INFO

Foreningen af Interne Revisorer
Nummer 71 | April 2019 | 24. årgang

Minitema:
Three Lines of Defense med fokus på samarbejdet med second line

Minitema: GDPR i praksis
- **DPO-ens rolle**
- **GDPR i intern revision**

Agile revision

Hvordan kommer du i gang?

Cybersikkerhed

Vejledninger fra Center for Cybersikkerhed tilgængelige for dig

Third-party Risk Management

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

Afdelingsdirektør, 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 72 udkommer i september 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.

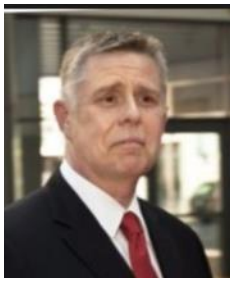
Indhold

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.iia.dk

Leder



Kim Stormly Hansen, Vicerevisionschef, Nykredit

Den interne revisionsbranche i Danmark

Tillad mig at komme med nogle personlige betragtninger om den interne revisionsbranche i Danmark.

Når man ser på foreningens medlemsfordeling står det klart, at der er en væsentlig overvægt af medlemmer fra den finansielle branche, ca. 60%. Dette er uden tvivl historisk betinget, som følge af krav om tilstedeværelsen af en intern revisionsfunktion i finansielle virksomheder af en vis størrelse, revisionsbekendtgørelsen og adgangen til at påtegne årsregnskabet.

Utallige globale survey's har gennem årene vist en vis ubalance, mellem det vores stakeholdere mente vi burde have fokus på, og det vi allokerede vores tid til. Generelt set tillader jeg mig at fortolke disse survey's som om, at vores stakeholdere har den opfattelse, at den operationelle revision har mere værdi end den finansielle revision, uden at vi skal komme ind på, hvordan de to former hver især defineres, og om det ene er en forlængelse af det andet, eller om det ene er en delmængde af det andet, eller der er en større eller mindre fællesmængde.

Globalt set har der været en bevægelse fra finansiel revision til operationel revision. Jeg er ikke bekendt med, at der er empiriske undersøgelser, som behandler vores stakeholderes holdning specifikt i Danmark eller behandler bevægelsen fra operationel revision vs. finansiel revision, men det er mit bud, at udviklingen sker langsommere i Danmark end globalt, især hvis man ser bort fra de større interne revisionsfunktioner.

Behovet for denne bevægelse styrkes efter min opfattelse af den øgede fokus på "ordentlighed" – ikke kun i den finansielle branche, men i offentligheden generelt og medierne specifikt. Det er min dybtfølte holdning, at vi som interne revisorer skaber størst værdi, når vi giver assurance på operationelle områder og ikke mindst på det lidt udefinerbare område Governance. Her tænker jeg på forhold som risikostyring, herunder ERM-processen, Conduct Management, Kultur osv.

Ikke mindst i forhold til revision af Governance er vores samarbejde med 2nd line of defence af stor betydning. Det er min oplevelse, at vi har brugt en del tid på at drøfte i hvilket omfang, vi kan basere os på dette arbejde, og i hvilket omfang 2nd line er tilstrækkeligt uafhængige. Jeg anbefaler, at vi i højere grad kommer i gang med at styrke samarbejdet med 2nd line.

For at opsummere vil jeg give 6 bud på fokusområder, som foreningen og branchen bør fokusere på i de kommende år.

1. Udarbejd retningslinjer eller vejledning i hvad operationel revision er og udføres
2. Øg, med udgangspunkt i ovenstående fokus på operationel revision, herunder særligt governanceområdet
3. Styrk samarbejdet med 2nd line of defence
4. Kig på samarbejdsmodellen med ekstern revision, både i relation den finansielle revision og i relation til intern revisions "køb af spidskompetencer" hos ekstern revision. Jeg tror ikke på "one size fits all"
5. Kig på generationsskifteproblematikken i branchen, herunder tiltrækning af unge talenter, og at vi ikke kun rekrutterer fra ekstern revision
6. Følg udviklingen i digitaliseringen og styrk kompetencerne på disse områder, så vi som interne revisorer kan være værdiskabende, ikke mindst i relation til dataanalyse.

Nye certificeringer

Ulrik Kjersgaard Friis, Coloplast (CIA)
Carsten Kibugi Røjgaard, Region Sjælland (CIA)
Jeanne Koch Rasmussen, PwC (CIA)
Chen Qian, PwC (CRMA)

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

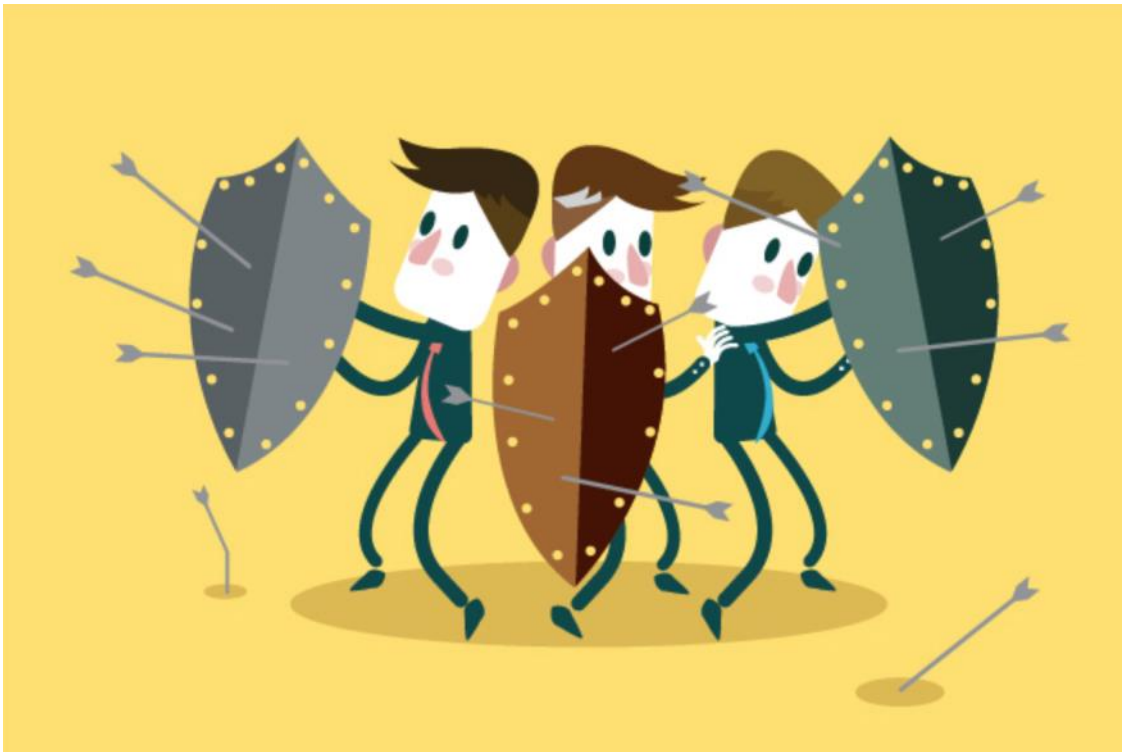
Ansøgningsfristen er 31. juli 2019. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iia.dk.

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.iia.dk findes der forslag til emner, som kan anvendes til inspiration.

Foreningen af Interne Revisorer
The Institute of Internal Auditors - Denmark

Minitema: Three Lines of Defense



Der er efterhånden skrevet en pæn mængde artikler om Three Lines of Defense-modellen, men emnet er dermed ingenlunde slidt eller uddebatteret. I stedet udvikler diskussionen sig løbende i takt med at 2nd line-funktionerne i særdeleshed modnes og best practice fæstner rod. Nye spørgsmål dukker op og muligheder byder sig. I dette minitema med Three Lines of Defense som overskrift, byder INFO på to artikler om emnet. Først og fremmest præsenterer Carina Kristiansen og Christian Pinholt – vinderne af IIA's prisopgave – deres konklusioner vedr. implementering af modellen i danske pengeinstitutter og dernæst berører Benjamin Vangaard – Manager i Deloitte – intern revisions værdiskabende kapacitet ved implementering af integreret risiko-styring på tværs af de tre forsvarslinjer.

God fornøjelse!

Foreningen af Interne Revisorer stiftede i 2017 **IIA Prisen**. Formålet med prisen er at fremme kendskabet til og forskningen inden for intern revision. Prisen blev første gang uddelt i efteråret 2018, hvor prisen gik til Carina M. Kristiansen og Christian Pinholt for deres hovedopgave om Intern revision og the Three Lines of Defense i mellemstore pengeinstitutter i Danmark.

Bedømmelsesudvalget begrundede tildelingen på følgende måde:

Vi har besluttet at uddele førsteprisen til jer. Årsagen hertil er, at hovedopgaven tager fat i et højaktuelt emne. Opgaven gør god brug af interviews og spørgeskemaer. Den sætter fokus på, at Three Lines of Defense ikke er fuldt ud implementeret, idet der fortsat er usikkerhed om grænsefladerne mellem de tre forsvarslinjer. Manglende dansk lovgivning om second line funktionernes opgaver angives som en af årsagerne hertil. Da opgaven forklarer de tre forsvarslinjers opgaver, kan opgaven være med til at skubbe den videre implementering af de tre forsvarslinjer og give inspiration til, hvorledes intern revision i højere og højere grad kan fokusere på værdiskabelse gennem operationel revision. Det er derfor vores opfattelse, at opgaven på fornem vis bidrager til forståelse af intern revisions arbejde og udviklingen af professionen.

Nedenfor indfører IIA Prisens vindere læserne i de primære problemstillinger og konklusioner fra hovedopgaven.

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

Carina Kristiansen

Christian Pinholt

I denne artikel undersøges det i hvor høj grad, danske pengeinstitutter har implementeret risikostyringsmodellen The Three Lines of Defense (3LoD). Intern revision har en essentiel betydning for, at pengeinstitutter besidder en effektiv risikostyringsproces gennem 3LoD, hvorfor implementeringen særligt anskues fra interne revisionschefers synspunkt. På baggrund af en række opstillede succeskriterier for en effektiv implementering af modellen er der udarbejdet en empirisk undersøgelse med udgangspunkt i respondenter fra både 2nd og 3rd line (intern revision).

Indledning

I kølvandet på den finansielle krise er fokus øget på de svagheder, der historisk har eksisteret relateret til corporate governance og risk management generelt i den finansielle sektor. Betydelige risici opstår løbende særligt som følge af den teknologiske udvikling, hvilket medfører et behov for kontinuerlige risikovurderinger. Som resultat heraf er lovreguleringen blevet skærpet for hele risikostyringsprocessen for finansielle virksomheder med henblik på at styrke samfundets tillid til den finansielle sektor og sikre finansiel stabilitet.

Der har længe eksisteret et lovkrav for finansielle virksomheder af en vis størrelse om eksistensen af en intern revisionsafdeling, men den finansielle krise har fremhævet funktionen herved. I forlængelse heraf er der opstået et øget behov for, at intern revision ikke fortsat skal være bestyrelses- og ledelsesorganets eneste assuranceinstans. Til gengæld skal intern revision indgå som et vigtigt led i den samlede risikostyringsproces, som består af flere organisatoriske kontrolled, der alle rapporterer opad i organisationen.

Med de skærpede lovkrav er der sat fokus på eksistensen af særskilte risikostyrings- og compliancefunktioner, hvorved der tilsigtes en risikostyrings- og lovgivningsmæssig kontrol, der figurerer uafhængigt af de indtægtsgenererende funktioner i de finansielle virksomheder. Idet dette skaber et ekstra kontrolled, modificeres grundlaget for intern revisions arbejdsopgaver, således at omfanget af operationel revision af det interne kontrolsystem forøges. Herefter er det blevet essentielt for intern revision at revidere de ekstra kontrolled, idet der skal udtrykkes en konklusion på baggrund af organisationens samlede risikostyring.

Udviklingen på risikostyringsområdet for finansielle virksomheder medfører et øget fokus på optimeringen af den samlede risikostyringsproces, hvor de forskellige kontrolled må samarbejde. I relation hertil har risikostyringsmodellen Three Lines of Defense (3LoD) fået en mere essentiel rolle, idet der heraf præciseres en organisatorisk opdeling i tre separate forsvarslinjer, som samlet bidrager til en effektiv risikostyring. Den indtægtsgenerende virksomhed samles i én forsvarslinje, mens blandt andet risikostyring og compliance udgør den anden særskilte forsvarslinje. Intern revision er den tredje forsvarslinje, som

rapporterer til bestyrelsen uafhængigt af de øvrige kontrolfunktioner. Modellen betragtes som "best practice" af The Institute of Internal Auditors (IIA), hvilket understreger intern revisions betydningen for en effektiv risikostyringsproces.

Three Lines of Defense (3LoD)

Hovedformålet med 3LoD-modellen kan præciseres som værende at identificere og implementere specifikke roller i organisationen, som skal koordineres effektivt og efficient, således at relevante kontroller ikke udelades, og ligeledes at der ikke sker duplikering heraf. Med prædefinerede roller og ansvarsområder i organisationen sikres imødekommelse af udfordringer ved risikostyring og -kontrol. Implementeringen af 3LoD-modellen skal søge at strukturere rollefordeling, ansvarsfordeling samt funktionsopdeling. I forlængelse heraf skal det blandt andet specificeres, hvem der identificerer risici, hvem der sørger for imødekommelse af risici ved kontrolimplementering og øvrige risikodækkende handlinger, samt hvem der funktionstester kontrollerne (IIA, 2013). Dermed vil virksomheder, der ikke har implementeret 3LoD, tendensere til at opleve udfordringer som overflødige kontroller, mangler i risikodækningen samt forenklede risikofunktioner, der ikke harmonerer og taler sammen, så det risikeres, at fokus ikke er på væsentlige risikoområder. En konsekvens heraf kan være, at væsentlige risici falder ned mellem de tre forsvarslinjer, eller at der foreligger forvirring linjerne imellem, idet det uoverskueliggør værdien samt effektiviteten af de enkelte funktioner. Derudover kan kompleks og modstridende rapportering fra funktionerne gøre det vanskeligt for ledelsesorganet effektivt at overvåge risikostyringsprocessen (EY 2013).

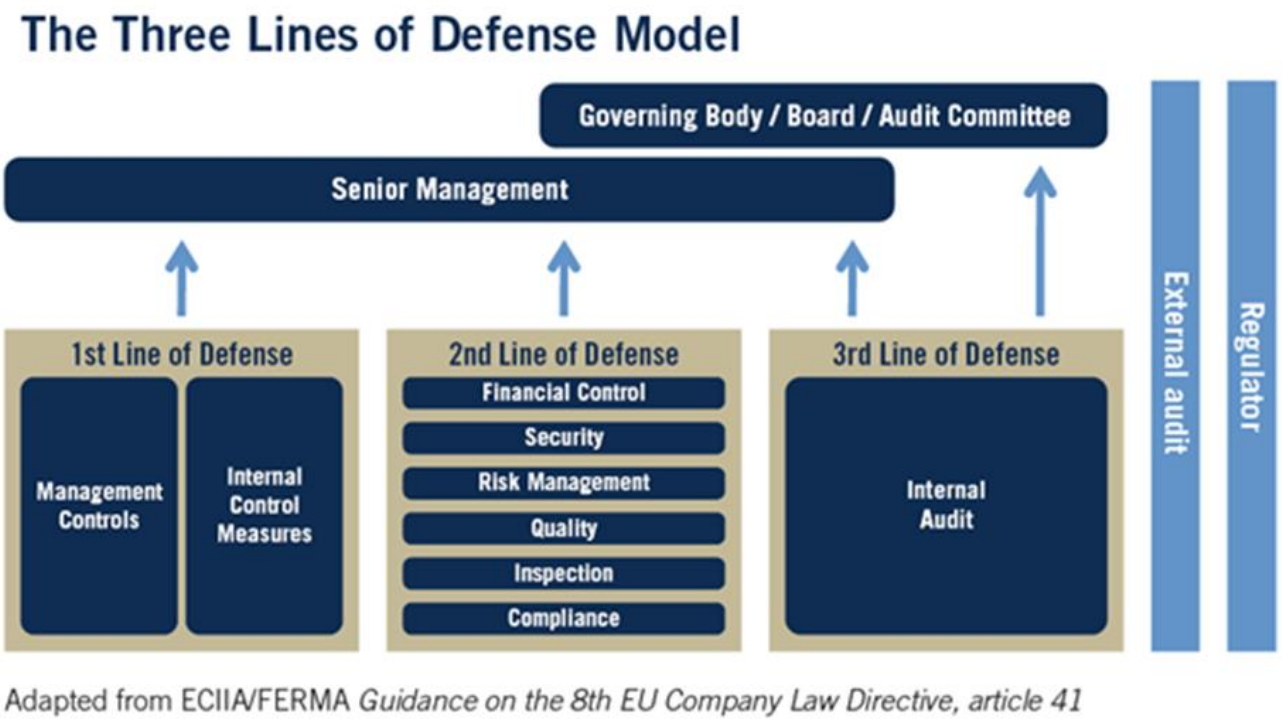
I modellen (se **Figur 1**) præsenteres tre forsvarslinjer, som bidrager med særskilte funktioner og ansvarsområder over for ledelsesorganet. Risikostyringsstrukturen er normalt stærkest, når de tre forsvarslinjer er separate og udtrykkeligt defineret (Basel Comittee 2011). I modellen lægges der dog også vægt på, at linjerne skal samarbejde og dele deres viden på tværs. Herved koordineres arbejdet i de enkelte forsvarslinjer, så der opnås et samlet integreret framework, så funktionerne arbejder sammen i en samlet struktureret risikostyringsproces i organisationen (PwC NL 2017). Gennem vidensdeling og koordination opnås effektivitet og efficiens, men det må naturligvis ikke kompromissere linjernes funktion. Intern revision må eksempelvis ikke medvirke i forretningsmæssige beslutninger, da det kan resultere i selvrevision.

Empirisk undersøgelse

Der er i forbindelse med artiklen udarbejdet en empirisk undersøgelse med grundlag i dybdegående interviews med udvalgte pengeinstitutters revisionschefer, nøglepersoner hos Finanstilsynets afdeling for finansiel rapportering samt formanden for IIA: Kim Stormly Hansen. Der er tillige indhentet spørgeskemadata fra adskillige respondenter med funktioner i 2nd line og 3rd line fordelt på 12 danske mellemstore pengeinstitutter.

Med henblik på at vurdere om pengeinstitutterne har implementeret 3LoD-modellen, er det nødvendigt at præcisere, hvad der forstås ved succesfuld implementering. En række succeskriterier er derfor fastsat med udgangspunkt i den empiriske analyse, der er udarbejdet af Baselkomitéen i 2014 (Basel 2014) samt af det udgivne position paper af IIA (IIA 2013). Nedenstående 5 succes-

Figur 1



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

kriterier er anvendt som et diskuterbart grundlag for vurderingen af en succesfuld implementering.

1) Struktureret risikostyringsproces & aktiv støtte fra ledelsen
Baseret på den empiriske undersøgelse foreligger der generelt stor enighed om, at risikostyringsprocessen i pengeinstitutterne er struktureret. Størstedelen af respondenterne både fra 2nd line og intern revision har tilkendegivet enten "enig" eller "meget enig" til spørgsmålet. Idet det er relevant at opnå en struktureret risikostyringsproces som led i implementeringen af 3LoD, kunne det tyde på, at respondenterne i et vist omfang forsøger at følge modellen, hvad enten de er bekendte med 3LoD eller ej.

2) Klar rapporteringsstruktur
Respondenterne af de fremsendte spørgeskemaer er blevet forespurgt, hvorvidt deres arbejdsopgaver indebærer rapportering til henholdsvis ledelsen og bestyrelsen vedrørende identifikation af kontrolsvagheder eller væsentlige risici.

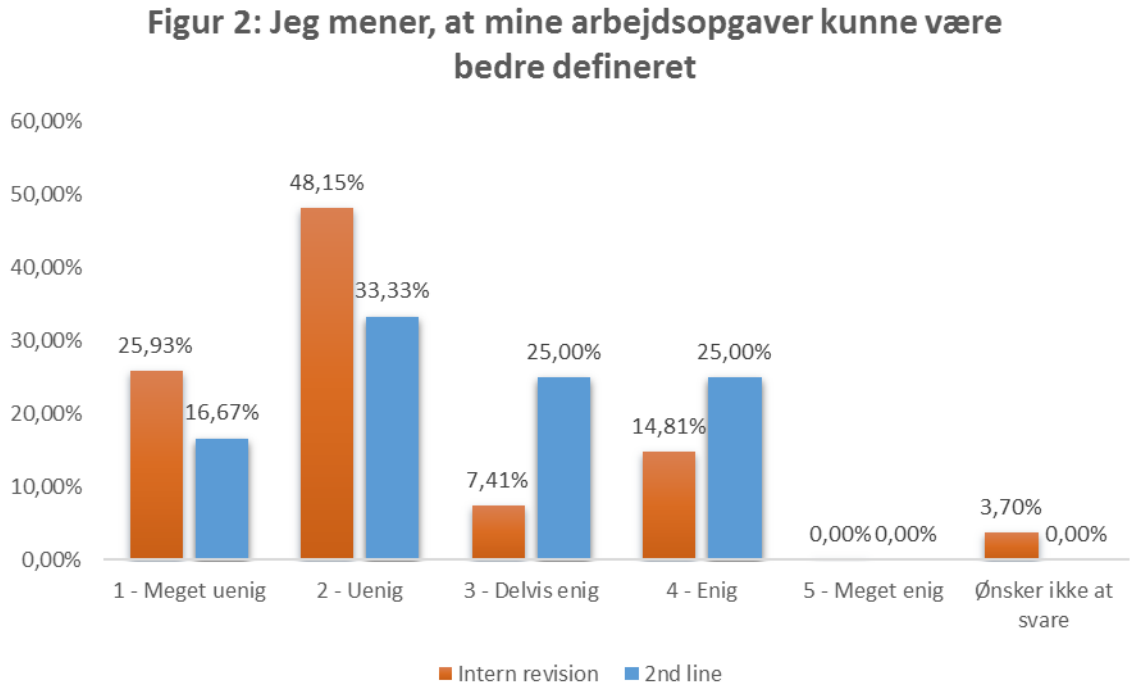
For intern revision er 92,59 % af respondenterne enige i, at der skal rapporteres til ledelsen, og for rapportering til bestyrelsen er andelen heraf 96,30 %.
For 2nd line-funktionen er der ligeledes stor enighed om rapporteringen til ledelsen som en del af arbejdsopgaverne, idet 95,84 % af respondenterne erklærer sig enige eller meget enige heri.

3) Klar ansvarsfordeling
Fordelingen af arbejdsopgaver i organisationen er kun i et begrænset omfang lovreguleret. Af LFV § 71, stk. 1, nr. 1 fremgår det dog, at der skal være en klar organisationsstruktur med en veldefineret og gennemskuelig ansvarsfordeling, for at der er en effektiv form for virksomhedsstyring i de finansielle virksomheder. Endvidere skal der organisatorisk være indrettet enheder med klart definerede arbejdsopgaver, hvortil alle medarbejdere har klare beføjelser, ansvarsområder samt referencelinjer, jf. ledelsesbekendtgørelsens § 9, stk. 1.
Afgørende er det dog, at der tages stilling til ansvarsfordelingen i strukturering af organisationen, samt at der implementeres en række procedurer, som sikrer, at de enkelte risici i virksomheden behandles. Det er således op til virksomheden selv, hvordan denne organisatorisk vil fordele de enkelte ansvarsopgaver.

<u>Klart definerede arbejdsopgaver</u>
Ved forespørgsel omkring spørgeskemarespondenternes egen opfattelse af, om deres arbejdsopgaver er meget klart defineret fremgår det, at respondenterne fra intern revision er 92,6% enige eller meget enige heri, mens samme andel kun er 75 % for 2nd line.

Respondenterne er ligeledes blevet forelagt spørgsmålet, om de mener, arbejdsopgaverne kunne være bedre defineret. Det fremgår af **Figur 2**, at 74,08 % af de interne revisorer mener, at arbejdsopgaverne kunne være bedre defineret, mens det kun er 50 % af de adspurgte i 2nd line.

Ovenstående indikerer i høj grad, at der specielt for 2nd line er et behov i de enkelte pengeinstitutter for, at arbejdsopgaverne præciseres nærmere. Der foreligger alle-



rede en række specificerede arbejdsopgaver og roller for intern revision, hvorfor behovet ikke umiddelbart synes lige så stort for de interne revisorer.

Nedenstående er IIA-formandens fortolkning af en løsning på problemstillingen:

"*Det er vigtigt, der er vejledninger til compliances arbejdsbredde og arbejdsdybde, samt hvad der skal foretages, når de tager stikprøver, og hvilken grad af sikkerhed de skal udtale sig med. Altså meget i relation til de standarder, vi har både i intern og ekstern revision."*

Samme princip vedrørende compliancefunktionens brede rammer kan udledes af Finanstilsynets udtalelser i forbindelse med undersøgelsen:

"Traditionelt har det været meget omkring det her med compliance og intern revision. Det er nok fordi, der er brede rammer for, hvordan man kan sætte compliancefunktioner op".

Dette indikerer derfor et behov for præcisering af 2nd lines arbejdsopgaver, herunder især compliance.

Intet unødvendigt overlap af arbejdsopgaver

Idet 2nd line-funktionen i pengeinstitutterne er blevet udvidet, har instanserne overtaget en stor del af det arbejde, som tidligere har ligget i intern revision. I den forbindelse indikerer en række af interviewrespondenterne, at der i visse tilfælde eksisterer tvivl om hvilke arbejdsopgaver, der skal udføres af de to forsvarslinjer hver især, hvilket blandt andet fremgår af nedenstående citater fra udvalgte respondenter:

"Da der blev oprettet en complianceafdeling første gang for 5-8 år siden, så følte de lige pludselig, at der var to revisionsafdelinger, og det er jo ikke meningen."

"Der har været en tendens til, at intern revision har varetaget alt det her, og i takt med at der er opstået krav til compliance, er der opstået lidt en kamp om, hvem gør hvad, i skal ikke tage vores arbejde osv. Så samarbejdsklimaet har ikke rigtigt været der, og det har skabt en frustration og irritation ude i virksomhederne."

I forlængelse af indførslen af krav om risikostyring og compliance er der ligeledes sket en operationalisering af intern revisions arbejdsopgaver. Der er således tale om en proces, hvor flere kontroller er kommet til, samt skærpede lovgivningskrav, hvilket har medført et behov for, at nogle af intern revisions tidligere opgaver er blevet overført til de nye 2nd line-funktioner.

Overordnet set redegør respondenterne for, at det ikke vil være muligt definitivt at adskille alle arbejdsopgaverne, men at det så vidt muligt forsøges at tilrettelægge revisionerne ud fra, hvad 2nd line-funktionerne kigger på. Dermed er der fokus på at fordele arbejdsopgaverne imellem 2nd line og 3rd line.

En række konkrete eksempler på de tilfælde, respondenterne har forelagt, hvor der kan forekomme dubleringsarbejde, fremgår af nedenstående citater:

"Hvis du ser på en kreditbevilling, så kan den være bevilget af en medarbejder i en filial, kontrolleret af en filialdirektør og måske også kontrolleret af filialcontrolling. Måske kommer 2nd line så og følger op i forhold til, om man er inden for nogle bevillingsbeføjelser eller lignende, og så kan vi komme og revidere engagementet bagefter. Så vi koordinerer det selvfølgelig, så vi har en eller anden fælles holdning til at sige tingene på den samme måde og sikrer, at vi anlægger den samme vurdering."

"Ved revision af fondsafdelingen skal forretningsgangene og kontrollerne revideres, og så har compliance stort set lige været og kigge på handelsmetoder osv., og så har de også kigget på forretningsgange og interne kontroller. Og risiko har måske også været der tidligere og kigget på, hvordan det ser ud i forhold til det operationelle risikobillede. Så det kan hurtigt blive sådan en sammenblanding af, at vi alle render efter den samme bold. Så det skal vi være bedre til at koordinere og øve os på."

Idet det er et krav efter revisionsbekendtgørelsen, at intern revision skal vurdere i hvor høj grad, de kan basere sig på kontrolfunktionens arbejde, er der behov for at kigge ned i 2nd lines arbejde og funktioner. Dermed vil der naturligt forekomme et vist overlap linjerne imellem, men der er således en essentiel forskel på, om 3rd line reperformer 2nd lines testede stikprøver, eller om de selv går ud i 1st line og tester de samme stikprøver.

For at undgå unødvendigt overlap af arbejdsopgaver vil 2nd line med fordel kunne teste de enkelte stikprøver med samme fokus som intern revision, så intern revision undgår at tage fat i de samme stikprøver på et senere tidspunkt. Det kræver dog kommunikation og koordination for, at den enkelte organisation kan rumme både 2nd line og 3rd line som kontrolinstans, hvilket adresseres i nedenstående citat:

"*Det er på mange områder blevet nemmere for intern revision, for vi læner os jo op af det arbejde, der bliver lavet i 2nd line. I forhold til organisationen er der så opstået nogle andre problemer. Vi skal passe på, vi ikke alle [2nd line og 3rd line] kommer rendende lige efter hinanden og skal kontrollere et område. Så man skal være bedre til at koordinere arbejdsopgaverne, hvilket vi øver os på alle sammen, så organisationen også kan rumme os. Det er vigtigt."*

Spørgeskemarespondenterne udbygger ligeledes ovenstående tilkendegivelser fra interviewrespondenterne, som anskuer, at der er plads til forbedring angående dubleringsarbejde - se **Figur 3** på næste side.

Af ovenstående indikeres det, at der foreligger en generel enighed i besvarelserne omkring dubleringsarbejde mellem henholdsvis intern revision og risk management samt intern revision og compliance. Det bemærkelsesværdige er her, at arbejdsopgaverne for disse funktioner er lovreguleret i blandt andet ledelsesbekendtgørelsen og revisi-

onsbekendtgørelsen. Ovenstående indikerer derfor i høj grad samme princip, som kunne udledes af interviewrespondenterne, idet det antydes, at der forekommer et overlap i arbejdsopgaverne mellem 2nd line og 3rd line. Man kan således spekulere i, om samarbejdet fungerer optimalt herimellem. Der skal derfor generelt både være adskilte linjer i organisationen, men der skal ligeledes være en løbende koordinering linjerne imellem, som sikrer, at 2nd line og 3rd line varetager forskellige ansvarsområder for at minimere unødvendigt overlap af arbejdsopgaver.

4) Separate linjer i risikostyringsfunktionen

Det er særligt essentielt, at intern revision bevarer uafhængigheden i forhold til de øvrige funktioner i virksomheden, for at formålet med intern revision opretholdes. Dette opnås derfor umiddelbart nemmest ved separate forsvarslinjer, der i organisationen er adskilt fra hinanden. Af citatet nedenfor adresserer Finanstilsynet problematikken med adskillelsen af linjerne i praksis:

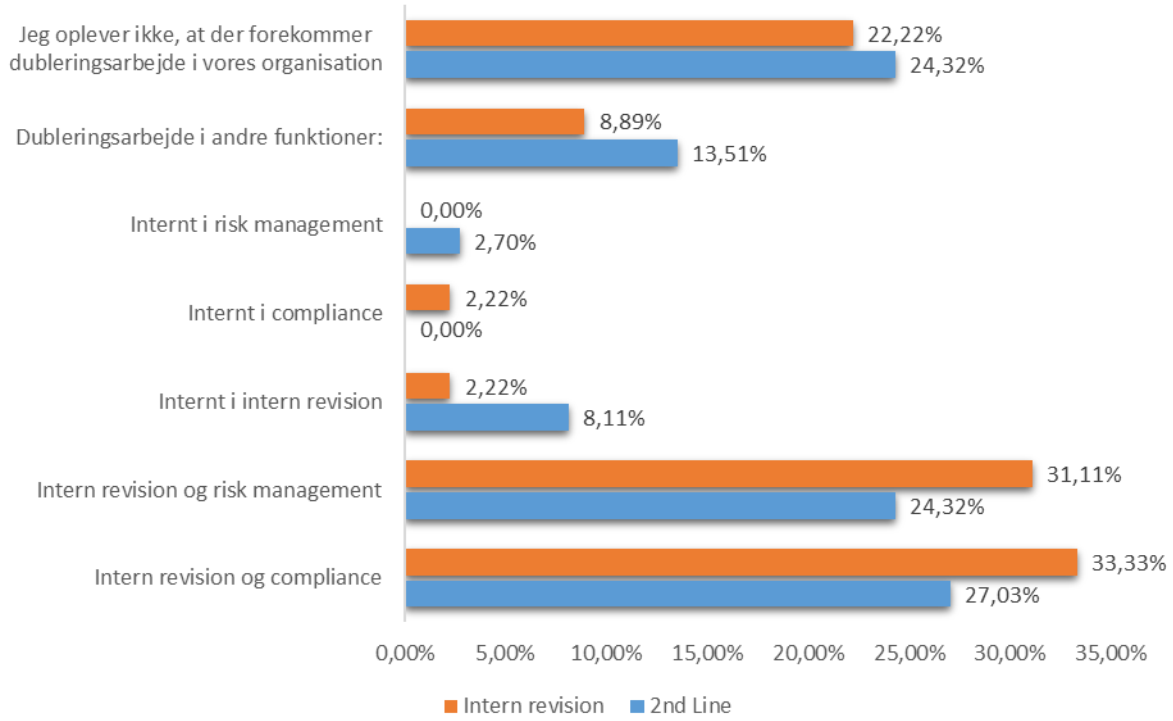
"Modellen er god, men hvis man skal sige noget om modellen i praksis, så er det, at man skal sikre, at der ikke er noget, der falder ned mellem forsvarslinjerne. Vi hører nogle gange nogle ude i praksis beklage sig lidt over, hvor går så snitfladen mellem linjerne. Hvis vi kigger på de her stiplede linjer imellem forsvarslinjerne, så skal de altså være der."

En række interviewrespondenter tilkendegiver, at skillelinjen mellem **1st og 2nd line** ikke organisatorisk er så skarpt defineret. Det kan derfor diskuteres, hvorvidt det er effektivt at forankre både 1st og 2nd line under samme afdeling, hvilket uddybes nedenfor:

"Vi kan ikke altid skelne 1st line og 2nd line ud i særskilte funktioner, som man kan i større banker. Det giver ofte mere gevinst, at dem, der sidder og kigger på markedsrisici og kapital, sidder ved økonomiafdelingen, fordi de skal jo spare med dem. Som revision, mener vi jo, at den 2nd line, som sidder og kontrollerer forretningen, de burde rent organisatorisk ikke være forankret under den samme chef, fordi så kan han jo bestemme, hvad de skal kigge på og ikke skal kigge på. Vi synes bare, det uafhængighedstab er mindre end den gevinst, det har, at de sidder sammen med de folk, som har fingeren på kreditområdet og har den faglige erfaring. Sådan vil det være mange steder, altså det her med, at det ikke er ren kontrol."

Pointen for mindre organisationer ligger altså i, at den gevinst, der ligger i at vidensdele i et tæt samarbejde under den samme chef, vurderes højere end det uafhængighedstab, der foreligger ved ikke at have en særskilt overvågende funktion på for eksempel kredit- eller markedsrisiko. Der er dog enighed omkring det uhensigtsmæssige i at være forankret under den samme ledelse i de to linjer.

Figur 3: I disse arbejdsfunktioner i mellem, mener jeg, der kan forekomme dubleringsarbejde



5) Samarbejde og kommunikation mellem linjerne
Som det forelægges af teorien bag 3LoD-modellen, er det essentielt for den effektive risikostyringsproces, at de enkelte linjer i organisationen samarbejder og kommunikerer med hinanden.

"Jeg tror, det er effektivt, hvis man får et fælles risikounivers. Hvis vi på tværs af organisationen kan definere og blive enige om, hvad risiciene er samt hvilke kontroller, der skal afdække det. Så kunne man altid pege over på de definerede risici og den ensartede forståelse. Men det er rigtig svært at blive enige om det."

Et samlet risikoframework i de enkelte pengeinstitutter vil kræve en aktiv deltagelse af instanserne i virksomheden samt en koordinering af funktioners roller som led i risikouniverset. Det ideelle udgangspunkt er derfor et velfungerende samlet risikoframework (ERM), idet dette vil medføre en effektiv implementering af 3LoD-modellen. En fælles risikostyringsproces skal derfor medføre, at organisationsfunktionerne bidrager til i samspil at identificere, vurdere og mitigere risici. Intern revision må i den forbindelse ikke udføre eller varetage risikobilledet, men de må gerne facilitere processen. Dette uddybes med nedenstående:

"Det er jo også lidt det, vi gør, når vi skal få risikostyringen og 2nd line til at tale sammen. Men generelt er samarbejdet og koordineringen mellem risiko, compliance og 2nd og 3rd line ikke god nok, og der er en stor udvikling med både at få effektiviseret det samarbejde og få defineret snitflader og talt sammen om, hvordan vi gør det her mest effektivt."

Idet behovet for et risikoframework i de enkelte organisationer adresseres, kunne der foreligge en indikation for, at kommunikationen kunne forbedres særligt mellem 2nd og 3rd line. Foruden indarbejdelse af koordineringsmøder med 2nd line indikerer flere respondenter et behov for en fælles rapporteringsform, hvor 2nd lines og 3rd lines vurderinger og konklusioner sammenholdes, idet bestyrelsen så i højere grad vil opleve et samspil i signaler fra organisationslinjerne. Der kan derfor argumenteres for, at et velfungerende ERM giver plads til, at en fælles rapporteringsform skaber værdi i organisationen.

Samme konklusion kan udledes af IIA-formanden ved nedenstående citat:

"At man har et fælles værktøj, et fælles stammesprog og en fælles rapporteringsform; både for compliance og risk management, men også for hele den samlede risikostyring i virksomheden. Det vil helt sikkert gøre det meget nemmere."

Det essentielle er således ikke, hvordan risici identificeres og kategoriseres i den enkelte organisation, men i stedet at der foreligger et fælles framework, som definerer en fælles tilgang.

Konklusion

På baggrund af respondenterne fra både interview- og spørgeskemaundersøgelserne kan det konkluderes, at pengeinstitutternes risikostyring generelt opfattes som værende struktureret, men med plads til optimering. En klar rapporteringsstruktur er vanskelig at vurdere, men respondenterne synes at have en klar forståelse af, hvad der skal rapporteres, samt hvem der skal rapporteres til. Det indikeres dog, at der med fordel kunne indføres en fælles rapporteringsform, hvor 2nd og 3rd line samarbejder om rapportering til ledelse og bestyrelse.

Specificeringen af arbejdsopgaver kan være vanskelig, fordi både 2nd line og 3rd line skal udgøre en kontrolinstans, hvorfor formålet i organisationen kan synes sammenligneligt. Det tilsigtes dog generelt i pengeinstitutterne at minimere omfanget af dubleringsarbejde herimellem, men idet 3rd line tillige skal kontrollere 1st line i organisationerne, vil der naturligt være to instanser, der har fokus på de samme kontroller. I forlængelse heraf kan det konkluderes af flere respondenter fra både 2nd og 3rd line, at der mellem de to funktioner forekommer et overlap af arbejdsopgaver. En af årsagerne hertil forelægges at være 2nd lines arbejdsopgaver, som med fordel kunne defineres bedre.

En række retningslinjer for 2nd line er således beskrevet i ledelsesbekendtgørelsen, men det indikeres, at denne begrebsramme ikke er tilstrækkelig, og at der fra pengeinstitutternes perspektiv er behov for en mere udførlig specifikation heraf. Modsætningsvist tilkendegives det af Finanstilsynet, at der ikke tilsigtes indførelse af yderligere vejledning for 2nd line, idet det er op til organisationerne selv at forme 2nd line samt at implementere 3LoD, så det passer til den konkrete virksomhed.

I relation til ansvars- og arbejdsfordelingen er der således flere indikatorer, der både taler for og imod en succesfuld implementering af 3LoD.

Den organisatoriske adskillelse synes at kunne betvivles mellem 1st og 2nd line, idet medarbejderne kan være forankret i samme afdeling under samme leder, selvom der fortsat består en funktionsmæssig adskillelse. Dette styrker til gengæld det samarbejde og kommunikation linjerne imellem, der tilsigtes for effektivt at implementere 3LoD. Kommunikationen i organisationen synes derfor at udgøre et essentielt kriterium for implementeringen, idet der skal være en skarp adskillelse af linjerne, men med manglende koordination vil der være en betydelig risiko for overlap af arbejdsopgaver. Ligeledes kan der være tvivl om, hvordan risici skal identificeres, måles og fortolkes, hvorfor en ideel løsning kan være et samarbejde i organisationen om kreering af et fælles risikoframework. Dermed tilsigtes en fælles organisationstilgang til hele risikostyringsprocessen, så alle funktioner har et samlet framework at forholde sig til. I den forbindelse vil en fælles rapporteringsform mellem 2nd og 3rd line ligeledes kunne bidrage til at samarbejde på tværs af forsvarslinjerne. Det kan således konkluderes, at der af flere respondenter tilkendegives at være plads til forbed-

ringer vedrørende det stærke samarbejde og koordineringen af et fælles risikoframework.

Reflektioner på baggrund af den empiriske undersøgelse

For at løse problemstillingen med tilrettelæggelse af 2nd line-funktionen, så der opnås et fælles organisatorisk risikoframework, indikeres det af den empiriske undersøgelse, at der er behov for en fælles vejledning med 2nd line funktioner i højsædet.

Et lignende værktøj er allerede tilrettelagt af IIA i Norge, hvorfor man med fordel kunne drage nytte heraf i Danmark. IIA Norge har udarbejdet best practice-vejledninger både for risikostyringsfunktionerne (IIA Norge 2017) og compliancefunktionerne (IIA Norge 2015) med henblik på at beskrive funktionen og arbejdsopgaverne for 2nd line både i ERM-sammenhæng samt i 3LoD. Der er tale om nyligt publicerede vejledninger i 2015-2017, hvorfor man de seneste år er begyndt at adressere problemstillingen samt fokusere på mulige tiltag til en løsning i Danmark.

Kildefortegnelse:

Basel Comittee 2014, Review of the Principles for the Sound management of Operational Risk (Basel Comittee on Banking Supervision), Bank for International Settlements.
Basel Comittee 2011, Principles for the sound Management of Operational Risk (Basel Comittee on Banking Supervision), Bank for International Settlements.
EY 2013, Maximizing value from your lines of defense, a pragmatic approach to establishing and optimizing your LOD model., EY.
IIA, 2013, POSITION PAPER: THE THREE LINES OF DEFENSE IN EFFECTIVE RISK MANAGEMENT AND CONTROL. Available: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdfJanuary].
IIA Norge 2017, Guidelines for the Risk Management Function, IIA Norge.
IIA Norge 2017, Guidelines for the Compliance Function, IIA Norge.
PwC NL 2017, The three lines of defense model of tomorrow, PwC NL

Lovgivning:

Bekendtgørelsen om ledelse og styring af pengeinstitutter m.fl. (BEK nr 1026 af 30/06/2016)

Bekendtgørelse om lov om finansiel virksomhed (LBK nr 1140 af 26/09/2017)

Bekendtgørelse om opgørelse af risikoeksponeringer, kapitalgrundlag og solvensbehov (BEK nr 295 af 27/03/2014)

Bekendtgørelse om revisionens gennemførsel i finansielle virksomheder m.v. samt finansielle koncerner (BEK nr 1912 af 22/12/2015)

Europa-Parlamentets og rådets direktiv 2013/36/EU af 25. juni 2013. Om adgang til at udøve virksomhed som kreditinstitut og om tilsyn med kreditinstitutter og investeringsselskaber, om ændring af direktiv 2002/87/EF og om ophævelse af direktiv 2006/48/EF og 2006/49/EF.

Europa-Parlamentets og rådets forordning (EU) nr.575/2013 af 26. juni 2013. Om tilsynsmæssige krav til kreditinstitutter og investeringsselskaber og om ændring af forordning (EU) nr. 648/2012.

GRC-teknologi: Risikostyring på tværs af forsvarslinjer

Benjamin Vanggaard, GRC-P, CCSA, Internal Audit Practitioner Manager, Risk Advisory (GRC), Deloitte

Denne artikel omhandler intern revisions deltagelse i forretningstransformationer, som har betydning for forsvarslinjerne virke; herunder såkaldte "Governance, Risk and Compliance (GRC)"-transformationer. GRC-transformationer et godt eksempel på, hvordan intern revision kan yde forretningsmæssig rådgivning uden nødvendigvis at gå på kompromis med uafhængighed og objektivitet.

Indledning

I april '18 skrev jeg et indlæg i INFO (#68) som omhandlede det opdaterede COSO ERM 17 rammeværkets øgede fokus på sammenhængen mellem risikostyring og forretningsmål. Jeg konkluderede følgende vedr. intern revision:

- Ledelsen har forventninger om et stigende fokus på konsulentydelser fra intern revision for at levere værdi
- Intern revision bør arbejde med at lukke de eksisterende kompetencemangler indenfor dataanalyse, forandringsledelse, teknisk viden (fx. GRC-værktøjer) og forretningsstrategi
- Intern revision bør i stigende grad drive/anbefale tekniske værktøjer for at bidrage til virksomhedens modenhedsrejse inden for integreret risikostyring

Ændringen i det ledende rammeværk for risikostyring og ovenstående trends har medført et øget fokus fra bestyrelseslokalerne på udfordringerne på tværs af forsvarslinjerne imod en integreret risikostyring og et ønske om at få del i de forretningsmæssige fordele som dette medfører.

Et af de områder som jeg ser som afgørende for at opnå en integreret risikostyring er implementering af GRC-systemer, som er software til understøttelse af arbejdet på tværs af forsvarslinjerne. Intern revision har i denne sammenhæng en unik mulighed for at bidrage med sin ekspertise.

En nyere undersøgelse fra OCEG[1] viser, at det i 46% af tilfældene i undersøgelsen er intern revision, der driver og influerer GRC-værktøjer i virksomhederne. Intern revision har således allerede i flere virksomheder drevet opstarten af GRC-rejsen med en business case igennem facilitering af forretningskrav, leverandørvalg – herunder forslag til kontraktindhold – samt risikovurderinger ift. det eksisterende IT-landskab. Samme undersøgelse viser også, at det kun er i få tilfælde at beslutningen om køb ligger hos IA (beslutningskompetencen).

Jeg vil i denne artikel belyse hovedelementerne i GRC-transformationen og intern revisions rolle heri. *Først* vil jeg tage jer igennem motivationen for at indføre GRC-systemer i virksomheden, således at business case og sammenhængen til intern revisions bidrag fremstår klart.

Dernæst vil jeg kort gennemgå den rejse som virksomheden må gennemgå for at opnå de gevinster, der er ved at indføre GRC værktøjer. Her bliver det tydeligt at GRC -værktøjer ikke kan stå alene i en forretningstransformation, men at styringsstrukturen, medarbejdere og processer også må geares igennem det organisatoriske design. Ud fra et sparringsmæssigt perspektiv, har intern revision en foranderlig rolle over tid som tager hensyn til virksomhedens modenhed indenfor GRC.

Herefter vil jeg beskrive de komponenter, som et typisk GRC-system består af for at give den praktiske referenceramme. Ikke overraskende har intern revision typisk deres eget domæne i værktøjet, som giver adgang til en dynamisk og risikobaseret revisionstilgang ved at give fuld indsigt i forsvarslinjernes arbejde.

Slutteligt vil jeg belyse den potentielle uafhængighedskonflikt, der er ved at intern revision involverer sig i rådgivning og implementering.

Motivationen for at indføre GRC-systemer

Implementering af GRC-værktøjer giver fordele på tværs af forsvarslinjerne. For forretningen optimeres forretningens målopfyldelse via systematisk tilgang til risikostyring og omkostningerne i forbindelse hermed nedbringes. For intern revision (og øvrige assurance-leverandører) effektiviseres revisionstilgangen via effektiv monitorering af såvel første som anden forsvarslinje (continuous auditing). **Se Tabel 1** på næste side for en detaljeret gennemgang af fordelene.

Disse fordele er med til at drive efterspørgslen for GRC-systemer og intern revisions tværfaglige kompetencer inden for det fulde spektrum af GRC.

Med motivationen på plads vil jeg nu skitsere den rejse, som virksomheden skal starte for at opnå de fulde forretningsmæssige fordele af GRC transformationen.

Forventninger til intern revision i rejsen mod integreret risikostyring

I Deloitte arbejder vi med et modenhedskoncept som udtryk for den tranformation, de fleste virksomheder skal igennem for at få det maksimale udbytte af GRC-relaterede investeringer. Forventningerne til intern revision varierer afhængig af virksomhedens aktuelle GRC-modenhed.

Tabel 1

Kategori	Formål	Påvirkning	Operationalisering
Forretnings-mæssige fordele	Øget (forretnings-) målopfyldelse (enhanced assurance)	Øget indsigt for ledelsen	Ledelsen har mulighed for at følge risikoafdækning, registrerede incidents og kontrolmiljøet ved have dashboards der viser data på tværs af modulerne (GRC modulerne gennemgås i senere afsnit).
		Koordinering mellem forsvarslinjerne (end-to-end perspektiv på risici og kontroller)	Integration af forsvarslinjer på tværs af domæner og afdelinger Rapporter og drill-down muligheder (one source of the thruth)
		Ensretning af processer	Indbyggede workflows (eksempelvis schedulerede test af kontroller, incident management (afvigelseshåndtering) og eskalering)
		Udnyttelse af specialisering i forsvarslinjerne (uden at miste integrationen)	ERM, Internal Control, Compliance og Internal Audit er styret i respektive moduler, i en integreret løsning, som sikrer optimal udnyttelse af kompetencer på tværs af domænerne
		Mulighed for rationalisering optimering af kontroller (nedbrydning af siloer)	Rationalisering og transformering af kontroller imod flere forebyggende kontroller og IT kontroller igennem **Continous Control Monitoring (CCM)** Centralisering af kontroller og ensretning af taxonomi "one language of GRC" samt afløftning af "byrder" fra decentrale enheder igennem shared-assurance i systemet
		Dele assurance på tværs af reguleringer/rammeværk	Systemet kan indeholde flere reguleringer (eksempelvis GDPR, Tax Control Framework). De samme kontroller kan mappes op imod flere rammeværk, hvilket gør det muligt at rapportere på specifikke rammeværk. Derved bliver det muligt at anvendte den samme assurance på tværs (adressere risk over financial reporting, tax og GDPR). Funktionaliteten gør det muligt at skalere kontrolapparatet på nye reguleringer.
	Nedbringelse af omkostningerne ved styring (reduce cost of controls)	Øget grad af automatisering af kontroller (forebyggende/IT i stedet for manuelle) igennem GRC-værktøjets mulighed for CCM (Continues Control Monitoring)	Igennem multipel system integration, kan værktøjet hente data fra flere datakilder og foretage aftestning. Herudover kan CCM lytte på data i systemer og rapportere ved ændringer (f.eks. kritiske felter i et ERP-system). CCM giver mulighed for at automatisere kontrollere, enten fuldt eller semi-automatisk.
		GRC-værktøjets mulighed for at arbejde undtagelses fokuseret	Som følge af CCM og testresultater kan der effektiv identificeres "fail"-results og derved kan indsatsen koncentreres omkring disse. Funktionelt løses dette igennem Issue management og eskalering.
Muligheder for Intern Revision	Effektivisering af revisions tilgangen (continuous auditing)	Dynamisk risikobaseret revisionstilgang	Risikovurdering (ERM) kræver opdateret Interne kontroller (IC) og en faciliteteret IA ændret revisionstilgang. Toolet kan til enhver tid identificere
		Dele viden og understøtte en lærende organisation	Virksomheden kan identificere og udpege "best-practice" igennem værktøjet. F.eks. kan arbejdspapirer og revisionsprogrammer genbruges og opdatere "bagkataloget".
		Standardisering og effektivisering af revisions tilgang	Systemet kan definerer standard revisionsprogrammer eller skabeloner som kan genbruges og opdateres centralt.
	Øget indsigt/ monitorering af første og anden forsvarslinje	Transparens I forsvarslinjernes arbejde og opfølgning	IA har mulighed for at trække rapporter på tværs af modulerne; eksempelvis opfølgning på undtagelser/afvigelser, opdateret risiko landskab, testresultater og kommentarer mv.

For virksomheder hvor rejsen netop er begyndt, forventes det at intern revision bidrager særligt med struktur og faglig sparring til første- og anden forsvarslinje for at løfte virksomheden til at være organiseret. Intern revision er ofte den eneste funktion, der har indsigt på tværs af forretningen og den dybe forståelse for risici med hands-on erfaring igennem test og rådgivning i de enkelte funktioner.

Når virksomheden modnes og bevæger sig imod en integreret risikostyring drevet af GRC-teknologi, hvor afdelinger arbejder sammen omkring de samme identificerede risici, forventes det at intern revision bidrager med at føre funktionerne yderligere sammen igennem en dybere faglighed og indspark omkring operationalisering af denne opgave.

GRC-løsningens byggesten og sammenhæng til forsvarslinjerne

GRC-systemer består typisk følgende moduler, som alle indeholder særegne funktionaliteter og understøtter GRC-processerne:

- Risk Management
- Internal Controls
- Compliance Management
- Internal Audit
- IT-GRC

Selvom modulerne måske syntes selvforklarende af navnene, vil jeg dog alligevel knytte et par ord til de mest relevante:

Risk Management hjælper med at identificere, kvantificere og kortlægge virksomhedens svar på risici (langt hen af vejen er dette et ERM-modul). Det er altså på mange måder et "start-modul". De registrerede risici og den løbende opdatering af risikobilledet anvendes i de øvrige moduler. Fokus har over de senere år rettet sig langt mere imod operationelle risici, og væk fra risici forbundet med (finansiel) rapportering.

Internal Control (IC) hjælper med at operationalisere det interne kontrolværk på tværs af *reguleringer* – grupperinger ift. relevans - (f.eks. ÅRL, IFRS, SOX, GDPR, Tax Control Framework, operationelle risici mv.). Således kan de samme kontroller benyttes på tværs. Modulet linker risici og kontroller til processer, stiller testresultater af kontroller til rådighed, registrerer afvigelser (fejlede kontroller) og håndterer registrering og behandling af uønskede hændelser. Under hele forløbet er der transparens for relevante interessenter om fremdrift, resultat, dokumentation og historik. Modulet tilbyder fleksibel og avanceret rapportering med mulighed for drill-down i de relevante dimensioner. *Et helt afgørende punkt for IC-modulet er muligheden for kontinuerlig kontrol monitorering/test.* Denne funktionalitet sætter GRC-systemet i stand til at "lytte" på forandringer i systemer (f.eks kritiske felter/konfiguration) og automatisere eller semi-automatisere manuelle kontroller (på tværs af kildesystemer). Funktionaliteten muliggøres ved at modulet indhenter flere datakilder (ikke kun ERP) og laver kontinuerlig integritets-test på data, baseret på forretningsregler (logi).

Compliance Management behandler udfordringen med styring og implementering af dirigerende kontroller, eksksempelvis politikker, som har til formål at fremme en ønsket adfærd og kultur for at nå en højere grad af målopfyldelse. Sign-off af politikker, styring af awareness -kampagner og registrering af brugerinput ift. surveys er eksempler på funktionalitet. Modulet giver f.eks. indsigt i *graden af compliance* på tværs af enheder, og er organisationens mulighed for positivt at kunne dokumentere kommunikation og awareness til medarbejderne i organisationen.

Internal Audit giver indsigt i første og andens forsvarslinjes risikohåndtering og adressering samt testresultater på tværs af modulerne. Revisionsprocessen kan dermed blive dynamisk og tilpasset udviklingen i virksomhedens risikolandskab og testresultater, som løbende registreres igennem Risiko-modulet. Derved undgår man (ofte) ukurante revisionsplaner, som ikke nødvendigvis prioriterer virksomhedens væsentligste risici til enhver tid. Modulet tilbyder en metodisk tilgang til revisionsprocessen; periodisk planlægning, herunder booking af kvalificerede ressourcer, valg af scope og formulering af arbejdsprogrammer. Observationer og findings under udførelsen kan registreres, rapporteres og arkiveres (med øvrige engagements). Modulet tilsikrer konsistent praksis med høj kvalitet på tværs af revisionsopgaver.

Den potentielle uafhængighedskonflikt

På trods af fordelene ved at intern revision involverer sig i GRC-transformationer, kan en sådan beslutning vække undren med henvisning til brud på uafhængighed og objektivitet, jf. IPPF Attribute Standard 1100). På trods af dette er det imidlertid min holdning, at det er en fordel, hvis Intern revision driver faciliteringen, da det åbner mulighed for at få trukket forsvarslinjerne op og revurdere samt tydeliggøre roller og ansvar på tværs. Dette vil samtidig åbne muligheden for at få designet systemet optimalt til intern revisions opgaver.

Det skaber selvfølgelig nogle udfordringer for intern revision, når der på den ene side forventes rådgivningsydelser fra ledelsen men på den anden side forventes revisionsydelser fra bestyrelsen (IPPF Attribute Standard 1130.A3); navnlig vil der være tale om truslen om selvrevision og bias.

Med opdatering af IPPF i 2015 kom IPPF Attribute Standard 1112 vedrørende revisionschefens opgaver uden for selve revisionsopgaven. Her fremgår kort, at der i sådanne tilfælde skal implementeres de nødvendige safeguards for at undgå en uafhængighedskonflikt. Eksempler på Safe-guards i GRC-implementeringer inkluderer:

- Intern revision begrænser sig til at have en faciliterende SME-rolle og rådgiver omkring funktionaliteter såsom framework implementering, workflow og rap-

portering. Hovedformålet er at komme rundt om værktøjets fulde potentiale.

- Intern revision tager ikke ledelsesmæssige beslutninger (f.eks. designer ikke kontroller eller øvrige interne kontrolaktiviteter og dermed påtager sig ledelsesmæssige ansvar, med risiko for efterfølgende selvrevision).
- Intern revision indgår som deltager i en projektstruktur ledet af forretningen

Under hensynstagen til sådanne safe-guards bør det være muligt at udbytte af intern revisions involvering i GRC transformation og dermed høste alle fordelene af integreret risikostyring på tværs af forsvarslinjer uden at gå på kompromis med standarder for uafhængighed og objektivitet.

Noter

[1]OCEG: 2019 GRC Technology Strategy "Findings of the 2019 OCEG GRC Technology Strategy Survey"


CROWNE PLAZA
IIA Årsmøde 2019
Afholdes
15.5.2019-16.5.2019
på Hotel Crowne Plaza
København
Tilmeld dig på
www.iia.dk
D I

Agile auditing

Beate Sætre, Deloitte

Snezana Janjic, Manager, Deloitte

Indledning

Intern revision som profession bliver regelmæssigt udfordret på at skulle skabe mere værdi, samtidig med at Intern Revision ofte skal kæmpe for sin eksistensberettigelse i organisationen. Interessenter kræver effektivitet i det arbejde intern revision bidrager med, bedre rådgivning omkring processer og kontroller, større grad af indsigt, tydeligere stillingtagen til findings og en bedre forståelse af det fremtidige risikolandskab samtidig med, at der er en forventning om, at der skal kunne ageres hurtigt og fleksibelt. Med andre ord, omgivelserne har hele tiden nye og øgede krav til intern revisions rolle, hvilket kræver at professionen er forandringsvillig, og forandrer sig i takt med at nye forventninger opstår.

Dette har medført et behov for en revisionsmetode, som er mere fleksibel i sin tilgang, og dermed kan imødekomme disse forventninger.

Agile auditing er en af de metoder, som er mest anvendelig for at imødekomme de aktuelle udfordringer og forandringer.

Hvad er Agile auditing?

Den agile tilgang til projektledelse og projektarbejde generelt har sin oprindelse i softwareudvikling. I dag ser vi dog at metoden bruges bredt i flere brancher og professioner, heriblandt af intern revision. Metodens hensigt er at reducere omkostninger og tid, samtidig med at kvaliteten i det udførte arbejde øges. Da parametrene tid, omkostninger og kvalitet sjældent er til forhandling, er den eneste parameter der kan skrues på vores fremgangsmåde, dvs. måden hvorpå målet skal nås. Hvor man historisk i interne revisionsafdelinger har udarbejdet en revisionsplan for typisk et år ad gangen, er Agile metoden yderligere kendetegnet ved et projektforløb, der er opdelt i flere korte perioder, eller 'iterations', og en større grad af involvering, således at forventninger og krav hele tiden kan redefineres, både i vores korte- og langsigtede planer.

Agile auditing tillader derfor:

- Løbende tilpasning efter interessenternes behov
- Acceleration i revisionsprocessen
- At give rettidig indsigt
- Reduktion i overflødigt arbejde
- Generering af mindre dokumentation

Agile auditing metoden ønsker ikke kun at ændre revisionsprocessen og projektløsningen, men også at ændre vores mindset, dvs. at Agile auditing skal bidrage til revisioner med et tydeligere resultat. I modsætning til revisioner der baserer sig på open-ended reviews eller oplistning af fejl, ønsker vi med Agile auditing at bekræfte eller afkræfte en hypotese eller understøtte et synspunkt (et skifte i tankegangen). På den måde styres revisionens formål, hvilket igen guider arbejdsgangen og rapporteringen (et skifte i proces).

Agile auditing bygger på et tættere, og hyppigere, samarbejde med Intern Revisions interessenter. Løbende identificeres nye prioriteringer, nødvendige ressourcer og forretningsmæssige behov og risici.

Et yderligere fokusområde i Agile auditing er at generere mindre dokumentation end vi hidtil har været vant til da kommunikationen omkring fremdrift i revisionerne løbende rapporteres, således at man ikke skal vente på at revisionen afsluttes førend resultater kan kommunikeres ud i organisationen. Tiden skal således ikke bruges på lange beskrivelser af hvert enkelt skridt af revisionsprocessen, men fokus skal hellere være på hyppigere rapportering således at forretningen gøres i stand til at træffe beslutninger rettidigt.

De fire nøgleelementer i Agile audting

Agile auditing metoden ligger op til mange tekniske detaljer hvorfor vi i Deloitte har defineret fire overordnede elementer, der er vigtige at forstå for at kunne implementere Agile auditing tankegangen:

Audit backlog - Agile revisioner skal operere med en 'backlog', dvs. en liste over de områder der skal revideres som løbende kan og skal opdateres. Listens elementer kan i begyndelsen være vage og mangle detaljer, men med tiden, hvor revisorer og interessenter definerer og præciserer disse detaljer, vil elementerne bevæge sig op og ned på listen ift. væsentlighed frem til at revisionen kan påbegyndes.

Definition of ready (DoR) – et område fra backlog'en anses som klar når intern revisor og de implicerede interessenter bliver enige om hvad der skal testes eller reviewes, og formål med opgaven defineres. Endvidere skal også intern revisions funktionen have de nødvendige ressourcer. Når et element er DoR, kan selve revisionsarbejdet påbegyndes.

Sprints – Når revisionen starter, rykkes elementet fra backlog'en. Det arbejde der skal gennemføres opdeles i sprints. Et sprint defineres som en tidsbestemt periode

hvor specifikke opgaver skal gennemføres. Den fastsatte tidsperiode skal motivere revisionsteamet til at arbejde med kortere deadlines, men uden at stresse ressourcerne - se **Figur 1** nederst på siden.

Definition of done (DoD) – DoD definerer den værdi der skal leveres i løbet af en sprint. En DoD kan for eksempel være en bestemt grad af sikkerhed, udvalgte færdiggjorte opgaver eller en rapport. Det er vigtigt at en DoD ikke er meget kompleks eller tidstung, da dette ikke kan forenes med definitionen af et sprint.

Disse elementer i revisionsmetodikken skal bidrage til strukturering af revisionsaktiviteter og tid på en måde, der tillader løbende ændringer i retning og ressourcer i takt med, at man bliver klogere. Dette er derfor en praktisk måde at strukturerer en revision på, da man ved den Agile revisionsmetode sjældent vil kende det endelige mål ved revisionens start.

Hvordan kommer man i gang med Agile auditing?

Som med langt de fleste metodologier skal man også her erkende at ikke alle organisationer er ens, og at Agile auditing metoden derfor skal tilpasses for at sikre en succesfuld implementering. Der er flere forskellige måder hvorpå metodikken kan opbygges, og Agile auditing bygger ofte på Scrum[1], men også andre velkendte metoder kan anvendes såsom Lean og Kanban. Det vigtigste er dog, at man vælger én metode og holder sig til denne for at sikre kontinuitet.

Først og fremmest skal man definere hvordan Agile auditing skal se ud i den pågældende organisation ved at udarbejde et manifest. Det skal overvejes, hvilke udfordringer organisationen står ovenfor, og på baggrund heraf skal man definere, hvad der er need-to-have og hvad der er nice-to-have, og reflektere over den overordnede målsætning man vil opnå i sin interne revisionsafdeling. Det udarbejdede manifest som et strategisk dokument skal herefter bruges som grundlag for diskussioner med ledelsen.

Resultatet ved brugen af Agile auditing metoden afhænger stærkt af ledelsen i den interne revisionsafdeling, audit committee, og andre ledere i og omkring virksomheden og deres opbakning.

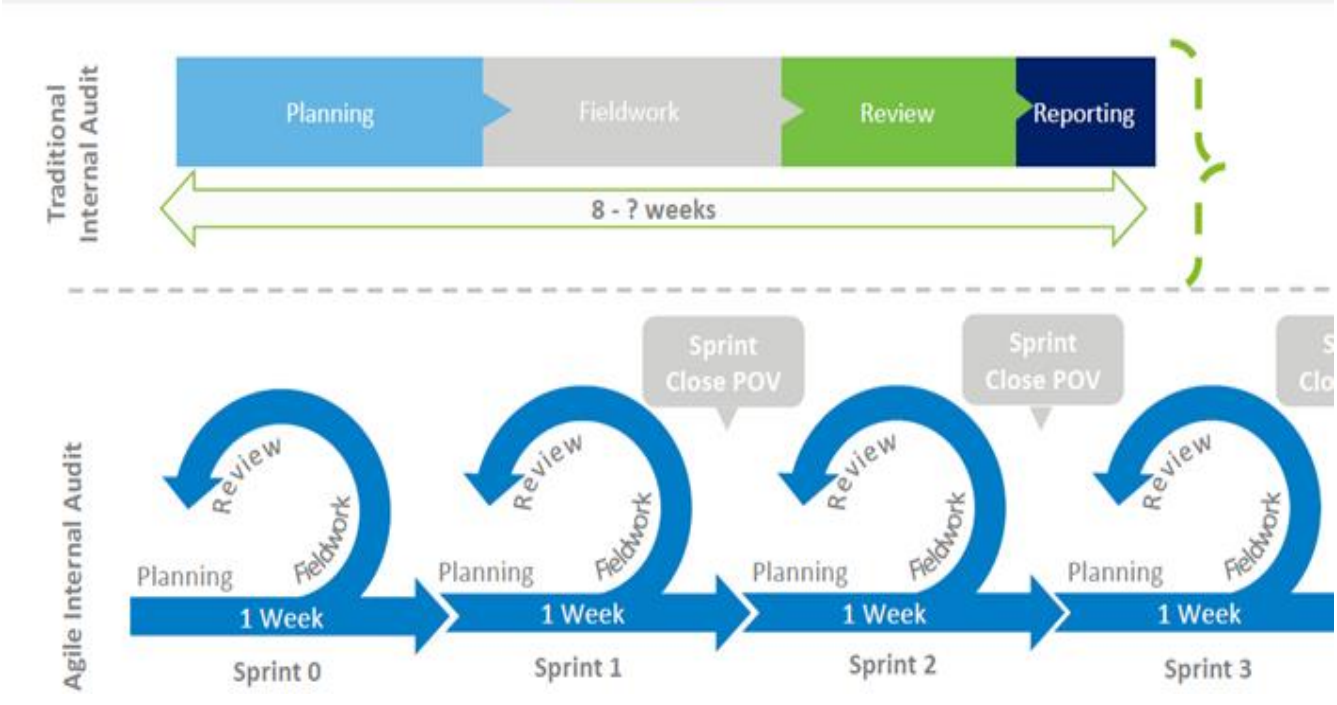
Hvad kræves af revisionsteamet for at være Agile?

Det anvendes tre forskellige rollebeskrivelser i et Agilt revisionsteam:

- Audit Product Owner,
- Audit Scrum Master og
- Core Audit Team.

Audit Product Owner – den person der skal oversætte revisions formål til forretningsmæssige mål, og sørge for at teamet skaber og udfører arbejdet så det opfylder revisionens vision og målsætning.

Figur 1



Audit Scrum Master – den person der sørger for fremgang i arbejdsprocessen, samtidig med at han/hun løser de aktuelle hindringer for teamet i løbet af et sprint. En Audit Scrum Master skal også sørge for at processen løbende forbedres, og følge op på at den aftalte proces overholdes.

Core Audit Team – den/de udførende personer. Deres rolle er at teste, dokumentere og rapportere som aftalt i løbet af hvert sprint.

Agile revisionsteams skal i højere grad have en tværfunktionel opbygning for at sikre større grad af faglighed. Samtidig kræves det at man kan etablere stabile teams, der arbejder sammen tilnærmelsesvist fuld tid, for at yde bedst muligt. Dette stiller således krav til kompetenceniveauet hos den enkelte medarbejder i interne revisioner, idet den enkelte vil have en større indflydelse på hvilken retning revisionen bevæger sig i, hvad der anses som det væsentligste ud fra en risikobaseret tilgang samt, hvilken grad af sikkerhed den interne revisionsfunktion skal yde til sine interessenter.

Til trods for at overvejelserne omkring implementering af en Agile auditing metode er mange og skal alignes igennem hele organisationen, er denne metode kommet for af blive. Dette vil i fremtiden bidrage til at interne revisionsfunktioner i højere grad kan forsvare deres eksistensberettigelse, og bringe den nødvendige rådgivning og overbevisning (assurance) til deres interessenter også i et miljø hvor stadig er et stadigt større pres på ressourcerne. Generelt oplever mange revisionsafdelinger en nedgang i ressourcerne samtidig med at forventningerne fra interessenter er stadigt stigende ift. rådgivning, revisionsoverbevisning og viden omkring fremtiden. Derfor er der behov for denne revisionsmetode, der gør interne revision mere effektiv.

Mange af de virksomheder, der har implementeret Agile audting, tilkendegiver, at have oplevet en øget effektivitet i deres arbejde, hvilket ligeledes har haft en positiv effekt på deres medarbejdere. Agile auditing involverer i højere grad medarbejderne, og giver dem et større ansvar, hvilket ofte fører til et større engagement og effektivitet, og er ligeledes en god måde at benytte al den viden den enkelte medarbejder besidder. Derfor har interne revisionsafdelinger der praktiserer Agile auditing også haft nemmere ved både at tiltrække og beholde talenter.

Med disse ord kan vi opfordre til at man begynder at overvejer den Agile tankegang i revisionsfunktionerne fremadrettet.

Noter

[1] Scrum er en agil metode som hviler på et sæt af agile principper og hvor fremgangsmåden er baseret på en trinvis og iterativ tilgang. Daglig skal teamet afholde et standup møde for at drøfte; "Hvad lavede jeg i går", "Hvad skal jeg lave i dag" og "Er der noget der forhindrer mig i at komme videre" – for på den måde at sikre fremgang.

Center for Cybersikkerheds forebyggende rådgivning og vejledning af virksomheder og myndigheder

Thomas Lund-Sørensen, chef for Center for Cybersikkerhed

Indledning

Center for Cybersikkerhed (CFCS) er nationalt kompetencecenter og har dermed påtaget sig en ledende rolle for at sætte varigt og konstruktivt præg på Danmarks indsats mod cyberangreb. Centerets trusselsvurderinger peger på, at cybertruslen mod Danmark er meget høj, og det vil den forblive et godt stykke tid. Der er derfor brug for at vi alle, virksomheder, myndigheder og os som borgere, forholder os til den nye virkelighed. I CFCS yder vi rådgivning og vejledning inden for alle relevante cybersikkerhedsområder til samfundsvigtige virksomheder og myndigheder.

En essentiel del af dette arbejde er de it-sikkerhedsvejledninger, som CFCS udgiver. Selvom CFCS har en særlig opgave med at rådgive de samfundsvigtige sektorer – energi, sundhed, transport, finans, tele og søfart – så er vejledningerne beregnet til at kunne bruges af alle myndigheder og virksomheder i Danmark som hjælp til arbejdet med at opnå et højt grundlæggende sikkerhedsniveau, som hjælper med at ruste samfundet til at modstå cybertruslerne. Vejledningerne kan være særligt interessante for interne og eksterne revisorer, for de peger typisk på områder, hvor virksomhederne med en rimelig indsats kan styrke cybersikkerheden væsentligt på en målbar facon.

Risikovurdering

En vejledning fra CFCS skal opfylde et behov. Vi arbejder med at opbygge en portefølje af vejledninger af høj kvalitet, som dækker over de fleste emner inden for domænet cybersikkerhed og bygger på CFCS' særlige viden og kompetencer. Cybersikkerhed er et stort område, som spænder bredt over vidt forskellige aspekter. Det betyder for eksempel, at når vi udgiver en vejledning om sikker brug af mobiltelefoner, så dækker det over et problemfelt, hvor man bliver i stand til at kunne tage stilling til, hvad man som enkeltperson kan gøre for at undgå at miste data der er værdifulde for én selv – som for eksempel billeder af familien – og hvad en arbejdsgiver kan og i visse tilfælde skal gøre for at sikre, at forretningshemmeligheder ikke falder i de forkerte hænder hvis en medarbejder får stjålet sin telefon. De to behov kan være i konflikt med hinanden, og der er ikke altid en entydig teknisk løsning, som passer til alle situationer. Derfor er en risikovurdering, der er nøje afstemt efter situationen, helt central i arbejdet med cybersikkerhed.

Vi arbejder nu med en model for vores vejledninger, hvor vi kommer med tre niveauer for hver anbefaling: God, bedre og bedst. Det kan bruges sådan, at man ud fra en risikovurdering vælger, hvilket niveau for den enkelte anbefaling, der er nødvendigt for at imødegå den risiko, man står over for. Det er en vigtig øvelse, uanset om man vurderer, at 'god' er tilstrækkeligt eller man finder ud af, at man har behov for at vælge anbefalingerne på niveauet 'bedst'. Vores inddeling i niveauer skal støtte organisationerne i at arbejde frem mod at forbedre deres sikkerhed, og modellen giver et godt udgangspunkt for at måle, om man har nået det ønskede sikkerhedsniveau.

Risikovurderingen er individuel for den enkelte organisation. Et udgangspunkt for at lave en risikovurdering kan være de trusselsvurderinger, der er en væsentlig del af Center for Cybersikkerheds arbejde. CFCS udarbejder en årlig vurdering af den samlede cybertrussel mod danske myndigheder og virksomheder. Som led i den nationale cyber- og informationssikkerhedsstrategi udarbejder CFCS også sektorspecifikke trusselsvurderinger for de seks samfundsvigtige sektorer. Derudover udgiver CFCS trusselsvurderinger for særlige cybertrusler, som for eksempel truslen fra bevidste og ubevidste insidere i organisationen. Disse trusselsvurderinger kan hjælpe med at sætte en ramme for en organisations egen risikovurdering.

Tekniske og strategiske vejledninger

CFCS udarbejder vejledninger som del af vores forebyggende arbejde. Emnerne afspejler ikke en systematisk gennemgang af cybersikkerhed fra A til Z, men bliver afdækket i takt med, at vi identificerer et behov. Det kan også være i samarbejde med en anden myndighed eller i dialog med andre interessenter i samfundet. Omdrejningspunktet er, at CFCS laver de vejledninger, som er mest vigtige, og hvor vi kan bidrage med svar eller anbefalinger, som henvender sig til danske myndigheder og virksomheder, på en måde der giver værdi for dem.

De mangeartede problemstillinger inden for cyberområdet betyder også, at vejledninger fra CFCS henvender sig til forskellige målgrupper afhængig af emnet. For alle organisationer er det vigtigt, at ledelsen har en strategisk forståelse for cybersikkerhed. Derfor henvender flere af CFCS' vejledninger sig til dem, der træffer de strategiske beslutninger, som er nødvendige for at skabe et fundament for god cybersikkerhed. Men der er også konkrete sikkerhedstekniske tiltag, hvor vi henvender os direkte til dem, der sidder med den faglige ledelse i organisationen. Andre gange henvender en vejledning sig til flere niveauer i organisationen. Vejledningen "Cyberforsvar der virker" klæder for eksempel den strategiske ledelse på til at kunne tage fat på at prioritere grundlæggende cybersikkerhed i organisationen, men den indeholder også anbefalinger om tekniske tiltag henvendt til fagledelsen.

National strategi

Regeringens nationale cyber- og informationssikkerheds-strategi 2018-2021 indeholder både opgaver og mandat, som styrker CFCS' forebyggende indsats som national kompetencecenter. Et væsentligt indsatsområde vil være at øge bredden i centerets rådgivnings- og vejlednings-indsats. Det gælder ikke mindst over for den private sektor.

Det indebærer, at CFCS vil fortsætte med at afdække cybersikkerhedsområdet for at opfylde behovet for vejledning og trusselsvurdering. Vi arbejder desuden på at udvikle vores vejledninger, så de ansvarlige ministerområder vil kunne bruge anbefalinger fra CFCS til egentlige bestemmelser inden for deres område.

Vejledningerne bliver dermed normerende for arbejdet med cybersikkerhed indenfor det pågældende område, men i udgangspunktet er de alene tænkt som fagligt kvalitetssikrede generelle eller specifikke anbefalinger til en bedre cybersikkerhed.

Anbefalingerne kan desuden bruges af virksomheder og myndigheder i kravfastsættelsen af informationssikkerhedskrav til leverandører i forbindelse med indgåelse af kontrakter.

Vi arbejder endvidere på, ligesom vi har gjort det inden for Forsvarsministeriets område, at vejledningerne vil få en form, så et ministerområde efter egen beslutning også kunne anvende anbefalingerne til at føre tilsyn efter og afdække, om de enkelte myndigheder eller leverandører lever op til anbefalingerne.

Den styrkede indsats på rådgivning og vejledning vil komme til at foregå i samspil med andre styrelser og myndigheder inden for det offentlige og med de private virksomheder. For at fokusere indsatsen er det nødvendigt at koordinere med sektorerne om, hvad deres behov er, så vi kan udarbejde vejledninger og anbefalinger, som svarer til behovet. Derfor er vi i CFCS også altid åbne over for forslag til, hvor der er behov for at gøre en ekstra indsats for at videreudvikle et sikkert digitalt Danmark.

Mere info:

Se tilgængelige publikationer på:
https://fe-ddis.dk/cfcs/publikationer/pages/publikationer.aspx

Minitema: GDPR i praksis

I dette nummer af INFO går vi videre i rækken af emner om GDPR. PFA Pension bidrager dels med en artikel om hvad DPO-funktionen er for en størrelse og hvilket samspil der er imod øvrige funktioner i 2LoD men også Intern Revision, og dels en artikel om hvorledes der er arbejdet med at overholde og føre kontrol med overholdelsen af GDPR i Intern Revision.

God fornøjelse!

Data Protection Officer

Jesper Jæger Granstrøm, Data Protection Officer, PFA Pension

Introduktion

EU's databeskyttelsesforordning har snart været gældende i et år – og den nye funktion, databeskyttelsesrådgiveren (DPO), er ikke helt så ny længere. DPO-funktionen har mange ligheder med både Intern Revision, Compliance og Informationssikkerhed og til dels risikostyringsfunktioner, men er stadig sin helt egen. Men hvad er det for en funktion, og hvordan påvirker den de andre assurance funktioner i virksomheden? Det vil jeg prøve at belyse i denne artikel – særligt i forhold til, hvad man som Intern Revision skal være opmærksom på.

Det regulatoriske grundlag - overordnet

Indledningsvist er det relevant lige at ridse op, hvad databeskyttelsesforordningen overordnet indeholder af krav til DPO'ens stilling og opgaver. Ud over bestemmelserne i databeskyttelsesforordningen, findes der vejledninger om DPO funktionen fra såvel Datatilsynet som Artikel 29-Gruppen[1].

DPO'en stilling

DPO'ens stilling er reguleret i databeskyttelsesforordningens artikel 38, hvoraf det fremgår, at DPO funktionen:

- Skal inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger
- Skal have de nødvendige ressourcer til at udføre sine opgaver
- Ikke må modtage instrukser vedrørende udførelse af sine opgaver og skal rapportere til den øverste ledelse

- Kan kontaktes af datasubjekter angående alle spørgsmål om behandling af deres oplysning og om udøvelse af deres rettigheder
- Er underlagt tavshed eller fortrolighed vedrørende udførelse af sine opgaver
- Kan udføre andre opgaver så længe der ikke opstår en interessekonflikt

Kravet om rapportering til den øverste ledelse kan ikke sidestilles med det funktionelle referencekrav, der gælder for Intern Revision, ligesom den øverste ledelse ikke skal læses som virksomhedens bestyrelse. Kravet betyder således, at DPO-funktionen skal have mulighed for at rapportere direkte til direktionen i selskabet om eventuelle svagheder eller overtrædelser af de databeskyttelsesretlige regler. Muligheden for at rapportere direkte til direktionen er DPO-funktionens virkemiddel overfor den øvrige del af organisationen, da DPO'en ikke har nogen direkte instruktionsbeføjelser overfor organisationen. Kravene om DPO-funktionens uafhængighed er således noget mere lempelige, end de krav, der gælder for Intern Revision – og dermed kan DPO-funktionen ikke opfattes som en del af tredje forsvarslinje.

Som det ses af kravene til DPO'ens stilling, så skal DPO-funktionen have en vis grad af uafhængighed, idet DPO'en ikke må modtage instrukser vedrørende udførelsen af sine opgaver. Det er dog ikke et uafhængighedskrav på linje med det, der gælder for Intern Revision, idet DPO'en gerne må udføre andre opgaver i virksomheden, så længe sådanne opgaver ikke kommer til at udgøre en interessekonflikt i relation til DPO'ens opgaver. En interessekonflikt vil opstå såfremt DPO'en udfører opgaver, hvor vedkommende fastlægger formålet med databehandlingen og/eller bestemmer hjælpemidlerne hertil. DPO'ens involvering i sådanne spørgsmål må således alene have en rådgivende karakter. Det kan på den baggrund udledes, at DPO funktionen ikke er en del af første forsvarslinje.

Bestemmelserne i artikel 38 medvirker også til at sikre en grad af personlig uafhængighed for DPO'en, idet vedkommende ikke må straffes eller afskediges for at udføre sine opgaver. Som det kendes fra Intern Revision har DPO'en således med udgangspunkt i lovgivningen et fundament for, selv at beslutte formål og indhold af opgaverne, så længe disse er sagligt og fagligt begrundede. Bestemmelsen betyder dog ikke, at en virksomhed ikke kan afskedige deres DPO – DPO'en kan afskediges på et sagligt grundlag efter de almindelige ansættelsesretlige regler, eksempelvis hvis vedkommende ikke udfører sine opgaver, misligholder ansættelsesforholdet eller som følge af samarbejdsvanskeligheder.

Baseret på kravene til DPO'ens stilling kan det således konkluderes, at funktionen indgår som en del af anden forsvarslinje i organisationen.

DPO'ens opgaver
Artikel 39 i databeskyttelsesforordningen indeholder minimumskravet til de opgaver, som skal varetages af DPO funktionen:

1. Underrette og rådgive om de databeskyttelsesretlige regler
2. Overvåge overholdelsen af de databeskyttelsesretlige regler
3. Rådgiver vedrørende konsekvensanalyser
4. Samarbejde med og være kontaktpunkt for Datatilsynet

Oplistningen af opgaver i artikel 39 er som nævnt en minimumsbestemmelse, og dermed ikke udtømmende. I de enkelte virksomheder kan DPO'ens opgaver med fordel formaliseres i en funktionsbeskrivelse, således der sikres en forventningsafstemning mellem funktionen, ledelsen og den øvrige organisation i forhold til, hvilke opgaver DPO-funktionen skal varetage. Der er ikke et formelt krav i databeskyttelsesforordningen om, at der skal udarbejdes en funktionsbeskrivelse.

Et grundlæggende karakteristika ved DPO'ens opgaver er, at de er af rådgivende karakter, hvilket er en naturlig følge af, at DPO'en ikke må fastlægge formålet med behandlingen af personoplysninger eller bestemme virkemidlerne hertil. Varetagelsen af opgaverne skal ske under behørig hensyntagen til den risiko, der er forbundet med behandlingsaktiviteterne[2], herunder behandlingernes karakter, omfang, sammenhæng og formål.

Som det fremgår ovenfor om DPO'ens stilling, så har DPO'en også en opgave i forhold til datasubjekterne, da de kan kontakte DPO'en angående alle spørgsmål om behandlingen af deres personoplysninger og om hvordan de kan udnytte deres rettigheder i henhold til forordningen.

Kompetencekrav
Det fremgår af artikel 37, at DPO'en skal udpeges på grundlag af sine faglige kvalifikationer, navnlig ekspertise indenfor databeskyttelsesret og –praksis samt evnen til at udføre de opgaver, der fremgår af artikel 39. Der er som sådan ikke en objektiv målestok for kompetenceniveauet, da det skal ses i forhold til den behandling af personoplysninger, der foretages i den pågældende virksomhed. Det betyder også, at en person, der er vurderet som kvalificeret til at varetage DPO opgaverne i en virksomhed/branche ikke nødvendigvis vil være vurderet som kvalificeret i en anden virksomhed/branche.

Fælles er dog kravet om kompetencer indenfor databeskyttelsesret og –praksis, hvilket er juridiske kompetencer, men det er ikke ensbetydende med, at DPO'en skal have en baggrund som jurist. Det er muligt at demonstrere de juridiske kompetencer på anden vis – eksempelvis gennem professionelle certificeringer i databeskyttelse, som IAPP (International Association of Privacy Professionals) tilbyder.

Herudover er der flere universiteter, advokatfirmaer og andre uddannelsesinstitutioner, der tilbyder kurser/ undervisningsforløb i databeskyttelse, som kan være med til at demonstrere, at man har de fornødne juridiske kompetencer.

Et andet vigtigt kompetenceelement for DPO'en er evnen til at sætte sig ind i og forholde sig til de behandlingsaktiviteter, informationssystemer, mv., som virksomheden anvender, ligesom man skal have en god risikoforståelse og kunne forholde sig til såvel tekniske som organisatoriske sikkerhedsforanstaltninger, der medvirker til at håndtere de identificerede risici.

Risikovinkel

Et gennemgående tema i databeskyttelsesforordningen er, at den dataansvarlige skal have en risikobaseret tilgang til implementeringen af de forskellige krav. En risikobaseret tilgang er ikke unik for databeskyttelsesområdet, og gælder også for mange af de øvrige assurance funktioner. Det særlige for den risikobaserede tilgang på databeskyttelsesområdet er dog den risikovinkel, som skal anlægges. For øvrige assurancefunktioner er grundlaget for vurderingen af risici de potentielle konsekvenser, som det kan have for virksomheden. På databeskyttelsesområdet er udgangspunktet anderledes, idet man her skal tage udgangspunkt i de potentielle konsekvenser, der kan være for individet (datasubjektet), hvor de klassiske "dyder" indenfor informationssikkerhed er nøgleelementer – dvs. fokus på:

- Fortrolighed
- Integritet
- Tilgængelighed

Inden vi ser på de særlige forhold vedrørende risikovinklen ud fra datasubjektets perspektiv er det relevant lige at have i baghovedet, hvor bredt begrebet behandling af

personoplysninger reelt er. I databeskyttelsesforordningens artikel 4 er behandling defineret som *"enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse."* Det betyder således, at stort set enhver håndtering af personoplysninger i virksomheden vil falde ind under denne definition.

Ud over definitionen på behandling er det også relevant at have for øje, hvornår hændelser skal anmeldes til Datatilsynet. I databeskyttelsesforordningens artikel 4 er brud på persondatasikkerheden defineret som *"et brud på sikkerheden der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet."* – og her skal man så lige huske på ovenstående meget brede definition af "behandling". Af artikel 33 i databeskyttelsesforordningen fremgår det, at alle brud på persondatasikkerheden skal anmeldes til Datatilsynet, medmindre det er usandsynligt, at bruddet på sikkerheden indebærer en risiko for den berørte persons rettigheder eller frihedsrettigheder. Her skal man være opmærksom på, at "risiko" ikke er kvantificeret – dvs. der er som sådan ikke nogen laveste barriere. Herudover skal man være opmærksom på, at det er virksomheden der har bevisbyrden for, at det er usandsynligt, at der er en risiko – dvs. det er ikke den eller de berørte personer, der skal godtgøre, at de har været udsat for en risiko, men virksomheden der skal påvise, at de ikke har været udsat for en risiko. Der er dog lidt hjælp at hente i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden – her fremgår det, at *"en risiko for fysiske personers rettigheder og frihedsrettigheder omfatter bl.a. diskrimination, identitetstyveri eller –svindel, økonomiske tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede"*. Heraf kan man se, at der dog skal være en vis substans før det vurderes, at der er en risiko, men samtidig er det også tydeligt, at det ikke kræver de store argumenter, at få noget til at passe ind under denne beskrivelse.

Da udgangspunktet for risikovurderingen er de mulige konsekvenser, der kan være for datasubjektet, skal man eksempelvis overveje konsekvenser i forhold til[3]:

1. Fysisk skade
2. Materiel skade
3. Immateriel skade
4. Forskelsbehandling
5. Identitetstyveri
6. Identitetssvig
7. Økonomiske konsekvenser/finansielle tab
8. Skade på personens omdømme
9. Sociale konsekvenser
10. Indflydelse på privatliv
11. Skade på menneskelig værdighed
12. Skade på personens legitime interesser
13. Begrænsning eller krænkelse af personens fundamentale rettigheder
14. Forhindrer personens udøvelse af kontrol med egne oplysninger

Som det fremgår af oplistningen ovenfor, så skal man tænke ganske bredt, når man vurderer risici ud fra datasubjektets perspektiv. Herudover skal man være opmærksom på både direkte og indirekte påvirkninger for datasubjektet. Et eksempel herpå er, at man almindeligvis ikke anser navn og adresseoplysninger som særligt følsomme og/eller risikofyldte, med mindre den pågældende person har adressebeskyttelse. Men hvis adresseoplysninger eksempelvis kompromitteres for fængselsbetjente kan det få store konsekvenser for vedkommende, hvis kriminelle udnytter disse oplysninger til at møde op på adressen for at lægge pres på vedkommende eller dennes nærmeste familie i forhold til udførelsen af jobbet som fængselsbetjent. Tilsvarende kan det have negative konsekvenser for en persons omdømme, hvis det offentliggøres, at vedkommende har adresse i et fængsel eller på et bosted for særligt udsatte personer.

Ved vurderingen af de mulige konsekvenser er det også vigtigt at forholde sig til, hvilken "påvirkningsgrad" konsekvenserne vil have for det enkelte datasubjekt. Dette kan eksempelvis gøres med udgangspunkt i nedenstående[4]:

- Lav – personen vil opleve få uhensigtsmæssigheder, der kan overkommes og imødegås uden større indsats fra vedkommende. Dette kan eksempelvis være, at personen skal genindtaste sine oplysninger, indsende en blanket igen, har haft en dårlig kundeoplevelse, vil blive irriteret og lignende.
- Medium – personen vil opleve betydelige uhensigtsmæssigheder, men kan overkommes med en rimelig indsats og gennem overvindelse af få besværligheder. Dette kan eksempelvis være, at personen har fået ekstra omkostninger, gennem en periode ikke har haft adgang til forretningsservices, oplever frygt, oplever mangel på forståelse, oplever hændelse eller behandling som værende stressende, oplever mindre påvirkninger af fysisk karakter og lignende.
- Høj – personen vil opleve betydelige konsekvenser, som kun kan overvindes gennem en betydelig indsats og konsekvenser for vedkommende. Dette kan eksempelvis være økonomiske konsekvenser, påvirkning af arbejdssituation, uberettiget afvisning af krav, dårligere helbred og lignende.
- Meget høj – personen vil opleve betydelige og indgribende konsekvenser, som det ikke er muligt, eller kun vanskeligt muligt at overkomme. Dette kan eksempelvis være tab af erhvervsevne, langvarige fysiske eller psykiske påvirkninger, død og lignende.

Risikovurderingen ud fra datasubjektets perspektiv vil naturligvis have en indflydelse på, hvorledes den operationelle-/forretningsmæssige risiko skal vurderes. Foretages der behandling af personoplysninger, hvor det er

vurderet, at der er en høj risiko for datasubjekterne, så vil den operationelle/juridiske risiko for virksomheden potentielt også være høj – alt afhængigt af omfanget af den pågældende behandlingsaktivitet.

Risikovurderingen danner grundlag for, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, som virksomheden skal implementere på det pågældende område. Det fremgår af artikel 32, stk. 1 i databeskyttelsesforordningen, at *"Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici…"*. Her er det særligt vigtigt at være opmærksom på, at virksomheden skal kunne påvise (dvs. dokumentere), at de implementerede tekniske og organisatoriske sikkerhedsforanstaltninger er passende. Tilsvarende skal man være opmærksom på, at henvisningen til "det aktuelle tekniske niveau" skal ses ud fra en markedsbetragtning og ikke ud fra virksomhedens forhold – det aktuelle tekniske niveau skal således opfattes som "state of the art" på vurderingstidspunktet. Det vil også sige, at der skal tages fornyet stilling til, hvad der kan anses som passende foranstaltninger i takt med den teknologiske udvikling.

Samordning med andre assurancefunktioner

DPO funktionen har som tidligere nævnt mange naturlige snitflader til såvel Compliance-, Informationssikkerheds- som risikostyringsfunktioner i virksomheden. DPO'ens opgaver indeholder elementer, som også indgår i de andre funktioners opgaver:

- Compliance skal forholde sig til virksomhedens efterlevelse af love og regler – det samme skal DPO, men alene på det databeskyttelsesretlige område
- Informationssikkerhed skal forholde sig til den samlede beskyttelse af virksomhedens informationer – DPO skal det samme for så vidt angå beskyttelse af persondata. Et brud på persondatasikkerheden vil altid også være et brud på informationssikkerheden, om end væsentlighedsvurderingen kan være "forskellig" idet de to funktioner vurderer ud fra hvert sit udgangspunkt
- Risikostyringsfunktioner skal forholde sig til det samlede risikobillede for virksomheden – DPO'en vurdere risici med udgangspunkt i datasubjektets forhold, men vurderingen heraf kan have betydning for risikovurderingen i et virksomhedsperspektiv

Det er derfor vigtigt med samordning på tværs af funktionerne, således at unødigt dobbeltarbejde undgås, ligesom der er gode muligheder for at lave en hel eller delvis fælles opgaveløsning på tværs af funktioner. Samordningen er vigtig ud fra såvel et funktionsperspektiv som ud fra et "brugerperspektiv" – organisationen vil opleve det som ineffektivt, hvis flere funktioner kommer og stiller de samme spørgsmål og/eller kommer med anbefalinger på samme område, selvom der er funktionsbestemte nuanceforskelle. Det vil blive oplevet som langt mere værdiskabende, at der er en "helhedstanke" på tværs af funktionerne, således at der både ved udførelse af vurderinger og ved kommunikation af anbefalinger, i videst muligt omfang tages højde for alle funktionernes eventuelle særlige krav.

Samordning med funktionerne i anden forsvarslinje er naturligvis også et vigtigt aspekt for Intern Revision, men vil dog alligevel have en lidt anden karakter. Hvis der ikke er en effektiv samordning på tværs af funktionerne i anden forsvarslinje vil det være et område, som Intern Revision kan påpege som del af deres vurdering af den etablerede governance og det implementerede interne kontrolsystem. Er der en velfungerende og effektiv samordning på tværs af funktionerne vil Intern Revision kunne udnytte dette i fastlæggelsen af egen revisionsplan, da der således vil være et stærkere fundament for at basere sig på de øvrige funktioners arbejde.

Etableringen af DPO-funktionen i praksis

Opstart af en ny funktion er altid både spændende og udfordrende. Man "arver" ikke noget som sådan, der skal føres videre, og kan derfor mere eller mindre starte med et blankt stykke papir. I mange virksomheder har der dog været gennemført større eller mindre projekter i forhold til implementeringen af databeskyttelsesforordningens krav, hvilket i nogen omfang også vil påvirker etableringen af DPO funktionen.

Gennem databeskyttelsesforordningens bestemmelser om DPO'ens opgaver og stilling samt vejledninger om DPO funktionen fra henholdsvis Datatilsynet og Artikel 29-Gruppen, er der et godt fundament for etableringen af funktionen og de overordnede rammer for funktionens virke. Men selvom der er et juridisk grundlag at starte ud fra, så er der fortsat mange ting, som er åbne for fortolkning, og hvor der ikke er en markeds- eller branchestandard som sådan (endnu).

Funktionsbeskrivelse

Så hvor starter man? To af de grundlæggende dokumenter, som man bør udarbejde er en funktionsbeskrivelse og en aktivitetsplan. Det er hele fundamentet for den organisatoriske forankring af funktionen og hvilken assurance, man forventer at funktionen skal kunne give til ledelsen.

Funktionsbeskrivelsen er forholdsvis let at gå til, når man tager udgangspunkt i databeskyttelsesforordningens bestemmelser. Der er endnu ikke udviklet en reel praksis eller øvrige branchestandarder for varetagelse af DPO funktionen, som kan påvirke indholdet af funktionsbeskrivelsen, og det vigtige er dermed alene, om alle databeskyttelsesforordningens formelle krav til DPO'ens stilling og opgaver er afdækket. Af hensyn til kravet om DPO'ens rapportering til den øverste ledelse bør man som virksomhed kunne dokumentere, at den øverste ledelse, dvs. som minimum direktionen, har fået forelagt funktionsbeskrivelsen samt har godkendt denne.

Aktivitetsplan

Som anført tidligere, så er et grundlæggende element i DPO'ens opgaver, at der er tale om en rådgiverfunktion. Det fremgår dog også af artikel 39, stk. 1, litra b, at DPO'en har en opgave vedrørende overvågning af virksomhedens overholdelse af de databeskyttelsesretlige regler, hvilket dermed har betydning for DPO'ens aktivitetsplan.

Da der er tale om en ny funktion er aktivitetsplanen lidt en "udfordring" de første år, idet man ikke har resultater fra tidligere års gennemgange, som man kan bygge videre på og anvende som grundlag for prioriteringen af opgaverne. Virksomhedens Compliancefunktion kan dog have foretaget gennemgange af det databeskyttelsesretlige område, som DPO-funktionen med fordel kan anvende i grundlaget for udviklingen af egen aktivitetsplan. Den store opmærksomhed, som databeskyttelsesforordningen havde op til dens ikrafttrædelse i maj 2018, betyder også, at der er en naturlig interesse fra ledelsens side i at få så meget/bred assurance som muligt i forhold til de gennemførte implementeringsaktiviteter og –projekter i virksomhederne. Der vil således være en naturlig interesse i, at der gennemgås så meget som muligt, og selvom man anlægger en risikobaseret tilgang til fastlæggelse af aktivitetsplanen, bliver det derfor lige så meget et spørgsmål om at kunne argumentere for, hvorfor noget er valgt fra, frem for hvorfor det er medtaget på planen. Derfor er koordinering med de øvrige funktioner i anden forsvarslinje også særligt vigtigt, så muligheder for at udnytte deres gennemgange eller foretage "joint assessments" identificeres. På den måde kan man opnå en bredere afdækning, end det er muligt kun med egne ressourcer. Samtidig giver det gode muligheder for at demonstrere overfor forretningen, at den nye funktion ikke bare er et add-on til governance apparatet, men kan samarbejde og interagere med de øvrige kendte funktioner.

Da der er tale om en ny funktion er det ligeledes vigtigt at få forventningsafstemt, hvad "pløjedybden" skal være for DPO'ens gennemgange – dvs. hvilken grad af assurance skal der gives. Noget vil være givet gennem de forventninger, der er til assuranceniveau fra andre funktioner i anden forsvarslinje, men der er stadig et behov for at få forventningsafstemt, hvad det er for en betryggelse, som DPO-funktionen skal give. Er det en tilgang, med høj grad af "self assessments" fra organisationens side, som DPO'en læser og forholder sig til med lav grad af verifikation og test, eller er det tættere på en gennemgang, som man kender fra Intern Revision med walkthrough af processer og forretningsgange og tilhørende test af kontrolaktiviteters design, implementering og effektivitet?

Databeskyttelsesforordningen og vejledningerne om databeskyttelsesrådgiveren giver som sådan ikke en direkte guidance i forhold til, hvor høj grad af assurance, den i henhold til artikel 39, stk. 1, litra b krævede overvågning skal give. Af Artikel 29-Gruppens vejledning om databeskyttelsesrådgivere fremgår det, at opgaven vedrørende overvågning navnlig omfatter at:

- Indsamle oplysninger, der identificerer databehandlingsaktiviteter
- Analysere og kontrollere databehandlingsaktiviteternes overholdelse af bestemmelserne
- Informere, rådgive og rette henstilling til den dataansvarlige eller databehandleren

Heraf kan man udlede, at der både skal foretages en grad af procesafdækning og verifikation af, at implementerede tekniske og organisatoriske foranstaltninger virker efter hensigten samt at der skal gives anbefalinger til ledelsen, hvis gennemgangen identificerer forbedringsmuligheder. Det vil med andre ord sige, at man ikke kan basere sig på "self assessments" alene, men på den anden side er der heller ikke krav til, hvilken grad af overbevisning, der skal ligge bag konklusioner og anbefalinger til forbedringer.

I lighed med funktionsbeskrivelsen bør DPO'ens aktivitetsplan fremlægges for og godkendes af den øverste ledelse. Her skal man dog være opmærksom på kravet i artikel 38, stk. 3 om, at DPO'en ikke må modtage in-

strukser vedrørende udførelsen af de i artikel 39 anførte opgaver. Dvs. ledelsen har som sådan ikke en mulighed for at "diktere", om opgaver skal tages ud af aktivitetsplanen, men kan selvsagt fremføre argumenter vedrørende den underliggende risikovurdering, som dermed kan have betydning for DPO'ens prioritering af indsatser.

Samarbejde med organisationen
Som ny funktion er der en særlig opgave i forhold til at få opbygget relationer til den øvrige del af organisationen. Dette gælder både forretningsorganisationen i forhold til at få indsigt i art og omfang af de behandlinger af personoplysninger, som den pågældende enhed foretager og i forhold til synlighed og awareness om DPO rollen. Hvis organisationen ikke ved, hvem DPO'en er og hvad der ligger i opgaven, så ved de heller ikke, hvem de skal tage fat i, når der er persondatarelaterede spørgsmål – og dermed vil virksomheden ikke være i stand til at leve op til kravet om, at DPO'en skal involveres rettidigt og tilstrækkeligt i alle spørgsmål vedrørende beskyttelse af persondata.

Åbenheden i den ledelsesmæssige opbakning til den nye funktion har stor betydning for, hvordan man bliver opfattet, når man kommer rundt i organisationen. Er det tydeligt for organisationen, at den øverste ledelse bakker op om DPO funktionen og kan se dens værdi, bliver det også lettere at få tid i kalenderen i de øvrige ledelseslag.

Stakeholder management er dermed en lige så vigtig opgave for DPO funktionen, som det er for Intern Revision og de øvrige funktioner i anden forsvarslinje.

Herudover er samordning med øvrige funktioner i anden forsvarslinje, som tidligere nævnt, et vigtigt aspekt i forhold til, at DPO funktionen forankres som en naturlig del af anden forsvarslinje, således at unødigt dobbeltarbejde undgås.

Netværk
Da DPO funktionen ikke er en veletableret rolle eller funktion i branchen endnu, kan det være relevant at deltage i faglige netværk. Jeg deltager selv i persondatanetværk hos nogle af de store advokathuse, som primært afdækker de juridiske forhold og vurderinger i forhold til databeskyttelsesområdet. Herudover har jeg været med til at opstarte et funktionsbaseret netværk for DPO'er i pensionsselskaber. Dette netværk er primært målrettet de mere funktionelle spørgsmål og problemstillinger, men kan også rumme de mere tekniske/juridiske vurderinger. Netværket bidrager til, at man kan drøfte nogle af de problemstillinger og udfordringer, der enten er branchespecifikke eller relaterer sig til de generiske i rollen som DPO.

Kompetencekravet
Jeg har en mangeårig baggrund fra Intern Revision og havde således ikke som sådan "papir" på, at jeg levede op til databeskyttelsesforordningens kompetencekrav, når det gælder den juridiske kompetence i databeskyttelsesret og –praksis. Jeg valgte derfor at tage to forskellige certificeringer gennem IAPP (International Association of Privacy Professionals) – CIPM (Certified Information Privacy Manager), der omfatter forhold vedrørende design og styring af et databeskyttelsesprogram/-proces i en virksomhed, og CIPP/E (Certified Information Privacy Professional/Europe), der omfatter det juridiske i databeskyttelsesforordningen. Begge certificeringer kræver, som man kender det fra bl.a. CIA, at man løbende efteruddanner sig for at holde certificeringerne ved lige. De to certificeringer medvirker således til at "dokumentere", at forordningens kompetencekrav efterleves på det juridiske område, ligesom fastholdelse af certificeringerne medvirker til at demonstrere efterlevelse af forordningens krav om løbende vedligeholdelse af sine kompetencer.

Revisionsvinklen

Hvad betyder etableringen af DPO funktionen så for Intern Revision? Ud fra et helt overordnet perspektiv er der bare tale om en ny funktion i anden forsvarslinje, som Intern Revision skal vurdere ud fra samme principper, som de øvrige funktioner.

Da der er tale om en nyetableret funktion er det naturligt at have et særligt fokus på den grundlæggende governance og metode for funktionen – dvs. områder som:

1. Funktionsbeskrivelse – er en sådan udarbejdet og omfatter den alle forordningens bestemmelser vedrørende DPO'ens stilling og opgaver? På hvilket organisatorisk niveau er funktionsbeskrivelsen godkendt?
2. Aktivitetsplan – er det tydeligt om aktivitetsplanen er baseret på en risikobaseret tilgang, hvor det er risikoen for datasubjekterne, der er det drivende? Tager aktivitetsplanen højde for de til rådighed værende ressourcer og kravene til, at DPO'en har en rådgivende rolle?
3. Anvendt metodik og dokumentation ved vurdering af forordningens efterlevelse – er der fastlagt et formaliseret grundlag for, hvordan DPO'en skal udføre og dokumentere sit arbejde, og understøtter de fastlagte principper og metoder den rolle og de opgaver, som fremgår af funktionsbeskrivelsen?
4. Rapportering – hvilken rapportering skal DPO'en udarbejde og til hvem?

Herudover er det relevant for Intern Revision at forholde sig til, hvordan samordningen er mellem DPO funktionen og de øvrige funktioner i anden forsvarslinje. Både i forhold til udformning og indhold af aktivitetsplanen samt i forhold til den anvendte metodik. Såfremt der er væsentlige forskelle i den grad af assurance, som de enkelte funktioner i anden forsvarslinje giver, så bør det også være tydeligt for ledelsen gennem den anvendte terminologi, således der ikke uforvarende skabes en forventningskløft mellem den faktisk leverede assurance og ledelsens opfattelse heraf. Transparensen af den leverede assurance er en forudsætning for, at ledelsen kan være i kontrol over virksomhedens risici.

Endeligt bør Intern Revision have et særligt fokus på, hvordan DPO funktionen interagerer med de øvrige forretningsenheder, således at virksomheden lever op til kravet om en tilstrækkelig og rettidig involvering af DPO'en i alle spørgsmål vedrørende beskyttelse af personoplysninger. Dvs. man som Intern Revision skal udnytte sin indsigt i virksomheden, og governance i forhold til, om DPO'en er "med" i de relevante fora, udvalg, mv., hvor der kan opstå væsentlige spørgsmål vedrørende behandling og beskyttelse af personoplysninger. Det betyder også, at Intern Revision bør forholde sig til, hvilken "standing/awareness" der er i organisationen i forhold til DPO'en og vedkommendes rolle. Hvis det ikke er bredt kendt i organisationen, at der findes en DPO, hvem det er og hvilken rolle/opgaver vedkommende har, så er der en øget risiko for, at DPO'en ikke bliver involveret tilstrækkeligt og rettidigt i spørgsmål vedrørende databeskyttelse.

Etableringen af DPO funktionen har også en anden betydning for Intern Revision, end at være endnu en assurance funktion, som der skal foretages vurdering af. Et gennemgribende element i databeskyttelsesforordningen er, at virksomheden som dataansvarlig og/eller databehandler, skal være i stand til at påvise, at forordningens krav efterleves. Det betyder med andre ord, at Intern Revision har fået en ekstra kollega i "koret", som efterspørger og efterprøver dokumentation af processer, forretningsgange og kontrolforanstaltninger fra virksomheden, herunder efterspørger revisionserklæringer eller anden assurance fra de af virksomhedens leverandører, der behandler personoplysninger på virksomhedens vegne (databehandlere).

Afslutning

Der er jævnligt historier i medierne om, at den ene eller anden virksomhed ikke har behandlet personoplysninger på en ansvarlig måde – det gælder både i forhold til sikring af fortrolighed af oplysninger og i forhold til anvendelsen af personoplysninger. Som samfund bliver vi stadig mere digitaliserede, og de teknologiske muligheder for at analysere på og samkøre data bliver til stadighed bedre og billigere. Det kan derfor være tillokkende for virksomheder at udnytte data, bare fordi man kan, selvom man måske ikke har lov til det. Sikring af privatlivets fred er en menneskeret, og DPO funktionen spiller en aktiv rolle i forhold til, at virksomheden lever op til sine forpligtelser i forhold hertil. Samordning mellem de forskellige assurancefunktioner i virksomheden har altid været vigtigt, hvor et af de gennemgående argumenter er, at man skal undgå dobbeltarbejde. Det er også helt korrekt ud fra en ren ressourcebetragtning og i forhold til den samlede grad af assurance, som ledelsen opnår gennem de forskellige funktioner. Men det er også vigtigt at have for øje, hvordan de forskellige funktioner i anden forsvarslinje, sammen med Intern Revision, gennem rådgivningsaktiviteter og anbefalinger er med til at påvirke den fremadrettede drift af virksomheden. Her er samordning mellem funktionerne også vigtig af hensyn til, at funktionerne ikke "spilles ud mod hinanden", eller at der ikke tages højde for alle relevante aspekter, når virksomheden eller dens produkter skal udvikles.

For virksomheden er det derfor vigtigt, at den gennem Intern Revision får den fornødne betryggelse i, at den etablerede DPO funktion er veletableret, velfungerende og effektiv – både som særskilt funktion og i samarbejde med de øvrige assurance funktioner. Og for DPO funktionen er det vigtigt, at der er et stærkt tværfunktionelt samarbejde, således at man er i stand til at udnytte det gode arbejde, som andre funktioner udfører, når man overfor ledelsen skal rapportere på, om de databeskyttelsesretlige regler efterleves.

Noter

[1]Artikel 29-Gruppen er den uafhængige europæiske arbejdsgruppe, der beskæftigede sig med anliggender i forbindelse med beskyttelse af privatlivets fred og personoplysninger frem til den 25. maj 2018, hvor databeskyttelsesforordningen trådte i kraft. Efter den 25. maj 2018 varetages arbejdet af European Data Protection Board (EDPB). Navnet refererer til, at grundlaget for arbejdsgruppen var artikel 29 i databeskyttelsesdirektivet (95/46/EC). Alle vejledninger udstedt af Artikel 29-Gruppen er tiltrådt af EDPB efter databeskyttelsesforordningens ikrafttrædelse og er dermed fortsat gældende.
[2]Definition af "behandling" er meget bred i databeskyttelsesforordningens forstand, og gennemgås nærmere nedenfor i afsnittet om risikovinkel.
[3]Datatilsynets vejledning om behandlingssikkerhed
[4]Datatilsynets vejledning om behandlingssikkerhed

GDPR i Intern Revision

Morten Bendtsen, Koncernrevisionschef, PFA Pension

Indledning

Den nye persondataforordning trådte i kraft den 25. maj 2018. I PFA har man kørt et stort implementeringsprojekt, som Intern Revision har været en del af.

I forbindelse med projektet har vi i Intern Revision udarbejdet og taget stilling til:

- Overblik over behandlingen af personoplysninger i Intern Revision
- Lovligheden og behov for samtykke til behandlingen
- Sikker kommunikation
- Videregivelse af personoplysninger internt og eksternt
- Opbevaring af personoplysninger i Intern Revision
- Sletteprocedurer
- Behovet for databehandleraftaler med eksterne konsulenter
- Behov for indsigtsret
- Risikovurdering og intern kontrol som skal udføres årligt i Intern Revision

Der er som del af projektet afholdt undervisning for alle medarbejdere i Intern Revision og alle har taget et e-learningsprogram og tilhørende test.

Governance i PFA

I PFA er der udarbejdet en række politikker og forretningsgange der gælder på tværs af de forskellige forretningsområder.
Intern Revision er et selvstændigt forretningsområde i PFA og skal dermed udarbejde en "Områdeforretningsgang for behandling af personoplysninger" - se **Figur 1** på næste side**.**

Forretningsgang

Forretningsgangen dokumenterer de overvejelser, der er truffet i projektfasen (se indledning).

Forretningsgangen angiver følgende årlige aktiviteter:

- Overblik over behandling af personoplysninger i Intern Revision skal gennemgås og ajourføres
- Præsentation og gennemgang af forretningsgangen for medarbejderne så det sikres, at risikovurdering og intern kontrol er kendte
- Udførelse af intern kontrol

Herudover skal der foretages et årligt review af forretningsgangen. Review-aktiviteten dokumenteres i PFA's GRC-system.

Lovlig behandling

Intern Revisions grundlag for behandling af personoplysninger er baseret på en lovbestemt opgaveløsning.

Intern Revision må kun behandle personoplysninger, der direkte kan henføres til en opgave i revisionsplanen for PFA-Koncernen eller i medfør af funktionsbeskrivelsen og politik for intern audit.

Herudover skal Intern Revision i relevant omfang følge principperne for behandling af personoplysninger i de forretningsgange for behandling af personoplysninger, som gælder for PFA Pension

Risikovurdering

Følgende risici er vurderet væsentlige for behandling af personoplysninger i Intern Revision:

- Sletning
- Arkivering
- Eksterne konsulenter
- Adgang til revisionslokaler
- Irrelevante data
- Adgangsstyring

Sletning – processen er ikke systemunderstøttet hvilket alt andet lige øger risikoen. Hovedreglen for sletning af data på revisionsdrevet er, at data der er ældre end 5 år + indeværende år skal slettes. Sletning på revisionsdrevet foretages centralt i Intern Revision en gang årligt.

Sletning i Outlook sker af data, som er ældre end 1 år + indeværende år. Sletning af data i Outlook sker årligt og decentralt hos de enkelte medarbejdere, hvilket endvidere øger risikoen.

Arkivering – Der er tale om ustruktureret data som arkiveres på afdelingsdrev. Det skal sikres at persondata, der er anvendt som revisionsbevis er arkiveret i rette mapper, således at der er et entydigt link til en konkret revisionsopgave, og dermed en lovlig behandling af personoplysninger.

Eksterne konsulenter – Intern Revision anvender ressourcer fra eksternt konsulenthus til udvalgte revisionsområder. Såfremt persondata tilgår konsulenthuset, skal der udarbejdes en databehandleraftale.

Adgang til revisionslokaler – Rengøringspersonalet glemmer at låse døre efter sig og uautoriseret personale får adgang til personoplysninger.

Irrelevante data – Ved nye opgaver, hvor data ikke er kendt, er der risiko for at der efterspørges flere personoplysninger end der reelt er behov for. Det er vigtigt at unødvendige personoplysninger slettes, hvis de ikke er nødvendige for udførsel af revisionsopgaven.

Adgangsstyring – Risiko for at medarbejdere udenfor Intern Revision har adgang til revisiondrevet og dermed revisionsdokumentation og eventuelle personoplysninger på kunder.

Risikovurderingen er dokumenteret i forretningsgangen ved anvendelse af et skema (før kontrol) - se **Figur 2** på næste side.

Intern kontrol

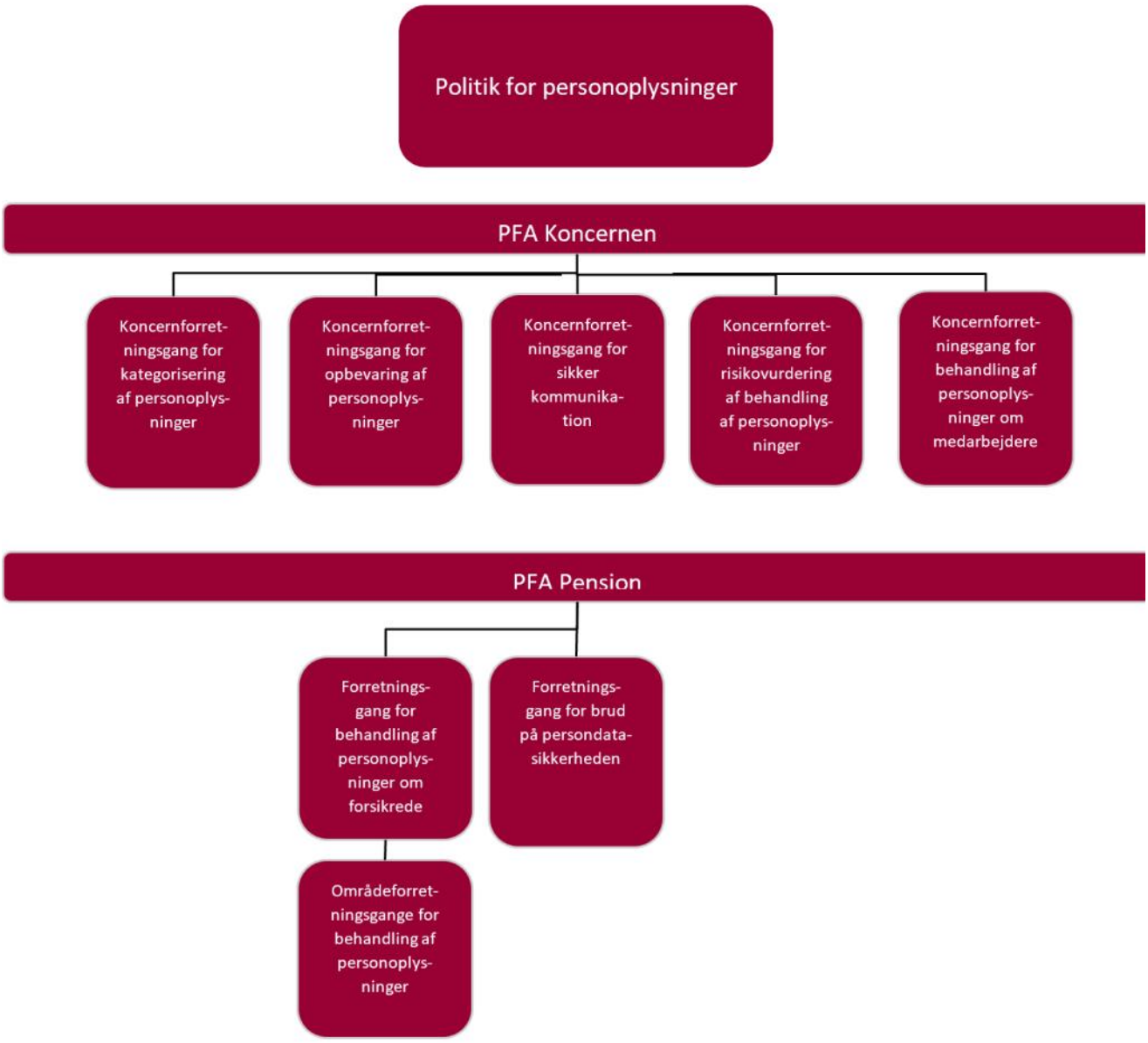
I henhold til forretningsgangen skal der årligt foretages intern kontrol.

De interne kontroller er linket til de risici, der er identificeret i risikovurderingen - se **Figur 3** på næste side.

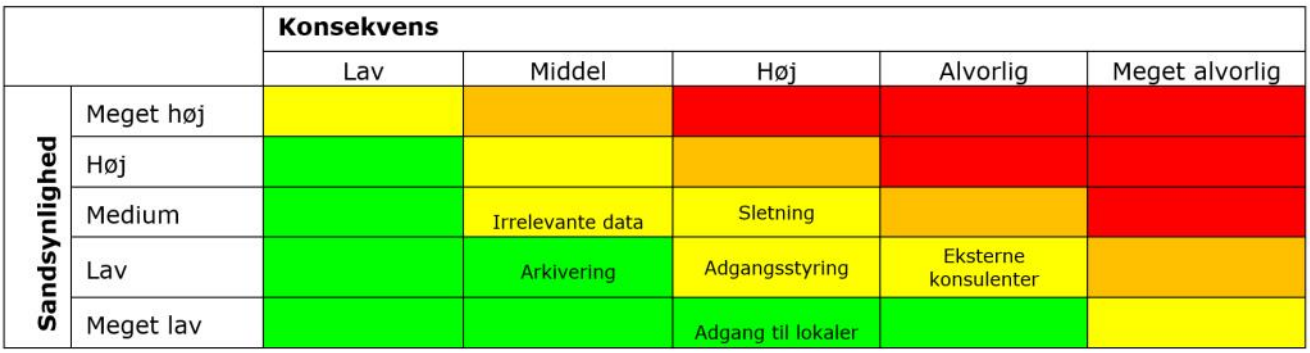
Afslutning

Som Intern Revision er det vigtigt, at vi er med til at vise at GDPR tages alvorligt og prioriteres. Det sker via forretningsgangen, den interne kontrol, kommunikationen til medarbejderen og de opmærksomhedspunkter vi har i NUR (Notat om Udført Revision) og eventuelt planlægningsnotat.

Figur 1



Figur 2



Figur 3

Risiko	Kontrolformål	Hjælp	Kontrol	Frekvens	Ansvar	Dokumentation
Sletning	Sletning sker i overensstemmelse med sletteregler i Intern Revision.	Revisionshåndbogen	Påse, at der er udsendt mail med instruks om sletning i Outlook og der er modtaget klarmelding fra alle medarbejdere i Intern Revision. Revisionsdrevet indeholder kun mapper dateret med indeværende år plus fem.	Årligt Årligt	Koncernrevisionschef Koncernrevisionschef	Mails arkiveres i mappen på revisionsdrevet "Persondata/ kontrol". Mail med klarmelding af sletning arkiveres i mappen på revisionsdrevet "Persondata/ kontrol".
Arkivering	Personoplysninger og anden dokumentation er arkiveret i respektive mapper på revisionsdrevet "Udført revision/ årstal".	Revisionshåndbogen Skabelon for NUR (Notat om udført revision).	I forbindelse med kvalitetssikring af den udførte opgave sikres, at der er "sign-off" for at personoplysninger og anden dokumentation er flyttet til revisionsdrevet og slettet i Outlook.	Løbende	Koncernrevisionschef	I NUR fremgår "sign-off" i et særskilt afsnit "Personoplysninger".
Eksterne konsulenter	Der indgås en databehandleraftale inden konsulenthus får adgang til eller får udleveret personoplysninger om kunder i PFA-koncernen.	Standardaftale indhentes hos Procurement. Kontraktindgåelsespolitik og forretningsgang.	I forbindelse med kvalitetssikring af planlægning af den respektive opgave sikres, at der er taget stilling til om det er nødvendigt for opgave- løsningen, at konsulenthus får adgang til personoplysninger. Databehandleraftale er indgået inden opgaveløsning igangsættes.	Løbende Løbende	Koncernrevisionschef Kontraktejer	I planlægningsnotat fremgår stillingstagen fra udførende medarbejder i et særskilt afsnit "Personoplysninger". Aftale arkiveres i mappen på revisionsdrevet "Persondata/ databehandleraftaler" og sendes til Procurement. Mail arkiveres samme sted.

Figur 3 (fortsat)

Risiko	Kontrolformål	Hjælp	Kontrol	Frekvens	Ansvar	Dokumentation
Adgang til revisionslokaler	Kun medarbejdere i Intern Revision har adgang til lokaler.	Facility Management. Indhent oversigt over udleverede nøgler.	Løbende observation af om lokaler er aflåst om morgen. Oversigt gennemgås. Antallet af nøgler og indehaver vurderes i forhold til arbejdsbetinget behov.	Drøftes på afdelingsmøder Årligt	Alle Koncernrevisionschef	Eventuel mail til Facility Management arkiveres i mappen på revisionsdrevet "Persondata/ kontrol". Oversigt dateres, attesteres og arkiveres i mappen på revisionsdrevet "Persondata/ kontrol".
Irrelevante data	Kun nødvendige personoplysninger arkiveres som del af revisionsdokumentationen.	Revisionshåndbogen Skabelon for NUR (Notat om udført revision).	I forbindelse med kvalitetssikring af den udførte opgave sikres, at der er "sign-off" for at irrelevante personoplysninger er slettet.	Løbende	Koncernrevisionschef	I NUR fremgår "sign-off" i et særskilt afsnit "Personoplysninger".
Adgangsstyring	Kun medarbejdere i Intern Revision har adgang til data på V: drevet.	Udtræk indhentes via EPI & Change.	Udtræk gennemgås og medarbejdere uden et arbejdsbetinget behov slettes. *Fejlkilde:* Medarbejdere uden for Intern Revision eller tidligere ansatte i Intern Revision.	Årligt	Koncernrevisionschef	Udtræk dateres, attesteres og arkiveres i mappen på revisions drevet "Persondata/ kontrol". Dokumentation af eventuelle sletninger arkiveres tilsvarende.

Third-party Risk Management

Anette K. Laursen, M.Sc.(Econ), CIA, Head of Audit, Nordea

Introduction

In October 2018 the Institute of Internal Auditors (Global) published a new Supplemental Guidance or Practice Guide "Auditing Third-party Risk Management".

The Practice Guide introduces the concept of a third-party risk management framework as an element of a larger enterprise risk management framework, considering that organisations come in all shapes, sizes, available resources, tools and techniques.

Third-party providers, as well as subservices or so-called fourth-party providers, present risks organisations should be in control of. Risks posed by third-party providers should be considered in the development of a comprehensive risk-based audit plan. Internal auditors must understand how the organisation structures its third-party risk management programmes, how third-party risk management processes relate to the organisation's risk appetite, and the roles and responsibilities of the participants in the third-party risk management process.

Risk exposures change when organisations rely on third-party suppliers or service providers. If a key third-party does not meet expectations or fail altogether, the resulting reputational and operational damage may be as significant or even exceed the damage suffered by the third-party itself. Examples where significant data breaches involving third parties have resulted in material losses have been experienced and exposed in the media.

Reputational damage is difficult to foresee and difficult to measure. Robust third-party risk assessment, due diligence and monitoring are therefore critical.

Well-informed internal auditors may disclose missed revenue or opportunities for cost savings, contribute to reducing fraud and operational risk and identify improvements to the third-party risk management processes. Thus, internal auditors may provide valuable third-party risk management assurance and help management improving the overall control environment.

Elements of a Third-party Risk Management (TPRM) Programme

Many organisations have a third-party risk management (TPRM) programme, which has developed organically over time. The processes may thus be inconsistent or fragmented across business lines, products etc.

Three key elements must be present for adequate TPRM. The elements are:

1. A framework specifically geared towards TPRM
2. A risk appetite statement
3. A TPRM governance structure

Framework

The purpose of the TPRM framework is to ensure that the risk exposures related to third parties are managed and monitored according to the organisation's risk appetite and governance requirements.

An effective TPRM framework should include:

- Sufficient policies, procedures and activities to support it (aligned with the organisation's risk appetite and stakeholder expectations, as well as industry standards)
- Effective governance structures supporting the policies, procedures and activities
- A structured support system covering:
  - Defined roles and responsibilities
  - Third-party inventory, risk rating criteria and risk assessment processes
  - Third-party risk management controls
  - Reporting requirements
  - Review process
  - Processes for classification, escalation and tracking of findings.

Risk appetite

The organisation must set limits for the level of risk exposure the organisation may suffer by outsourcing services, products etc.

The risk appetite should consider the negative levels of risk exposure (e.g. fines and reputational damages), as well as the positive benefits (e.g. improved quality and efficiency, and reduced costs) the organisation may incur. If the positive benefits outweigh the risk exposure, senior management/the board may decide to outsource in line with the policy.

When an organisation follows a strategy involving outsourcing to a third-party, management must clearly communicate the minimum requirements regarding the capabilities of the third-party candidates, in terms of governance, risk management and internal controls the third-party should have in order to comply with the organisation's risk appetite.

In order to evaluate and conclude on changes to risk conditions and measures and determine whether actions are needed to stay in line with the risk appetite, senior management, the board and appropriate committees should be provided with relevant risk information, dashboards and reports.

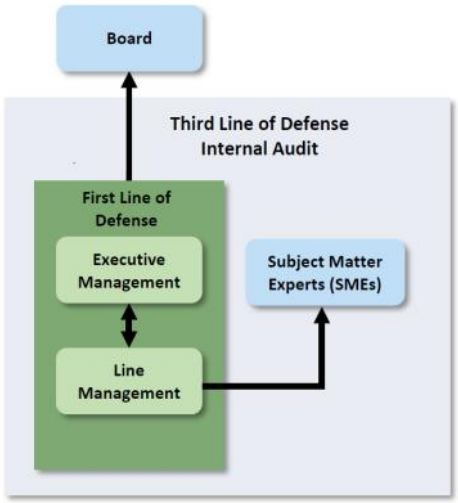
TPRM governance structure

The governance structures of third parties may vary widely depending on the use of third parties, the complexity and size of the organisation, as well as the maturity level of TPRM and the risk appetite. However, the various governance structures share a common characteristic: Those requesting the service must be responsible for managing the overall risk exposure the third-party brings to the organisation. They become owners and maintainers of the organisation's risk appetite, no matter how simple or sophisticated the TPRM programme is in terms of governance structure and process.

The IIA Practice Guide operates with a basic, a defined and a standardised model for TPRM governance.

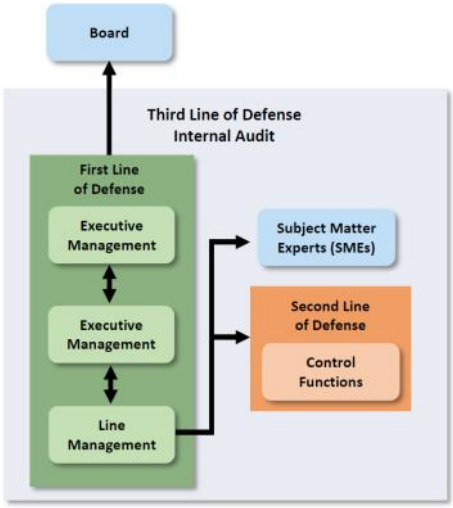
Basic model
Basic TPRM governance may be a part of organisations with more informal TPRM processes and procedures.

In the decentralised structure, managers are responsible for identifying needs for third-party services, thus acting as relationship owners. The managers are also responsible for due diligence, recordkeeping, monitoring, review and modifications. Documentation may be informal and inconsistent across business areas.



The basic structure may create a conflict of interest, especially when relationship managers have a bias towards a specific third-party. Another risk is the inconsistency in the level of due diligence and review of the third parties.

Defined model
Defined TPRM governance may be a part of organisations with more defined TPRM processes and procedures.

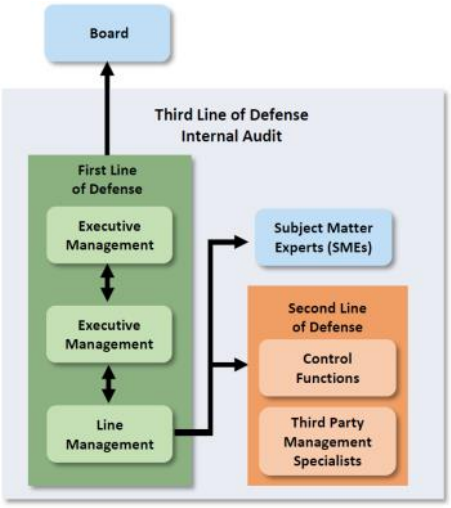


At this level, managers are still responsible for contracts and SLAs. The difference to the basic model is that staff who constitute a formal second line of defence assist managers acting as relationship owners.

In this stage of TPRM development, committees or groups may have the responsibility of addressing third-party business cases, selection and contracting prior to approval from the senior management/board.

Standardised model
The standardised model is recommended in highly regulated industries and for globally complex organisations.

In this model, third-party specialists form an important part of the first or second line of defence of TPRM, depending on how the organisation defines the lines of defence. However, the managers are still the third-party risk exposure owners in the first line of defence.

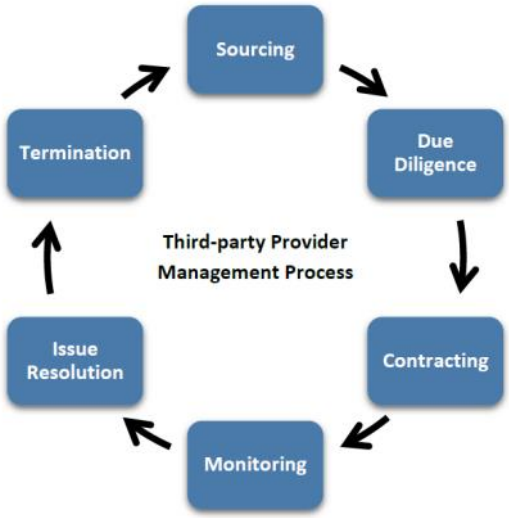


TPRM process and the role of internal audit

In general, the TPRM policy and programme procedures are intended to help achieve the business objectives for entering a third-party provider relationship, while satisfying regulatory requirements/ expectations (if any) and minimising the risk of unanticipated costs, legal disputes and asset losses.

Management must as risk owners identify, assess, manage and monitor the risk associated with each third-party relationship on an ongoing basis.

Elements of the ongoing TPRM process can be illustrated as follows:



Sourcing

Sourcing practices for third parties vary widely depending on nature of the service, complexity of the organisation as well as other factors. However, before choosing to engage a third-party, management must understand the business context and drivers that determine the risks associated with the effort.

A sound business case should be built addressing key benefits and risks of the outsourcing. Outsourcing may be a solution to address business risks, or it may create new business risks. The risk assessment at this stage should include implementation risks and probable impacts if the third-party fails to deliver the anticipated results.

To assess the effectiveness of an organisation's TPRM processes, internal auditors should start at the beginning. Obtaining the business case and any other relevant strategy-related documents concerning the initiative to engage a third party provides valuable information that will be useful throughout the internal audit engagement.

Due diligence

Before selecting the third-party to contract with, a proper due diligence should be performed. Categories of information gathered may include:

- Ownership structure and background
- Company performance and financial health
- Company location
- Business model and practices
- Potential conflicts of interest
- References
- Service delivery capability, status and effectiveness
- Pricing and billing
- Press coverage/legal actions
- Corporate governance policies
- Environmental policies
- Ethics, code of conduct etc.

On-site visits may provide further insights by validating information already gathered.

The level of due diligence is dependent on the criticality of the outsourcing arrangement. The level of due diligence for each tier of criticality should be predetermined and documented in the TPRM policy and procedures. Also, review and escalation requirements and red flags should be described in the TPRM policy and procedures.

The justification and the approval of the due diligence must be documented and retained in the third-party file and updated on a regular basis.

Internal audit may have a role in ensuring that proper due diligence and risk assessments have been conducted, not only at the beginning of a relationship with a third party, but also on a regular basis in line with the third party's risk exposure level.

Contracting

The contract is an important control in the third party-risk management process, as it is the best resource to communicate the organisation's risk appetite, minimum standards of internal controls and expected standards of service etc.

The contract should provide for a mutually beneficial relationship and protect the organisation if disputes, complaints or failures arise.

One significant risk in outsourcing arrangements is the failure to evaluate soft controls, such as cultural norms and expectations on both sides. Another risk is inadequate contract review.

A right-to-audit clause should be part of the organisation's standard contract and be clear on who is able to exercise that right and to what extent.

Monitoring
A key responsibility of third-party relationship owners is to monitor the third-party to ensure compliance with the contract and requirements for the service.

Key Performance Indicators (KPIs) to monitor may be a mix of both standard and customised KPIs. In addition, the owner should e.g.:

- Complete or update periodic analyses of risk and exposures
- Obtain required attestation, audits and financial reports
- Ensure reports are reviewed by subject matter experts
- Review relevant third-party policies, compliance programs, data security programs and reports specified in the contract
- Conduct on-site monitoring visits (if agreed in the contract).

For critical third parties with ISAE no 3402[1] and related reports available to the organisation, these reports should be reviewed annually by the third-party relationship owner.

A third-party tracking system is a leading practice that may assist internal auditors in designing their work programs. This can be as simple as an Excel spreadsheet or complex software. Relationship owners may document third-party due diligence, contracts, SLAs and other information in the tracking system. The most functional and beneficial tracking systems aggregate risks by third party, product, relationship owner, department/function, and more.

Issue Resolution
The third-party relationship owner will usually be responsible for monitoring and addressing issues. The responsibility includes (cf. above) periodic risk assessments dependent on the risk exposure level of the third-party, and monitoring of changes by the third-party such as business, organisational structure, legal actions, regulatory issues etc.

Internal auditors' work related to issue resolution should:

- Examine the organisation's escalation process for elevating concerns regarding third-party risk exposure levels, non-performance, lack of quality, as well as other issues that may arise
- Determine whether the organisation is collecting any penalties that may be due from a third party as set forth in the contract
- Confirm that management is addressing potential contract breaches appropriately by increasing or changing SLAs, monitoring processes, etc.

Termination
Already in the contract negotiations, termination conditions are important and necessary to protect the organisation. Several risk factors can contribute to the loss or the damage the organisation may sustain from early termination. Also, certain risk factors can contribute to loss if a contract is not renewed.

Risks that may be managed by appropriate and complete termination conditions include:

- Data, equipment, material or technology retrieval
- Evidence of material, technology or data destruction
- Circumstances requiring arbitration
- Events which may lead to litigation
- Responsibilities for separation and termination costs
- Alternatives if the third-party becomes unavailable.

Normally, the internal audit function will not be involved in the termination of third party relationships. However, it is possible that internal audit may be involved in an advisory capacity, subject to Standard 1210 – Proficiency and 1210.C1 or they may validate that appropriate conditions (such as retrieval or destruction of data) are fulfilled. As a minimum, internal audit should confirm there are thorough descriptions of termination conditions in the contracts as part of the audit procedures.

Auditing TPRM

In a risk-based audit plan the internal audit activity should aim to perform engagements covering the TPRM framework and associated processes.

The coverage could be approached in several ways, including:

- Auditing the TPRM framework
- Auditing the TPRM process
- Auditing a component of the third-party risk process
- Including TPRM in process, product or unit audits.

In general, the objectives for a third-party risk management-focused audit should relate to the organisation's current business objectives and strategies.

In its appendices, the IIA Practice Guide provides further help in relation to the following areas:

- Evaluating a Third Party's Conduct and Ethical Values
- Due Diligence Considerations
- Contract Review Considerations
- Testing and Evaluating Third-party Risk Management
- Sample Third-party Risks and Red Flags/ Warning Signs
- Audit Considerations for Fourth Parties.

The EBA Guidelines on outsourcing arrangements[2] which come into force on September 30th, 2019 are aiming to establish a more harmonised framework for all financial institutions and set out specific provisions for the institutions' governance frameworks regarding their outsourcing arrangements and the related supervisory expectations and processes.

The Guidelines set the following requirements for the internal audit function:

The internal audit function's activities should cover, following a risk-based approach, the independent review of outsourced activities. The plan and programme should include the outsourcing arrangement of critical or important functions.

Regarding the outsourcing process, the internal audit function should at least ascertain:

a. *That the institution's or payment institution's framework for outsourcing, including the outsourcing policy, is correctly and effectively implemented and is in line with the applicable laws and regulation, the risk strategy and the decisions of the management body*
b. *The adequacy, quality and effectiveness of the assessment of the criticality or importance of functions*
c. *The adequacy, quality and effectiveness of the risk assessment for outsourcing arrangements and that the risk remain in line with the institution's risk strategy*
d. *The appropriate involvement of governance bodies, and*
e. *The appropriate monitoring and management of outsourcing arrangements.*

Noter

[1] International Standards for Assurance Engagement, No. 3402, Assurance Reports on Controls at a Service Organization

[2] EBA/GL/2019 as of 25 February 2019

Nye medlemmer

Nye medlemmer i IIA fra 5.12.2018 – 27.3.2019

A.P. Møller
Sam Xi Liu

Arbejdernes Landsbank
Marit Magnussen

ATP
Dennis Breitowicz
Jacob Scheffmann Hänsch

Danske Bank
Mikkel Sverdrup Henriksen

Deloitte
Jonas Larsen
Mads Frederik Schilling Schubart
Snezana Janjic
Jakob Lindberg

Finanstilsynet
Henry Victor Luján

Forsvarsministeriets Interne Revision
Ask Ransdal Haugegaard

Global Risk Clinic
Michael Jensen

KPMG
Charlotte Pontoppidan Frost

Nordea
Daniel Halstad

Nykredit
Stinus Nielsen

Rigspolitiet
Anne Mette Rasmussen

Saxo Bank
Peter Erikstrup

Semler Gruppen
Patrick Bidstrup

Skandinaviska Enskilda Banken
Morten H. Raskov

Tryg
Henrik Schou-Olssen

Ørsted Services
Sezen Yildirim Unnu

Uddannelsesaktiviteter

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

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

Kurser og gå-hjem møder

02.05.2019: Kursus for Forsikringsrevisorer
15.05.2019 - 16.05.2019: IIA Årsmøde 2019

"Bagsmækken"

Foreningens adresse

Foreningen af Interne Revisorer (IIA)
Att.: Vicerevisionschef 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.iia.dk eller til:

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

Jobannoncer

Jobannoncer for medlemmer kan bringes på foreningens hjemmeside og/eller i INFO.
Annoncer bringes kun i INFO, såfremt der er plads hertil.
Annonceudkast sendes til redaktionens adresse, jf. side 1, eller til glt@nykredit.dk.

Certificeringer

Nærmere oplysninger om certificeringer kan fås på IIA´s internationale hjemmeside www.globaliia.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
Vicerevisionschef
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 ✉ abrpwe@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