

INFO

Foreningen af Interne Revisorer

Nummer 70 | December 2018 | 23. årgang

Minitema

- Tre bud på fremtidens interne revision

Anbefalinger

Opnå den ønskede effekt
med din rapportering

Ny IIA Practice Guide

Auditing Capital Adequacy
and Stress Testing for Banks

IIA Prisen 2018 ● EBA's retningslinjer om intern ledelse

INFOs redaktion

Ansvarshavende redaktør

Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
Express Bank
☎ 36 39 52 61 ✉ bisv@expressbank.dk

Øvrig redaktion

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

Seniorspecialist
Lea Kehlet Halsø
Nykredit
☎ 44 55 93 01 ✉ lea@nykredit.dk

Chief Expert, CIA
Vanita Shukla Hork
Nordea
☎ 30 12 84 34 ✉ vanita.hork@nordea.com

Revisionschef
Michael Ravbjerg Lundgaard
DSB
☎ 24 68 06 01 ✉ mirl@dsb.dk

Revisionschef
Louise Claudi Nørregaard
PensionDanmark
☎ 61 55 84 88 ✉ lcn@pension.dk

Chefspecialist, CIA
Tobias Zorde
Nykredit
☎ 21 18 54 97 ✉ tzo@nykredit.dk

Revisor
Klaus Nordmann Østrup
Københavns Kommune
☎ 33 66 24 13 ✉ zx7z@ir.kk.dk

Næste nummer

INFO 71 udkommer i april 2019.
ISSN: 1903-7341 (Elektronisk version).

Indlæg til INFO

Artikler i INFO påskønnes med en vingave.

Forsidefoto

UnknownNet

Redaktionens adresse

Foreningen af Interne Revisorer (IIA)
Att.: Seniorspecialist Glenn Thunø
Intern revision, Nykredit
Kalvebod Brygge 1-3
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
Vinder af IIA Prisen 2018	4
Nye certificeringer	4

Minitema: Fremtidens interne revision

Netværksmøde for revisionschefer i den finansielle sektor	7
Intern revisions påtegning - er det en saga blot?	9
Skal intern revision skabe eller følge den teknologiske udvikling?	12

Det er både, hvad vi skriver, og hvordan vi skriver det...

When recommendations go unaddressed	16
Hvordan opnår revisor den ønskede effekt med sin rapportering?	21

Vejledning om alternative investeringer og prudent Person	25
Auditing Capital Adequacy and Stress Testing for Banks	30
EBA's retningslinjer vedrørende intern ledelse "guider" intern revision godt på vej	34
Nye medlemmer	38
Bagsmækken	39

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".

www.iaa.dk

Leder



Anita Laugesen, Internal Audit Manager, CIA, Nordea

Året 2018 er snart gået, og du sidder nu med årets sidste udgave af INFO foran dig. Juleudgaven om man vil. Du skal nu ikke læse om julemad eller nisser, men artiklerne byder på emner som fremtidens interne revision samt opfølgning på revisionsbemærkninger, så de kan måske give en tiltrængt pause fra alt juleriet.

Morten Bendtsen fra det finansielle udvalg giver os en opdatering fra et netværksmøde i oktober hvor en række revisionschefer var samlet for at drøfte hvordan en værdiskabende og compliant intern revision ser ud i dag og fremover. En række interessante indlægsholdere gav deres input til emnet og den efterfølgende debat handlede bl.a. om hvor intern revisions ressourcer skal findes fremover for at sikre den rette udvikling.

Inden for samme tema har Birgitte Rousing Svenningsen analyseret fakta om regnskabspåtegningen og kigget nærmere på i hvilke institutter intern revision påtegner regnskabet i dag. Hun diskuterer hvordan påtegningen tidligere har været set som intern revisions eksistensgrundlag, men at det nu i højere grad er assurance, insight og objectivity der er eksistensgrundlaget. Hendes bud på fremtiden er at flere interne revisionsafdelinger vil følge trop og fravælge at påtegne årsregnskabet.

Den teknologiske udviklings betydning vil uden tvivl have stor betydning for intern revisions fremtid. Christian Reimar og Jacob Bjørnholdt fra EY stiller spørgsmålet: "Skal intern revision skabe eller følge den teknologiske udvikling?" Uden at afsløre for meget er deres bud på et svar at hvis intern revision vil tilføre værdi og være en strategisk partner for forretningen bør vi udnytte teknologiens øgede muligheder for mere effektivt at monitorere interne kontroller og identificere risici og dermed tage del i at skabe udviklingen.

Redaktionen genopfrisker i denne udgave en artikel om opfølgning på revisionsbemærkninger – eller mangel på

samme - og Michael Ravbjerg Lundgaard fra DSB uddyber emnet med sine kommentarer til hvordan revisor opnår den ønskede effekt med sin rapportering. Ikke overraskende er en del af svaret ejerskab - både fra ledelsens side, men også fra revisors side for at sikre at de risici der bliver rapporteret, bliver gjort forståelige for modtageren og at man, hvor nødvendigt, arbejder sammen for at finde den bedste måde at adressere risikoen på.

Lotte Pia Møllerup fra EY fører os igennem det europæiske banktilsyns (EBA) retningslinjer for finansielle virksomheder, GL 11, sammenholdt med den danske lovgivning på området. Her kommer hun ind på forventninger til intern revision og opbygningen af de tre forsvarslinjer samt øvrige betragtninger vedrørende risikostyring og governance.

Ane Præstekjær fra EY giver os en gennemgang af Finanstilsynets "Vejledning om alternative investeringer og gode investeringsprocesser i lyset af prudent personprincippet". Denne vejledning er et tegn på tilsynets øgede fokus på området og et godt råd er derfor at intern revision i liv- og pensionselskaberne tager dette i betragtning i deres planlægning og Ane giver forslag til hvilke delområder revisionen bør dække.

Fra europæisk regulatorisk side er der forventninger om at bankers interne revision reviderer capital adequacy og stress-testing. Pille Lindskog fra Nordea giver en introduktion til hvordan den nye Practice Guide fra IIA kan anvendes til planlægning af revisioner inden for området og hvordan der bør tages udgangspunkt i bankens risiko appetit.

Ud over INFO er der gang i mange andre aktiviteter i IIA; på den finansielle temadag i november blev IIA prisopgaven uddelt for første gang. Derudover vil i igennem artiklerne også flere gange se referencer til det igangværende IIA strategiarbejde, som I vil komme til at høre mere om i løbet af 2019. Og I kan glæde jer til en ny og opdateret hjemmesiden der forventes klar først i det nye år.

God læselyst samt en glædelig jul og et godt nytår!

**GODT
NYTÅR
2019**

Vinder af IIA Prisen 2018

IIA Prisens 1. præmie gik i 2018 til Carina Kristiansen og Christian Pinholt for opgaven:

Intern revision & implementeringen af the Three Lines of Defense i mellemstore danske pengeinstitutter.

På billedet ser du en glad Christian der på vegne af ham og Carina modtager en gavecheck på **25.000**.

Der var desværre ikke opgaver der var kvalificeret til 2. præmien.

Du kan i rammen på modsatte side læse mere om IIA prisen 2019, herunder formålet og hvad en hovedopgave skal opfylde for at kunne komme i betragtning til IIA Prisen.

Næste nummer af INFO vil indeholde en artikel skrevet med udgangspunkt i hovedopgaven.



Nye certificeringer

Niels Thomsen, Lidl - CIA
Lin Du, Novo Nordisk - CIA
Claus Bo Jensen, DSB - CIA

Et stort tillykke med certificeringen !!!!



IIA PRISEN

Prisopgave om intern revision

Foreningen af Interne Revisorer uddeler 2 præmier til hovedopgaver på cand. merc. aud. studiet

1. præmie: 25.000 kr.

2. præmie: 15.000 kr.

Prisens formål er at fremme kendskabet til og forskningen inden for intern revision.

Hovedopgaven skal omfatte et emne og en problemformulering, som er relevant for forståelsen af intern revisions arbejde og betydning for de virksomheder, som har eller overvejer at etablere(t) en intern revisionsfunktion. For at komme i betragtning skal hovedopgaven være afsluttet i perioden 1. august 2018 til 31. juli 2019.

Ansøgningen indsendes elektronisk til foreningens formand på ksh@nykredit.dk. Ansøgningen skal indeholde

- 1) kontaktinformationer
- 2) problemformulering, indledning og konklusion
- 3) hovedopgaven

Ansøgningsfristen er 31. juli 2019. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iaa.dk.

Prisoverrækkelsen vil ske i løbet af efteråret 2019. Bedømmelsesudvalget består af Dorthe Tolborg (Danske Bank), Kim Klarskov (CBS) og Birgitte Rousing Svenningsen (Express Bank).

Den/de studerende bestemmer selv emnet for hovedopgaven, og på foreningens hjemmeside www.iaa.dk findes der forslag til emner, som kan anvendes til inspiration, .

Minitema: Fremtidens interne revision



Med forskellige udgangspunkter giver de tre næste artikler "Netværksmøde for revisionschefer i den finansielle sektor", "Intern revisions påtegning – er det en saga blot?" og "Skal intern revision skabe eller følger den teknologiske udvikling?" et bud på, i hvilken retning intern revision bør bevæge sig i fremtiden. Er fremtiden fokus på revision af de operationelle processer? Bliver interne revisionsafdelinger med hovedfokus på regnskabsrevision overhalet indenom? Skal intern revision udvide perspektivet og være en integreret del af IT-implementeringer? Via disse tre artikler, kan du få inspiration til eftertanke om, hvilken retning du ønsker at føre din revisionsafdeling i.

God læselyst!

Netværksmøde for revisionschefer i den finansielle sektor



Morten Bendtsen, Koncernrevisionschef, CIA, PFA Pension

Indledning

Der er bevægelse i intern revisions fokusområder i de finansielle virksomheder, og regulatoriske krav betyder, at intern revision i højere grad end tidligere skal fokusere på revision af de operationelle processer.

Den 11. oktober 2018 afholdt en arbejdsgruppen under IIA's Finansielle udvalg¹ derfor et netværksmøde for revisionschefer i den finansielle sektor². I alt deltog 16 revisionschefer i mødet.

Hovedtemaet for mødet var:

"Hvordan ser en værdiskabende og compliant intern revision ud i dag og fremover?"

For at komme med input til drøftelserne holdt følgende talere indlæg om deres syn på, hvordan intern revision skaber værdi for virksomheden – herunder hvad der forventes af samspillet imellem intern og ekstern revision:

- Group CEO Allan Polack, PFA Pension
- Bankdirektør og CRO Carsten Rasch Egeriis, Danske Bank

Owen Jackson, Deloitte North West Europe gav en opdatering på, hvor de interne revisionsfunktioner er på vej henset fra et UK perspektiv.

Hovedbudskaber

Allan Polack lagde meget vægt på at intern revision skal være med til at øge risikoforståelsen og styrke de forbyggende kontroller i forretningen. Han var optaget af en klar ansvarsdeling i 3LoD, omkostningseffektivitet og minimalt overlap af roller og ansvar. Allan ser fremadrettet, at den tekniske udvikling vil kræve forandringer for den interne revision.

Carsten Egeriis var optaget af risikokultur og kulturelle revisioner. Han lagde også afgørende vægt på at intern revision forbliver en uafhængig assurance provider og i bedste fald en talentfabrik for forretningen.

Owen Jackson påpegede, at udviklingen bl.a. var drevet af skandaler, hvor intern revision ikke havde gjort deres job godt nok. Trenden bevæger sig over mod kultur, cyber-risiko, finansiell kriminalitet, modelrisiko og kundebehandling. Han så stadig intern revisions kerneydelse som assurance provider på interne kontroller, governance, risikostyring, digitalisering m.v. Men han så også et behov for at intern revision bevæger sig henimod en rådgivende rolle og dermed hjælper virksomheden med at blive bedre og hurtigere til at forebygge og forstå sine risici.

Samlet set bekræftede alle tre indlæg, at forventningen til intern revision er, at vi er proaktive og forandringsparate og vi skal byde mere ind på nye områder, end vi gør i dag for at sikre vores fremadrettede værdiskabelse.

Den efterfølgende debat påviste, at det område hvor der er størst usikkerhed er, hvorledes vi bliver i stand til at tiltrække, udvikle og fastholde de rigtige kompetencer – hvor er intern revisions fødekanaler for talent og nye kompetencer.

I takt med at kravene til intern revision ændrer sig, er det ikke sikkert, at ekstern revision skal være vores primære leverandør af medarbejdere.



¹ Lars Maagard, Morten Bendtsen og Dorthe Tolborg

² Revisionschefer i finansielle virksomheder med 3 eller flere medlemmer af IIA.dk var inviteret samt Jens Ringbæk - Deloitte, Per Rolf Larssen - PwC og Lars Rhod Søndergaard - E&Y

Næste træk

Den fremtidige rolle og fokusområder for intern revision må afhænge af, i hvilket omfang intern revision vil kunne fremstå som en objektiv og uafhængig funktion. Det er i samfundets og aktionærernes interesse, at virksomheder underkastes en særlig omfattende og grundig revision, udført af revisorer med detailkendskab til den pågældende virksomhed.

For at skabe et bedre grundlag for, at kunne imødekomme nye risici og udvise proaktivitet bør interne revisorer fokusere på revision af de operationelle processer.

I sidste ende er det et spørgsmål om, hvorvidt bestyrelsen, og dermed aktionærerne, opnår samme værdi ved at intern revision ikke udfører en fuldstændig finansiel revision. Det kræver, at interessenterne har tilstrækkelig information til at vurdere, hvad der er væsentligt og dermed skaber størst værdi. Vi skal altså skabe en klar forståelse for vores risikounivers og "operating model".

Dernæst har vi en opgave i at forklare virksomhederne, hvad vores rolle indebærer og hvordan arbejdsdelingen er mellem den interne revisor, den daglige ledelse i virksomheden og ekstern revision.

IIA.dk vil arbejde videre med at understøtte udviklingen af intern revision. Bestyrelsen har igangsat et strategiarbejde inden for fire hovedområder og vil også se nærmere på de hovedbudskaber, der blev rejst på netværksmødet.

De fire hovedområder dækker:

- Advocating and promoting the profession
- Network and collaboration
- Training and education
- Standards and resources



Intern revisions påtegning – er det en saga blot?



Birgitte Rousing Svenningsen, Revisionsschef, CIA, CISA, Express Bank

Indledning

I forbindelse med den bevægelse, der har været i intern revisions fokusområder de seneste år, er det også blevet diskuteret, hvorvidt intern revision skal påtegne årsregnskabet. I en årrække har intern revision i finansielle virksomheder påtegnet årsregnskabet. Dette er et unikt fænomen i Danmark. Jeg har sat mig for at undersøge udbredelsen af påtegninger, men først vil jeg redegøre for lovgivningen på området og den historisk udvikling heraf.

Lovgivning

Intern revision i finansielle virksomheder er reguleret af revisionsbekendtgørelsen der stammer fra 1949 og på daværende tidspunkt havde den ikke nogen bestemmelser om påtegning af årsregnskaber. Det kom først senere. Jeg har ikke været i stand til at fastlægge præcist hvornår kravet kom, men det er formodentlig i 1960-erne eller 1970-erne. Den gang blev det indført som et krav, hvilket vil sige, at revisionschefen skulle påtegne årsregnskabet.

Jeg husker fra min studietid og de første mange år som intern revisor, at mange interne revisorer opfattede påtegningen som intern revisions eksistensgrundlag.

Med den øgede internationalisering i dette århundrede blev det sværere og sværere at bevare kravet, idet kravet også omfattede finansielle datterselskaber af udenlandske koncerner. De udenlandske koncerner var ikke vant til, at revisionschefen skulle påtegne årsregnskabet. I 2004 blev revisionsbekendtgørelsen ændret således, at den interne revisions påtegning af årsregnskabet ikke længere er et krav. Bestyrelsen for den finansielle virksomhed kan vælge, om revisionschefen skal afgive en påtegning på årsregnskabet.

Udvikling

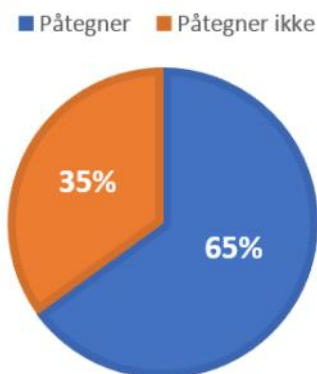
Nu står vi her 14 år efter, at revisionsbekendtgørelsen blev ændret, og det blev muligt at fravælge, at revisions-

chefen skal påtegne årsregnskabet, og det er derfor interessant at undersøge, hvordan udviklingen har været.

Personligt er jeg bekendt med, at Nordea fra starten har udnyttet muligheden. Danske Bank fulgte trop for få år siden og det sidste nye er, at det forventes, at 2018 bliver sidste år, hvor Nykredits årsregnskab bliver påtegnet af intern revision. De helt store spillere på markedet har således enten allerede fravalgt påtegning eller står over for at fravælge påtegning i den nærmeste fremtid.

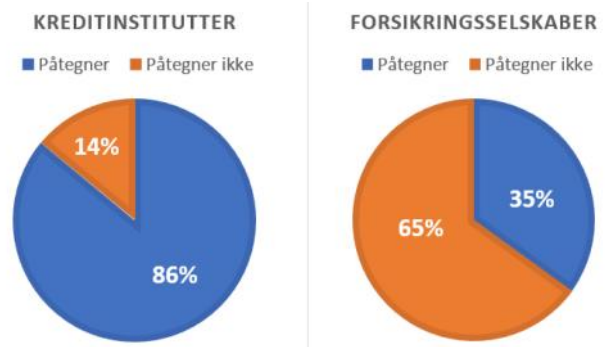
Men afspejler de store finansielle virksomheder også det generelle billede? For at belyse dette har jeg fået hjælp af Finanstilsynet ved specialkonsulent Pernille Dalby Nielsen. Jf. Pernille er fordelingen således, at 65% af revisionscheferne påtegner årsregnskabet og 35% påtegner ikke årsregnskabet. Dette er illustreret i nedenstående diagram:

PÅTEGNING AF ÅRSREGNSKABER



Det kan konkluderes, at de store finansielle virksomheder ikke afspejler det generelle billede. Hvor 2 ud af de 3 store har fravalgt påtegning, er det kun 1 ud af 3, når der ses på alle finansielle virksomheder med intern revision. Billedet bliver endnu mere skævt, hvis der tages hensyn til, at Nykredit planlægger af fravælge påtegningen i fremtiden.

Jeg har modtaget en underopdeling af tallene fra Finanstilsynet:



Det ses af de to figurer, at billedet er væsentligt forskelligt for kreditinstitutter og forsikringsselskaber. Det er således primært forsikringsselskaber, som har fravalgt påtegning.

Der er ikke lavet undersøgelser af, hvorfor forsikringsselskaber i højere grad har fravalgt påtegning. Man kan derfor kun gætte sig til årsagen. En mulig årsag kunne være, at forsikringsselskaberne generelt gennemsnitligt må antages at være mindre end kreditinstitutterne, hvorfor bestyrelserne kan mene, at revisionschefen ikke skal pålægges at påtegne årsregnskabet, idet det også pålægger revisionschefen en række opgaver. Revisionschefen skal således tage del i revisionen af alle væsentlige og risikofyldte områder. Det kan i små interne revisionsafdelinger være en udfordring både ressource- og kompetencemæssigt. Det er dog nok ikke den primære årsag, idet 86% af revisionscheferne i kreditinstitutterne påtegner, selv om der også er mange små kreditinstitutter.

Årsagen er formodentlig mere historisk betinget, og bunder måske også i det faktum, at nogle interne revisorer stadig opfatter påtegningen som intern revisions eksistensgrundlag.

På baggrund af disse tal kan det overvejes, om de 3 store spillere på markedet er på vej ud på en glidebane - det vil sige på vej væk fra der, hvor intern revision giver værdi - eller om de 3 store spillere har set lyset og er foran udviklingen. For at få svar herpå, har jeg undersøgt om intern revision mister sit eksistensgrundlag, hvis påtegning fravælges.

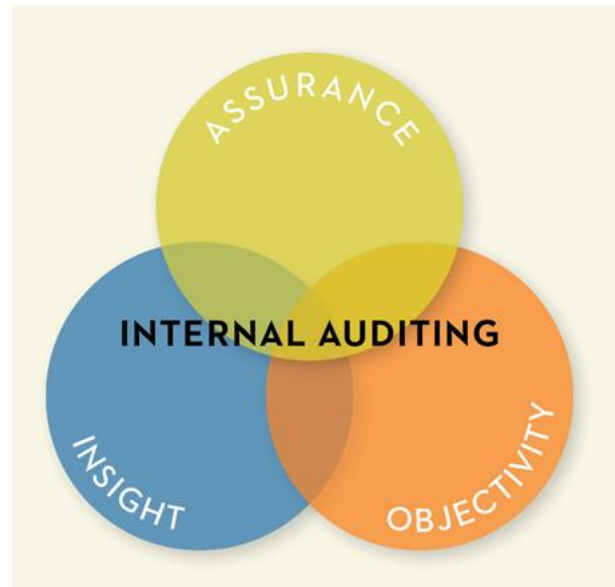
Eksistensgrundlag

Svaret herpå fandt jeg i IIA's definition af værdiskabelse. I 2008 nedsatte IIA en arbejdsgruppe, som skulle se på, hvilken værdi intern revision giver. Resultatet af arbejdsgruppens arbejde var, at intern revision giver værdi på nedenstående 3 hovedområder:

- **Assurance** = Governance, Risk and Control. Internal audit provides assurance on the organisation's governance, risk management, and control processes to help the organisation achieve its strategic, operational, financial and compliance objectives
- **Insight** = Catalyst, Analyses and Assessments. Internal audit is a catalyst for improving an organisation's effectiveness and efficiency by providing insight and recommendations based on analyses and assessments of data and business process.
- **Objectivity** = Integrity, Accountability and Independence. With commitment to integrity and accountabili-

ty, internal audit provides value to governing bodies and senior management as an objective source of independent advice.

Dette er også illustreret i nedenstående figur.



Som det er illustreret, så har intern revision et eksistensgrundlag og endda en vigtig opgave i relation til at hjælpe virksomheden med at opnå sine mål. Intern revisions eksistensgrundlag fjernes derfor ikke, selv om påtegning fravælges.

Både Nordeas og Danske Banks revisionsproces tager udgangspunkt i IIA standarder og UK code, hvorfor det må antages, at de interne revisionsafdelinger i disse virksomheder ser sig som værdiskabende gennem en systematisk og objektiv vurdering af virksomhedens ledelsessystem, risikostyring og interne kontroller.

Udfordringer ved påtegning

Der er således et eksistensgrundlag, selv om påtegning fravælges, men giver påtegning af årsregnskabet ikke også en værdi, således at den interne revision bør fortsætte med at påtegne?

Det må formodes, at revisionshonoraret til ekstern revision vil stige - dog marginalt, hvis en intern revision stopper med at lave regnskabsrevision og som følge heraf stopper med at påtegne årsregnskabet. Min opfattelse er dog, at regnestykket ikke bliver 1 til 1. Det er der flere årsager til. Min grundlæggende opfattelse (hvilket også er bekræftet af praktiske eksempler) er, at den samlede revision af årsregnskabet er for omfangsrig, når årsregnskabsrevisionen bliver udført af både den interne og den eksterne revision. Dette kan skyldes traditioner, men

kommer til udtryk ved, at de eksterne revisioner i deres samarbejde med de interne revisioner har anlagt et lavere væsentlighedsniveau, når de interne revisioners planlagte revisionshandlinger skulle aftales. Revisionshandlinger, som ikke i alle tilfælde er absolut nødvendige for revisors erklæring på regnskabet og derfor revisionshandlinger, som falder væk, når ekstern revision overtager den fulde revision af årsregnskabet. Hvis den interne revision ikke udfører årsregnskabsrevision, bør der derfor være ressourcer til rådighed til andre opgaver. Herunder primært til, at den interne revision kan hjælpe virksomheden med at opnå virksomhedens mål via en systematisk og objektiv vurdering af virksomhedens ledelsessystem, risikostyring og interne kontroller.

En anden ulempe er, at intern revision bliver sat i samme bås som ekstern revision, hvis revisionschefen påtegner årsregnskabet. Det betyder også, at intern revision må forvente at blive påvirket af fremtidens teknologi, hvor man må formode, at visse af den eksterne revisions opgaver vil blive overtaget af robotter.

Fremtiden

Man kan kun gisne om fremtiden, men jeg er dog af den opfattelse, at de 3 store spillere på markedet har set dagens lys. De øvrige interne revisionsafdelinger bør følge efter, så den interne revisions påtegning er en saga blot, idet intern revisions altoverskyggende værdi ligger i assurance, insight og objectivity.

Hvorvidt udviklingen vil gå i den retning, og hvor hurtigt den vil gå afhænger formodentlig af flere faktorer. Disse faktorer er ukendte, hvorfor det kunne være interessant, hvis der blev lavet en undersøgelse af, hvorfor så få virksomheder har fravalgt påtegning. Dette kunne passende være et emne for en cand.merc.aud. kandidatafhandling.

Under alle omstændigheder må det dog antages, at udviklingen vil afhænge af, om IIA formår at forklare, hvilken værdi intern revision kan give i forhold til at hjælpe virksomheden med at opnå sine mål. Erfaringer fra de store finansielle virksomheder kan bidrage til at udbrede denne forståelse. Også IIAs igangværende strategiprojekt har til formål at bidrage hertil, idet strategiprojektet tager udgangspunkt i IIAs definition af værdiskabelse.

Konklusion

På trods af, at det er 14 år siden, at muligheden for fravalg af påtegning blev indført for finansielle virksomheder, er intern revisions påtegning ikke en saga blot.

Det er dog min opfattelse, at de 3 store spillere på markedet har set dagens lys ved at fravælge påtegning, hvilket understøttes af IIAs definition på værdiskabelse. Efter

min opfattelse vil interne revisionsafdelinger med hovedfokus på regnskabsrevision blive overhalet indenom og tabe sin værdi på grund af den teknologiske udvikling og på grund af virksomhedernes behov.

Hvis man på nuværende tidspunkt påtegner årsregnskabet, og årsregnskabsrevisionen udgør hovedparten af den interne revision, bør man studere IIAs mangfoldige litteratur om værdiskabelse, forholde sig til det og kritisk spørge sig selv, om man leverer den mest optimale værdi til ens arbejdsgiver.

Med denne bemærkning vil jeg slutte mine kommentarer til udviklingen. Har mine kommentarer vakt opsigt, og har man lyst til at udforske litteraturen om intern revisions værdiskabelse, er man altid velkommen til at kontakte mig. Mine kontaktinformationer findes bagerst i INFO.



Skal intern revision skabe eller følge den teknologiske udvikling?



Christian Reimar,
Senior Konsulent, Risk
Transformation, Ernst &
Young P/S



Jacob Bjørnholdt, Konsu-
lent, Risk Transformation,
Ernst & Young P/S

Indledning

I takt med at nye teknologier forandrer virksomhedsbilledet, får professionen intern revision (IR) behov for nye færdigheder og en digital tilgang. Denne tilgang bør fokusere på skabelsen af bedre og mere rettidig indsigt i strategiske og forretningsmæssige risici.

Det globale risikobillede er fortsat under hastig forandring, og virksomheder skal ikke længere kun fokusere på risici inden for organisationens egne rammer.

IR skal enten være omstillingsparat og følge den teknologiske udvikling eller omfavne teknologiens frembrud og gribe teten i denne transformationsalder.

En ting er sikkert; IR skal flytte sig væk fra compliance-rolle og i stedet blive en strategisk rådgiver i fremtiden. I dag opererer de fleste virksomheder i et konstant skiftende miljø, hvor fleksibel og hurtig beslutningstagen er en forudsætning for at eksistere, og status quo ikke længere er acceptabel. Eksempelvis er kun 60 virksomheder fra 1955's Fortune 500 liste repræsenteret i 2017 grundet nye virksomheders innovative tilgange og udnyttelse af teknologiske opbrud på markedet. De teknologiske disruptions kan altså ikke forbigås og kræver øjeblikkelig handling.

Siden teknologiens frembrud som middel til at fremskynede forretningsmæssige resultater har teknologien været den primære enabler til implementering og eksekvering af strategi. Det teknologiske frembrud skaber i dag stadig udfordringer i forhold til styring, vurdering, standardisering og overvågning af resultater og risiko, da bæredygtige kontrolfokuserede funktioner ikke er blevet etableret ved implementeringen af disse systemer.

Tilgangen til IR har været let forandret i 20 år, hvilket kræver en ny metodologi

Tilgangen og metodologien til intern revision har de seneste 20 år oplevet en inkrementel udvikling, der har hjulpet funktionen til at gøre de samme ting hurtigere og skabe mere fokus på risiko. Professionens formål har dog ikke udviklet sig radikalt, da den grundlæggende tilgang og metodologi er forblevet mere eller mindre uforandret. Behovet for opbrud i IR-professionen har aldrig været større end nu, og IR bør tage en aktiv rolle i teknologiens frembrud og udnytte nye muligheder til fortsat at kunne levere rådgivning til ledelse og fremadrettede indsigter samt bidrage til skabelsen af tillid i organisationer.

Samtidig skal IR rådgive i forhold til skabelsen af en korrekt risikoprofil, der bidrager til opnåelsen af langsigtede strategiske mål.

Konvergerende kræfter vil udfordre effektiviteten og relevansen af IR, herunder:

- ▶ Tempoet i forandring
- ▶ Banebrydende teknologier
- ▶ Forskellige forretningsmodeller
- ▶ Arbejdsstyrkens skiftende struktur
- ▶ Stigende lovkrav
- ▶ Globalisering

Fremtidens interne revision

I lyset af teknologiens opbrud og dets forretningsmæssige følger bør IR som profession genoverveje intern revisions formål, hvorledes IR udføres, og hvilke personer der er rigtige for opgaven.

Mandatet vil forblive intakt, men der vil være et skift i IR-funktionens rolle og fokus, hvor-IR funktionen bør:

- Være fleksibel, proaktiv, stærkt forbundet med virksomheden og se fremadrettet
- Fortsat vurdere og udfordre effektiviteten af interne kontroller
- Være en strategisk samarbejdspartner
- Udnytte nye teknologier til at skabe bedre og mere forudsigende indsigter
- Udfordre risikorammen og se ud over downside-risici og inkludere upside- og outside-risici.

IR er unikt positioneret til at bidrage med meget mere

- ▶ Hvad hvis IR var foran nye risici og var i stand til at vurdere og kvantificere dem hurtigt, så virksomheder kunne konvertere disse risici til muligheder?
- ▶ Hvad hvis IR ikke længere testede, om finansielle og lovmæssige krav var overholdt, men i stedet styrede en række online dashboards til at registrere fejl?
- ▶ Hvad hvis IR kunne supportere virksomheder med et real-time view af status på risikostyring i alle forretningsområder?
- ▶ Hvad hvis IR havde en fleksibel talent-model, der gjorde det muligt at ringe efter de rigtige ressourcer og kompetencer på det rette tidspunkt?

Downside-risici indbefatter potentielle negative hændelser, som organisationen bør beskytte sig imod.

Upside-risici relateres direkte til organisationens evne til at eksekvere strategi og opnåelse af målsætninger, hvilket er roden til at skabe nye muligheder og vækst.

Outside-risici omfatter hændelser uden for virksomhedens kontrol og rammer, der både kan have en positiv og negativ indflydelse på organisationen.

Historisk har organisationer og IR-funktioner primært fokuseret på downside-risici, men bør fokusere på alle tre kategorier i fremtiden. IR bør bryde ud af de vanterammer, udvide sit mandat og proaktivt indvirke på virksomhedsforandringer og analysere betydningen for virksomhedens risikoprofil. Hvis IR's rolle skal være at supportere virksomheder i real-time i forhold til risikostyring og være foran og rådgive i forhold til nye risici, bør IR tidligt tage en aktiv rolle i udviklingen af nye systemer, processer og produkter for at bidrage med rettidig rådgivning i forhold til kontrol design og fortsat at kunne hjælpe ledelsen med at øge effektiviteten både under og efter implementeringen.

Til trods for niveauet af opbrud i forretningsbilledet behøver IR's rolle i forhold til at levere assurance, forretningsindsigt og strategisk rådgivning ikke at forandre sig. Dog skal formålet med IR være mere fleksibelt. Assurance bør

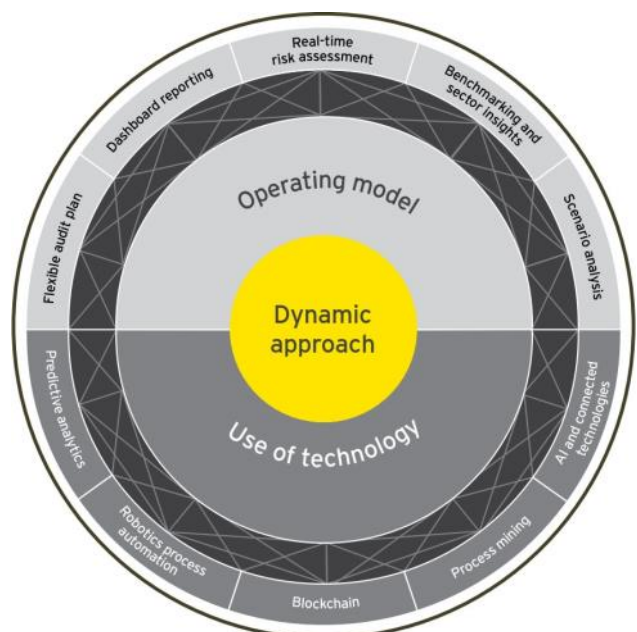
være mere omfattende end blot en vurdering af, om finansielle og lovmæssige krav er overholdt.

Dette giver IR-funktionen mulighed for at levere mere værdiskabende rådgivning. IR skal aktivt samarbejde med ledelsen og medvirke til forståelsen af alle organisationens risici og validere, om risici er identificeret, håndteret og afdækket korrekt af forretningen.

En ny operationsmodel bør forandre IR-professionen

De teknologiske megatrends (RPA, AI, Machine Learning m.v.) bør udnyttes i fremtidens IR-funktion i en fleksibel og dynamisk operations-model. I fremtiden bør IR kunne reagere på et udviklende risikobillede. Dette vil skabe en dynamisk rapporteringsmodel i real-time, der leverer indsigt og feedback baseret på forskellige stakeholderes interesser. Organisationer skal i samarbejde med IR implementere nye teknologiske megatrends, der løbende kan kontrollere interne kontroller, identificere risici og vurdere mængden af risici, som organisationer har pålagt sig. Operations-modellen bør omfatte følgende karakteristika:

Fleksibilitet – Den nye tilgang kræver en hurtig og fleksibel plan, der tager et skiftende forretningsbillede i betragtning og er i overensstemmelse med organisationens strategiske retning og prioriteter. IR bør i samarbejde med organisationen identificere nye risici for at levere rettidig indsigt og rådgive i forhold til, hvorledes disse risici kan håndteres.



Er IR klar til at reagere på ændringer i en organisations risikoprofil, digitalisere dens tilgang og levere mere fremadrettet indsigt og strategisk rådgivning?

Proaktivitet – IR bør ikke længere fokusere på hændte begivenheder, men i stedet overdrage testning og validering af virksomhedens kontrolmiljø til første og anden forsvarslinje. Denne overdragelse kan bl.a. muliggøres ved implementeringen af GRC-systemer, som løbende hjælper med at overvåge interne adgangs-, proces- og lovgivningsmæssige kontroller.

GRC-systemer kan hjælpe organisationer til at bevæge sig væk fra de traditionelle assurance-aktiviteter, så IR i stedet kan fokusere på at vurdere tilstrækkeligheden af det udførte arbejde, governance, proces- og kontroldesign og derved levere den bedst mulige assurance for stakeholdere.

IR skal yde rådgivning, der bidrager til virksomhedens forståelse og evaluering af nye og eksisterende risici for derved at hjælpe ledelsen med skabe kort- og langsigtede handlingsplaner, der proaktivt adresserer risiko.

Indsigtsfuldhed – Den tidligere operationsmodel har ofte rapporteret, hvad virksomheder allerede vidste, grundet måden assurance er blevet udført på. IR skal gå trinnet længere og forstå, hvad der faktisk foregår i organisationen, og fokusere på værdifuld viden for ledelsen, inklusive industriindsigt, benchmarking, adfærdsmæssige analyser m.v.

Digitaliseringen skal skabe fundamentet for denne transformation, så den interne revision ikke længere bruger tid på at opdage og påvise mangler, men direkte analyserer eventuelle mangler identificeret af f.eks. GRC og rådgiver organisationen i eventuelle problemstillinger.

Den nye arbejdsstyrke

Den digitale revolution vil skabe et opbrud i de nuværende arbejdsgange, og ordsproget "vores medarbejdere er vores største aktiv" kan blive forkert. Nye teknologier kræver nye kompetencer og arbejdsgange, hvorfor oplæring af nuværende medarbejdere og en statisk diversificeret arbejdsstyrke ikke længere er nok.

IR har behov for en fleksibel arbejdsstyrke, hvor kompetencefordelingen er fleksibel. Denne arbejdsstyrke-portefølje skal indeholde kernerevisionspersonalet, gæsterevi-

sorer, freelancere, underleverandører og en kontinuerlig personalerotation, der sikrer en fleksibel balancering af kompetencer, der bedre kan imødekomme opbrud på markedet. Den nye arbejdsstyrkeportefølje muliggør, at IR målbevidst kan fokusere på værdiskabende initiativer, men skaber samtidig behovet for et mere fleksibelt, adaptivt samarbejds-orienteret arbejdsmiljø.

Konklusion

En nytænkende IR-funktion kan skabe stor værdi for virksomheder gennem en digitaliseringsrejse, der bør starte i dag. IR-professionen bør skride til handling og skabe fundamentet for, hvorledes fremtiden skal formes. Dette fundament skal definere den interne revisions fremtidige formål i overensstemmelse med organisationens strategiske mål. Dette kræver en beslutning om, hvorledes nye megatrends kan integreres i IR-professionen, og hvordan det ændrer formålet. IR skal ikke længere fokusere på validering og testning af kontroller, men udvide perspektivet og blive en værdifuld strategisk samarbejdspartner for virksomheder og være en integreret del af it-implementeringer med fokus på en proaktiv tilgang til risikohåndtering.

IR bør handle for at imødekomme sine fremtidige ambitioner. Der skal bygges en business case, der demonstrerer intern revisions egenskaber og udviklende rolle med digitalisering for at fange stakeholderes opmærksomhed.

Effektiviteten skal forøges i vurdering af finansielle og lovmæssige krav, så ressourcer kan frigøres for i stedet at fokusere på strategisk risiko og funktionens fremtidige stadie. Teknologien skal derfor videreudvikles og udnyttes til det fulde potentiale i en transformeringsproces, hvor IR-funktionen fortsat kan følge virksomhedens forandringer i vision og målsætninger.



IIA Årsmøde 2019

**Afholdes
15.5.2019-16.5.2019**

**på Hotel Crown Plaza
København**

**Sæt allerede nu kryds
i kalenderen**

Det er både hvad vi skriver, og hvordan vi skriver det

“When recommendations go unaddressed” er titlen på en artikel, som vi genoptrykker fra *Internal Auditor*, december 2017. Artiklen giver forskellige eksempler på, hvad der ofte går galt, når revisor i sin skriftlige kommunikation overfor ledelsen i virksomheden skal kommunikere sit budskab om behov for at implementere kontroller m.m., der kan mitigere risici. Et af budskaberne i artiklen er, at intern revision, for at finde løsningen herpå, først skal forstå, hvorfor anbefalinger ikke bliver implementeret. Vi følger denne problemstilling i artiklen “Hvordan opnår revisor den ønskede effekt med sin rapportering”, hvor der i et handlings- og løsningsorienteret perspektiv sættes fokus på behovet for at forstå modtagernes perspektiv og informationsbehov, samt giver eksempler på og forslag til at forbedre den skriftlige kommunikation.



When recommendations go unaddressed

Article by Jane Seago. Jane Seago is a business and technical writer in Tulsa, Okla.

This article was reprinted with permission from the December 2017 issue of *Internal Auditor*, published by The Institute of Internal Auditors, Inc., www.theiia.org.

The situation: An internal auditor makes a series of recommendations to an internal audit client, who refuses to implement one of the recommendations or address the finding.

The internal auditor's view: The recommendation covers an important point. Her supervisor agrees that the risk of not implementing the corrective action or addressing it would be significant for the organization.

The client's perspective: He concurs with the finding, but believes the corrective action would take too much time and use too many resources.

The outcome: After several unsuccessful attempts to persuade the client of the validity of the recommendation, the issue is elevated to the CEO. Lacking resolution with that step, the recommendation is sent to the audit committee. The internal auditor and her chief audit executive (CAE) attend the audit committee meeting to discuss the recommendation, gaining support from the committee and the chief financial officer. The issue is resolved (ideally, the client attends the audit committee meeting and hears the committee's decision directly, but if that is not possible, the audit committee minutes can be used to inform the client) and a cordial working relationship continues.

Although the details of this scenario may vary, it likely describes a situation that is all too familiar to most internal auditors. The recommendations the internal auditor presents may not always be welcomed or feasible, but making those recommendations is integral to internal audit's role. That role, as Michael Levy, director of in-



ternal audit at Student Transportation Inc. in Wall, N.J., describes it, is “to spotlight issues and ensure that the appropriate people are aware and informed.”

But raising awareness and sharing information do not always produce the needed results. An audit client may decline to implement even the most well-researched and clearly explained recommendation, leaving risks that may affect the organization’s ability to achieve objectives unmitigated. When this happens, Standard 2600: Communicating the Acceptance of the Risk directs the CAE to discuss the matter with senior management or elevate the issue to the board, if necessary.

What’s Behind the “No”?

As with many instances, when two parties fail to see eye to eye, inadequate or flawed communication may be to blame. In the case of unaddressed recommendations, perhaps the internal auditors did not fully explain the value of a recommendation, or they did not adequately define what “recommendation” means within the organization’s culture, or they did not describe the potential consequences of failure to implement the recommendation.



Executive management and the board are no longer looking for the ‘novel’ version of reports.

Michael Levy

Or, perhaps it is not a case of inadequate communication, but too much of it. “Many times, auditors tend to include every detail of the audit in the report,” Levy says. “I find that executive management and the board are no longer looking for the ‘novel’ version of reports that has become common over the years.” Internal auditors must focus on creating well-organized reports that stick to the point, covering what the reader needs to know, not everything the auditor knows. Each recommendation should be supported by a full description of the related risk, which will help establish the importance of the recommendation and the potential implications if it is left unaddressed.

Kevin Alvero, senior vice president of internal audit at Nielsen in Tampa, Fla., recommends using a categorization approach to clarify communication with the client. “If you clearly categorize recommendations based on risk (high, medium, low), you greatly reduce the chances that the most important ones will go unaddressed,” he explains. “I think that is very intuitive to people: They understand that if they don’t address the high-priority re-

commendations, there is a risk of that issue going forward.” In an annual audit process, recommendations that appear multiple times may move to a higher risk category — a signal to management about their importance relevant to risk.



If they don’t address the high-priority recommendations, there is a risk of that issue going forward.”

Kevin Alvero

At Principal Financial Group in Des Moines, Iowa, Cindy Bolton, audit director, reports that implementation of an enterprise risk management framework has encouraged communication around risk and risk metrics by the chief risk officer (CRO) and all the risk officers throughout the business. “We have a lot of discussion about risk and controls from the second and third lines of defense, as well,” she adds, “and a lot of time working in partnership with the second line, so the message to the first line is one continuous stream.”

Besides communication, another possible reason for nonimplementation relates to resources. The benefits to be derived from the recommendation may not justify its cost, in the eyes of the client. Or the drain on other, non-financial resources may be prohibitive (although, if the recommendations are focused on issues that exceed the organization’s established risk tolerance, this should justify adding resources). Auditors have a responsibility to understand the business well enough to be aware of the financial impact of the recommendations they are making. “Otherwise,” Alvero says, “they are not fully serving the needs of the client.”

When building an understanding of an issue that will be included in the audit report, internal auditors need to consider the cost, impact, and significance related to the issue. This enables the auditor to balance the high cost to remedy and the possible low impact and likelihood of misstatement the issue may potentially have. Although the internal auditor should definitely take the lead in these considerations, it should not be a solitary exercise. The client should play an active role.

Avoiding the cost-benefit objection can be as simple as discussing with the client the feasibility of various approaches and devising a management action plan in conjunction with management. When those discussions are held, the result “is not ‘internal audit recommends and management responds,’” Bolton says. “Management is already involved.”

If the cost of a recommendation is unknown, an approach might be to divide it into two parts: management researching the cost of possible solutions and internal audit determining whether these solutions adequately address the recommendation. This enables progress to be made, rather than hitting a brick wall of “no” the minute the cost is considered. Another workaround for expensive recommendations is for internal audit to make additional recommendations (such as extra reviews and quality reviews) to satisfy them.

“Developing recommendations is one of the areas where we, as a profession, have an opportunity to act as consultants and not only add value directly to the organization, but also to our stakeholders,” Levy notes. “Many times, when recommendations are developed in a vacuum, without management’s input, the desired outcome is not reached.”

Communication and resources are not the only roadblocks to implementing recommendations. Kevin Patton, director of internal audit at The Ohio State University in Columbus, points out that a client’s adoption of a recommendation may be affected by changes to existing information systems or implementation of new information systems, which often take longer than estimated. “System issues seem to take more time to resolve than other comments, such as financial and operational,” Patton explains. “In those cases, we ask the unit how they are mitigating the risk and get an understanding of their processes.” In some companies, moving to a new platform could make a recommendation obsolete, causing management to decide a short-term fix is not worth the cost. As with costly recommendations, the auditor should understand the business well enough to be aware of systems plans before making a related recommendation.

Other possible situations that may affect the client’s willingness or ability to implement a recommendation include a change in business strategy, loss of staff or changes in staffing, or competing priorities in the client’s area. Ongoing communication with clients is critical to internal audit’s effectiveness in such circumstances. It will help ensure that the internal auditor is informed on the client’s issues and can function as a partner in addressing them.

The Fine Art of Follow-up

IIA Standard 2500: Monitoring Progress states that the CAE “must establish and maintain a system to monitor the disposition of results communicated to management.” Item 2500.A1 speaks of the CAE’s responsibility to establish a follow-up process to monitor and ensure that management actions have been implemented or senior management has accepted the risk of not doing so. Item

2500.C1 specifies that it is internal audit’s responsibility to monitor (to the extent agreed with the client) the disposition of results of consulting engagements.

Whatever the reason for failure to implement internal audit recommendations, that failure has the potential to expose the organization to risk. Therefore, internal audit has a distinct role in monitoring whether management implements the controls it agreed to. While the size and nature of the risk will influence the type and amount of follow-up activity, *Following Up Recommendations/Management Actions*, a 2016 paper from the U.K.’s Chartered Institute of Internal Auditors, outlines general post-recommendation activities that need to be made clear to the client before the audit:

- How outstanding recommendations/management actions will be tracked.
- How resolutions will be reported and validated.
- What follow-up action might be needed.
- How this will be carried out to provide assurance that identified risks are being addressed appropriately.

Warren Hersh, auditor general at New Jersey Transit in Newark, says a robust follow-up process must begin with the establishment of the department’s verification philosophy, which generally will follow one of two approaches: 1) actually performing a follow-up audit, testing to verify that corrective actions have been implemented; or 2) accepting the representation of management on the status of corrective actions. In Hersh’s experience, following the first approach takes significant resources and focus. His current department uses the second approach, with one variation. “If we have an audit that has significant findings that impact the key risks faced by the department, in addition to reporting to the audit committee, we automatically schedule a follow-up audit either later in the audit plan year or in the next audit plan year.”



If we have an audit with significant findings ... we automatically schedule a follow-up audit.”

Warren Hersh

Hersh’s team uses audit management software to monitor the status of corrective actions, and that status is reported at every audit committee meeting because it gets the attention of senior management.



We accept their word it's done [when dealing with low-rated recommendations]."

Cindy Bolton

comments remain, Patton discusses those in detail with the audit and compliance committee.

But there is another possibility as well. Management may decide to accept the risk and not resolve the comments. These situations also are elevated to the audit and compliance committee for discussion. Patton notes, "Of course we hope it doesn't get to that point. And it rarely does for us."

Principal Financial Group's process for follow-up is similar to that of Ohio State, with progress checks quarterly. Bolton explains that recommendations are rated critical, high, moderate, and low. Anything moderate or higher receives additional testing to make sure it is implemented to internal audit's satisfaction. Low items are not tested as vigorously: "We accept their word it's done." A quarterly report on the percentage completed and the status of follow-up items is issued to senior management and the audit committee.

Understand the Reason

Alvero points out the need to determine the reason for nonimplementation. Did management make a business decision, choosing not to take the recommended action based on the risk to business objectives balanced against other factors, such as cost and resources? Or did management simply ignore the recommendation?

"Making a business decision not to implement a recommendation is not necessarily a red flag," he says. "It is not the same as ignoring a recommendation, which

obviously would be a concern." Investigation may be needed into the extent of the refusal to implement, because that is generally not a one-unit decision. In many companies, the business office, the CRO, the audit committee, and other individuals or groups, depending on organizational structure, would have to support the decision.

In some cases, limited resources within the internal audit department may affect follow-up efforts. In these cases, Hersh advises internal audit to prioritize the key risks and then focus on implementation of corrective actions for the more significant risks. He considers this necessary when assessing whether management has inappropriately accepted a risk, in internal audit's opinion, by not implementing corrective actions.

Working Toward One Goal

Ultimately, as with so many business transactions, *what* is being done is often secondary to *how* it is being done. For its recommendations to carry weight and earn full consideration, internal audit must act as a trusted advisor to the business, establishing and demonstrating a mindset of cooperation and collaboration, not an adversarial relationship. As Bolton puts it, "We have different units, different priorities, different purposes, but ultimately we are one company. We are all working together, trying to do the right thing."



Hvordan opnår revisor den ønskede effekt med sin rapportering?



Michael Ravbjerg Lundgaard,
Revisionschef, DSB

Indledning

I dette nummer af INFO har vi gengivet en artikel fra Internal Auditor, med overskriften "When recommendations go unaddressed". I tilknytning hertil vil vi med nærværende artikel sætte fokus på nogle af de årsager, der kan være til, at såvel revisors anbefalinger, som mange timers hårde arbejde med at udarbejde revisionsrapporter og management letters m.m., ikke altid gengældes med ejerskab og prioritering fra ledelsens side.

Indledningsvist kan vi se på den forskellighed der ligger i, hvordan interne revisorer fremstiller de forhold, der vurderes at være behov for at mitigere risici for. Der ligger ikke en empirisk undersøgelse bag dette, men blot mine erfaringer fra eget mangeårigt virke som ekstern og intern revisor, samt drøftelser jeg har haft med andre i forskellige netværk. Hermed også sagt, at der i praksis sagtens kan være andre måder end de nedenfor anførte.

Facilitering af løsninger

Den helt traditionelle model, som fremgår af lærebøger og IIA's politikker og procedurer, baserer sig på de 5 C'er: Condition, Criteria, Cause, Consequence og Corrective action. Dette bliver ofte samlet i et rapportformat, hvor vi beskriver Observationen, Risikoen og dernæst Intern revisors Anbefaling til mitigering af risikoen. Ofte beder vi ledelsens besvare dette, ved at kvittere for, at de vil efterkomme anbefalingen og hvad deadline er for implementering heraf, hvis ikke vi selv har anført den.

En variant heraf er, at producere rapporten uden at give Anbefaling til løsningen. Rationalet skulle, som jeg har fået det oplyst, være, at revisor mener at deres uafhængighed bliver kompromitteret, hvis det er revisor der kommer med løsningen. En løsning som de (muligvis) efterfølgende selv skal revidere. Jeg vil ikke gå længere ind i den problemstilling, blot konstatere, at vi som revisorer har forskellige holdninger hertil.

I min revisionsafdeling implementerede vi for nogle år siden en lidt anderledes variant, som er inspireret af tankesættet omkring Trusted advisor. Vi udarbejder såvel Observationer som anfører vores vurdering af Risiciene, der knytter sig hertil. Herefter går vi i dialog med ledelsen, og starter en proces, hvor vi faciliterer, at de parter, der har "aktier" i problemet og problemets løsning, bliver sat sammen og drøfter observationens indhold og risici. Sammen med intern revision drøftes forskellige løsnings tiltag, og der udtænkes sammen med parterne en aktionsplan, indeholdende deadlines. Revisors rolle er her primært at være sparringspartner og sikre, at relevante risici adresseres i løsningen.

Fremgangsmåden koster lidt mere tid af Intern revision, men til gengæld opnår vi nogle løsninger, som har opbakning hos dem der ejer problemet. Problemet bliver anskuet med såvel revisors som kundens perspektiv, ligesom alle led i kæden er blevet involveret, og dermed har opnået vished om problemets omfang og effekt på de enkelte ansvarsområder.

Klarhed i budskabet

Når vi arbejder med de 5 C'er, så har vi en skabelon for, hvordan vi skal strukturere vores beskrivelse af forholdet. Det ses imidlertid ofte, at vores (manglende) evne til at formulere os i tekst, spænder ben for, at kunden forstår og modtager budskabet. Det er min erfaring, at i såvel revisionsrapporter som i de skemaer, der anvendes til beskrivelse af Observation og Risiko, har revisor for vane, at fylde spalteplassen ud med velmente men voluminøse beskrivelser og sprogligt uklart formulerede sætninger. Ledelsen ser ikke den store værdi i, at revisor fortæller hvor mange stikprøver de har taget, hvordan de har udvalgt dem, hvad revisor oplevede af udfordringer på sin vej, hvad man historisk set har af erfaringer, eller beskrivelser af, hvem der gør hvad og hvorfor i organisationen. Ledelsen vil ofte efterspørge en kort, præcis og klar formulering af fakta indeholdende:

- Kort og præcis beskrivelse af forholdet
- Forholdets vigtighed
- Årsagsbeskrivelse
- Risiko for virksomheden
- Hvornår og om forholdet bliver løst.

Den korte beskrivelse af forholdet indleder emnet og leder læseren videre, hvad han skal forvente af resten af beskrivelsen af forholdet. Den første sætning skal fungere som en avisoverskrift, der pirrer din interesse for at læse videre.

Sarah Swanson¹, forfatter og kursusinstruktør, skriver i artiklen "Three editing tips to keep up the sentence flow mojo", om en metode til at formulere den gode emnesætning. Prøv at tage en af de sætninger du har formuleret og foretag så nedenstående "saneringsøvelse":

- Identificer hvad der er evidens for. Hvis der er meget evidens, så indkreds det til det mest evidente
- Identificer risikoen eller årsagen
- Kombiner evidens og risiko/årsag I en sætning
 - √ [Årsagen] førte til [evidens]
 - √ [Evidens eller konklusionen] har medført [implikation/risiko].

Et eksempel på en indledende beskrivelse, som er meget præcis, men ikke adresserer årsag og/eller risiko kunne være: "I perioden januar – september, har lederen af X afholdt rejseomkostninger for XX tkr, for både sig selv og sit team".

Beskrivelsen af forholdet kunne i stedet beskrives som: "Uklare guidelines for afholdelse af rejseomkostninger har medført et u hensigtsmæssigt stort forbrug".

Sætningen her adresserer i første led årsagen, og i næste led forholdets implikation/risiko.

Udover den indledende emnesætning, skal hver del af observations- og risikobeskrivelsen, være kort og relevant beskrevet. For at sikre dette, anbefaler Sarah Swanson², at hver sætning indeholder et af følgende elementer, ellers er der alt andet lige tale om fyld:

Baggrund, Evidens, Konklusion, Årsag eller Risiko.

Forstå kundens perspektiv

Selvom revisor gør sig umage med at levere budskaberne klart og tydeligt, så er der fortsat risiko for, at ledelsen ikke prioriterer implementeringen af en løsning. Det handler blandt andet om, at arbejde med multiverse perspektiver og revisors evne til, og fokus på, at forstå forretningen og den kontekst de ser observationen/problem-et i.

I den systemiske organisationsteori anvendes begrebet det multiverse perspektiv, hvor man arbejder med anerkendelsen af, at et forhold er forskelligt, afhængigt af,

hvilket perspektiv man ser det fra. Ud fra et systemisk perspektiv handler kommunikation om at skabe og medskabe koordinerede virkelighedsforståelser. Disse teorier kan med fordel anvendes af revisor, når han skal forstå ledelsens syn på de observationer, som revisor har vurderet væsentlige. At anerkende, at en sag kan ses fra mere end én side, er første led i, at revisor bruger sin spørgeteknik til at forstå, hvordan ledelsen ser på forholdet. I hvilken kontekst ser de forholdet, har de en viden herom, som revisor med fordel kunne tage med i sin risikobetragtning, hvordan ser de på implikationen af forholdet, herunder hvor ressourcekrævende det vil være at udbedre forholdet?

Hvis man forstår kundens perspektiv, og signalerer at man interesserer sig herfor, er der alt andet lige bedre mulighed for, at revisor også kan skabe forståelse hos ledelsen for de risici, som revisor kan fremhæve, konteksten taget i betragtning. Det kan være med til at skabe buy-in hos ledelsen, og de kan bedre se, hvad de får ud af at implementere løsningen. Revisor faciliterer derved, at man i fællesskab kommer bagom problemet, forstår flere perspektiver på problemstillingen, og kan vurdere hvilke løsninger og ressourceindsats problemets løsning berettiger til.

I artiklen fra Internal Auditor fremhæves det tillige, at løsninger, der er afhængige af it-systemudvikling, ofte kræver længere implementeringstid end forventet, hvilket kan medføre at Observationer udestår som uløste. Hvis revisor i sin dialog med kunden om løsningerne sikrer, at der er opmærksomhed herpå, er realistisk omkring den reelle implementeringsperiode og spørger ind til planlagte systemændringer m.m., så er forudsætningerne for at fastsætte realistiske deadlines bedre til stede. Revisor bør i den sammenhæng sikre, at det med ledelsen drøftes og aftales, hvilke kompenserende kontroller der kan udføres, inden den endelige løsning er på plads.

Revisors ajourførte viden om virksomheden

Som Intern revisor kan det være en udfordring at holde sig ajour med, hvad der sker i virksomheden på såvel operationelt niveau, ledelses niveau, som det mere strategiske niveau. Revisor kan med fordel dyrke sit netværk internt i virksomheden og holde kontakt til de forskellige organisationslag, hvilket kan være nøglen til, at have en løbende kommunikation og opnå indsigt i virksomhedens forhold. Hvad er i fokus, hvad er udfordringerne, hvad er strategien og ikke mindst løbende ændringer eller tilpasninger til strategiens aktiviteter? En sådan opsøgende proaktiv informationsindsamling giver revisor en bedre platform for at fungere som Trusted advisor eller business partner, og i forhold til i revisionsplanen at kunne adres-

¹ Sarah Swanson: Misti Training Institute, Audit writers hub: Three editing tips to keep up the sentence flow mojo

² Sarah Swanson: Misti Training Institute, Audit writers hub: 6 strategies that streamline audit issue writing

sere ledelsens udfordringer i tilrettelæggelsen af de enkelte revisioner.

Det er vigtigt, at den ajourførte viden og forretningsforståelse ikke blot anvendes i den overordnede planlægning, men tillige adresseres i udførelsen af de enkelte revisioner. Her har ledelsen af den interne revision en opgave i at sikre, at viden overdrages til hele intern revision, og revisorerne formår at bruge oplysningerne i deres tilrettelæggelse, og praktiserer i henhold hertil ved udførelsen af revisionen. Der skal være sammenhæng i mellem det, den interne revision praktiserer, og det ledelsen af den interne revision signalerer.

I den virksomhed jeg arbejder i, har vi de seneste år praktiseret at afholde 1-2 årlige møder med en række chefer, underdirektører og direktører for at drøfte, hvad der aktuelt er fokus på, hvilke aktiviteter der forventes igangsat i henhold til strategien, og hvorvidt den pågældende leder ser nogle forhold i eget eller andres områder, som Intern revision med fordel kunne interessere sig for. Møderne giver os input til vores revisionsplan, herunder om der løbende er behov for at ændre og omprioritere i den løbende plan. Udover at vi løbende holder kontakt med flere lag i organisationen, og ajourfører vores viden, så giver mødet og dialogen os en mulighed for at opbygge og fastholde en relation og et syn på Intern revision som Trusted advisors, der kan hjælpe virksomheden.

Løsningsorienteret opfølgning

Når en Anbefaling/løsning ikke implementeres til tiden, så rapporteres dette typisk til revisionsudvalget og ledelsen. I et forsøg på, at udvise "forståelse" for virksomhedens udfordringer, så har jeg ofte accepteret, at en deadline

udsættes. Når dette sker forholdsvis kort tid efter, at revisionsrapporten blev udarbejdet, giver det naturligvis anledning til at reflektere over, om vi var gode nok til at udfordre ledelsen på, om den aftalte deadline var realistisk og bl.a. tog højde for planlagte systemændringer/nødvendige systemtilpasninger. Især med Anbefalinger/løsninger, som har en længere horisont til deadline, er det erfaringen, at forholdene kan ændre sig betydeligt, hvilket kan betinge en anden løsning, eller at ledelsen vurderer, at de under de aktuelle omstændigheder vil acceptere risikoen.

I sådanne tilfælde må man som revisor forsøge at forstå ledelsens bevæggrunde herfor, herunder om rette beslutningstager har været involveret. Hvis revisor efter en vurdering heraf finder, at der grund til at være uenig med ledelsen i deres vurdering af risicienes væsentlighed, er der mulighed for, at eskalere forholdet til revisionsudvalget. I min optik må det generelt betragtes som en sidste udvej, da det alt andet lige ikke virker befordrende for samarbejdet mellem revisor og ledelse, herunder revisors arbejde med at fungere som Trusted advisor/business partner.

Revisors revisionsrapporter og observationer vinder alt andet lige større gehør, hvis vores adfærd afspejler vores ønske om at være Trusted advisors, og vi etablerer og demonstrerer et mindset, der signalerer samarbejde og fælles forståelse for virksomhedens risici og målsætninger. Dette bør vi kombinere med, at vi i vores kommunikation gør os selv og vores kunde/ledelsen helt klart hvad budskabet i rapporteringen skal være, holder os til pointen, sætter os i modtagerens sted og forstår deres informationsbehov.





Drive Your Career Forward

IIA Certifications and Qualifications

An IIA Professional Credential can move your career in the right direction, whether you're just starting down the audit path or taking your career to new heights. Drive to new opportunity, with increased earning potential, deeper knowledge, and enhanced credibility.

Invest In Your Tomorrow, Today.
www.TheIIA.org/Certification

 **The Institute of
Internal Auditors** | *Global*

141731

Vejledning om alternative investeringer og prudent person



Ane Præstekjær, Senior Manager, Ernst & Young P/S

Indledning

Den 27. juni 2018 udstedte Finanstilsynet "Vejledning om alternative investeringer og gode investeringsprocesser i lyset af prudent person-princippet".

Vi har i branchen talt om prudent person i en længere årrække. Først frem imod selve lovimplementeringen af Solvens II-reglerne pr. 1. januar 2016, hvor prudent person-begrebet var helt nyt, og herefter i diverse fora og

erfa-grupper på alle niveauer i selskaberne for at dekomponere begrebet og arbejde med det i praksis. Siden er implementeringen påbegyndt med forskellig hastighed i selskaberne.

Finanstilsynet udstedte vejledningen som deres udtryk for, at forankringen og implementeringen af prudent person i investeringsprocesserne ikke havde haft det ønskede omfang eller kvalitet.

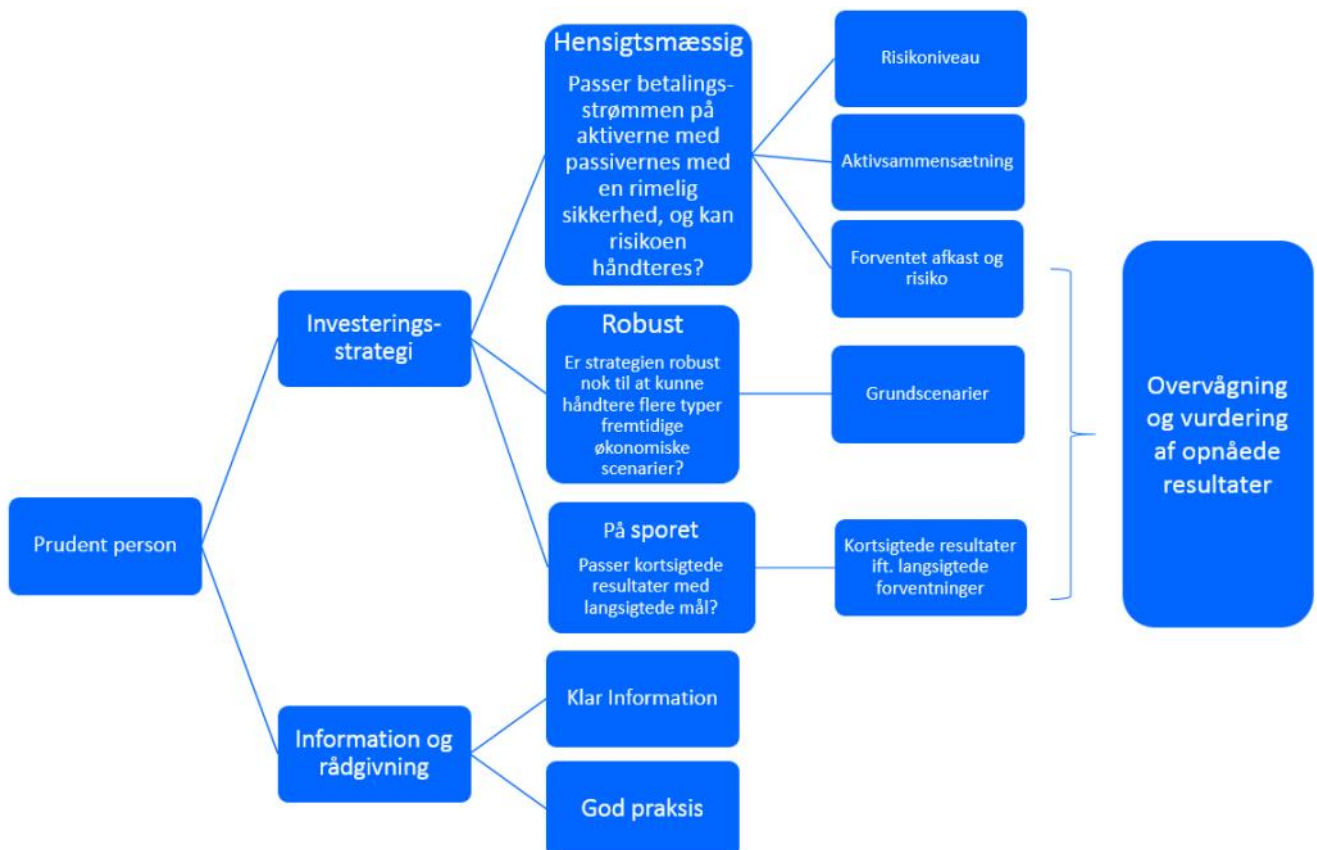
Nærværende artikel indeholder en overordnet gennemgang af vejledningen og begrebet prudent person i forhold til investeringsprocessen samt min vurdering af, hvordan den kan inddrages i den interne revision.

Hvem gælder vejledningen for?

Vejledningen er som udgangspunkt målrettet livsforsikringselskaber og tværgående pensionskasser.

Det kan imidlertid også forventes at Finanstilsynet vil forvente, at ledelser i skadesforsikringselskaber der også investerer i alternative investeringsaktiver tillige forholder sig til vejledningens retningslinjer for processer og det interne kontrolsystem.

Figur 1: Prudent person begrebet



Vejledningen gælder alle investeringsaktiver – uanset om det er investeringsaktiver knyttet til forsikringstagernes interesser (de forsikringsmæssige hensættelser, både markedsrente og gennemsnitsrente) eller i forhold til selskabernes egne midler (egenkapitalens investeringer).

Hvad betyder prudent person?

Prudent person-princippet tager afsæt i, at et selskab skal "opføre sig ordentligt" i forhold til håndteringen og forvaltningen af sine investeringer.

Figur 1 på forrige side illustrerer prudent person-begrebet i sin helhed.

Vejledningen er målrettet mod de dele, der vedrører investeringsstrategien, i forhold til de alternative investeringer.

Et selskab må kun investere i aktiver, der har en risiko-profil, som selskabet kan *forstå* og *håndtere*. Sammen-sætningen af aktiverne skal have sammenhæng til arten og varigheden af selskabernes forsikringsforpligtelser.

Kriterierne for at opfylde prudent person-princippet i investeringsprocessen bliver ofte forkortet PPP-kriterierne. PPP-kriterierne er, at selskabet skal kunne:

- Identificere risici
- Måle risici
- Overvåge risici
- Forvalte risici
- Kontrollere risici, og
- Rapportere om risiciene til (ultimativt) bestyrelsen.

Tabel 1: PPP kriterierne

PPP-kriterierne	Nøgleord
Identificere risici	Både i processen før investeringsbeslutningen – Hvilke typer risici påvirker investeringen; eksempelvis geografiske, skattemæssige, regulatoriske, politisk risici Og i processen efter investeringsbeslutningen – Følge hvilke potentielle risici der er eller kan opstå, eksempelvis overvågning af ny lovgivning både i Danmark og udlandet, og vurdere eventuelle nye risici afledt heraf
Måle risici	I processen før investeringsbeslutningen – Fastsættelse af et afkastkrav med en dekomponeret risikopræmie, der skal afspejle investerings risici Og i processen efter investeringsbeslutningen – At grundlaget for værdiansættelsen er korrekt og i overensstemmelse med de risici, der er identificeret
Overvåge risici	I processen efter investeringsbeslutningen – Følge udviklingen i de risici, der er identificeret – Forventet i forhold til realiseret afkastkrav til brug for risikostyringen
Forvalte risici	Både i processen før investeringsbeslutningen – At identificere de handlemuligheder, selskabet ønsker at have, i tilfældet af at forudsætninger ændrer sig. Ultimativt: hvordan kan selskabet komme ud af investeringen. Dette kan være en særlig udfordring jo mindre en investor man er. – At sikre, at selskabet ved aftaleindgåelsen har de ønskede handlemuligheder Og i processen efter investeringsbeslutningen – At handle, såfremt målings- og overvågningsaktiviteter giver anledning hertil
Kontrollere risici	Der skal implementeres interne kontroller inden for alle områderne (identifikation, måling, overvågning, forvaltning og rapportering). Der stilles dermed krav til funktionsadskillelse, og risikostyringsfunktionen forventes at have en aktiv rolle i alle faser.
Rapportere om risici	Bestyrelsen skal give klare retningslinjer for krav til rapportering om udviklingen i risiciene knyttet til de alternative investeringer, herunder hvilke parametre og informationer, der ønskes rapportering om. Tilsvarende for de øvrige ledelseslag, i form af eksempelvis investeringskomitéen, risikokomitéen og direktionen. Der skal implementeres procedurer der sikrer, at rapporteringen sker rettidigt og på alle ønskede parametre.

Hvad er forskellen fra den tidligere lovgivning og prudent person ?

Hvad angår **typen og omfanget** af investeringsaktiver omfattede de tidligere investeringsregler specifikke krav til bl.a. spredning og kongruens. Prudent person-princippet indeholder ikke sådanne krav og synes umiddelbart at give friere rammer for hvilke investeringer, selskabet kan foretage.

Disse friere rammer skal imidlertid ses i sammenhæng med de øgede krav til politikker og processer.

Hvad angår **politikker og processer** var de grundlæggende forudsætninger i den eksisterende lovgivning, at:

- Selskabernes direktion og bestyrelse skulle være fit-and-proper i forhold til at have tilstrækkelig viden, faglig kompetence og erfaring til at kunne udøve sit hverv eller varetage sin stilling, jf. Lov om finansiel virksomhed
- Selskaberne skulle have politikker i overensstemmelse med selskabets risikoprofil, og forsvarlige processer og interne kontroller på investeringsområdet til at afdække alle væsentlige risici, jf. Lov om finansiel virksomhed uddybet i Ledelsesbekendtgørelsen fra 2010.

Med prudent person-princippet er kravene til investeringsområdets processer og interne kontroller blevet meget mere konkrete, bl.a. afspejlet i PPP-kriterierne, der blev indarbejdet i dansk lovgivning via opdateringen af Ledelsesbekendtgørelsen i december 2015.

Et nærmere blik på PPP-kriterierne

PPP-kriterierne skal indarbejdes i selskabets investeringsprocesser, og i **Tabel 1** på forrige side er PPP-kriterierne præsenteret.

Der er i vejledningen vist et eksempel på, hvordan Finanstilsynet opfatter udgangspunktet for en struktureret proces for håndteringen af alternative investeringer, og hvordan PPP-kriterierne skal indarbejdes (Se **Figur 2** nederst på siden for en gengivelse af figur 1 i vejledningen - Figurens tekst er gengivet i **Tabel 2** på næste side).

En særskilt vinkel på efterlevelse af PPP-kriterierne er, når selskaber investerer via eksterne mandater, eksempelvis i private equity-fonde med eksterne fund managers.

Grundlæggende er kravet det samme: Samtlige PPP-kriterier er relevante, og selskabet skal etablere egne

Figur 2: Gengivelse af vejledningens figur 1



Tabel 2: Figur 2 i tabelformat

Fase 0 Før investering	Fase 1A Initialvurdering	Fase 1B Intern analyse	Fase 1c Due diligence	Fase 2 Investeringsbeslutning	Fase 3 Efter investering
Før investeringsmuligheden modtages/opsøges	Første screening af investeringen	Dybdegående intern analyse af investeringen	Fyldestgående analyse af investeringen	Samlet investeringsbedømmelse	Efterfølgende asset management
Interne styringsdokumenter udarbejdes	Initial vurdering af afkast vs risiko	Identifikation og måling af risici	Yderligere identifikation og måling af risici	Beslutning træffes (skal/skal ikke)	Dvs. løbende overvågning, kontrol, forvaltning m.m.
Forretningsgange, retningslinjer, processer m.v.	Kilder: fra det kapitalsøgende selskab	Kilder: eksterne (offentlige tilgængelige oplysninger)	Kilder: rådgivere og eksperter	Kilder: sammenfatning af alle kilder	Kilder: eksterne oplysninger+oplysninger fra selskabet

processer og have kendskab til samt overvåge, at den eksterne fund manager efterlever PPP-kriterierne. Dette analogt med, at ansvar ikke kan outsources.

Der er i al væsentlighed næppe nogen overraskelser i de beskrevne processer, heller ikke i at selskaberne skal følge op på eksterne fund managers. Selskaberne har også før PPP-kriterierne arbejdet med risici og interne kontroller. Det nye er de specifikke krav.

Et væsentligt spørgsmål mange selskaber stiller er derfor, hvornår "nok er nok", dels i selve processerne dels i dokumentationskravet. Overvejelser omkring dette er eksempelvis:

- Hvordan kan en organisation helt konkret dokumentere, om kendskabet til risici knyttet til en given investering er tilstrækkeligt dybt
- Hvor mange personer/specialister skal inddrages i risikovurderingen af en investering, dels in-house dels fra eksterne parter
- Hvornår er der foretaget en tilstrækkelig due diligence af en ekstern investment fund manager
 - Vurdering af omdømme i branchen
 - Realiserede ift. forventede afkast (kan være information, der ikke er offentlig tilgængelig)
- Hvor meget rapportering skal forlanges fra en ekstern investment fund manager
 - Hvilken grad af look through i fondene; henholdsvis på akkumuleret niveau og per enkeltinvestering? Der kan særligt i udenlandske fonde være begrænsninger på, hvilke informationer der ønskes givet, fordi de danske selskaber ofte er små investorer sammenlignet med de øvrige.

- Hvilken detaljeringsgrad af oplysninger er nødvendig om interne kontroller i fondene?
- Hvor ofte skal selskabet modtage rapportering fra fondene?

Udviklingen i praksis vil afklare dette. Særligt det sidste punkt er en stor udfordring både på for eksisterende og nye fonde, for skal eksisterende fonde afvikles hvis tilstrækkelig look through ikke er muligt?

Afsluttede såvel som pågående inspektioner synes at indikere, at Finanstilsynets krav er høje, og at der kun i begrænset omfang tages hensyn til proportionalitetsprincippet.

Inddragelse i revisionsplanlægningen

Finanstilsynet har med vejledningens udstedelse og flere temainspektioner i branchen vist deres fokus på området. Derfor har selskabernes implementering af vejledningen tilsvarende højt fokus, typisk drevet i et samarbejde imellem investeringsafdelingen, økonomiafdelingen¹ samt risikostyringsfunktionen.

Det tilsvarende høje fokus bør være tilfældet i den interne revision.

Den operationelle revisions overordnede fokusområder kan sammenfattes i Governance, Compliance, Det interne kontrolsystem og Risiko-/kapitalstyring². Samtlige fokusområder er påvirket af vejledningen.

Revisionsplanlægning skal som altid tage afsæt i en væsentlighedsvurdering. Den revisionsmæssige angrebsvinkel vil afhænge af kompleksiteten og omfanget af de alternative investeringer, herunder frekvensen for at gennemføre nye alternative investeringer.

Afhængig af væsentlighedsvurderingen og hvor i processen organisationen i øvrigt er med implementeringen af vejledningen, kan revisionen nedbrydes i en række delområder (se **Figur 3** nederst på siden).

Revisionsplanen for 2019, der i mange selskaber snart skal udarbejdes, bør have vejledningens implementering i fokus – uanset hvilke revisionsområder, der på et tidligere tidspunkt er udmeldt som forventede fokusområder for 2019. Som udgangspunkt bør revisionsplanen omfatte flere af delområderne nævnt ovenfor, hvor fokus selvfølgelig kan være forskelligt. Det kan eksempelvis være relevant at inddrage delområde 2 og 4 i revisionen i 2019, såfremt omfanget af nye alternative investeringer forventes at være begrænset, eller processerne har været stærke i forvejen. Delområde 5 vil have et naturligt overlap til revisionen af second line-funktionerne.

Revisionsplanlægningen for 2020 bør tænkes ind i revisionsplanen for 2019, idet der højst sandsynligt vil være områder, der ikke når at blive revideret i dybden i 2019.

Opsummering

Vejledningen er gældende for liv- og pensionselskaberne, men bør også have et vist fokus i skadesforsikringselskaberne.

Igennem vores drøftelser med flere selskaber om vejledningens betydning er der ingen tvivl om, at vejledningen har medført krav til styrkelse af kontrolmiljøet og flere

steder helt nye processer. Det må forventes at være tilfældet i langt hovedparten af selskaberne.

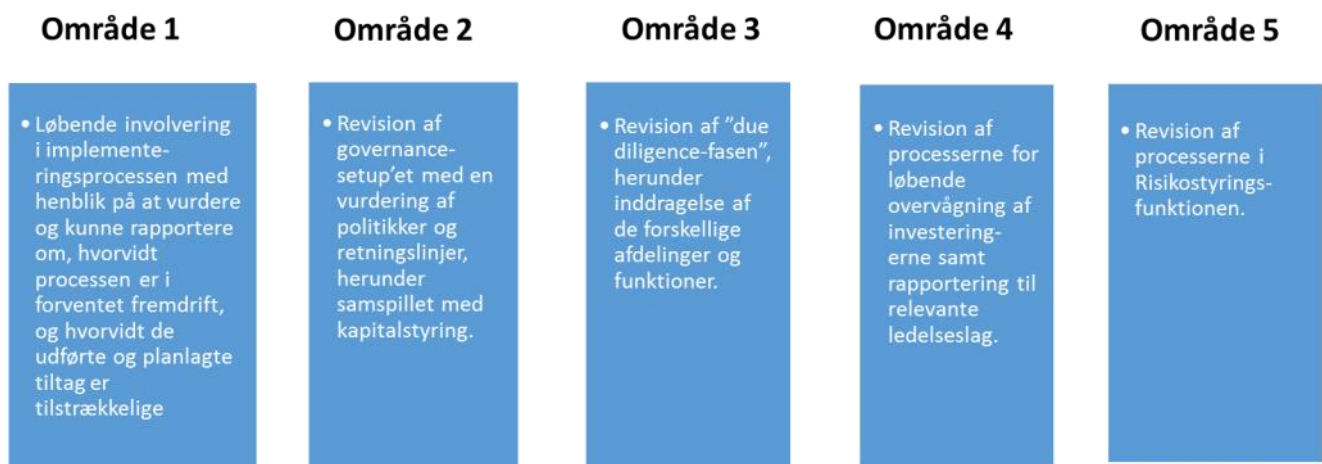
Hvis der ikke allerede er høj fokus på implementering i organisationen, bør intern revision være med til at understøtte, at det igangsættes, og inddrage området i revisionsplanlægningen for 2019 – og fremadrettet.

Noter

¹ Afhængig af, hvor ansvaret for controlling uden for investeringsafdelingen er placeret.

² Definitionen af de overordnede fokusområder for den operationelle revision varierer i sprogbrug. Her er anvendt de overskrifter, vi bruger i EY.

Figur 3: Delområder



Auditing Capital Adequacy and Stress Testing for Banks



Pille Lindskog, CIA, CISA, CFSA,
CCSA, Head of Audit Group
Treasury & ALM, Nordea

Introduction

"Auditing Capital Adequacy and Stress Testing for Banks" that was published in May 2018 is one of the latest Practical Guides for IIA members in the financial services area.

The guidance is well-timed, filling the relative void of supporting material for auditors considering regulatory expectations in the capital adequacy area. It also aims at satisfying the needs of international readers; the Practice Guide includes references to both European and US regulations, leaving it to the readers' discretion to navigate to the suitable ones. In this article I will be reflecting on the guidance from the European perspective.

European legislation

As a response to several global financial crises, the capital adequacy requirements for firms in the financial sector have been specified by the Basel Committee of Banking Supervision (BCBS) and the Bank for International Settlements (BIS). The Basel Committee has introduced and has been revising the framework for capital adequacy in banks since 1988, where the latest implemented update is known as Basel III¹.

As a guiding principle, financial institutions are expected to have sufficient/adequate amount and type of capital to cover all material risks to which they are exposed in a situation of stress. For that purpose, amongst others, banks need to understand their risk profile and have systems in place to capture, quantify and monitor those risks.

For internal auditing in the capital adequacy area, the European Banking Authority (EBA), whose main task is to provide a single set of harmonised prudential rules for financial institutions throughout the EU, has mentioned their expectations in several instances. For example, the

internal audit function is expected to "adequately cover(s) all areas in a risk-based audit plan, including Internal Capital Adequacy Assessment Process (ICAAP), Internal Liquidity Adequacy Assessment Process (ILAAP) ..."2. In addition, the relevant supervisors are to collect information from the banks including "... their internal audit reports covering ICAAP and ILAAP"3.

In fact, the Capital Requirements Regulation (EU) No. 575/2013 even defines some mandatory areas for the internal audit functions to cover (e.g. Internal Ratings-based approach (IRB), Internal Models Approaches/Internal Model Methods (IMA/IMM) reviews, Internal hedges).

As the largest bank supervisor in Europe, the European Central Bank (ECB) has issued some guidance on the subject4 according to which "...Internal reviews of the ICAAP are expected to be carried out comprehensively by the three lines of defence, including business lines and the independent internal control functions (risk management, compliance and internal audit), in accordance with their respective roles and responsibilities."

Although the risk-based approach adopted by most internal audit functions seems generally accepted as normal practice, in addition to the expectations from the financial institutions' own management bodies, the regulators' attention towards the internal audit functions' coverage of the capital adequacy subject cannot be overlooked.

One might also argue that the expectations on the internal audit function are developing in two directions. On the one hand, internal audit needs to be able to assess the "big picture" i.e. the relationship between the business model, strategic planning, risk management and capital buffers enabling stable operations through different economic cycles.

On the other hand, internal audit functions are expected to possess rather technical skills and competences to be able to add value on a very "hands-on" level, e.g. challenging the quality of the data sets used to quantify the risks or arguing whether the relevant risk quantification methods are fit for purpose.

Auditing capital adequacy and stress testing

For planning and performing the audit engagement, the IIA Practice Guide provides references to relevant IIA Standards, while suggesting the steps to be taken in assessing the capital planning and stress testing processes.

These include:

Standard 2200 – Engagement planning

1. Understand the context and purpose of the engagement (Standard 2201).
2. Gather information to understand the area or process under review (Standard 2201).
3. Conduct a preliminary risk assessment of the area or process under review (Standard 2201).
4. Form engagement objectives (Standard 2210).
5. Establish engagement scope (Standard 2220).
6. Allocate resources (Standard 2230).
7. Engagement work programme (Standard 2240)

Standard 2330 - Documenting the information

Standard 2400 – Communicating results

The Practice Guide leaves an open door for choosing the specific approach, method or frequency to cover the capital planning process, merely suggesting that the internal audit plan should provide assurance to senior management and the Board that the process is operating properly and within regulatory guidelines over a reasonable period of time, depending on the size, business model and risks of the institution.

The BCBS has among the other guidance for internal audit⁵ said: *“The scope of internal audit should include all provisions of this regulatory framework and in particular the bank’s system for identifying and measuring its regulatory capital and assessing the adequacy of its capital resources in relation to the bank’s risk exposures and established minimum ratios.”*

Also, there is an expectation that: *“Internal audit should review management’s process for stress testing its capital levels, taking into account the frequency of such exercises, their purpose (e.g. internal monitoring vs. regulator imposed), the reasonableness of scenarios and the underlying assumptions employed, and the reliability of the processes used.”*

While planning the audit engagement, it is important for auditors to identify the banks’ capital adequacy related objectives and means for reaching those (governance, processes, resources, models, capital instruments etc.). This information is acquired through participation in relevant meetings and reading relevant documentation (charters, policies, instructions, process and model descriptions and risk modelling, as well as stress testing results).

Capital adequacy - regulatory requirements

The Basel standard requires banks to maintain a minimum capital adequacy ratio. That requirement is split between Tier 1 and Tier 2. Common Equity Tier 1 (CET1) capital is considered of the highest quality, also known as “going concern” capital and includes common shares, retained earnings etc. Tier 2 capital (CET2) is also known as “gone-concern” capital. The first one is meant to absorb unexpected losses⁶ without requiring a bank ceasing all its activities and the other one should be used in the bail-out. In addition, banks are expected to keep a Capital Conservation Buffer and a Capital Countercyclical Buffer.

As the regulatory capital requirements are by nature on the conservative side, the internal auditors also need to understand how the bank’s capital planning (and management) process allows it to not only maintain regulatory compliance, but also generate expected results for its shareholders/stakeholders (e.g. by reviewing the use of the concept/model of Economic Capital).

One major help in the risk assessment of the area are the reports and examination by the regulators (including SREP), as well as development of relevant metrics such as CET1 or Leverage ratio.

While forming the criteria for evaluation by internal audit, capital adequacy may be assessed against internal and external requirements or leading practices. The CRR and related EBA guidelines can be used for assessing any of the elements in ICAAP processes. BCBS guidelines are also often used as best practice criteria by auditors. In addition, for example, while assessing governance for capital management the IIA’s Three Lines of Defence model⁷ may be used for inspiration.

Capital Planning Process

According to the BCBS guidance for internal audit functions: *“... The scope of internal audit should include all provisions of this regulatory framework and in particular the bank’s system for identifying and measuring its regulatory capital and assessing the adequacy of its capital resources in relation to the bank’s risk exposures and established minimum ratios.”*

The IIA Practice Guide provides a description of a Capital Planning Process as a basis for internal auditors’ assessment of capital adequacy, particularly how it is accounting for the level of capital needed today, and how well it predicts the level of capital needed under stressed financial and economic scenarios.

A bank's capital strategies and, as a result, their capital planning processes start with the organisation's stated risk appetite. The Risk Appetite Framework forms the basis of capital policies and governs the strategies and processes the organisation uses to meet its objectives. Once a bank has established its Risk Appetite Statement for remaining solvent, which may change from year to year, and articulated its capital policy throughout the organisation, it has a solid base with which to design its capital strategies.

Capital planning is the underpinning that allows the bank to allocate capital (based on the risk appetite cascading) to strategies, business lines and products it plans to pursue in the upcoming years.

Internal auditors should assess whether the bank involves a solid cross-section of departments — both first line and second line of defence — in proposing plans and challenging the assumptions constructed in the strategic plan that will feed into the capital planning process.

Capital for risk types - Credit, Market and Operational risk

As the bank's capital ratio is by definition the relation of its capital to its Risk Exposed Assets (or Risk Weighted Assets - RWA) the importance of understanding of the risks (and risk management processes) needs to be underlined. The RWAs, as named in the Practice Guide, are the estimation of the risks in the bank's balance sheet including, but not limited to, credit, market and operational risks.

In addition to traditionally reviewing the business processes for risk management, internal auditors should obtain evidence that their bank is using the approaches approved by relevant regulatory bodies for measuring credit, market and operational risks, and that they maintain capital in compliance with regulatory guidelines and for reaching the goals as expected by shareholders.

The IIA Practice Guide elaborates on the accepted risk measurement and audit approaches by risk type.

Credit Risk

Capital for credit risk covers all assets in the bank's portfolio that have an element of credit risk, each weighted according to its respective riskiness. Banks must maintain a certain percentage of RWAs as capital to meet any losses that arise due to deterioration in asset quality.

Capital for credit risk can be ascertained using the standardised approach or an internal ratings-based approach using models such as A-IRB (Advanced Internal Rating

Based) and F-IRB (Foundation Internal Rating Based) approach. The A-IRB allows banks to estimate Probability of Default (PD), Loss Given Default (LGD), Exposure at Default (EAD), and maturity of an exposure on their own.

One needs to observe that the Capital Requirements Regulation (CRR) Article 191 in fact poses internal audit with a regular audit requirement in terms of "*institution's rating systems and its operations, including the operations of the credit function and the estimation of PD's, LGD's and EL's and conversion factors*".

The F-IRB applies fixed values to the LGD and EAD parameters (provided by regulators), whereas the bank may estimate PD themselves. For the Standardised approach the regulators prescribe risk weights for various asset classes. The approach in auditing this methodology is up to auditors' discretion and risk assessment (mainly).

Market risk

Capital for market risk consists of assets that are exposed to movements of underlying market factors. For example, the value of a trading portfolio may decrease due to changes in the value of market risk factors e.g. currency and commodity prices, interest rates, and stock and security prices. Banks weight the risks of such assets and must allocate capital as a percentage of RWA to ensure they are able to meet any losses arising due to movements in market prices. Capital requirements for market risks can be measured through either the standardised approach or internal models approach (IMA), respectively.

As such the key component of market risk is pricing. The instruments in the trading book are marked to market on a daily basis. Instruments in the banking book are not priced until they reach maturity or are reclassified into the trading book. The total IMA capital requirement is the aggregation of Global Expected Shortfall (ES), Default Risk Charge (DRC) and Stressed Capital Add-on for Non-modellable Risks (SES).

In case the bank has permission to use the internal models approach, CRR Article 368 poses the requirement on the internal audit function to regularly review such a model.

The standardised approach consists of Sensitivities-based Method, Default Risk Charge and Residual Risk Add-on (RRAO). In this case auditors' discretion in choosing audit approach and priority applies.

Operational Risk

Capital for operational risk comprises the capital that

must be maintained to offset operational losses due to exposure to internal or external events involving people, processes and technology. The use of internal models for quantifying operational risk is not permitted as the nature of some operational risk exposures (e.g. misconduct) have not been considered conducive to measurement by models. The valid standardised approach is based on the Business Indicator (BI), the Business Indicator Component (BIC), and the Internal Loss Multiplier (ILM) and is covered by auditors according to their discretion and risk assessment.

Stress testing

The BCBS guidance⁸ expects that *"Internal audit should review management's process for stress testing its capital levels, taking into account the frequency of such exercises, their purpose (e.g. internal monitoring vs. regulator imposed), the reasonableness of scenarios and the underlying assumptions employed, and the reliability of the processes used"*.

Stress testing for capital adequacy purposes is not unknown or new to banks. There is, however, an increasing complexity and uncertainty in the banks' operating environment, which complicates, for example, the selection of relevant scenarios. This is also seen in regulatory guidance⁹. Banks should be able to demonstrate coherence between stress testing, business model, strategic planning and risk management. The stress testing models should therefore be agile i.e. it should be possible to run stress testing more frequently than once a year to support risk management and planning.

Stress testing involves evaluating a bank's consolidated risk exposure and financial position under severe, yet plausible, scenarios (both macroeconomic as well as idiosyncratic for the bank), and is central to the iterative process of strategy selection amongst others. As it is forward-looking, it ensures that risks are captured in the strategic plan and risk exposures are kept at levels consistent with thresholds established in the Risk Appetite Framework. For that purpose, the organisation should also establish and maintain a repeatable, dependable and well-controlled environment for stress testing.

Internal auditors should examine the scenario development process to ensure that all parties are involved at the appropriate stage and that data from all relevant parties is considered appropriately.

In addition, the appropriateness of the technical environment for stress testing, relevant model risk management, not to mention the actual use of the stress testing results, are the areas for internal auditors to cover.

Conclusion

The IIA Practice Guide "Auditing Capital Adequacy and Stress testing for Banks" provides inspiration for assessing capital management in the financial institution. In addition to suggesting one possible approach for internal auditors, the guidance also describes international standards and presents some key principles for capital adequacy as such.

It must be noted, though, that the risk management processes leading to quantification of required capital or ICAAP for that matter include numerous underlying processes, models and governance constellations, each of which could and should be risk assessed by internal audit and prioritised for separate reviews. Due to the wide spectrum of subjects involved, the key challenge in auditing capital adequacy is finding and allocating adequate resources to perform the job.

Notes

¹ Global regulatory framework for more resilient banks and banking systems (Basel, Switzerland: Bank for International Settlements, 2011). <https://www.bis.org/publ/bcbs189.pdf>.

² EBA/GL/2018/03: Final Report – Guidelines on the Revised SREP and Supervisory Stress Testing.

³ EBA/GL/2016/10: Guidelines on ICAAP and ILAAP Information Collected for SREP Purposes.

⁴ ECB Guide to the internal capital adequacy assessment process (ICAAP)

⁵ "The internal audit function in banks", (June 2012, Bank for International Settlements), <https://www.bis.org/publ/bcbs223.pdf>

⁶ In addition to the reserves that are kept for the expected losses

⁷ The Institute of Internal Auditors. The IIA's Position Paper: The Three Lines of Defense in Effective Risk Management and Control (Altamonte Springs: The Institute of Internal Auditors, 2013), 2-6.

⁸ "The internal audit function in banks", (June 2012, Bank for International Settlements), <https://www.bis.org/publ/bcbs223.pdf>

⁹ Final Report on Guidelines on Institutions' Stress Testing, EBA/GL/2018/04, July, 19th 2018.

EBA's retningslinjer vedrørende intern ledelse "guider" intern revision godt på vej



Lotte Pia Møllerup, Senior Advisor,
Ernst & Young P/S

Baggrund

Tillid til det finansielle system er afgørende og en forudsætning for at det finansielle system kan bidrage til økonomien som helhed. Derfor er effektive interne styringsordninger grundlæggende, hvis finansielle virksomheder hver for sig og det samlede finansielle system skal fungere godt.

I de seneste år har interne styrings spørgsmål fået øget opmærksomhed fra forskellige internationale finansielle myndigheder. Et fælles træk har været at rette fokus på de finansielle virksomheders svage eller utilstrækkelige interne styringspraksis for fremover at sikre fastsættelsen af en hensigtsmæssig risikostrategi og passende risikovillighedsniveauer, en holistisk risikostyringsramme og effektive rapporteringslinjer til ledelsesorganet.

Det er afgørende, at der findes interne styringsrammer, herunder interne kontrolmekanismer og risikostyring, der er tilstrækkeligt integreret. Målet er, at det skal være med til at sikre en ensartet metode og terminologi, således at der sikres et holistisk syn på alle risici. En vigtig parameter har også været, at interne kontrolfunktioner sikres passende ressourcer, status og/eller ekspertise.

Reviderede retningslinjer

Med henblik på at sikre en sund intern styringspraksis og for at fremme en god risikokultur på alle niveauer kom det europæiske banktilsyn - European Banking Authority (EBA) - i september 2017 med en rapport indeholdende revidere retningslinjer vedrørende intern ledelse (EBA/GL/2017/11). En dansk udgave af de reviderede retningslinjerne kom i marts 2018. Retningslinjerne har fundet anvendelse fra den 30. juni 2018 og samtidig blev EBA's retningslinjerne vedrørende intern ledelse (GL 44) fra 27. september 2011 ophævet.

I henhold til artikel 16, stk. 3, i forordning (EU) nr. 1093/2010 skal de kompetente myndigheder og finansielle institutioner bestræbe sig på at efterleve retningslinjerne bedst muligt. Retningslinjerne afspejler EBA's syn på passende tilsynspraksis eller på, hvordan EU-retten bør anvendes inden for et bestemt område. De kompetente myndigheder, som er omfattet af retningslinjerne, bør efterleve disse ved i fornødent omfang at indarbejde dem i deres praksis.

Finanstilsynet har den 21. maj 2018 meddelt EBA, at de vil overholde retningslinjerne og kreditinstitutter og investeringsselskaber bør derfor forholde sig til og overholde retningslinjerne.

Bemærk, at retningslinjerne er underlagt proportionalitetsprincippet, og skal derfor anvendes hensigtsmæssigt under hensyntagen til især institutionens størrelse, interne organisation og natur samt kompleksiteten af dens aktiviteter.

Retningslinjer præciserer de interne ledelsesordninger, - procedurer og -mekanismer, som kreditinstitutter og investeringsselskaber skal gennemføre for at sikre en effektiv og forsigtig ledelse.

Retningslinjernes Del V - Ramme for og mekanismer for intern kontrol - indeholder bl.a. en detaljeret beskrivelse af de interne risikostyrings-, compliance- og revisionsfunktioner, og afsnit 22 (se **Boks 1** på næste side) vedrører den interne revisionsfunktion.

Nedenfor gennemgås retningslinjerne i forhold til den interne revisionsfunktion.

Dansk lovgivning

Retningslinjerne skal ses i sammenhæng med de danske lovregler vedrørende intern revision. Ifølge lov om finansiel virksomhed kan Finanstilsynet fastsætte en række regler om intern revision, jf. Bekendtgørelse om revisionens gennemførelse i finansielle virksomheder m.v. samt finansielle koncerner.

Det fremgår bl.a. af bekendtgørelsen, at i virksomheder, der i de to seneste regnskabsår på balancetidspunktet i gennemsnit har haft 125 eller flere fuldtidsansatte, skal der oprettes en intern revision. Derudover kan bestyrelsen bestemme, at der skal oprettes en intern revision, og har den ikke gjort det, skal bestyrelsen mindst én gang om året drøfte behovet for at oprette en intern revision under hensyntagen til virksomhedens kompleksitet, herunder hvorvidt virksomheden outsourcer og insourcer aktiviteter.

Boks 1 - EBAs retningslinjer- afsnit 22 Intern revisionsfunktion

197. Institutterne bør oprette en uafhængig og effektiv intern revisionsfunktion, under hensyntagen til de i del I anførte proportionalitetskriterier, og udpege en person, der er ansvarlig for denne funktion i hele instituttet. Den interne revisionsfunktion bør være uafhængig og i tilstrækkeligt omfang have autoritet, betydning og ressourcer. Navnlig bør instituttet sikre, at den interne revisionsfunktionens medarbejdere er tilstrækkeligt kvalificerede, og at dens ressourcer, navnlig dens revisionsværktøjer og metoder til risikoanalyse, er tilstrækkelige i forhold til instituttets størrelse og placeringer samt arten, omfanget og kompleksiteten af de risici, der er forbundet med instituttets forretningsmodel, aktiviteter, risikokultur og risikovillighed.

198. Den interne revisionsfunktion bør være uafhængig af de reviderede aktiviteter. Den interne revisionsfunktion bør derfor ikke kombineres med andre funktioner.

199. Den interne revisionsfunktion bør på grundlag af en risikobaseret tilgang uafhængigt revidere og foretage objektiv kontrol af, at alle et instituts aktiviteter og enheder, herunder outsourcete aktiviteter, overholder instituttets politikker og procedurer samt eksterne krav. Hver enhed inden for koncernen bør være omfattet af den interne revisionsfunktion.

200. Den interne revisionsfunktion bør ikke være involveret i at udforme, udvælge, fastsætte og implementere specifikke interne kontrolpolitikker, -mekanismer og -procedurer samt risikogrænser. Dette bør imidlertid ikke hindre ledelsesorganet i dets ledelsesfunktion i at anmode om input fra den interne revision om spørgsmål vedrørende risiko, intern kontrol og overholdelse af gældende regler.

201. Den interne revisionsfunktion bør vurdere, om instituttets ramme for intern kontrol, jf. afsnit 15, er både virkningsfuld og effektiv. Navnlig bør den interne revisionsfunktion vurdere:

- a) hensigtsmæssigheden af instituttets ledelsesramme
- b) om eksisterende politikker og procedurer fortsat er tilstrækkelige og overholder juridiske og tilsynsmæssige krav samt instituttets risikovillighed og -strategi
- c) procedurerne overholdelse af de gældende love og bestemmelser og af ledelsesorganets beslutninger
- d) om procedurerne implementeres korrekt og effektivt (f.eks. transaktioners overensstemmelse, det faktiske risikoniveau osv.) og
- e) tilstrækkeligheden, kvaliteten og effektiviteten af den kontrol og rapportering, der er foretaget af forretningsenhederne og risikostyrings- og compliancefunktionen.

202. Den interne revisionsfunktion bør navnlig kontrollere rigtigheden af processerne og således sikre pålideligheden af instituttets metoder og teknikker samt de antagelser og informationskilder, der anvendes i dets interne modeller (f.eks. risikomodellering og regnskabsmæssige målinger). Den bør ligeledes evaluere kvaliteten og brugen af kvalitative værktøjer til identifikation og vurdering af risiko og de risikobegrænsende foranstaltninger, der er truffet.

203. Den interne revisionsfunktion bør i hele instituttet have uhindret adgang til alle instituttets registre, dokumenter, oplysninger og bygninger. Dette bør omfatte adgang til ledelsesinformationssystemer og referater fra alle udvalg og beslutningstagende organer.

204. Den interne revisionsfunktion bør overholde nationale og internationale faglige standarder. Et eksempel på de faglige standarder, der henvises til her, er de standarder, der er udarbejdet af Foreningen af Interne Revisorer.

205. Det interne revisionsarbejde bør udføres i henhold til en revisionsplan og et detaljeret revisionsprogram, der følger en risikobaseret metode.

206. En intern revisionsplan bør udarbejdes mindst én gang om året på grundlag af de årlige mål for den interne revisionskontrol. Den interne revisionsplan bør godkendes af ledelsesorganet.

207. Alle revisionsanbefalinger bør underkastes en formel procedure for de relevante ledelsesniveauers opfølgning, så det sikres, at der findes en effektiv og rettidig løsning, der skal indberettes.

Den interne revision skal fungere uafhængigt af den daglige ledelse. Den interne revision ledes af en revisionschef. Ansættelse og afskedigelse af revisionschefen kan alene foretages af bestyrelsen. Hvervet som intern revisionschef og vicerevisionschef kan ikke forenes med hvervet som bestyrelsesmedlem.

Den interne revisionschef betragtes som en nøgleperson og er således omfattet af kravene for ledelsesmedlemmers egnethed og hæderlighed (fit & proper).

Governance i forbindelse med kontrolfunktioner

Bestyrelsen bør sikre en tilstrækkelig og effektiv ramme for intern ledelse og intern kontrol, der omfatter en klar organisatorisk struktur og velfungerende uafhængige interne risikostyrings-, compliance- og revisionsfunktioner, hvor de to førstnævnte funktioner bør være underkastet revision udført af den interne revisionsfunktion. Funktionerne bør i tilstrækkeligt omfang have autoritet, betydning og ressourcer til at varetage deres funktioner ansvarligt for implementeringen af fx interne kontrolprocedurer, som sikrer et overblik over risici og effektiv ledelse af virksomheden.

Bestyrelsen er ansvarlig for at fastslå og overvåge, om rammen for og processerne og mekanismerne i forbindelse med den interne kontrol er hensigtsmæssige og effektive, og for at føre tilsyn med alle forretningsområder og interne enheder, herunder interne kontrolfunktioner. Virksomhederne bør fastlægge, opretholde og regelmæssigt ajourføre hensigtsmæssige skriftlige politikker, mekanismer og procedurer for den interne kontrol, som skal godkendes af bestyrelsen.

Bestyrelsen bør kende og forstå virksomhedens retlige, organisatoriske og operationelle struktur ("know your structure") og sikre, at denne stemmer overens med virksomhedens godkendte forretnings- og risikostrategi og risikovillighed. Virksomhedens struktur og aktiviteter, herunder deres overholdelse af lovgivning og faglige standarder, bør være underkastet regelmæssig revision udført af den interne revisionsfunktion på grundlag af en risikobaseret tilgang.

Bestyrelsen skal overvåge gennemførelsen af aktiviteterne i den interne revisionsplan, efter forudgående inddragelse af risikoudvalget og revisionsudvalget.

De tre forsvarslinjer

Retningslinjerne omhandler "de tre forsvarslinjer for at håndtere og styre risici". Forretningsenhedernes løbende kontroller er første forsvarslinje. Til dette formål bør de enkelte forretningsområder have passende processer og

kontroller på plads, der har til formål at sikre, at risici identificeres, analyseres, måles, overvåges, forvaltes, rapporteres og holdes inden for rammerne af institutionens risikovillighed, og at forretningsaktiviteterne overholder både eksterne og interne regler.

Risikostyrings- og compliancefunktionen udgør anden forsvarslinje. Risikostyringsfunktionen har ansvaret for at identificere, overvåge, analysere, måle, styre og rapportere om risici. Den udfordrer og bistår i gennemførelsen af risikostyringsforanstaltningerne i forretningsområderne for at sikre, at processerne og kontrollerne af første forsvarslinjes aktiviteter er korrekt udformet og effektive. Compliancefunktionen overvåger overholdelse af lovmæssige krav og interne politikker.

Intern revision er den tredje forsvarslinje, og de gennemfører risikobaserede og generelle revisioner og gennemgår de interne styringsordninger, processer og mekanismer for at fastslå, at de er sunde og effektive, implementeret og konsekvent anvendt. Intern revision er også ansvarlig for den uafhængige gennemgang af de to første forsvarslinjer.

Revisionsudvalget skal bl.a. overvåge, om virksomhedens interne kvalitetskontrol- og risikostyringsystemer, og i givet fald dets interne revisionsfunktion, fungerer effektivt med hensyn til finansiel rapportering i det reviderede institut, uden at krænke dets uafhængighed.

Intern revision

Intern revision bør have tilstrækkelige ressourcer og et tilstrækkeligt antal kvalificerede medarbejdere. Medarbejderne bør opkvalificeres løbende og modtage uddannelse efter behov.

Derudover bør intern revision have tilstrækkelige IT-systemer og IT-understøttelse til deres rådighed, med adgang til de interne og eksterne oplysninger, der er nødvendige for at leve op til deres ansvar. Intern revision bør herudover have adgang til alle nødvendige oplysninger vedrørende forretningsområder og relevante datterselskaber.

Hvis operationelle opgaver i forbindelse med den interne revision bliver helt eller delvist outsourcet, er den interne revisionschef henholdsvis bestyrelsen stadig ansvarlige for aktiviteterne.

Den interne revisionsfunktion rapporterer direkte til og er direkte ansvarlige over for bestyrelsen.

Intern revisions uafhængighed

Intern revision forventes at opfylde følgende betingelser med henblik på at sikre uafhængighed:

- medarbejdere må ikke udføre operationelle opgaver, der falder inden for de aktiviteter, som de forventes at overvåge og kontrollere
- intern revision er organisatorisk adskilt fra de aktiviteter, som det påhviler dem at overvåge og kontrollere
- den interne revisionschef bør ikke være underordnet en person, der har ansvar for at håndtere de aktiviteter, som intern revision overvåger og kontrollerer, og
- aflønningen af intern revisions medarbejdere bør ikke være knyttet til udøvelsen af de aktiviteter, som intern revision overvåger og kontrollerer, og bør ikke på anden måde påvirke deres objektivitet.

Ramme for risikostyring

Som en del af den overordnede ramme for intern kontrol bør virksomhederne have en helhedsorienteret ramme for risikostyring for hele instituttet, der rækker på tværs af alle dets forretningsområder og interne enheder, herunder interne kontrolfunktioner, under fuld anerkendelse af den økonomiske substans af alle dets risikoeksponeringer.

Rammen for risikostyring bør være omfattet af en uafhængig intern kontrol, f.eks. udført af den interne revisionsfunktion, og bør revurderes løbende i forhold til instituttets risikovillighed, under hensyntagen til oplysninger fra risikostyringsfunktionen og fra risikoudvalget, hvis et sådant er nedsat.

Intern revisions rolle i forhold whistleblower

En finansiel virksomhed skal ifølge lov om finansiel virksomhed have en ordning, hvor dens ansatte via en særlig, uafhængig og selvstændig kanal kan indberette overtrædelser eller potentielle overtrædelser af den finansielle regulering begået af virksomheden, herunder af ansatte eller medlemmer af bestyrelsen i virksomheden. Indberetninger til ordningen skal kunne foretages anonymt.

Det fremgår således også af retningslinjerne, at virksomheder bør etablere og opretholde passende interne advarselspolitikker og -procedurer, som gør det muligt for medarbejderne at indberette potentielle eller faktiske overtrædelser af lovgivningsmæssige eller interne krav gennem en særlig, uafhængig og selvstændig kanal. Det kan fx ske via compliancefunktionen, den interne revisionsfunktion eller en uafhængig intern whistleblower procedure.

Kilder

Lov om finansiel virksomhed:

<https://www.retsinformation.dk/Forms/R0710.aspx?id=193767>

Bekendtgørelse om revisionens gennemførelse i finansielle virksomheder m.v. samt finansielle koncerner:

<https://www.retsinformation.dk/eli/lta/2015/1912>

EBAs retningslinjer vedrørende intern ledelse:

https://www.eba.europa.eu/documents/10180/2164689/Guidelines+on+Internal+Governance+%28EBA-GL-2017-11%29_DA.pdf/cee4e8f4-765c-452d-902c-b09ffa979010



Nye medlemmer

Nye medlemmer i IIA fra 4.9.2018 – 4.12.2018

A.P. Møller-Mærsk

Sigurdur Palsson

Danske Bank

Christian Barrett
Igor Mandzo

Handelsbanken

Helle Mørch Skou

JN Data

Iben Merete Nøhr Nielsen

Jyske Bank

Karsten Dahl

Nordea

Sabrina Zimmerer

Ringkjøbing Landbobank

Sanne Møberg Mikkelsen

Sampension

Aran Taghizadeh
Rasmus Skov
Randi Risum Boesen

Ørsted

Michael Randrup

Uddannelsesaktiviteter

Er du opdateret på IIAs kursusudbud? Som altid findes datoer og emner for gå-hjem møder, kurser og konferencer på foreningens hjemmeside www.ii.dk under rubriken "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.

Kurser og gå-hjem møder

25.04.2019: Kursus for pengeinstitut- og realkreditrevisorer

02.05.2019: Kursus for Forsikringsrevisorer

15.05.2019 - 16.05.2019: IIA Årsmøde 2019

“Bagsmækken”

Foreningens adresse

Foreningen af Interne Revisorer (IIA)
 Att.: Vicervisionschef Kim Stormly Hansen
 Intern revision
 Nykredit
 Kalvebod Brygge 1-3
 1780 København V

CVR nr. 73954215

Indmeldelse i foreningen

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

Chefsekretær Dorte Dreijøe
 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, eller til glt@nykredit.dk.

Certificeringer

Nærmere oplysninger om certificeringer kan fås på IIA's internationale hjemmeside www.globaliaa.org eller ved kontakt til:

Heino Hansen, Internal Audit Manager, CIA, Nordea
 ☎ 31 18 38 01 ✉ heino.hansen@nordea.com

Peer Højlund, Chefspecialist, Nykredit
 ☎ 44 55 93 14 ✉ phc@nykredit.dk



Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

Formand

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

Næstformand

Audit Director
 Jesper Siddique Olsen
 Danske Bank
 ☎ 45 12 76 58 ✉ jol@danskebank.dk

Kasserer

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

Sekretær

Internal Audit Manager, CIA
 Anita Damgaard Laugesen
 Nordea
 ☎ 55 47 33 18 ✉ anita.laugesen@nordea.com

Bestyrelsesmedlemmer

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

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

Revisionschef, CIA, CISA
 Birgitte Rousing Svenningsen
 Express Bank
 ☎ 36 39 52 61 ✉ bisv@expressbank.dk

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

Revisionschef
 Michael Ravbjerg Lundgaard
 DSB
 ☎ 24 68 06 01 ✉ mirl@dsb.dk

Professor
 Kim Klarskov Jeppesen
 CBS - Copenhagen Business School
 ☎ 38 15 23 06 ✉ kkj.acc@cbs.dk