af Finanstilsynet i 2014 konstaterede, at Finanstilsynet ikke stiller et eksplicit krav om, at intern revision skal udføre operationel revision af alle risikofyldte og væsentlige områder i virksomhederne under tilsyn."

Den præcise ordlyd af IMF's observation og anbefaling til banker går på:

"There is a gap in the relevant executive order in not directing ***that internal auditors of banks must review risk management, compliance and control functions***.

From their review of audit books and discussions with bankers, the assessors saw evidence that some such reviews are done (at least for the largest banks), but it is important that the executive order be appropriately updated."

"Modify regulations to direct internal auditors to review risk management, compliance and control functions."

IMF's observation og anbefaling vedr. forsikringsselskaber var stort set sammenfaldende med den for banker.

Drøftelserne gav anledning til at påpege, at IMF's krav umiddelbart kunne tolkes som en revision af de etablerede risikofunktioner dvs. 2. forsvarslinje i 3LoD modellen.

Finanstilsynets fortolkning virker umiddelbart lidt bredere.

Definition af operationel revision

Gennem høringsarbejdet og i bekendtgørelsen optræder følgende definitioner på operationel revision:

Reference	Indhold
Høring § 2 nr. 2	***Operationel revision***: En vurdering af virksomhedens processer og interne kontrolsystemer med det formål at teste og rapportere, om de er i overensstemmelse med de af ledelsens fastsatte mål og overholder kravene i lovgivningen.
Bek. § 2 nr. 2	***Operationel revision***: En revision af virksomhedens processer og interne kontrolsystem med det formål at teste og rapportere, om de er tilrettelagt og fungerer på betryggende vis.
Bek. § 22 stk. 1	Den af interne revision udførte revision skal omfatte virksomhedens administrative og regnskabsmæssige praksis på alle væsentlige og risikofyldte områder i virksomheden, herunder forretningsgange og interne kontrolprocedurer, jf. bilag 4.

Reference	Indhold
Bilag 4	***Operationel revision*** indebærer en vurdering af virksomhedens processer, med det formål at teste og rapportere, om de er tilrettelagt og fungerer på betryggende vis. Operationel revision omfatter, ud fra en vurdering af væsentlighed og risiko, ***forretningsgange og interne kontrolprocedurer, vedrørende årsregnskabet***. Dette gælder uanset om intern revision deltager i den finansielle revision eller ej. Operationel revision omfatter, ***afhængig af virksomhedens aktivitet og størrelse, bl.a.*** en ***procesgennemgang*** med fokus på **kvalitet**, pålidelighed, dokumentation og kontroller på alle væsentlige og risikofyldte områder i virksomheden **(herunder også risikostyrings- og compliancefunktionen)**, en vurdering af pålideligheden af den finansielle- og operationelle rapportering, overholdelse af love og regler samt sikring af virksomhedens værdier.

Som det ses af ovenstående tabel er der fra høring til bekendtgørelse og gennem bekendtgørelsen og til bilag 4 afvigende nuancer af definitionen. Debatten gav anledning til, at påpege, at der herved er risiko for uklarhed omkring hvad der skal revideres og dermed kravet til Intern Revision.

Der bør arbejdes på, at Finanstilsynet ensretter definitionerne gennem bekendtgørelsen.

Der var ligeledes en livlig debat omkring et muligt krav om finansiel revision. I den ene ende af skalaen blev fremført, at der skulle udføres fuld finansiel revision også selvom revisionschefen ikke påtegner årsregnskabet og ikke deltager i den finansielle revision.

Der blev opnået konsensus omkring, at Intern Revision som del af en operationel revision ikke reviderer "disclosure-delen", men kan forholde sig til regnskabsprocessen generelt herunder hvilken proces regnskabsfunktionen har etableret for at sikre sig, at årsregnskabet aflægges korrekt i forhold til lovgivningens krav (fx at de gennemgår IFRS tjeklister). Herudover bør Intern Revision deltage i møder hvor årsregnskabet behandles fx revisionsudvalgsmøder.

I forbindelse med løbende revision bør den Intern Revision som minimum forholde sig til, at transaktioner og handlinger afspejles og klassificeres korrekt i bogføringen, kundesystemer m.v. således, at de er retvisende og anvendelige til intern- og ekstern rapportering.

I større komplekse virksomheder ses det af bilag 4, at der er vide rammer for operationel revision, bl.a. inkluderer det kvalitet i processerne. Kvalitet i processerne kan fx omfatte en vurdering af i hvilket omfang processen understøtter ledelsens mål og fokusområder fx omkostningsbevidsthed, lønsomhed, prissætning, kundetilfredshed m.v.

Ny erklæring

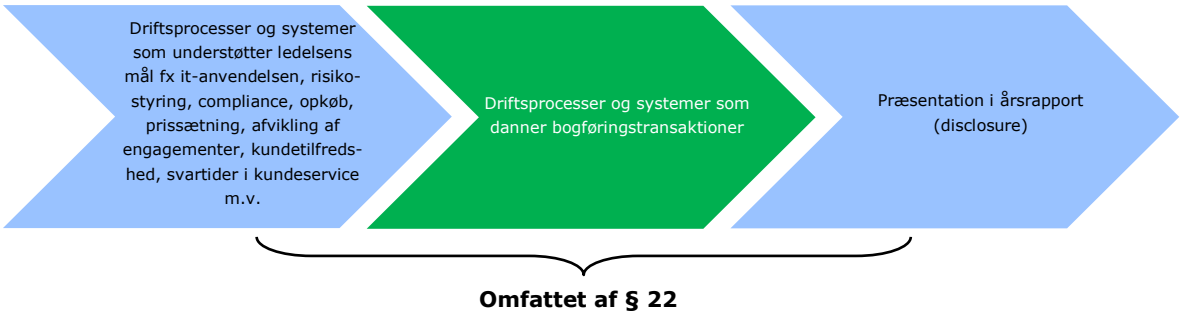
Som konsekvens af § 22 skal Intern Revision afgive en konklusion i årsprotokollatet. Jf. § 28 stk. 4 skal konklusionen være enslydende med Ekstern Revisions konklusion jf. § 12. Dvs. Intern Revision skal afgive konklusion om, hvorvidt virksomhedens administrative og regnskabsmæssige praksis på væsentlige områder, herunder forretningsgange og interne kontrolprocedurer, er tilrettelagt og fungerer på betryggende vis.

I denne forbindelse skal vi endvidere konkludere, hvorvidt

1) virksomhedens samlede system-, data- og driftssikkerhed er og fungerer betryggende, og

2) om vi er blevet bekendt med forhold, der er i strid med kravene i lovgivningen vedrørende finansielle virksomheder m.v. og tilhørende ledelsesbekendtgørelse.

Det blev debatteret om det nye krav skal omfattes som et ønske om dobbelt sikkerhed fra Finanstilsynets side.



Vi mener ikke der skal udføres dobbelt arbejde, men det indskærpes, at Intern Revision skal være primært udførende i forhold til bl.a. kontrol- og ledelsessystemer og Intern Revision skal tage ansvar for indholdet af erklæringen og ikke blot forlede sig på Ekstern Revision.

Omvendt bør det inden for rammerne af revisionsaftalen stadig være muligt, at "insource" specialistviden fra Ekstern Revision fx på IT-området, kapital- og risikostyring og på aktuarområdet. Kravene til Intern Revision i den situation vil svare til kravene ved outsourcing (se senere).

De nye krav vil øge behovet for koordinering mellem Intern og Ekstern revision.

Ved en kommende gennemskrivning af revisionsbekendtgørelsen bør det overvejes i hvilke tilfælde erklæringen kan gives af Intern Revision alene. Ligeledes bør det overvejes om Intern Revision i de tilfælde de ikke påtegner årsregnskabet og/eller ikke deltager i finansiel revision skal udtale sig om regnskabsmæssig praksis.

Outsourcing

Intern Revision må gerne benytte eksperter eller outsource den operationelle revision under iagttagelse af god revisorskik, jf. ISA 620 og ISA 220. Det skal bemærkes, at Intern Revision bl.a. skal være i stand til at vurdere specialisternes kompetencer og objektivitet, at Intern Revision skal opnå en tilstrækkelig forståelse af specialisternes ekspertiseområde og at Intern Revisions ansvar for den samlede konklusion ikke kan mindskes ved brug af specialister eller outsourcing.

Det er fortsat Intern Revision, der skal afgive konklusionen efter § 22, og kunne stå inde for ansvaret for konklusionen og derfor skal have tilstrækkelige ressourcer og kompetencer til at vurdere specialistens revision, jf. § 24, stk. 2.

Væsentlighed og omfang

Erklæringen i § 22 (§ 12) er i alt overvejende grad positivt formuleret, hvilket indebærer krav om høj grad af sikkerhed. Der bør anvendes ISA begrebsramme for erklæringsopgaver med sikkerhed.

Hvad der konkret skal udføres, afgøres under hensyntagen til god revisorskik og dermed væsentlighed og risiko på det pågældende område.

Samlet set vil der være tale om relativt omfattende handlingerne hvis der er tale om en større og kompleks finansiel virksomhed.

I en operationel revision går man fra finansielle revisionsmål og dermed den iboende risiko for fejl i regnskabet til risikoen for fx fejl i processer, manglende regeloverholdelse eller utilstrækkelig kapital- og risikostyring.

Jf. § 22 skal vi, som del af den operationelle revision, forholde os til følgende områder som pr. definition er vurderet væsentlige for alle finansielle virksomheder:

- Kreditområdet
- Markedsrisikoområdet
- Operationelle risici
- Forsikringsmæssig afdækning
- Likviditetsområdet
- Forsikringsrisici
- Investeringsområdet.

I forhold til den finansielle revision er disse områder ligeledes vigtige hvilket gør, at den operationelle revision både direkte og indirekte kan anvendes som grundlag for den finansielle revision og risikovurdering.

Påvirkning af Intern Revision

Det var indlægsholdernes opfattelse, at mindre interne revisionsafdelinger i både pengeinstitutter og forsikringsselskaber/pensionskasser kunne blive udfordret af de nye krav.

Tilbagemeldingen fra de jyske pengeinstitutter var, at man er forholdsvis rolig og føler sig godt rustet i forhold til, hvor stor en del af revisionsopgaven, der allerede dækkes i dag. Det kan ses i lyset af, at kompleksiteten i de lokale pengeinstitutter er mindre og Intern Revision har et godt overblik over alle områder af virksomheden.

Afsluttende bemærkninger m.v.

Der var enighed om, at den nye revisionsbekendtgørelse har visse redaktionelle mangler og bør gennemskrives en gang til.

Når det er sagt er der også, som bekendtgørelsen ligger, vide rammer for hvad, der kan inkluderes i Intern Revisions arbejde.

Vi har således en mulighed for at tage vores funktionsbeskrivelse og revisionsstrategi op til revision med ledelse, revisionsudvalg og bestyrelse.

Hvordan kan Intern Revision bedst skabe værdi og være relevant for virksomheden? hvad skal vi have fokus på fremover? eller skal vi overhovedet ændre fokus? Det er spørgsmål vi kan overveje.

Højdepunkter fra Årskonferencen 2015

Operationel revision – hvad er meningen?
Jan Parner, Finanstilsynet

Intern revision skal foretage operationel revision af virksomhedens administrative praksis med udgangspunkt i ledelsesbekendtgørelserne.

Kravet om operationel revision kan give anledning til genovervejelse af organiseringen af intern revision:

- Ressourcer
- Kompetencer
- Anvendelse af eksterne eksperter
- Outsourcing af dele af revisionen.

Operationel revision er ikke et kanonisk begreb. Noget som ikke nødvendigvis altid er lavet tidligere.
Området vil være under fortsat modning, både fra lovgiver og fra sektoren.

Operationel revision – hvad betyder det i praksis
Dorte Tolborg, Danske Bank

The following needs to be transparent for the employees:

- What's in it for me?
- Can I do it?
- Will my efforts be rewarded?

The changes and the impact need to be explained to the stakeholders.
Significant changes from financial to operational audit:

- Not substantive testing even though a control is not effective
- Focus on root cause.

Operationel revision i industrien i praksis
Michael Ravbjerg Lundgaard, DSB

Bestyrelsens ønske:

- Indtil foråret 2013, 100% finansiel revision
- Sommeren 2013, 40% operationel revision
- Fra 2016, 100% operationel revision.

Revisionsmål:

- Efterlevelse af love, politikker, kontrakter, retningslinjer
- Sikring af aktiver
- Pålidelighed i ledelsesrapportering
- Effektivitet, risikostyring og økonomi i processer og operationer
- Opfyldelse af virksomhedens strategiske mål.

Nyt fra Finanstilsynet, herunder hvordan ser Tilsynet den operationelle revision implementeret
Pernille Dalby Nielsen, Finanstilsynet

Revisionsbekendtgørelsens definition af operationel revision vil formodentlig blive justeret i løbet af 2015.

Operationel revision omfatter også processer vedr. finansiel rapportering. Operationel revision har fokus på kvalitet, pålidelighed, dokumentation og kontroller inkl. Risikostyrings- og compliancefunktion. Operationel revision omfatter tillige pålidelighed af rapportering, overholdelse af love og regler samt sikring af værdier i virksomheden.

Effektive former for virksomhedsstyring indebærer en klar organisatorisk struktur med en veldefineret, gennemskuelig og konsekvent ansvarsfordeling og effektive procedurer til at identificere, forvalte, overvåge og rapportere om de risici, virksomheder er eller kan blive udsat for, samt hensigtsmæssige interne kontrolmekanismer, herunder en god administrativ og regnskabsmæssig praksis og fyldestgørende interne kontrolprocedurer.

IIA UK Code for internal auditors – Post Implementation Reflections
Bruce Elcock, KPMG, UK

Different organisations still face different challenges in meeting the requirements.

All organisations have gaps – some commonality but less than expected. Auditing culture continues to be a challenge.

The CIIA Guidance provides a benchmark against which firms can measures their Internal Audit function.

Centralised operations: The future of operating models for Risk, Control and Compliance
Lars Rhod Søndergaard, EY

Udfordringer og risici ved centralisering/outsourcing:
- Alle forandringer indebærer risici
- Passende governance og klare roller/ansvar
- Udformning af service level agreement (ved outsourcing eksternt eller inden for koncern)
- Regulatoriske og skattemæssige hensyn.

Planlægning:
Tværgående revision baseret på centralisering inden for virksomheden (on shore).
Revision af shared service centers (off shore/near shore).
Overvejelser om behov for erklæringer fra outsourcing leverandører (ISAE 3402 erklæring eller lignende).

Revision af "Cultural and Behaviour Risks"
Anne-Louise Thon Schur, PWC

Our Internal Audit functions have started thinking about how they can assess culture and behaviours, and their wider organisations will be at various stages of defining, changing and monitoring culture. The value that Internal Audit can bring is clear:
- Utilising the function's position
- Behavioural root causes
- Enhancing Internal Audit's value as a function.

Base Camp Horserød – et indblik i en helt anden verden
Anders Weirup, tidligere Nordisk Fjer

Bestyrelsesdilemmaer
- En ekstrem karismatisk top/koncernchef
- Ingen reel dialog med bestyrelse/meddirektører
- Magtfuldkommenhed (25 år) fører til solkongesyndrom
- Nepotisme
- Konstant ekspansion og låneoptagelse + ny equity
- Negative finansanalyser og meget kritisk presse
- Forbudt at åbne breve og læse kritiske analyser
- Ingen/begrænset ekstern dokumentation
- Skift i regnskabsprincipperne 36 gange over få år
- Ofte udskiftning af eksterne revisorer
- Røde advarselslamper i hobetal, men man lader stå til
- Særpræget makkerpar (JP og "rigsforstanderen").

Internal Audit's Value Proposition
- Mark L. Stock, PwC

The role of Internal Audit is changing: Protecting future promised value as well as protecting past value created.

We are now seeing a shift in IA's role moving out of the safe zone and navigating the wider risk landscape.

There is now a recognition by stakeholders that more value is 'created' or 'destroyed' by risks not being effectively mitigated/dealt with across the other risk quadrants – market, strategy, unknown.

Den økonomiske udvikling i Danmark i et internationalt perspektiv
- Steen Bocian, Danske Bank

- Olieprisen er begyndt at stige
- Dollarstyrkelsen har taget en puster
- Vi har også fået en pæn rentestigning
- Men fremgangen vil alligevel fortsætte
- Den globale vækst er ikke så lav endda
- Lave og negative renter er ikke et dansk fænomen – og det forsvinder ikke lige med det samme
- Kæmpe valutareserve – som dog er begyndt at skrumpe
- Dansk økonomi i skrøbelig bedring
- Det private forbrug er vendt… men langsomt
- Men vi skal være opmærksomme på ubalancer.

Forventninger til intern revision
- Carol Sergeant, Danske Bank

Key strategic and business decisions are made on the basis of unaudited data that is mostly not independently challenged or verified!

The board pulls a lever, but is it connecting in the right way and is the organization capable of producing the desired outcome?

Internal Audit is a strategic resource that is crucial to the Board, so that we can be confident we are getting a true picture and that when we pull a lever the organization will deliver the intended outcome.

Operationel revision i revisionskomité perspektiv
- Anders Gjelstrup, Deloitte

Revisionskomitéens hovedopgaver:

- Overvåge effektiviteten af det interne kontrolsystem, risikostyringssystem og evt. intern revision
- Overvåge den lovpligtige revision
- Overvåge og kontrollere revisors uafhængighed
- Overvåge regnskabsaflæggelsesprocessen.

Operationel revision - en mangfoldighed af muligheder, dvs. der skal træffes valg og fravalg.

Vær med til at sætte dagsordenen! Vær relevant!

IIA årskonference 2016
Best Western
NYBORG STRAND
HOTEL OG KONFERENCECENTER
Afholdes i dagene
25.5-26.5.2016
Sæt allerede nu
kryds i kalenderen

Den nye udbyggede IIA begrebsramme

Tobias Zorde, Senior Internal Auditor, CIA, Nordea

Baggrunden

Mens de fleste af os i branchen har benyttet sommermånederne til at tømme bevidstheden for alt hvad der har med revisionens glæder at gøre, har en international indsatsgruppe i IIA regi arbejdet for fuld tryk for at klargøre det nye udbyggede International Professional Practices Framework (IPPF).

Projektet har i virkeligheden været undervejs længe, idet behovet for ændringer allerede blev bekræftet ved en omfattende høring, hvis resultater blev offentliggjorte i november 2014. Høringen gav anledning til 845 svar og 4000 individuelle kommentarer. Overordnet set støttede 85% af respondenterne i hovedtræk de foreslåede ændringer.

Baggrunden for ændringsforslagene var, da man i IIAs ledelse diskuterede de mange nye krav som finansielle tilsynsmyndigheder pålagde interne revisorers arbejde. Ifølge Jane Seago, tidligere Chief Communications Officer i ISACA, skønnede man, at denne eksplosion af krav ville øge presset på bestyrelser i forhold til at forstå den centrale rolle intern revision spiller i god ledelse.[1]

Øgede forventninger fra stakeholdere sammen med en naturlig udvikling i revisionsbranchen udgjorde altså drivkraften bag ændringerne.

Ændringerne

IPPF er først og fremmest blevet udbygget med et mission statement. Dette mission statement skal med sine blot 16 ord tjene til at levere en kort og præcis angivelse af, hvad formålet med intern revision er. Den lyder som følger:

"To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight." [2]

Herudover består IPPF stadig af to niveauer – nemlig "mandatory guidance" og "recommended guidance" (tidligere refereret til som "strongly recommended"). Mandatory guidance består fortsat af 1) standarderne, 2) Code of Ethics og 3) Definition of Internal Auditing. Ingen af disse er ændret i første omgang. Til gengæld er Mandatory guidedance udbygget med de såkaldte "Core Principles". Disse kerneprincipper beskrives som følger:

"*The Core Principles, taken as a whole, articulate internal audit effectiveness. For an internal audit function to be considered effective, all Principles should be present and operating effectively. How an internal auditor, as well as an internal audit activity, demonstrates achievement of the Core Principles may be quite different from organization to organization, but failure to achieve any of the Principles would imply that an internal audit activity was not as effective as it could be in achieving internal audit's mission (see Mission of Internal Audit)."* [3]

Kerneprincipperne består af 10 korte beskrivende sætninger, som skal indfange essensen af den eksemplariske interne revision. Kerneprincipperne gengives ikke her i deres helhed, men kan findes på theiia.org. Ligegyldigt hvordan man vender og drejer det, synes kerneprincipperne ikke ligefrem at tilvejebringe banebrydende ny indsigt. Men de tjener alligevel deres formål; nemlig at facilitere formålet og nytten af intern revision på en tilgængelig og effektiv måde. Hvis et af kerneprincipperne alligevel skal gengives her, bliver det følgende:

"[Internal audit] *aligns with the strategies, objectives, and risks of the organization."* [4]

[1] https://iaonline.theiia.org/2015/a-new-framework-for-a-new-age

[2] https://na.theiia.org/standards-guidance/Pages/Mission-of-Internal-Audit.aspx

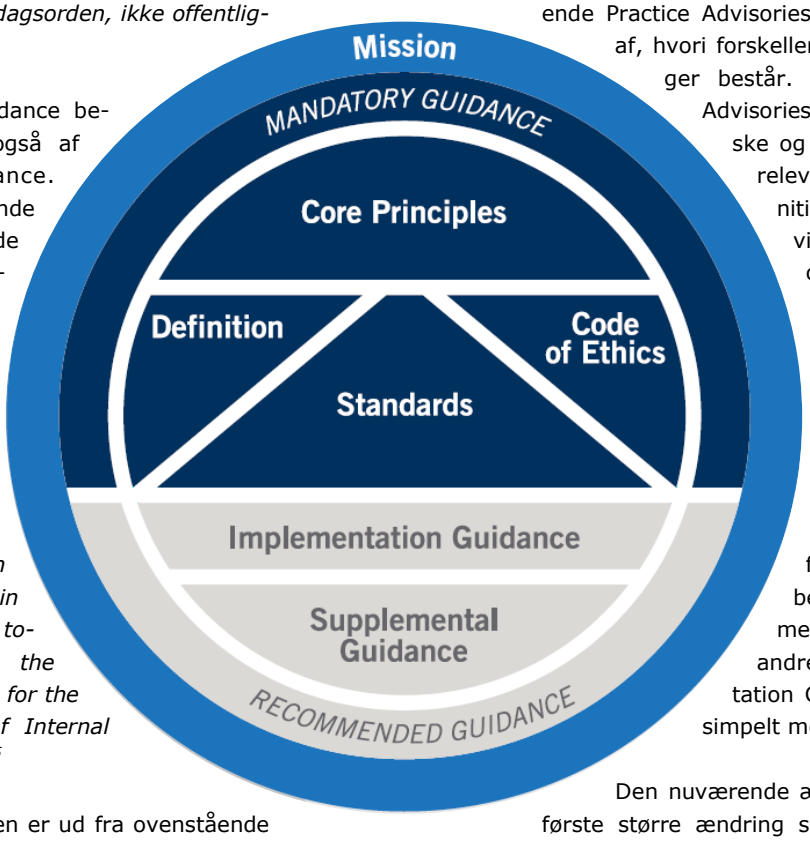
[3] https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx

[4] https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx

Dette kerneprincip kan fortolkes i retning af, at være en kommentar til lovgiverne, der undertiden forsøger skabe intern revision i sit eget billede med sin egen dagsorden. Her siger kerneprincippet så – *intern revision tilhører bestyrelsen og dennes dagsorden, ikke offentligheden.*

Udover mandatory guidance består IPPF som sagt også af recommended guidance. Den mest udslagsgivende ændring er her, at de såkaldte Practice Advisories over tid skal erstattes af såkaldte *Implementation Guides*. På theiia.org fremgår følgende:

"Implementation Guidance will be more comprehensive than Practice Advisories in guiding practitioners toward conformance to the International Standards for the Professional Practice of Internal Auditing (Standards)." [5]



Formålet med ændringen er ud fra ovenstående i første omgang ikke indlysende. Indtil videre er der udgivet to Implementation Guides, hvoraf den ene er "IG2110 - Governance". IG2110 omhandler ikke overraskende standard "2110 – Governance" som hører til den obligatoriske del af IPPF.

Ved ikrafttrædelsen af IG2110 udgår tre Practice Advisories som ligeledes omhandler standard 2110.

Sammenligner man den nyindførte IG2110 med de udgående Practice Advisories tegnes der et billede af, hvori forskellen mellem de to løsninger består. Hvor de tre Practice Advisories er meget formalistiske og deskriptive f.s.v.a. de relevante begreber og definitioner, så er IG2110 i videre omfang direkte omsættelig til praksis. Tendensen eksemplificeres allerede ved den første overskrift i IG2110 som pålyder "Getting started"; en overskrift der efter sigende skulle gå igen som en fast designmæssig bestanddel af Implementation Guides. Med andre ord virker Implementation Guide formatet ganske simpelt mere spiseligt.

Den nuværende ændring af IPPF er den første større ændring siden 1999. Udover at gøre begrebsramme nemmere at markedsføre internt i branchen, så stilles også nye redskaber til rådighed, der forhåbentligt vil bidrage til at fastholde og udvikle forståelsen af intern revisions relevans iblandt stakeholdere.

[5] https://na.theiia.org/standards-guidance/recommended-guidance/Pages/Practice-Advisories.aspx

Minitema: 2nd line funktioner

Er "Three lines of defense" bare det nye "black" eller er det noget, som vi som interne revisorer skal have med i vores overvejelser? Skal vi som intern revisor revidere 2nd line funktioner? Eller skal vi bare lade dem leve deres eget liv. På de næste sider finder du synspunkter herom. Måske også et par enkelte overraskelser….

God fornøjelse

Har intern revision en udfordring i relation til 2nd line of defense?

Kim Stormly Hansen, Vicerevisionschef, Nykredit

Betragtningerne i nærværende artikel er primært baseret på mine oplevelser fra den finansielle branche. Det er imidlertid min vurdering, at de bekrevne forhold – med en vis tilpasning – også er eller vil blive relevante for større virksomheder udenfor den finansielle branche, ikke mindst i PIE-virksomheder (Public Interest Entities).

2nd line of defense

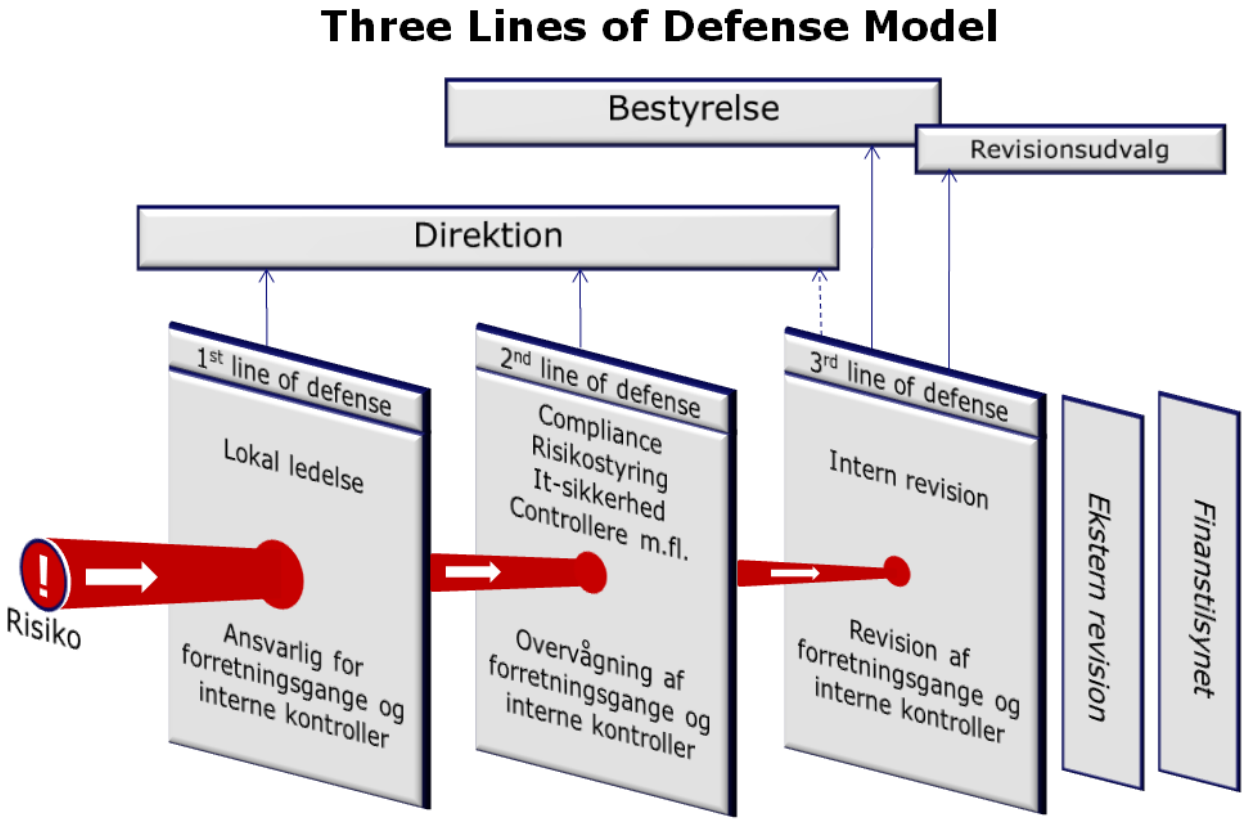
Anden forsvarslinje udgøres af forskellige "kontrol–enheder" eksempelvis It-sikkerhed, Risikostyring, compliance, kreditcontrollere og Koncernøkonomi. Fælles for disse enheder er, at de dels har en driftsmæssig opgave og dels en governanceopgave (kontrolopgave) i relation til 1st line og virksomheden som helhed. Eksempelvis har It-sikkerhed både en opgave i, at rådgive og bistå med implementering af sikkerhedsløsninger (driftsopgave) og i at overvåge efterlevelsen af it-sikkerheden i virksomheden (governanceopgave), lige som Risikostyring både har en opgave i at beregne risici og i at varetage risikostyringen.

I den perfekte verden har virksomheden etableret et effektivt ERM (Enterprise Risk Management) koncept, som sikrer, at disse enheders arbejde sker koordineret indbyrdes og i overensstemmelse med ERM-konceptet, herunder fælles risikodefinition, risikoidentifikation, arbejdsdeling, rapportering og med anvendelse af et fælles styringsværktøj.

Dette er imidlertid ikke altid tilfældet, idet kontrolenhederne ofte opererer uafhængigt af hinanden, herunder med forskellige organisatorisk referencer, forskellig definition og kategorisering af risiko, manglende koordination af kontrolbesøg og uensartet rapportering.

At det så også forekommer, at koordinationen med intern revision ikke er optimal kan medføre ineffektivitet og "irritation" i organisationen, ligesom det kan være svært at skelne 2nd og 3rd line fra hinanden.

Det kan godt være, at vi som revisorer ser den soleklare



forskel på 2nd og 3rd line, men jeg tror, at ledelsen har en pragmatisk holdning til, om en assurance er givet af en "begrænset" uafhængig enhed, som compliance, eller en "overvejende" uafhængig enhed, som intern revision.

Compliance

Virkefelt

Det er erfaringsmæssigt primært Compliance og Risikostyring, der giver anledning til udfordringer. Det primære lovgivningsmæssige grundlag for etablering af en compliancefunktion er set med intern revisions øjne Bekendtgørelsen om ledelse og styring af pengeinstitutter m. fl.[1]

Heri "defineres" compliancerisiko som:

".. risikoen for virksomhedens manglende overholdelse af den for virksomheden gældende lovgivning, markedsstandarder eller interne regelsæt …"

Unægtelig en "definition" som kan tolkes meget bredt, så bredt, at der kan indfortolkes, at Compliance skal se på alt, eksempelvis også regnskabslovgivningen.

Hvis man søger på et internationalt input på forskellen mellem compliance og intern revision, dukker der som første hit en interessant artikel op, skrevet af Jonathan Bowdler (UK Head of Governance, Risk and Compliance, International Compliance Training):

"The Compliance Function is concerned with regulatory risk only, and the scope therefore of operations is more restricted than that of the Internal Audit Function, who are concerned with all risks to the organisation. And of course Compliance must be audited to make sure that we are doing what we have said we will do. So do try not to annoy them!"

Unægteligt en noget snævere "definition" af Compliances virkefelt. Jeg tror, at disse forskelle – både nationalt ctr. internationalt og nationalt fra virksomhed til virksomhed kunne reduceres væsentligt, hvis Finanstilsynet kom med mere klar og præcis regulering på Complianceområdet.

Hvis vi ser på forsvarslinjernes ansvar og ikke mindst Intern revisions og compliances roller (i en virksomhed, hvor intern revision påtegner) ses forskellen på regulering tydeligt (figur 1 på næste side).

[1] For en mere detaljeret beskrivelse af lovgrundlag kan der henvises til artiklen "Compliancefunktionen i den finansielle sektor" i Revision & Regnskabsvæsen nr. 12 - 2014

"Revision" af compliancefunktionen

Det er min oplevelse, at kravene om "revision" af compliancefunktionen fortolkes og håndteres forskelligt fra virksomhed til virksomhed.

I revisionsbekendtgørelsens § 45 stk. 2 står:

"Den interne revision skal som en del af udførelsen af de i stk. 1 nævnte arbejdshandlinger gennemgå rapporteringen til bestyrelsen fra compliancefunktionen ….. Den interne revision skal som minimum i revisionsprotokollatet vedrørende årsrapporten rapportere om de bemærkninger om revisionsforhold, som gennemgangen giver anledning til, med angivelse af, om der er truffet passende foranstaltninger i tilfælde af eventuelle mangler….."

Vær opmærksom på, at denne paragraf specifikt går på værdipapirhandlere. Betyder det, at det så kun er de aktiviteter, som vedrører dette område, der er omfattet?

I revisionsbekendtgørelsen bilag 2 pkt. 14:

"Revisor skal vurdere, om risikostyringsfunktionen og compliancefunktionen har de nødvendige ressourcer til at udføre opgaverne forsvarligt. Revisor skal endvidere vurdere, om rapporteringen fra disse to funktioner er tilfredsstillende, herunder om de to funktioner er adskilt fra hinanden og fra de øvrige funktioner i virksomheden (hvis dette kræves i lovgivningen for den pågældende virksomhed). Såfremt revisor bliver bekendt med svagheder i organisationen eller driften af risikostyrings- eller compliancefunktionen, skal dette omtales i revisionsprotokollen, idet en svaghed på dette område kan have omfattende konsekvenser for virksomheden på længere sigt."

Denne henviser til revisionsbekendtgørelsens § 12, som omhandler den administrative og regnskabsmæssig praksis. Betyder det, at vi skal se på alt det arbejde, som compliance beskæftiger sig med?

I revisionsbekendtgørelsens bilag 4, pkt. 2.2.2:

"Intern revision skal, ud fra væsentlighed og risiko, gennemgå og vurdere, om de i virksomheden etablerede processer til håndtering af compliancefunktionens aktiviteter er betryggende."

Denne henviser til "Intern revisions opgaver og ansvar". Her tales om "virksomhedens praksis på alle væsentlige og risikofyldte områder i virksomheden, herunder forretningsgange og interne kontrolprocedurer". Er det det samme som administrative og regnskabsmæssige procedurer?

Figur 1: Forsvarslinjernes ansvar og roller

Forsvarslinjernes ansvar

1st line - Forretningsområde	2nd line - Compliance	3rd line - Intern revision

• Risikoejer
• Skal forstå de risici, som forretningsområdet indeholder og etablere forretningsgange og interne kontroller, som afdækker og reducerer disse risici (sund risikokultur)
• Udfører interne kontroller og udarbejder ledelsesrapportering herom
• Sikrer betryggende ressourcer og kompetencer til at håndtere risici
• 1st line skal kunne fungere uafhængigt at 2nd og 3rd line
	• Kortlægger, vurderer og rapporterer om compliancerisici i koncernen
	• Vurderer om 1st lines metoder og procedurer er effektive i relation til at overholde lovgivning og minimere compliancerisici
	• Vurderer om forretningen implementerer regler korrekt og efterlever dem – med fokus på processer og kontroller
	• Rådgiver og bistår 1st line med at reducere compliancerisici
	• Rådgiver og bistår ved risikohændelser
	• Fokuserer på, at der er procedurer og kontroller, som efterleves, og mindre fokus på at regne efter
		• Reviderer i samarbejde med ekstern revision alle forhold relevante for at årsregnskabet giver et retvisende billede og afgiver revisionspåtegning
		• Udfører alle revisionsopgaver i henhold til Finanstilsynets revisionsbekendtgørelse (inkl. 55 erklæringer)
		• Identificerer, rapporterer og følger op på konstaterede svagheder
		• God revisionsskik
		  • Skal basere sig på arbejde udført af 1st og 2nd line
		  • Krav til udførelse og dokumentation (revisionsbevis)

Roller

Intern revision	Compliance
• Mandat i Revisionsbekendtgørelsen • Bestyrelsens forlængede arm • Funktionsbeskrivelse og revisionsaftale godkendt af bestyrelsen • Må ikke deltage i andet arbejde end revision • Koncernrevisionsplan godkendes af bestyrelsen • Løbende revisionsrapporter til lokal ledelse og ansvarlig koncerndirektør • Rapporterer observationer, risiko, anbefalinger og ledelsens svar • Revisionsprotokollater på bestyrelsesmøder	• Mandat i FIL §71, MiFID, hvidvask, UCITS mv. • Direktionens forlængede arm • Retningslinjer godkendt af direktionen • Fungerer som sparringspartner i 1st line • Årsplan godkendes af koncerndirektionen • Løbende compliancerapporter til lokal ledelse og ansvarlig koncerndirektør • Rådgiver og bistår forretningen med at nedbringe risici inden rapportering • Rapporterer risiko, gennemførte og aftalte foranstaltninger • Årsrapportering på bestyrelsesmøde i februar/marts og halvårsrapportering til direktion og risikoudvalg

I Solvency II direktivet i artikel 46 fremgår det at:

"Forsikrings- og genforsikringsselskaber indfører et effektivt internt kontrolsystem. Systemet skal mindst omfatte administrative procedurer og regn-kabsprocedurer, en intern kontrolstruktur, passende rapporteringsrutiner på alle niveauer i selskabet og en compliancefunktion.
2. Compliancefunktionen skal bl.a. rådgive administrations-, ledelses- eller tilsynsorganet om overholdelsen af de love og administrative bestemmelser, der vedtages i henhold til dette direktiv. Den skal også foretage vurderinger af de potentielle konsekvenser af lovændringer for det pågældende selskabs virksomhed samt identificere og vurdere compliancerisici".

Endvidere vil de kommende krav til intern revisions konklusion på den administrative praksis alt andet lige omfatte de krav til compliance, som fremgår af Bekendtgørelse om ledelse og styring i pengeinstitutter m. fl.

Vi har på det seneste set tilsynsbesøg rettet mod 2nd og 3rd line, som har givet anledning til påbud på området. Jeg tror, at det er vigtigt, at vi som profession udvikler en praksis på området – meget gerne i tæt dialog med Finanstilsynet.

Det er forventningen, at der vil være et indlæg på temadagen for den finansielle sektor den 5. november 2015, der behandler dette emne.

Risikostyring

Som det fremgår af ovenstående er en del krav fælles for compliancefunktionen og risikostyringsfunktionen.

Der er endvidere i henhold til lov om finansiel virksomhed § 80b krav om etablering af et særskilt bestyrelsesudvalg benævnt "risikoudvalget". Der er endnu ikke kommet retningslinjer for arbejdsdelingen mellem revisionsudvalg og risikoudvalg, hvilket giver anledning til nogle praktiske udfordringer med hvilke forhold, som skal behandles hvor http://www.eciia.eu/wp-content/uploads/2014/10/ECCIA_FERMA_Brochure_v8_HD1.pdf.

Vi har på det seneste set tilsynsbesøg rettet mod 2nd og 3rd line, som har givet anledning til påbud på området.

Jeg tror, at det er vigtigt, at vi som profession udvikler en praksis på området – meget gerne i tæt dialog med Finanstilsynet.

IIA, Danmark deltog i 2014 i samarbejde med ECIIA og FERMA (Federation of European Risk Management Associations) i udarbejdelsen af "guidance" vedrørende revisionsudvalg og risikoudvalg rettet mod EU kommissionen og de enkelte medlemslandes lovgivere. I appendix 1 hertil er opstillet en tabel (se figur 2 på de to næste sider), som viser et forslag til hvilke forhold, som skal behandles hvor. Som det fremgår, er der et meget (alt for) stort overlap.

Sammenfatning

Det er min oplevelse, at compliancefunktionens og risikostyringsfunktionens virkefelt defineres relativt forskelligt fra virksomhed til virksomhed. Det er min vurdering, at en regulering på området vil være formålstjenestelig.

Det er endvidere min oplevelse, at kravene til "revision" af disse funktioner fortolkes og håndteres relativt forskelligt. Det er min vurdering, at der er behov for etablering af en praksis på området, meget gerne i tæt samarbejde med Finanstilsynet.

Endelig er der et behov for retningslinjer for hvordan revisionsudvalget og risikoudvalget "deler" opgaverne i mellem sig.

Figur 2: ECIIA/FERMA—forslag til hvilke forhold som skal behandles hvor

	RESPONSIBILITIES	Risk Committee	Audit Committee
1	**Review risk management systems**		
a	To recommend to the Board the framework and system to manage risks	x	
b	To discuss the enterprise's risk tolerance, risk appetite and strategy with management and CRO and give an opinion on acceptability of the proposed levels of risk to the Board	x	
c	To be informed by management, including the CRO of any changes in conditions or circumstances or new opportunities that could impact the allocation of risk appetite to the different risk categories and provide advice to the Board	x	
d	To oversee the conduct of, and review the results of, enterprise wide risk assessment, like proposed strategic acquisitions or disposals	x	x - Relevant to be able to challenge financial reporting
e	To assess and evaluate the risk profile in light of the activities concerning risk appetite, risk development and risk aggregation and provide advice to the Board	x	
f	To help coordinate activities of the various standing committees for risk oversight	x	x
g	To initiate and monitor special investigations into areas of corporate risk and break-downs in internal control	x	x
h	To review the nature and level of insurance coverage	x	
i	To engage management, including the CRO, in promoting a positive risk culture	x	
j	To monitor the effectiveness of risk management functions throughout the undertaking and ensure that infrastructure, resources and systems are in place for risk management and are adequate to maintain a satisfactory level of risk management discipline	x	x
k	To monitor the independence of risk management functions throughout the organization	x	x
2	**Chief Risk Officer (CRO) or equivalent Head of Risk Management**		
a	To advice the Board about the appointment and, when and if appropriate, replacement of the CRO and ensures that the function gets the necessary means to operate	x	
b	To assess the performance of the framework and procedures in place	x	x - Relevant for monitoring of internal control and financial reporting
c	To organize regular communication with the CRO, who is also permanently invited at the risk committee meetings	x	
3	**External audit**		
a	To review the external auditor's reporting		x
b	To exchange with the audit committee on the risks identified in the financial reporting process (including sustainability reports) and their impact		x

Figur 2 fortsat: ECIIA/FERMA—forslag til hvilke forhold som skal behandles hvor

4	Relationship and coordination		
a	In coordination with the audit/risk committee, to understand how the undertaking's internal audit work plan is aligned with the risks that have been identified and with risk governance (and risk management) information needs	x	x
b	To exchange with the audit/risk committee on the risks identified by internal auditors, their impact and recommendations	x	x
c	To identify areas where assurance is required, and to ensure that appropriate assurance is received and that this informs and updates the organization's risk profile	x	x
5	**Report annually on the effectiveness and efficiency of risk management in the organization**	x	x
6	**Review annually the performance and terms of reference of the Committee in order to determine whether it is functioning effectively by reference to best practices**	x	x
7	**Oversee the integrity of the financial reporting process and financial reports**		
a	After review with the management and the external auditors, the Committee will recommend to the Board for approval the financial statements and reports that are intended for publication.		x
b	They will also review any significant financial reporting issues and report to the Board		x
8	**Review the efficiency of internal control and risk management systems**		
a	They review the adequacy and effectiveness of:		
	• The company's policies and procedures to assess, monitor and manage financial and non-financial business risks	x	x
	• Internal control systems	x	x
	• Legal and ethical compliance programs		x
b	They will regularly meet with the management, the external auditors and the internal auditors and other assurance functions to discuss issues and concerns warranting committee attention, including but not limited to their assessment of the effectiveness of the internal controls and risks management systems and the process for improvement.	x	x
c	They receive the reports from the support functions	x	x
9	**Review and appraise the audit activities: independence, objectivity and effectiveness of the audit process**		
a	The Committee makes recommendations to the Board for the appointment and replacement of the external auditors.		x
b	They approve all non-audit services and advise the board on statements to be made in the annual report regarding the statutory auditor's provision of non-audit services		x
10	**Supervise the internal audit function**		
a	The committee recommends to the Board the appointment or dismissal of the chief audit executive		x
b	They review the scope of the internal audit plan, including the work program and the quality control procedures and should also approve the internal charter.		x
c	They assess the performance, independence and objectivity of the internal audit function.		x

Revision af Compliance

Yahya Ibrahim, Manager i Group Internal Audit, Takeda Pharmaceuticals

Showaib Nabi, manager i advisory services, EY

Indledning

I mange store danske virksomheder, er der efterhånden oprettet selvstændige compliancefunktioner, som har til formål at sikre, at medarbejderne i koncernen holder sig inden for både lovgivningens krav og egne formulerede politikker og forretningsgange. Kravene til compliancefunktioner er stigende og virksomhederne forsøger at bruge compliancefunktionen som et effektivt redskab til at forbygge og opdage compliancebrud før myndighederne slår ned, hvilket i sidstnævnte tilfælde kan give alvorlige ridser i selskabets image og blive dyrt.

Ledelsen i virksomhederne er ikke de eneste der stiller krav til compliancefunktionen. I den nye bekendtgørelse om revisionens gennemførsel i finansielle virksomheder (ny bekendtgørelse) skal revisor vurdere, om compliancefunktionen har de nødvendige ressourcer til at udføre opgaverne forsvarligt. Ydermere er det et krav, at revisor skal vurdere, om rapporteringen fra compliancefunktionen er tilfredsstillende. Såfremt revisor bliver bekendt med svagheder i compliancefunktionen, er det et krav, at dette bliver omtalt i revisionsprotokollen.

Sarbanes-Oxley afsnit 404 kræver, at virksomheder evaluerer effektiviteten af det interne kontrolmiljø ved hjælp af et passende framework. Virksomhedens eksterne revisorer vil forvente, at selskabet reviderer komponenterne i compliancekontrolframeworket sammen med finansielle og operationelle kontroller. Disse krav gør revision af compliancefunktionen uundgåelig. Men hvad skal komponenterne i en revision af en virksomheds compliance-program så omfatte?

Revisionsplanen

For at sikre fuldstændig dækning bør komponenterne i complianceprogrammet omfatte test af virksomhedens compliance med specifikke juridiske krav og sine egne interne compliancepolitikker og procedurer samt vurdering af tilstrækkeligheden af selve compliance-programmet. Hvis virksomheden har gennemført omfattende risikovurderinger, bør de mest betydningsfulde compliancerisici være identificeret og passende kontrol implementeret. Disse vurderinger bør give en detaljeret roadmap omkring, hvor testressourcerne skal fokuseres mod samt give oplysninger om firmaets politikker og procedurer, der bør følges i driften af virksomheden.

Hvis virksomheden ikke har foretaget en risikovurderinger, bør revisionsplanlægningen starte med virksomhedens code of conduct og compliancepolitikker for at identificere de risikoområder, der skal målrettes i mod. Andre faktorer, der bør overvejes ved udarbejdelse af revisionsplanen omfatter virksomhedens industri, størrelsen af organisationen, den geografiske placering, seneste lovgivningsmæssige fokus og sagsanlæg, whistleblowers samt medarbejder- og/eller kundeklager.

Revisionsplanen bør også omfatte vurdering af tilstrækkeligheden og effektiviteten af selve compliance-programmet. Udgangspunktet her kunne være følgende:

- Indeholder complianceprogrammet alle de påkrævede elementer?
- Hvad er virksomhedens historie mht. bøder, sagsanlæg og håndhævelser af regler?
- Hvad afspejler operationelle revisionsrapporter vedrørende compliance med interne processer?
- Hvor mange af whistleblower-episoderne er relateret til compliancesvagheder?

Formålet med revisionen

I visse virksomheder er compliance ikke forankret i en afdeling og der er ikke en Chief Compliance Officer (CCO) der er ansvarlig for alt compliance i organisationen. Fornyligt foretog Deloitte en undersøgelse blandt 70 nordiske virksomheder, og her viste det sig at 68% af finansielle virksomheder havde en selvstændig CCO, i ikke-finansielle virksomheder var andelen kun på 32%. I mange virksomheder kan compliance blive fordelt i forskellige afdelinger, derfor er det vigtigt at forstå complianceorganisationen, og hvem der har ansvaret for complianceprogrammet.

Før compliancerevisionen påbegyndes, bør man identificere de forventede og acceptable niveauer af performance. Det er urealistisk at forvente, at selv det mest effektive complianceprogram forebygger eller afslører alle complianceproblemstillinger. Så hvad er et acceptabelt niveau af performance? Naturligvis afhænger svaret af det fagom-

råde, der testes. Fem procent i fejlprocent kan være acceptabelt i vurderingen af, om krav om overholdelse af beløbsgrænser i forbindelse med køb af gaver til virksomhedens egne ansatte, mens enhver forekomst af price-fixing er uacceptabelt.

Hvornår er compliancefunktionen klar til revisionen og hvad er tidsrammen?

Undersøgelsen lavet af Deloitte viste også, at 84% af medarbejderne i compliancefunktionen i de adspurgte virksomheder var nye i jobbet. Der er derfor to komponenter mht. revisionens tidsmæssige placering, der bør overvejes: Hvor hurtigt efter implementeringen eller udrulning bør der gennemføres revisionstests, og hvilke aktivitet fra hvilken tidsperiode vil blive vurderet? Ifm. den første overvejelse er det vigtigt, at der går tilstrækkelig tid efter implementering af nye processer og/eller efter uddannelse så medarbejdere kan nå at tilpasse sig, og at driften fungerer problemfrit.

Skal revisionen udføres af en specialist?

Der er en række forskellige typer af ressourcer, der kan benyttes til at udføre compliancerevisioner: Interne og eksterne ressourcer såvel som specialister på området. De to vigtigste faktorer, der bør overvejes ifm. beslutningen blandt de forskellige faglige ressourcer, er uafhængighed og ekspertise.

Den nye bekendtgørelse lægger op til outsourcing som en mulighed i forbindelse med revision af compliancefunktioner. Generelt bør revisorer foretrækkes ifm. transaktionstest, hvorimod specialister, for eksempel advokater, konsulenter eller miljømæssige ingeniører, er mere egnede ifm. operationelle gennemgange inden for områder, der kræver specialiseret viden. I begge tilfælde skal den revi-derende have en vis uafhængighed fra den underliggende proces eller funktion.

Hvordan bør revisionen udføres?

Hvis revisionen indebærer transaktionstests, skal man beslutte, om der vil gøres brug af en analytisk eller statistisk stikprøvemetode. Fordelen ved statistiske stikprøver er, at det tillader, at der drages konklusioner om graden af compliance for hele populationen baseret på resultaterne af stikprøverne. På den anden side kan resultaterne fra en analytisk stikprøvetagning ikke projiceres for hele populationen, men forekomsten af fejl i stikprøven kan angive områder, der kræver yderligere revidering.

Uanset hvilken stikprøvemetode, der anvendes, er det altid relevant at overveje at bruge interviews og spørgeskemaer til at indhente yderligere oplysninger fra medarbejdere. Disse værktøjer kan hjælpe med at identificere områder, der skaber bekymring enten hos ledelsen eller hos medarbejder samt at fremhæve styrker eller svagheder i complianceprogrammet.

En anden vigtig overvejelse er, hvilken type af dokumentation der skal oprettes som en del af revisionsplanen. For at revisionsresultaterne skal have nogen som helst form for integritet, skal metoden være underlagt kontrol og nøje analyser. I overensstemmelse hermed bør der udarbejdes arbejdspapirer til at dokumentere revisionsprocessen, og disse skal samtidig opbevares i en passende periode til gennemgang af ledelsen, bestyrelsen eller af myndigheder, alt efter gældende regler.

Rapportering

Uanset om der rapporteres skriftligt eller mundtligt, bør revisionsresultaterne kommunikeres til nogle eller alle af følgende interessenter: Lokal forvaltning, afdeling, virksomhedens øverste ledelse eller bestyrelse. Skriftlige rapporter bør inkludere ledelsens kommentarer, handlingsplaner og forfaldsdatoer. Udførelsen af ydelserne bør efterfølges af opfølgende validering af færdiggørelse samt revurdering af effektiviteten af foranstaltningerne.

Revisionsresultaterne kommer enten til at vise effektiviteten af complianceprogrammet eller huller og mangler i programmet. Uanset hvad giver de værdifulde oplysninger, som ledelsen kan bruge til løbende at forbedre complianceprogrammet.

Et effektivt complianceprogram

Efter alt det hårde arbejde med at vedtage en code of conduct og passende politikker, gennemføre et compliancetræningsprogram samt gennemføre Compliance Risk Assessment, kan man næppe bebrejde den compliance-ansvarlige i at ville holde en lille pause, før han/hun kaster sig ud i at takle næste problemstilling. Men denne pause må vente lidt endnu, eftersom et effektivt complianceprogram også er nødt til at omfatte revision og overvågning.

Nye medlemmer

Nye medlemmer i IIA fra 10.04.2015 – 31.08.2015

A.P. Møller-Maersk
Jacob H. Pappoe
Henri Billot

Danske Andelskassers Bank
Carsten Strandholt

Danske Bank
Søren Jonstrup

Deloitte
Molly McGee
Keld Danielsen

DLR Kredit
Nina Koustrup Klargaard

DR
Lene Andersen

EY
Allan Lunde Pedersen
Klaus Skovsen

JN Data
Kenneth Waaben Nielsen

Københavns Kommune
Louise Weinreich Hansen

NNIT
Berit Frandsen

Novozymes
Thomas Løndorf

Nykredit
Alexandra Steenstrup Berthelsen

PwC
Søren Krogh Voss

RevisorGruppen Danmark
Morten Koch-Hansen

Scan-Group
Charlotte Hoby

Skatteministeriet
Karsten Petersen

Sparekassen Sjælland
Henriette Klarholt Jensen

Sparekassen Thy
Lone Kragh

Thorngaard Reifling
Jacob Reifling

Tryg
Kim Gundelach

VP SECURITIES
Vincent Andreassen

Uddannelsesaktiviteter

Er du opdateret på IIA's kursusudbud? Som altid findes datoer og emner for gå-hjem møder, kurser og konferencer på foreningens hjemmeside www.iia.dk under rubrikken "Uddannelse", hvor tilmelding til arrangementerne også foretages.

Nedenfor er fremhævet kommende planlagte kurser og møder, men listen bliver hele tiden opdateret, så det er bestemt værd at foretage et besøg på foreningens hjemmeside.

Kursusdag for Forsikringsrevisorer, 30. september 2015
Afholdes på Forsikringshøjskolen, Rungsted.

Temadag for den finansielle sektor, 5. november 2015
Afholdes på Trinity Hotel og Konferencecenter

Gå-hjem møde med Finanstilsynet, 3. december 2015
Mødet afholdes hos Nykredit, Kalvebod Brygge 47

Årskonference 2016, 25. maj 2016 - 26. maj 2016
Afholdes på Hotel Best Western Nyborg Strand.

”Bagsmækken”

Foreningens adresse

Foreningen af Interne Revisorer (IIA)
Att.: Vicerevisionschef Kim Stormly Hansen
Intern revision
Nykredit
Anker Heegaards Gade 4-6
1560 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.

Certificering

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

Partner Lars Maagaard, KPMG P/S
☎ 61 62 18 90 ✉ lmaagaard@kpmg.com

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

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

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

Kasserer
Koncernrevisionschef Morten Bendtsen
PFA Pension
☎ 39 17 60 12 ✉ mob@pfa.dk

Sekretær
Senior Audit Manager, CIA, Afdelingsdirektør
Anette Kauffmann Laursen
Nordea
☎ 55 47 33 19 ✉ anette.laursen@nordea.com

Bestyrelsesmedlemmer
Regional Chief Auditor, CIA, CISA
Neil Jensen
RSA Scandinavia
☎ 40 42 64 26 ✉ njz@codan.dk

Koncernrevisionschef, COR
Pia Sønderlund Nielsen
Finansministeriet
☎ 25 26 27 72 ✉ pnn@fm.dk

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

Revisionschef, CMA, CIA, CISA
Birgitte Rousing Svenningsen
Europæiske Rejseforsikring
☎ 33 27 84 82 ✉ brs@europaeiske.dk

Revisionschef
Jesper Jæger Granstrøm
PostNord
☎ 33 61 50 12
✉ jesper.jaeger.granstroem@postnord.com

Director, CIA, CISA, CGEIT
Johan Bogentoft
PwC
☎ 29 27 62 96 ✉ Joa@pwc.dk