INFO

Foreningen af Interne Revisorer
Nummer 69 | September 2018 | 23. årgang

Hands on: Få konkret inspiration til

- **Strukturering af operationel revision**
- **Værdien af compliancefunktionen**
- **Ideel anvendelse af Process Mining**

Outsourcing er fortsat "hot"

Gennemgang af nye retningslinjer fra European Banking Authority

Audit of Model Risk Management

Bliv klogere på den nye IIA Practice Guide

IIA International Conference 2018 ● **CIA - praktisk håndbog**

INFOs redaktion

Ansvarshavende redaktør
CIA, CISA
Birgitte Rousing Svenningsen
☎ 30 65 41 30 ✉ Birgitte.Rousing@svenningsen.eu

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
☎ 55 47 33 08 ✉ vanita.hork@nordea.com

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

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

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

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

Næste nummer
INFO 70 udkommer i december 2018.
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

Birgitte Rousing Svenningsen, CIA, CISA

Hands-on
Selv om der ikke er uanet mængder af teoribøger om intern revision, så findes der dog et fornuftigt antal. Disse beskriver blandt andet intern revision med udgangspunkt i "The International Professional Practices Framework" udgivet af vores moderorganisation. Begrebet "Operational Auditing" har tillige været velbeskrevet i årtier af Andrew Chambers fra England. Fælles for teoribøgerne er dog, at de i begrænset omfang beskriver, hvorledes metodikken implementeres i praksis, og i det hele taget hvordan man i praksis udfører intern revision på bedste vis. Det prøver vi i det nummer af INFO at råde bod på, idet bladet indeholder en række artikler med detaljerede og praktiske information om, hvordan man gør. Kort sagt – hands-on artikler.

Operationel revision
Operationel revision er en relativ ny metodik i intern revision i Danmark, hvorfor metodikken fra en praktisk indgangsvinkel kun er beskrevet i mindre omfang. For nogle er det derfor et ukendt spøgelse. Dette er ikke tilfældet for Niklas Pind fra Express Bank, som i nogle år har arbejdet hermed. I artiklen "Intern revision og udførelsen af operationel revision" giver han sit bud på, hvordan man i praksis strukturerer operationel revision. Niklas peger på, at den anvendte metodik for operationelle revisioner tager sit afsæt i de tre kerneområder – Compliance, Efficiency og Management. Endvidere giver artiklen et indblik i, hvordan revisionens og rapporteringens faser er struktureret under den operationelle revisionsmetodik. Artiklen giver således et hands-on billede, som er god inspiration, og som medvirker til at svare på, hvordan gør man.

Process mining
Et af værktøjerne, som man kan anvende til såvel operationel revision som til finansiel revision, er process mining. Ved hjælp af nogle konkrete eksempler giver Martin Schantz Pickardt fra PwC os et indblik i, hvordan process mining kan anvendes. Helt lavpraksis så identificerer process mining de faktiske datastrømme i virksomheden, hvorefter revisor kan vurdere, om de er effektive, og om de er i overensstemmelse med de af ledelsens ønskede flows.

Compliancefunktion
Three-line of defense har vi efterhånden hørt nok til, men for at få det optimale ud af modellen er det væsentligt, at den interne revisor forstår at anvende det arbejde, som udføres af second line funktionerne – heriblandt compliancefunktionen. For at kunne gøre dette skal revisor i første omgang vurdere tilstrækkeligheden af compliancefunktionen. Men ud fra hvilke kriterier?

Tobias Zorde fra Nykredit oplister på systematisk og detaljeret vis, hvilke kriterier man bør forholde sig til. Artiklen er ment som et inspirationsoplæg, men kan i mange tilfælde anvendes 1:1. Hvorfor der ikke længere er en undskyldning for, at man ikke ved, hvordan man skal gribe en revision af compliancefunktionen an.

Model Risk Management
Mere hands-on får vi i artiklen "Audit of Model Risk Management". Med udgangspunkt i bl.a. den nylige offentliggjorte Practice Guide fra IIA, beskriver Clara Dyhrberg fra Nordea, hvordan revision af Model Risk Management kan gribes an i praksis.

Outsourcing
Vi slutter af med en artikel om det altid hotte emne "outsourcing". Med udgangspunkt i specielt lovgivningen og vejledninger for pengeinstitutter gives der svar på nogle af de konkrete problemstillinger som findes i den praktiske verden. Dette omfatter grundlæggende hvordan outsourcing defineres, hvilke forhold man skal være opmærksom på ifm. outsourcingskontrakter, koncernintern outsourcing, cloud løsninger og den interne revisors rolle.

Artikler for alle interne revisorer
Forfatterne bag de fleste af artiklerne kommer fra finansielle virksomheder, hvor vi også finder de fleste interne revisorer i Danmark. De praktiske eksempler og opskrifter på, hvor går man det i praksis, er dog ikke dediceret rettet mod den finansielle sektor, men kan også anvendes af alle andre interne revisorer, idet hovedparten af dem bygger på internationale IIA principper. I denne sammenhæng kan der også gøres reklame for CIA certificeringen, som udbydes af IIA. Denne certificering giver et overblik over standarder og vejledninger fra IIA og information om, hvordan intern revision udføres også uden for Danmarks grænser. Camilla Jonassen og Carsten Kibugi Røjgaard har på siderne 6-8 skrevet om, hvordan du griber studierne an og med succes får en CIA certificering.

God læselyst!

Nyt fra redaktionen

Birgitte Rousing Svenningsen, CIA, CISA

Positive budskaber er altid dejlige at bringe. Det er mig en glæde at kunne annoncere, at vi har fået to nye redaktionsmedlemmer. Morten Bendtsen fra PFA og Vanita Shukla Hork fra Nordea har således meldt sig til at hjælpe med arbejdet i redaktionen.

Morten har tidligere været medlem af redaktionen, men har holdt en mindre pause. Morten kommer med adskillige års erfaring fra intern revision i Nordea, Danske Bank, Finansiel Stabilitet og PFA. Vi er glade for gensynet med Morten i redaktionen.

Vanita har sin baggrund fra 1. og 2. line funktioner i Nordea, før hun kom til den interne revision i Nordea i 2014. Vanita har derfor mulighed for at bidrage med et internationalt perspektiv.

Vi ser med stor glæde frem til samarbejdet med de to nye redaktionsmedlemmer.

Nye certificeringer

Martin Pickardt, PwC - CIA
Suraj Anvekar, Mærsk - CRMA
Benjamin Jensen - CCSA
Thomas N. Sørensen, Ørsted - CIA, CRMA

Et stort tillykke med certificeringen !!!!

Der er fra og med 2018 indført et årligt uddannelseskrav på min. 2 CPE points omhandlende "Code of Ethics", til alle IIA certificerede. IIA har udviklet et OnDemand kursus som du kan læse mere om på https://ondemand.theiia.org.

Specialist til revision af kapital- og risikostyringsområdet i København

Vil du være med til at løfte arbejdet med revision af kapital- og risikoområdet i Danmarks største realkreditinstitut? Så har vi måske dit næste job.

Din kommende arbejdsplads
Nykredit er Danmarks største udlåner med udlån på 1.200 mia. kr. og en egenkapital på mere end 75 mia. kr. I Intern Revision hjælper vi bestyrelsen og revisionsudvalget med at beskytte virksomhedens aktiver, omdømme og bæredygtighed. Vi gør dette ved at vurdere, om alle væsentlige risici er identificerede, rapporterede samt underlagt behørig kontrol og ved at udfordre den daglige ledelse til at forbedre governance, risikostyring og intern kontrol, hvor der er behov.

Intern Revision er en progressiv og teamorienteret afdeling på 17 medarbejdere, hvor der lægges vægt på at være på forkant med nye standarder og metoder. Vi har korte beslutningsveje, og du får i høj grad mulighed for at påvirke din egen arbejdsdag. Vi lægger vægt på, at dit arbejdsliv og fritids-/familieliv er i balance og tilbyder blandt andet flextid og en attraktiv pensionsordning.

Dine arbejdsopgaver
Du bliver en del af et ambitiøst og innovativt team, som beskæftiger sig med revision af kapital- og risikostyringsområdet. Ansvarsområdet spænder bredt og dækker blandt andet over gennemgang af Nykredits interne modeller til beregning af kredit- og markedsrisici samt opgørelse af kapitalbehovet. Området er præget af en konstant udvikling, hvilket kræver, vi er på forkant med metoder og lovgivning.

To dage er sjældent ens i Intern Revision, hvorfor du skal trives med at kaste dig ud i områder, du ikke er hjemmevant i. Du kommer bl.a. til at:

- deltage i etableringen af en risikobaseret revisionsplan
- være Audit Lead på revisionsopgaver eller deltage som ressource
- kommunikere konklusioner til vores stakeholders
- følge op på revisionsobservationer
- vedligeholde netværket inden for vores revisionsområdet
- udføre continuous monitoring-aktiviteter.

Hvem er du?
Du har stærke analytiske evner, som du kombinerer med en praktisk "hands-on"-indstilling. Du har et højt fagligt niveau understøttet af en relevant kandidateksamen med hovedvægt på økonomi og statistik, som f.eks. cand.polit, cand.oecon, cand.merc.mat eller lignende. Erfaring fra kapital- og risikostyringsområdet og et kendskab til SAS/SQL vil være en fordel.
Det er helt afgørende, at du er indstillet på at tillære dig revisionsdisciplinen, som foregår i kombination mellem on-the-job-træning og undervisning af vores Operations Team. Du skal endvidere have stærke kommunikative evner, da vedligeholdelse af netværket i forretningen er central for din succes. Endelig har du som specialist fokus på detaljerne, således at du sikrer struktur og kvalitet og samtidig bevarer overblikket for at sikre det rette fokus.

Er du interesseret?
Søg jobbet online. Har du spørgsmål til stillingen eller Nykredit som virksomhed og arbejdsplads, kontakt chefspecialist Tobias Zorde, 21185497 / tzo@nykredit.dk, eller seniorrekrutteringspartner Rasmus Bothmann, 50495542 / rbo@nykredit.dk.

Ansøgningsfrist 13.oktober 2018

OM NYKREDIT
Nykredit er en finansiel koncern, der sammen med vores partnerbanker i Totalkredit vil være danske boligejeres foretrukne finansielle partner. Vi står op for at rykke endnu tættere på vores kunder - og går du en ekstra mil for dem, for projektet og for Nykredit, gør vi det samme for dig. Du har mange muligheder for at være med til at udvikle Nykredit, samtidig med at din karriere altid vil være i bevægelse. Mod nye udfordringer, andre opgaver og større ansvar i Nykredit.

Altid i bevægelse

CIA uddannelsen - praktisk dagbog

Bestyrelsen har i sin strategi for IIA fastlagt en målsætning om, at foreningen skal medvirke til en høj faglig standard blandt interne revisionsafdelinger ved at gennemføre relevant, udviklingsorienteret og målrettet uddannelse. Et af de områder, som har høj prioritet, er ønsket om at øge antallet af certificerede interne revisorer blandt foreningens medlemmer.

Det er derfor rigtig glædeligt, at det er lykkedes at lave en aftale med IIA Global i USA om et samarbejde, som betyder, at IIA kan tilbyde forberedelseskurser til CIA certificeringen i Danmark. På nuværende tidspunkt er forberedelseskurser til CIA eksamen del 1 og del 2 veloverstået.

Vi har på redaktionen hermed fornøjelsen af, at kunne præsentere to kursisters oplevelser som en slags praktisk "dagbog" omkring læseforløbet, undervisningen og eksamen.

Camilla Jonassen, Internal Auditor, Arbejdernes Landsbank

Som revisor ligger det i vores DNA altid at opsøge nye muligheder for fortsat professionel og personlig udvikling. CIA har længe været anerkendt i udlandet og derfor var det rigtigt interessant, at IIA Danmark ville udbyde dette specifikke "turbo" CIA forløb. Jeg har længe overvejet at tage en CIA, men er bare ikke kommet i gang, så dette forløb gav rigtig god mening.

Undervisningen foregår på engelsk med en amerikansk underviser som benyttes af IIA Global ikke kun i USA, men også i andre dele af verdenen. Hun er super engageret, med højt humør og god indlevelse. Hun forstår at formidle teorien i det modtagne undervisningsmateriale, som består af fysiske bøger, samt online sitet CIA Learning System.

Undervisningen foregår over 2-3 dage pr. del, hvor tilhørende undervisningsmateriale gennemgås i heftigt, men dog kontrolleret, tempo. Det kan tydeligt mærkes, at underviseren er vant til at undervise ud fra materialet. Det fysiske undervisningsmateriale gennemgås fra A- Z. Det kræver en god portion koncentration at følge med, men som afbræk i gennemgangen er der indlagt gruppearbejde ved bordene, hvor der er mulighed for diskussion, samt små interne quizzer. Generelt er der en god diskussion på holdet, hvor teori sættes op imod praksis og dette er nødvendigt da teorien i de amerikanske lærebøger ikke altid er enslydende med vores kendte praksis fra Danmark. Der er enkelte ting i pensum, samt i tidligere eksamensspørgsmål som inddrages i undervisningen, hvor både elever og underviser ikke er helt enige i undervisningsmaterialet.

Selve eksamensformen kræver tilvænning og forberedelse. Som eksamensforberedelse er det nødvendigt, at man tager sig tid til at genbesøge undervisningsmaterialet, bruge en del tid på at besvare de små quizzer samt gennemføre prøveeksamen, som er tilgængelig via online sitet CIA Learning System. Man bør gøre dette om og om igen.

Ved ankomst til eksamen skal man være opmærksom på, at den første eksamen kan virke en smule afskrækkende da der foreligger en del regler/restriktioner fra IIA Global, såsom at dit fingeraftryk bliver taget et par gange for korrekt identifikation, eventuelle briller bliver "testet" for teknik, der må ikke medtages andet til eksamen end nøglen til det skab, hvor du har opbevaret din taske og jakke, og du må ikke tage trøjer af/på til eksamen ved varme/kulde.

Det kan tydeligt mærkes, at uddannelsen har grobund i det amerikanske, da eksamen udmunder sig i en besvarelse af spørgemål med multiple choice muligheder. For at forstå spørgsmålene er det nødvendigt at man er fortrolig med engelsk , da man er under tidspres. Ydermere skal man være forberedt på, at der ved udarbejdelse af spørgsmålene ikke er tænkt på, at der er eksaminander (som os her i Danmark) som ikke har engelsk som modersmål og dermed vil der forekomme ord og ordstillinger, som man, uagtet ens sproglige formåen, kan være ret usikker på. Til eksamen må der medbringes en engelsk ordbog, hvilket kan være en god støtte. Som beskrevet tidligere vil der være eksamensspørgsmål hvor praktikken fra Danmark ikke helt stemmer overens med teorien fra lærebøgerne og her er det vigtigt at holde hovedet koldt og besvare spørgsmålene i overensstemmelse med teorien fra lærebøgerne – når man først man besidder revisionserfaring, kan dette faktisk være lidt vanskeligt til tider.

For mit eget vedkommende har eksamensformen været en personlig udfordring, hvor mit fokus har været at tage mig den tid til spørgsmålene som jeg egentlig har, fremfor at stresse igennem eksamen.

Det er min vurdering, at "turbo-forløbet" er en rigtig god måde at få gennemgået pensum på. Vores hold består af personer fra mange forskellige virksomheder og samtidigt af personer som ikke arbejder som interne revisorer til hverdag. Denne kombination åbner for en rigtig god diskussion i timerne, og hjælper ligeledes til, at man opbygger et bredt netværk.

Carsten Kibugi Røjgaard, Chef for Intern Kontrolenhed i Region Sjælland

Jeg har valgt at læse CIA for at styrke mine kompetencer inden for intern revision, og samtidig få et større netværk med ligesindede som arbejder med intern revision og interne kontroller. Jeg har bestået del 1, jeg har været på forberedelseskursus del 2 og er nu tilmeldt eksamen på del 2.

Der er nogle krav man skal opfylde for at kunne blive certificeret og man skal indsende dokumentation til IIA Global omkring uddannelse, erfaring, egnethedsvurdering, identifikation mv. Det er en god ide at have alt dette på plads, inden man går i gang med undervisningsforløbet.

I forbindelse med tilmelding til forberedelseskursus, bestilte jeg CIA Learning System. Man modtager både bøger og adgang til et online learning system med bl.a. quiz spørgsmål, hvor man kan teste sin viden.

Op til forberedelseskurset er det en god idé som minimum at tage en "pre test", så underviseren kan se kursusdeltagerens viden inden for de enkelte dele som skal gennemgås på kurset. Underviseren på forberedelseskurserne, Deanna Sullivan, er ret god og hun formår at gøre undervisningen både interessant og sjov. Deanne sørgede for en god blanding af klassisk undervisning, quiz spørgsmål, gruppearbejde og klassediskussioner.

Da jeg læste op til eksamen valgte jeg at læse tidligt om morgenen, mens kone og børn sov og der var ro til at læse. Så havde jeg stadig tid til at lave ting sammen med dem om aftenen efter arbejde, og om morgenen var jeg udhvilet og klar til at læse op på stoffet.

I min eksamensforberedelse fokuserede jeg på at besvare quiz spørgsmål i online systemet for at se hvilke områder, som jeg var stærk i, og hvilke områder jeg skulle bruge mere tid på at læse op. Fordelen ved at lave quiz spørgsmål er også, at man får umiddelbar feedback efter hvert spørgsmål med en forklaring på hvad der er det rigtige svar.

Det giver også en læring i forhold til de forskellige områder, hvor man svarede forkert, men også områder hvor man var i tvivl. Det synes jeg har virket rigtigt godt. Samtidig er træningen i quiz spørgsmål også træning i eksamensformen, da eksamen sker med udgangspunkt i tilsvarende quiz spørgsmål.

Op til eksamen læste jeg så op på de områder, hvor jeg var et stykke fra beståelsesprocenten. På den måde fokuserede jeg min tid på de områder, hvor der var behov for at læse op.

Samtidig med selvstudierne er jeg også med i en studiegruppe med tre andre kursusdeltagere fra forberedelseskurserne. Vi har mødtes tre gange, og vi har gennemgået quiz spørgsmål og eksamen mv. Det har også været en rigtig god hjælp at drøfte spørgsmål med de andre fra studiegruppen.

Jeg tilmeldte mig til eksamen ret tidligt i forløbet. På den måde forpligtede jeg mig selv med en tidsfrist, men jeg sørgede samtidig for at have nok dage til at kunne forberede mig bedst muligt til eksamen. Jeg lagde eksamensdatoen en mandag og brugte weekenden til at forberede mig intenst de sidste par dage inden eksamen. Jeg havde også sikret mig opbakning til, at jeg kunne fokusere på min eksamensforberedelse, så min familie gav mig ro til det.

Det er vigtigt at komme i god tid til eksamen, da indtjekning kan tage lidt tid. Eksamen er en multiple choice test efter samme opskrift som de online quiz spørgsmål, der i IIA's CIA Learning System. Til eksamen fokuserede jeg på hurtigt at besvare de spørgsmål, som jeg umiddelbart kunne besvare. De lidt sværere spørgsmål flagede jeg og gemte til den sidste del af eksamen, så jeg var sikker på at kunne nå at besvare alle spørgsmål.

Jeg synes kombinationen af forberedelseskursus, bøger, online quiz spørgsmål og læsegruppe giver et godt læseforløb og gør det nemt at forberede sig til eksamen. Et godt råd er selvfølgelig at afsætte den fornødne tid og sikre sin families opbakning til at studere nogle timer om ugen - og især op til eksamen.


CERTIFIED
INTERNAL
AUDITOR

IIA International Conference 2018

Peer Højlund, Chefspecialist, Nykredit samt medlem af IIA's uddannelses-udvalg

Årets internationale IIA konference blev afholdt i Dubai i perioden 7. – 9. maj. Konferencens vært kunne stolt indlede med at oplyse, at der var tale om første gang, at en IIA global konference fandt sted i Mellemøsten, og at der samtidig var tale om rekord, med over 3000 deltagende fra mere end 100 medlemslande.

Som det er sædvane bestod konferencen af et mix af **general** sessions og **break-out** sessions fordelt på op til 11 samtidige streams. Det samlede program for konferencen kan ses her: www.iia.dk/materialer/2018-ic-brochure.pdf

Med et så stort antal indlæg spænder emnerne selvfølgelig vidt, men de mest gennemgående temaer faldt indenfor 3 kategorier, henholdsvis

1) digitalisering/robotics/artificial intelligence
2) cybersikkerhed samt
3) besvigelser og korruption.

Specielt et indlæg af Wael Ahmed Fattouh, Partner, Cybersecurity and Technology Risk, PwC gav stof til eftertanke ved at tilgå det vi traditionelt kalder it-revision på en lidt anden måde – set fra stakeholders/revisionsudvalgets side, og rapporteret som:

- IT Governance, eks. risikovurderingsproces, awareness, third party risk data inventory
- Data privacy, eks. privacy by default og privacy by design
- IT Security and Applications, eks. nøglekontroller, funktionsadskillelse og end user computing
- IT Cybersecurity, eks. adgangssikkerhed, patching og SOC
- Change Management and Computer Operations, eks. change, outsourcing og beredskab.

Konferencen havde følgende **general** sessions:

- **Global issues impacting business**. Richard Quest fra CNN styrede en paneldiskussion hvor to ministre fra henholdsvis Saudi Arabien og Dubai stillede op til nærgående spørgsmål om demokrati, kvinders rettigheder mv.
- **A whole new world? Exponential Technology Development and its implications for individuals, organisations and the society** – om vigtigheden af at gøre sig bevidst om den igangværende "4. Industrielle revolution", herunder hvordan forandringerne i verden omkring os påvirker vores virksomheder.
- **Triple I's. Information technology, Innovation and Internal Audit.** Samme tema, denne gang med fokus på hvordan intern revisions dagligdag, arbejde og (måske?) berettigelse påvirkes.
- **Keeping secure in the physical and digital realms through artificial intelligence.** Se omtale nedenfor.
- **Reaching new heights with innovation.** Se omtale nedenfor.

Generelt er det min vurdering, at deltagelse i konferencen giver et rigtig godt udbytte, i form af inspiration til arbejdet hjemme på kontoret. Selvfølgelig er der både gode og mindre gode indlæg, men særligt de to **general** sessions på sidste dag om henholdsvis **artificial intelligence**, og **reaching new heights with innovation** skilte sig ud og efterlod et dybere indtryk.

Indlægget om artificial intelligence blev fremført af den kun 14-årige (!) indisk/canadiske dreng, Tanmay Bakshi, der har udviklet apps siden han var 5 og arbejdet med kunstig intelligens siden han var 8. I et usædvanligt højt tempo blæste han samtlige delegerede tilbage i stolene og fik gjort os klogere på anvendelse, forventninger, muligheder og trusler forbundet med kunstig intelligens. Jeg noterede mig, at han så positivt på fremtiden og, at der nok skulle blive brug for os alle sammen fremover, om end indholdet af vores arbejde nok kommer til at ændre sig.

I forlængelse af førnævnte session afsluttedes konferencen med en sidste fælles session, fremført af Mohammed Alabbar, stifter og formand for Dubais største entreprenørvirksomhed mv., Emaar Properties.

Han lagde ud med at henvise til indlægget om kunstig intelligens med budskabet om, at det er mennesker som Tanmay Bakshi vi er oppe imod i fremtidens konkurrencemiljø – innovative, hurtigt opfattende, hurtigt arbejdende og omstillingsparate – og betonede vigtigheden af at følge med, eller blive ladt i stikken. De gamle dage er slut, og hvis virksomhederne (og deres revisorer) ikke evner at imødegå den disruption, der aktuelt skyller ind over os, vil vi hurtigt blive ligegyldige, herunder konstant udvikling af ny teknologi, etablering af nye forretningsmodeller, forkastelse af traditionelle politiske systemer, ændring i krav til arbejdstid og tilgængelighed for arbejdspladsen, samt ændringer i kundens forventninger og kundens adfærd osv. osv. M. Alabbar opfordrede os til at spørge os selv, hvor gode vi selv er til forandring, når selve det at forandre sig, er forudsætningen for at overleve i det aktuelle konkurrencebillede.

Som afslutning på konferencen fratrådte Mike Peppers som Global Chairman. Ny mand på posten for 2018/2019 er Naohiro Mouri, Japan. Hans præsentation af tema for den kommende periode kan ses her:
https://www.theiia.org/sites/auditchannel/Pages/player.aspx?v=prMjM2ZjE66akNDs12hGtd3p2EZNqq-y

Næste års globale konference afholdes i Anaheim, Californien i dagene 7. til 10. juli.

Intern revision og udførelsen af operationel revision

Niklas Pind, Head of Internal Audit, Express Bank

Indledning

Som ansvarlig for en intern revision i en mindre nordisk konsumer bank, der er en del af en stor international bank, har jeg det privilegium, at have adgang til og arbejde efter en detaljeret og dokumenteret revisionsmetodik. Det primære fokus er at tilføre værdi gennem udførelse af forskellige former for operationelle revisioner. Intern revision er i mit tilfælde ikke involveret i den finansielle revision af årsregnskabet og anden finansiel rapportering. Dette varetages helt af ekstern revision, hvor samarbejdet består i at udveksle rapporter, konklusioner og generelt dele viden, som er relevant for begge parter.

Enkelte interne revisionsfunktioner er en del af en større koncernrevision, som har ressourcer til at formulere og vedligeholde interne standarder for forskellige typer af revisioner. Mindre interne revisionsfunktioner er mere udfordret og overladt til egne forestillinger om hvad en operationel revision skal indeholde. Selvom beskrivelsen i denne artikel er på et meget overordnet niveau, så er håbet, at det kan give lidt inspiration og viden til de medlemmer, som netop nu sidder med den udfordring det er, at redefinere sin revisionstilgang og overgå til at udføre flere operationelle revisioner.

Revisionsmetodik

I den anvendte revisionsmetodik rækker omfanget af operationel revision længere end den traditionelle operationelle revision, der har et mere direkte fokus på procedurer og udførte kontroller. Den anvendte metodik for operationelle revisioner tager sit afsæt i tre kerneområder - se **Figur 1** herunder.

Den operationelle revision dækker alle forsvarslinjer, dvs. de aktiviteter og kontrolprocesser, der udføres i både første og anden forsvarslinje. Alle afdelinger og områder

Figur 1: Operationel revision - 3 kerneområder

1. Audit Compliance

- Undersøge, om der er etableret og implementeret relevante procedurer, herunder at:
  - implementerede procedurer er i overensstemmelse med koncernprocedurer
  - implementerede procedurer er i overensstemmelse med relevant lovgivning og standarder på området
- Undersøge, om det implementerede kontrolmiljø i dets opbygning, organisation og sammensætning er i overensstemmelse med koncernens interne kontrolcharters og lovgivningsmæssige principper og krav

2. Audit Efficiency

- Vurdering og test af relevansen og effektiviteten i:
  - implementerede procedurer
  - implementerede kontroller
  - implementeret organisation
- Vurdering af om de reviderede processer benytter sig af en effektiv brug og allokering af interne ressourcer, herunder:
  - personalemæssige ressourcer
  - medarbejderes kendskab til og viden omkring opgaver og ansvar
  - teknologiske (IT) ressourcer og systemer

3. Audit Management

- Vurdering af ledelsens evne og succes til at:
  - kommunikere relevante strategiske og operationelle mål og delmål til det reviderede område, primært ved at definere key performance indicators (KPI'ere)
  - Styre og følge op på de udstukne KPI'ere
  - definere, kommunikere og implementere det krævede interne kontrolmiljø og organisation i det reviderede område
  - følge op på og håndtere rapporterede svagheder

har dedikerede medarbejdere, såkaldte "operational permanent control" medarbejdere, som enten fuldt ud, eller som en del af deres andre opgaver, udfører kontroller i afdelingen. Disse medarbejdere er med til også at promovere en sund kontrolkultur i de enkelte afdelinger. I anden forsvarslinje undersøger revisionen primært om compliance og risikostyringsfunktionerne har udført deres opgaver i henhold til nedskrevne charters, procedurer, lovgivning osv.

Den enkelte operationelle revision har til formål at konkludere og rapportere til ledelse, bestyrelse og revisionsudvalg primært på følgende hovedområder, baseret på de tre kerneområder ovenover:

1. Har banken (det reviderede område) formået at implementere relevante og effektive procedurer, som er i overensstemmelse med koncernens regler, samt lokal lovgivning?
2. Har banken (det reviderede område) formået at implementere en relevant og effektiv organisation i det revidere område, herunder:
   - er der etableret tilstrækkelig funktionsdeling?
   - kender væsentlige medarbejdere deres opgaver og ansvar?
   - er der allokeret tilstrækkelige personalemæssige ressourcer til området?
3. Har banken (det reviderede område) implementeret relevante og effektive (IT) systemer, og er de sikret tilstrækkeligt (administrering af adgange, roller, data, backup osv.)?
4. Er der defineret en strategi for det reviderede område, hvor relevante og målbare key perfomance indicators (KPI'ere) er formulerede, kendte og anvendte?
5. Har de ansvarlige for det revidere område defineret og dokumenteret en beskrivelse af de væsentligste risici (risk mapping), samt defineret en tilstrækkelig dækkende kontrolplan?
6. Er kontroller udført korrekt og rettidigt (både i første og anden forsvarslinje)?
7. Er ansvars- og opgavefordelingen mellem første og anden forsvarslinje defineret og respekteret?
8. Foretages der rapportering af resultater, kontroller, incidents osv. fra området til alle krævede modtagere, og foretages det på bagrund af korrekte data og rettidigt?

I forhold til operationelle revisioner, der har et mere smalt fokus på kerne kontrolmiljøet, udvider de i ovenstående beskrevne operationelle revisioner dette til også konsekvent at inkludere en vurdering af operationel performance, organisation og anvendelse af ressourcer. Dvs. det reviderede område vurderes ikke kun ud fra en betragtning om evnen til at administrere et pre-defineret kontrol setup, men også om ledelse og det reviderede område forstår og understøtter bankens strategiske og operationelle mål. Dette er ud fra en betragtning om, at intern revisions opgave er at give assurance til bestyrelsen (og andre væsentlige stakeholders, herunder ledelsen) om banken på en tilstrækkelig kontrollet måde er i stand til at opnå de af bestyrelsen udstukne strategiske og operationelle mål. Dette kan der ikke alene konkluderes på, hvis der fokuseres ensidigt på det implementerede kontrolmiljø. Der er en forbindelse mellem kontrol og drift, hvilket måske er hvad nogle bestyrelser og virksomhedsledelser efterlyser i revisionsrapporterne, som kun rapporterer på svagheder i kontrolmiljøet uden synlig sammenhæng til strategier og mål.

Herudover indeholder udførelsen af de operationelle revisioner ligeledes en relativ høj grad af "indbygget" compliance revision, da en del af den operationelle revision inkluderer en vurdering og test af, om relevant lovgivning er overholdt og implementeret i relevante processer, procedurer, kontroller osv. Omvendt vil dedikerede compliance revisioner ligeledes indeholde en vis grad af den operationelle revisions elementer, hvor den primære forskel på en operationel og compliance revision er, om genstanden for revisionen er en proces, risiko eller aktivitetsområde (compliance sekundær fokus), eller en specifik lovgivning (f.eks. hvidvask, databeskyttelse, outsourcing etc.), hvor overholdelse af en bestemt lovgivning er primær fokus. En dedikeret compliance revision vil ofte være opbygget omkring en mere detaljeret "paragraf for paragraf" gennemgang, hvor den operationelle revision primært identificerer og kontrollerer de væsentligste elementer i en relevant lovgivning.

Det er forventeligt, at alle ledelsesniveauer har fokus på kontrolmiljøet, men den primære interesse herfor er nok størst på bestyrelses-, revisionsudvalgs- og lovgiverniveau (følges bankens strategi på en kontrolleret måde). Den daglige ledelse har mere fokus på virksomhedens evne til at præstere ift. til de af bestyrelsen udstukne strategiske mål, overordnede budget mål osv., hvor kontrolmiljøet kun er ét område ud af mange områder, som skal styres for at opnå den ønskede performance.

Derfor opfattes konklusionerne fra de udførte operationelle revisioner ofte af ledelsen som at indeholde en større værdi, hvis der er en stærkere sammenhæng mellem kontrol og drift. De afgivne revisionsanbefalinger skal ikke kun løses for at forbedre kontrolmiljøet, men også for at forbedre det reviderede områdes evne til at opnå den ønskede operationelle performance på baggrund af et effektivt og tilpasset kontrolmiljø.

Den endelige revisionsrapport indeholder revisionsanbefalinger, som kan dække ethvert af ovenstående områder, men den endelige rating er baseret på ledelsens evne og kapacitet til at implementere et tilstrækkeligt kontrolmiljø afstemt til bankens strategiske og operationelle mål. På denne måde bliver ledelsen altid ansvarlig for og målt på baggrund af de styrker og svagheder, som er identificeret. Den overordnede konklusion er derfor en direkte rapportering til bestyrelsen og andre væsentlige stakeholders om hvorledes den indsatte ledelse er i stand til at forvalte bankens ressourcer på en kontrolleret måde for at opnå de udstukne strategiske og operationelle mål.

Revisionens faser

De udførte operationelle revisioner er opdelt i 4 faser - se **Figur 2** nedenfor. Den traditionelle opdeling i planlægning-udførelse-rapportering er i dette tilfælde udvidet således, at udførelse er opdelt i 2 faser; "Evaluation" og "Investigation".

Rapporteringens faser

Den anvendte revisionsmetodik indeholder klare krav og regler for hvornår og hvordan et revisionsteam annoncerer og holder ledelsen og det reviderede område orienteret omkring udførelsen af en revision. I **Figur 3** på næste side er vist hvilke rapporteringsfaser der gennemgås og udføres kronologisk, og de hænger sammen med revisionens faser, som beskrevet ovenover og vist i **Figur 3**.

Viden, ressourcer og udførelse af operationelle revisioner med et bredere fokus

I sidste ende er det dog klart, at udførelsen og afrapportering af operationelle revisioner, som beskrevet her, kræver flere revisionstimer end en revision, der mere begrænset dækker et kernekontrolmiljø, og kun inkluderer andre operationelle elementer, såfremt de er direkte årsag til svagheder i kontrolmiljøet. Herudover kræver den her beskrevne rapportering og informationsproces også flere ressourcer, end blot at aflægge en rapport ved endt revision.

Flere tiltag er udført for at gøre revisionsprocessen så effektiv som mulig. F.eks. er der adgang til et omfattende bibliotek af pre-definerede revisionsinstrukser, som dækker alle væsentlige risiko- og aktivitetsområder. Ud over at sikre, at revisionsteams ikke ved planlægningen af en ny revision skal bruge ressourcer på dette, så sikrer dette ligeledes en mere ensartet revision på tværs af organisatoriske enheder.

Figur 2: Operationel revision - 4 faser

1. Planlægning	2. Evaluation (gennemgang)	3. Investigation (test)	4. Rapportering
• Grundlæggende planlægning af ressourcer, team osv. • Fastlæggelse af scope • Udvælgelse af revisionsinstruks • Planlægning af interviews • Udarbejdelse og udsendelse af materialeliste • **Udarbejdelse og udsendelse af "assignment letter" (se næste afsnit)** • **Afholdelse af "Kick-off" møde (se næste afsnit)**	• Gennemgang af det modtagende materiale • Udførelse af interviews • Første identifikation af væsentlige styrker og svagheder (første identificering af potentielle revisionsanbefalinger) • Udvælgelse af delområder, som skal testes yderligere (investigation) • **Afholdelse af "evaluation" møde (se næste afsnit)**	• Planlagte tests udføres • Foreløbige identificerede styrker, svagheder og revisionsanbefalinger understøttes yderligere med detaljeret revisionsbevis fra de udførte test	• Endelige konklusioner formuleres • Endelig og formel accept (kommentering) indhentes fra det reviderede område på de formulerede revisionsanbefalinger • **Afholdelse af "wrap-up" møde (se næste afsnit)** • **Udsendelse af revisionsrapport (se næste afsnit)**

Figur 3: Operationel revision - hvilke rapporteringsfaser gennemgås og udføres

1. Assignment Letter (sendes ud via mail):	2. Kick-off møde	3. Evaluation møde	4. Wrap-up møde
• Første orientering til ledelsen og det kommende reviderede område • Start- og slutdato for revisionen • Præsentation af revisionsteamet • Revisionens scope • Forventelige datoer for afrapporteringsmøder og udsendelse af revisionsrapporten • Udsendelse af foreløbig materialeliste	• Ledelsen og væsentlige medarbejdere fra det reviderede område deltager i mødet • Det tidligere udsendte "assignment letter" gennemgås • Udsendt materialeliste gennemgås • Gennemgang af det videre revisionsforløb	• Ledelsen og væsentlige medarbejdere fra det reviderede område deltager i mødet • Foreløbige styrker og svagheder præsenteres • Præsentation af de udvalgte detaljerede tests og en gennemgang af hvad revisionen forventer af materiale for at udføre testene	NB! Wrap-up mødet er en endelig afrapportering. • Ledelsen og væsentlige medarbejdere fra det reviderede område deltager i mødet • De endelige identificerede styrker, svagheder og revisionsanbefalinger præsenteres • En narrativ konklusion formuleres og præsenteres (executive summary) • Den endelige rating på den udførte revision præsenteres
↓	↓	↓	↓

5. Revisionsrapport

- Primært sammensat af materiale og informationer fra de tidligere afholdte møder, og i forhold til ledelsen og det reviderede område indeholder revisionsrapporten ingen nye informationer og konklusioner.
- Primært tiltænkt en kreds af stakeholders, som ikke har været en del af de tidligere afholdte møder, i særdeleshed lokal bestyrelse og revisionsudvalg, samt relevante funktioner på koncernniveau.

Yderligere, så forsøges der i videst mulige omfang at anvende og basere revisionsbevis på allerede udført arbejde i kontrolfunktionerne i anden forsvarslinje, primært compliance og risikostyringsfunktionen, såfremt revisionen af disse giver et tilfredsstillende resultat. Herudover er der i den anvendte revisionsmetodik muligheden for visse lempelser for revisioner, der ud fra særskilte kriterier, vurderes at være mindre komplekse eller som dækker et mindre væsentligt risikoområde, hvorved dele af den krævede revisionsmetodik kan udføres i en "light" udgave.

Slutteligt, så er det ikke mindst i samråd med bestyrelse, revisionsudvalg og ledelse, at det ønskede omfang af operationelle revisioner skal findes, herunder i hvilken form og omfang rapportering ønskes. Der har i de senere år været en klar trend i og ønske fra lovgivers side om, at danske interne revisionsfunktioner skal udføre mindre finansiel og mere operationel revision, herunder compliance revisioner. De seneste sager i pressen omkring hvidvask af penge samt identifikation og monitorering af kunder og transaktioner, viser kun aktualiteten i ikke kun at have primær fokus på den finansielle revision. At intern revision mindst skal dække og rapportere til bestyrelse og revisionsudvalg på alle væsentlige risikoområder er på overordnet niveau defineret i lovgivningen. IIA standarderne er selvklart en vigtig kilde til vores arbejde og kontekst, men hvis en mindre revisionsfunktion ønsker at bevæge sig fra den finansielle til den operationelle revision, så er der meget få kilder, der kan give en mere informativ indgang til hvad en operationel revision egentlig skal/kan indeholde. Som skrevet indledningsvist, så er håbet, at denne artikel kan give lidt inspiration, samt et opråb til andre om at dele viden og lignende erfaringer omkring udførelsen af operationel revision.

Revision af compliancefunktionen i finansielle virksomheder – et praktisk orienteret inspirationsoplæg

Tobias Zorde, Chefspecialist, CIA, Nykredit

Indledning

Revisionsbekendtgørelsen kræver, at vi i intern revision, som en del af vores § 27 konklusion, vurderer, om compliancefunktionen har de nødvendige ressourcer til at udføre sine opgaver forsvarligt. Vi skal endvidere vurdere, om rapporteringen fra denne funktion er tilfredsstillende, herunder om den er uafhængig fra andre kontrolfunktioner og forretningen i øvrigt. Revisionsbekendtgørelsen foreskriver i øvrigt, at intern revision skal vurdere om de i virksomheden etablerede processer til håndtering af compliancefunktionens aktiviteter er betryggende. Formålet med nærværende artikel er at tjene som inspirationsoplæg til, hvordan vi kan indrette kriterier til brug vurdering af compliancefunktionen og, endvidere, at kaste lys på de mest åbenlyse faldgruber.

En vigtig sondring

Lovgivningen kræver at finansielle virksomheder skal have en compliancefunktion, hvis formål er at vurdere og kontrollere, at virksomheden har metoder og procedurer, der er egnede til at opdage og mindske risikoen for virksomhedens manglende overholdelse af den for virksomheden gældende lovgivning, markedsstandarder eller interne regelsæt. Dette bør vække intern revisions interesse ud fra minimum følgende to dagsordner:

1. Tilrettelæggelse af revisionsstrategi

Eksistensen af en compliancefunktion skaber et meget sandsynligt scope-overlap mellem denne og intern revision. Uagtet om compliancefunktionen betragtes som en decideret assurance-leverandør eller et udbygget lag af intern kontrol, skal intern revision overveje, hvordan dette påvirker revisionsstrategien; f.eks. i hvilket omfang intern revision kan basere sig på arbejde udført af compliancefunktionen.

2. Efterlevelse af Revisionsbekendtgørelsen

Revisionsbekendtgørelsen kræver, at intern revision, som en del af sin § 27 konklusion, vurderer compliancefunktionen på nogle generelle parametre; i særdeleshed tilstrækkelighed ift. ressourcer, rapportering og uafhængighed, samt om virksomhedens processer vedr. compliancefunktionen er betryggende. Formålet med dette at sikre, at compliancefunktionen er indrettet i overensstemmelse med Ledelsesbekendtgørelsens § 17.

Sondringen mellem disse to dagsordner er vigtig! I begge tilfælde foretages en vurdering af compliance funktionen, men på trods af dette adskiller de sig på tre punkter. Som vedrører reaktionsmønster, revisionsgenstand og vurderingskriterier.

Når dagsordenen vedrører tilrettelæggelse af revisionsstrategi er revisionsgangstanden, hvad end der nu er i scope i overensstemmelse med vores opgaveportefølje. Såfremt der er scope-overlap med compliancefunktionen, bliver det aktuelt, at overveje hvordan dette påvirker revisionsstrategien. Her måles compliancefunktion op imod vurderingskriterier, der dybest set har til formål at fastslå, hvor meget deres indretning og arbejdsgange

Tabel 1: Reaktionsmønstret på identificerede svagheder

	Revisionsgenstand	Vurderingskriterier	Reaktionsmønster
Tilrettelæggelse af revisionsstrategi	Dikteret af revisionsplanen	• "Ligner de os?" • IPPF standard 2050 og supplerende vejledninger • ISA 610 (til inspiration)	Tilpasning af revisionsstrategi
Efterlevelse af revisionsbekendtgørelse	Compliancefunktionen på sine egne præmisser	• Ressourcer • Afhængighed • Rapportering • Betryggende processer	Rapportér svagheder og inddrag i § 27 konklusion.

ligner vores egne i intern revision[1]. I det omfang de så ikke ligner os, vil reaktionsmønstret være, at vi kun i begrænset omfang baserer os på deres arbejde.
Omvendt, når dagsordenen vedrører efterlevelse af Revisionsbekendtgørelsen, er revisionsgenstanden compliancefunktionen på sine egne præmisser. Vurderingskriterierne dikteres overordnet set i Revisionsbekendtgørelsen og vedrører ressourcer, uafhængighed og rapportering. Vurdering af disse kriterier kræver dog yderligere orientering i retskilderne, navnlig Ledelsesbekendtgørelsen, men der er adskillelige yderligere omtale af Compliancefunktionen i diverse EU lovgivning og vejledende materiale fra de Europæiske tilsynsmyndigheder (navnlig ECB, EBA, EIOPA, ESMA). Reaktionsmønstret på identificerede svagheder vil her være tilpasning af § 27 konklusionen med mulighed for særskilt rapportering - se **Tabel 1** på forrige side.

Spørgsmål vedrørende den første dagsorden – tilrettelæggelse af revisionsstrategi – har efterhånden været genstand for drøftelse i mange år. Denne forbliver uhyre relevant; især i takt med at compliancefunktioner kontinuerligt modner, vinder fodfæste og etablerer best practice på tværs af branchen. Vi skal i resten af denne artikel dog udelukkende interessere os for den lidt mindre omtalte anden dagsorden – nemlig hvordan vi i praksis tilrettelægger vores arbejde med at vurdere compliancefunktionen på dens egne præmisser som påkrævet i revisionsbekendtgørelsen. Det skal dog bemærkes, at det vil være indlysende at lade denne vurdering føde ind i vores overvejelser vedrørende den første dagsorden; dog kan vi ikke nødvendigvis slutte modsætningsvis.

Specifikation af vurderingskriterier

Når vi skal vurdere compliancefunktionen, kræver Revisionsbekendtgørelsen som nævnt, at vi inddrager fire områder, nemlig:

- Uafhængighed
- Ressourcer
- Rapportering
- Betryggende processer

For at foretage denne vurdering er der naturligvis behov for at tage stilling til, hvordan "tilstrækkelighed" forstås inden for hvert område. Det er derfor nødvendigt at orientere sig i retskilderne med den forhåbning, at vi kan tegne et billede af, hvilken standard vi bør måle compliancefunktionen op imod. Dette billede skal afvejes ift. vores forretningsmodel, men umiddelbart synes nedenstående kilder som minimum at skulle inddrages for pengeinstitutter:

- Ledelsesbekendtgørelsen for pengeinstitutter (LBEK)
- EBA Guidelines on internal governance under Directive 2013/36/EU (GL11)
- Europa-Parlamentets og Rådets direktiv 2014/65/EU om markeder for finansielle instrumenter (MiFID II)
- ESMA Guidelines on certain aspects of the MiFID compliance function requirements (ESMA 388)

Listen er hverken udtømmende eller udtryk for en prioriteret rækkefølge[2]. Dog har Ledelsesbekendtgørelsen en særstatus, da anvendelsesområdet for denne i al væsentlighed er sammenfaldende med Revisionsbekendtgørelsen.

Kriterier vedr. uafhængighed

For at compliancefunktionen kan betragtes som uafhængig, opremser retskilderne en række kriterier, som skal efterleves - se **Tabel 2** herunder og på næste side.

Tabel 2: Kriterier vedrørende uafhængighed

Vurderingskriterier	Referencer
Fratrædelse og ansættelse Ifølge GL 11 skal virksomheden skal have en dokumenteret proces for fratrædelse og ansættelse af compliancefunktionens leder – "den complianceansvarlige". ESMA 388 kræver eksplicit at fratrædelse og ansættelse foretages af direktionen eller bestyrelsen.	• GL 11, 157 • ESMA 388, GL 6
Vederlag LBEK fastslår, at metoden til at fastsætte vederlag for medarbejdere i compliancefunktionen ikke må bringe deres uafhængighed i fare. GL 11 specificerer, at medarbejdere ikke må modtaget performance afhængig variabel aflønning.	• LBEK • GL 11 159 • LBEK § 17, stk. 4, nr. 4

Tabel 2 (fortsat): Kriterier vedrørende uafhængighed

Vurderingskriterier	Referencer
Organisatorisk placering og referenceforhold Compliancefunktion inklusiv den complianceansvarlige skal være organisatorisk uafhængig fra de områder, de er udpegede til at monitorere og kontrollere. Medarbejdere, der er en del af compliancefunktionen, må ikke deltage i leveringen af de tjenesteydelser eller udførelsen af de aktiviteter, de kontrollerer. Den complianceansvarlige må ikke være ledelsesmæssigt underordnet en person, der har ansvar for udførelsen af de aktiviteter, compliancefunktionen kontrollerer. Den complianceansvarlige skal være under direkte ledelsesmæssig reference til direktionen og have mulighed for at udtale sig direkte til bestyrelsen.	• LBEK § 17, stk. 4, nr 2 • LBEK § 17, stk. 4, nr 3 • ESMA 388, GL 6 • GL 11 155 • GL 11 189 • GL 11 158

Tabel 3: Kriterier vedrørende ressourcer

Vurderingskriterier	Referencer
Kompetencer, kvalifikationer og træning Compliancefunktionen skal have de nødvendige kompetencer og sagkundskab. Dette skal sikre at medarbejdere forbliver kvalificerede via adgang til relevant træning på fortløbende basis.	• LBEK § 17, stk. 4, nr. 1 • GL 11 160 • GL 11 190
Fuldtidsansatte Compliancefunktionen skal have et tilpas antal kvalificerede fuldtidsansatte afstemt til forretningsmodel og forretningsomfang.	• LBEK § 17, stk. 4, nr. 1 • GL 11 160 • ESMA 388, GL 5
Adgange Compliancefunktionen skal have adgang til al relevant information inklusiv databaser.	• ESMA 388, GL 5 • LBEK § 17, stk. 4, nr. 1
IT understøttelse Compliancefunktionen skal være understøttet af tilstrækkelige IT systemer.	• GL 11 161 • ESMA 388, GL 5
Den complianceansvarlige Den complianceansvarlige skal have tilstrækkelig bred viden, erfaring og kundskab til at tage ansvaret for compliancefunktionen og sikre at den er drevet effektivt.	• ESMA 388, GL 5
Involveret i budgetter Compliancefunktionen skal have allokeret et budget der er konsistent med det niveau af compliancerisiko, som virksomheden er eksponeret imod. Den complianceansvarlige skal konsulteres forud for budgettets vedtagelse. Alle beslutninger vedrørende væsentlige budgetnedskæringer skal være skriftligt dokumenterede og indeholde detaljerede forklaringer.	• ESMA 388, GL 5

Kriterier vedr. uafhængighed er den gruppe af kriterier, der er mest objektive sammenlignet med de øvrige. Som det er tilfældet for de øvrige grupper, introduceres dog også her et vist fortolkningsrum som følge af proportionalitetsprincippet. Herudover skønnes etablering af revisionsprogram dog ikke at give anledning til udfordringer og vil typisk tage udgangspunkt i inspektion af politikker, charters, organisationsdiagrammer mm.

Kriterier vedr. ressourcer

For at compliancefunktionen kan betragtes havende tilstrækkelige ressourcer, er en række kriterier relevante - se **Tabel 3** på forrige side.

Spørgsmålet om ressourcer, herunder kompetencer, er ofte et følsomt område, hvorfor det her er ekstra vigtigt at have et knivskarpt revisionsprogram. Umiddelbart synes en fornuftig tilgang at være at tage udgangspunkt i, at der foreligger dokumentation for, at de rette overvejelser er blevet foretaget i form af eksempelvis gap-analyser og/eller øvrige former for selv-vurderinger. Her kan intern revision så vurdere, om kriterier og analyser er fuldstændige, velbegrundede og genstand for mitigerende tiltag i det omfang, der er konstateret mangler.

Kriterier vedr. rapportering

Retskildernes krav vedrørende rapportering er sparsomme og formalistiske: - se **Tabel 4** herunder.

De nævnte krav afvejes i forhold til de vurderingskriterier vi stiller op omkring, hvorvidt compliancefunktionens processer er betryggende, idet disse nødvendigvis må være en forudsætning for retvisende og tilstrækkelig rapportering. Dette bringer os til sidste gruppe af vurderingskriterier.

Kriterier vedr. betryggende processer

At opstille de relevante vurderingskriterier vedr. compliancefunktionens processer kræver noget fortolkning. I første omgang må vi konstatere, at nogle af disse kriteri-

Tabel 4: Kriterier vedrørende rapportering

Vurderingskriterier	Referencer
Rapporteringsfrekvens Compliancefunktionen skal rapportere med en passende frekvens og mindst årligt.	• LBEK § 17, stk. 4, nr. 2 • ESMA 388, GL 3
Rapportmodtagere Rapportering fra compliancefunktionen skal tilgå direktion og bestyrelse.	• LBEK § 17, stk. 4, nr. 2 • ESMA 388, GL 1

Tabel 5: Kriterier vedrørende betryggende processer

Vurderingskriterier	Referencer
Compliancepolitik Bestyrelsen skal påse, at der etableres en veldokumenteret compliancepolitik, som er kommunikeret til alle medarbejdere.	• GL11 191
Risikobaseret tilgang Compliancefunktionen skal have en risikobaseret tilgang, som dikterer funktionens aktiviteter og allokering af ressourcer. Risikovurderingen skal opdateres løbende, således at fokus og scope forbliver relevant.	• ESMA 388, GL 1
Complianceplan Compliancefunktionen skal etablere et veldokumenteret og struktureret monitoreringsprogram, som har afsæt i risikovurderingen og er i overensstemmelse med compliancepolitikken.	• ESMA 388, GL 2 • GL11 193
Metodik Compliancefunktionen skal have tilpas sofistikerede værktøjer og metodikker, som er afstemt til virksomhedens forretningsmodel og risiko. I alle tilfælde vil det ikke være tilstrækkeligt at have en metodik, der udelukkende er baseret på desk-reviews.	• ESMA 388, GL 2

er allerede er omfattet af de øvrige områder – altså uafhængighed, ressourcer og rapportering. Det vi mangler er den konkrete aktivitetsstyring, som i sidste ende skal sikre grundlaget for compliancefunktionens konklusioner. Vi er i retskilderne her ikke hjulpet af Ledelsesbekendtgørelsen om må derfor skele til de internationale kilder, hvor vi finder kravene opgjort i **Tabel 5** på forrige side.

Disse vurderingskriterier er rammebaserede, hvilket efterlader yderligere rum for fortolkning. Her er det igen vigtigt at have et skarpt revisionsprogram, der sikrer at vurderingen har et objektivt grundlag. Det vigtige er at påse, at ledelsen og compliancefunktionen har gjort sig de relevante overvejelser i forhold til at sikre, at der er sammenhæng mellem risiko, metode og aktiviteter, og at dette er velbegrundet og veldokumenteret. Såfremt dette udmønter sig i rapportering fra compliancefunktionen, der ikke stemmer overens med de øvrige interne kontrolfunktioners rapportering (som det hedder i GL 11), herunder intern revision, kan der være grund til at overveje, om processerne skal tilpasses.

Afslutningsvis

På baggrund af de omtalte faldgruber og vurderingskriterier burde fundamentet for et relevant revisionsprogram være lagt til efterlevelse af Revisionsbekendtgørelsen krav om vurdering af compliancefunktionen. Intern revision kan vælge at udvide scopet, såfremt dette skønnes relevant i forhold til risikovurderingen i øvrigt. Endvidere kan intern revision lægge vurderingen til grund for tilrettelæggelsen af sin revisionsstrategi, der hvor der er scope-overlap med compliancefunktionen. Her vil det være relevant at udvide vurderingskriterierne med skelen til IPPF 2050 og ISA 610.

Der rettes en tak til Morten Bendtsen, Koncernrevisionschef i PFA Pension, og Lars Maagaard, CAE i Nykredit, for at have lagt grundlaget for denne artikel og ageret sparringspartnere igennem processen.

Noter

[1] IPPF standard 2050 og supplerende vejledninger stiller krav til, hvilke kriterier intern revision bør inddrage i disse overvejelser. Man kan også skele til ISA 610, som dog er specifikt møntet på forholdet mellem intern og ekstern revision. Ingen af disse italesætter eksplicit vurderingskriterierne ud fra en "ligner de os" tankegang, så denne fortolkning er på forfatterens egen regning.

[2] Den væsentligste eksklusion vedrører forsikringsselskaber og dermed Solvency II lovgivning og relaterede EIOPA vejledninger.


CROWNE PLAZA
IIA Årsmøde 2019
Afholdes
15.5.2019-16.5.2019
på Hotel Crown Plaza
København
Sæt allerede nu kryds
i kalenderen
D I

Audit of Model Risk Management

Clara Dyhrberg, PhD, Internal Audit Manager, Nordea

Introduction

The predominant guideline on audit of Model Risk Management (MRM) has for some time been the Supervisory Guidance on Model Risk Management from Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB) from 2011. This guideline is still valid and relevant.

However, in March 2018, the Institute of Internal Auditors (IIA) published a Practice Guide which gives more comprehensive and detailed guidance on audit of MRM. Highlights of the new Practice Guide are presented in this article.

In addition, references are made to European as well as US regulation. Regulation and supervisory expectations towards internal audit are not the same in the US and Europe, but with the aim of describing best practice for auditing MRM, references are made to regulation from both jurisdictions.

Since audit of MRM in many ways is similar to the audit of any other risk management area, emphasis has been placed on circumstances and topics which make the audit of MRM different from the audit of other risk management area.

Model Risk

In the two above-mentioned papers, Model Risk is defined as: *"The potential for adverse consequences from decisions based on incorrect or misused model outputs or reports"*.

Model risk occurs for two primary reasons:

1. Fundamental errors in model data, rationale, hypothesis and methodologies may produce inaccurate outputs when viewed against the design objective and intended business uses, or/and
2. The model or its results may be used incorrectly or inappropriately.

In other words, sources of model risk are related to the use of the model and the model output, model design, and input data.

The Model Risk Management Process

MRM is an organisation-wide activity that involves multiple departments, functions and roles in the organisation. IIA's Practice Guide describes the MRM framework by dividing it into three areas of activity: 1) Governance, Policies, and Controls 2) Model development, implementation and use and 3) Validation.

Governance, Policies, and Controls

As for any other area subject to internal audit review, effective governance, policies, procedures and controls must be in place to cater for proper oversight by the Board and senior management. Policies and procedures must cover the entire MRM framework, be sufficiently detailed, define roles and responsibilities, set standards for documentation, model development, model validation, model use, and requirements in relation to any third-party involvement. Third parties may be involved in a number of MRM activities, including IT system management, model development or validation.

Organisations can use the Three Lines of Defence model to build out the roles and responsibilities. The first line of defence is the operational management, which according to IIA's Practice Guide would include model developers, users and owners who are responsible for identifying, quantifying and mitigating model risk. The second line includes other oversight, risk management and compliance functions, including validation (initial and on-going validation) and reporting. The third line of defence is the internal audit function, which independently performs assurance activities and reports to the Board of Directors.

For certain model types, regulation prescribes independence of certain roles and responsibilities, which then would prevail over the IIA Practice Guide.

Additionally, a well-functioning MRM framework includes a model inventory. The model inventory must include basic information about the models, their significance for the organisation and validation status.

Model development, implementation and use

Models can be built in-house or purchased. If models are built in-house, it is important that:

- knowledgeable and experienced developers are assigned to perform the model development
- the quality of input data is assessed and improved if necessary
- proper testing of the model is performed for proper

assessment of model quality and limitations by model developers and/or model validators
- users are involved in the development process and provide their feedback.

When developers and users are satisfied with tmodel performance, the model can be moved to initial validation. If the model fails validation, it must go back to the developer. If the model passes validation, supervisory approval can be applied for, if relevant for the model in question. In some cases, the application submitted to supervisors must include an audit opinion. Finally, when supervisory approval has been granted, the model can move on to implementation. IT implementation must follow the organisation's IT change management procedures, users must be informed and trained, and policies and procedures must be created or updated to comply with the new model. Throughout the model's life, business must maintain appropriate processes and controls to limit model risk and support accurate results aligned with the model's intended use.

Validation

Validation is the key control of model performance. Initial validation occurs before the model is taken into use and on-going validation takes place throughout the model's life. Validation frequency can be based on a risk assessment performed by management, or regulation supervisors or other stakeholders may require validation to be performed at certain intervals.

The validation team should be able to effectively challenge the model. According to the FRB, OCC's Supervisory Guidance on Model Risk Management, 'effectively challenge' means: *"Critical analysis by objective, informed parties who can identify model limitations and assumptions and produce appropriate changes".*

In order to effectively challenge the model, validators must be sufficiently competent and influential to ensure that corrective actions are taken.

Validation of the model should ideally be performed by a party which is independent from model developers and users. In some cases, this is not possible, for instance if the relevant technical knowledge is not available elsewhere in the organisation, in which case compensating controls must be put in place.

If the ongoing validation shows that a model does not perform adequately, the model must be adjusted or redeveloped.

Auditing Model Risk Management

From FRB, OCC's Supervisory Guidance on Model Risk Management: *"Internal audit's role is not to duplicate model risk management activities. Instead, its role is to evaluate whether model risk management is comprehensive, rigorous and effective."*

Internal Audit provides assurance to the Board and senior management that model risk is adequately controlled, and that the internal controls within the MRM framework are operating effectively.

As part of their MRM audit work, internal auditors must confirm that the MRM framework is integrated into the organisation's overall risk management framework, including the risk appetite framework and risk reporting to management and the Board.

The MRM framework includes modelling and validation methodologies, model design and operation, compliance with legislation, governance, policies, procedures and activities conducted to address the risk of model error. Internal audit must assess all these aspects of the MRM framework.

The IIA Practice Guide describes the following steps for conducting an MRM audit engagement:

1. Planning the engagement (IIA Standards 2200 and 2201)
   a) Understand the context and the purpose of the engagement (IIA Standard 2201)
   b) Gather information to understand the area or the process under review (IIA Standard 2201)
   c) Conduct a preliminary risk assessment (IIA Standard 2210.A1)
   d) Form engagement objectives (IIA Standard 2210)
   e) Establish engagement scope (IIA Standard 2220)
   f) Allocate resources (IIA Standard 2230)
   g) Document plan (IIA Standard 2240)
2. Testing and Evaluating Model Risk Management (IIA Standards 2300 and 2330)
3. Reporting the Engagement Results (IIA Standards 2330, 2410 and 2440).

From the above, it is clear that performing an audit engagement within the MRM area is in many ways not significantly different from performing an audit engagement for any other risk management area.

The following sections offer an overview of topics specific to the MRM framework, how these parts of the MRM framework should be assessed and evaluated by Internal Audit, and how some of these parts of the MRM framework can be used for audit planning.

The Model Inventory
As mentioned above, a well-functioning MRM framework includes a model inventory. Management is responsible for maintaining a complete and accurate model inventory. All new models, models in use and retired models must be listed in the model inventory. The model inventory should include basic information about the models and their validation status.

The model inventory should also include a risk classification of the models based on the significance of the individual model for the organisation, model complexity and other relevant measures.

Additionally, the model inventory can have information about internal audit reviews and findings.

Internal Audit must confirm that processes and procedures are in place to ensure accurate, complete and updated information in the model inventory, and that the level of detail in the inventory is reasonable. This would include an assessment of definitions and procedures around the models' risk classification.

The model inventory is a valuable tool for annual MRM audit planning as well as for planning of individual MRM audit engagements, for instance when taking samples of models for testing operating effectiveness of controls in the MRM framework. For the purpose of using the model inventory for audit planning, audit of the model inventory must lead to the conclusion that reliance can be placed on the information in the model inventory.

In the SR 15-18 letter on Supervisory Assessment of Capital Planning and Positions for LISCC Firms and Large and Complex Firms, the Division of Banking Supervision and Regulation, FRB, states that:
"Other supervisory expectations for the internal audit function relating to the capital adequacy process include:
…… Assessing accuracy and completeness of the model inventory…"

Model Validation
Validation is a key control in the MRM framework. Internal auditors must evaluate the adequacy and comprehensiveness of the validation activities, process and methodologies. The validation must include assessment of model performance, modelling methodology, model limitations, model documentation and other aspects of conceptual soundness[1], data and IT controls, data quality, user assessment, and the processes around model monitoring and use.

Internal auditors must confirm that the validation process is comprehensive and that validators review all key risk areas. Substantive testing should be performed on a sample of models to ensure that validation is accurate and that standards have been followed. Additionally, internal auditors must confirm that the validators meet the criteria for effective challenge mentioned above.

The relevance and extent of validation activities must be assessed for all models in the organisation. The frequency of validation and the completeness of the validation activity must be assessed by internal auditors. As for any other control, internal auditors must confirm that proper processes are in place for validation issues to be logged, monitored, addressed and escalated if necessary.

For most models, back-testing is a relevant challenge of the model. For some model types, stress-testing would be a relevant challenge of the model as well. These tests can be performed by model developers or validators. Back-testing or stress-testing procedures and results can be relevant subjects for auditing, depending on their significance for challenge of the model[2].

Validation results are valuable inputs to audit planning and risk assessment, as they highlight models and areas with increased risk. However, validation results can be used for audit planning only if audit work has confirmed that reliance can be placed on the validation results.

Model Use
As mentioned earlier, a source of model risk is that the model or its results may be used incorrectly or inappropriately. Internal auditors must confirm that models and their results have been used appropriately.

Additionally, internal auditors must confirm that model results are used consistently throughout the organisation. As an example, proper and rigorous risk management requires that the output of risk measurement models is used consistently throughout the organisation's risk management framework, including in the 1st line operational

[1] Conceptual Soundness involves assessing the quality of the model design and construction. It entails review of documentation and empirical evidence supporting the methods used and variables selected for the model. For a rigorous description of the term 'Conceptual Soundness', see FRB OCC's *Supervisory Guidance on Model Risk Management*.
[2] Note that the stress-testing used for model challenge is not the same as the stress-testing used for capital planning.

activities such as line management, risk reporting, and internal as well as regulatory capital calculations.

Auditor Resources
In addition to the usual requirements to auditor's skills and independence, internal auditors performing the MRM audit engagement must have a clear understanding of the regulatory requirements applying to the area.

Additionally, adequate quantitative expertise is needed to assess the methodology and conceptual soundness of modelling and validation techniques and standards, the comprehensiveness of quantitative model testing, and to be able to replicate modelling and validation results for accuracy assessment.

As models typically are integrated into the organisation's IT systems and involve significant data management maneuvers, internal auditors must additionally possess the necessary skills to evaluate controls, processes, and procedures around IT systems and databases.

MRM Audit Planning

As mentioned above, MRM is an organisation-wide activity that involves multiple departments, functions and roles, and the number of models in financial organisations can be huge. Thus, audit review planning must take a risk-based approach and rotation plans can be used for full coverage of the MRM framework over a period of time. Such an approach is in line with recent regulation, from which a couple of examples are cited below:

ECB's Guide for the Targeted Review of Internal Models: *"…it is expected that, on an annual basis, the institution will carry out a general risk assessment of all aspects of the rating systems in order to define the appropriate internal audit work plan. When an area shows signs of increased risk (including, but not limited to, new processes, warnings from data quality reports or internal validation reports, or new exposures in the range of the application of the rating system etc.), it should be subject to a thorough new review ("deep dive"). For other areas where no significant change has occurred the internal audit may keep its opinion unchanged."*

FRB, Division of Banking Supervision and Regulation, SR 15-18 letter on Supervisory Assessment of Capital Planning and Positions for LISCC Firms and Large and Complex Firms: *"When defining the annual audit universe and audit plan, the internal audit function of a firm should focus on the most significant risks relating to the capital planning process. The firm may leverage existing or regularly scheduled audits to ensure coverage of all the capital planning process components …"*

References

Board of Governors of the Federal Reserve System, Division of Banking Supervision and Regulation: SR 15-18 letter on Supervisory Assessment of Capital Planning and Positions for LISCC Firms and Large and Complex Firms. December 2015.

Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency: Supervisory Guidance on Model Risk Management, OCC 2011-12. April 2011.

ECB, Banking Supervision: Guide for the Targeted Review of Internal Models. February 2017.

The Institute of Internal Auditors: Practice Guide – Auditing Model Risk Management. March 2018.

Process Mining - fordele og anvendelsesmuligheder set fra et internt revisionsperspektiv

Martin Schantz Pickardt , Manager, PwC

Indledning

Betragter man Process Mining (PM) ud fra et internt revisionsperspektiv, kan det konkluderes, at PM, som et dataanalytisk værktøj, med fordel kan anvendes i flere faser i interne revisionsprojekter. PM giver et nutidigt, fuldstændigt og objektivt billede af en proces, som er fri for forældede og ufuldstændige beskrivelser af en proces, for eksempel i form af narrativer, procesdiagrammer og risiko-/kontrolmatricer. Derved kan PM være med til at forbedre den indledende risikovurdering, den fremadrettede planlægning og udførelse af revisionen samt den løbende kommunikation og afrapportering til interessenterne.

Denne artikel giver læseren en kort introduktion til begrebet PM for derefter at komme med forslag til, hvordan PM kan understøtte interne revisionsprojekter. Derudover berører artiklen de generelle overvejelser og forberedelser, man bør foretage sig inden PM anvendes.

Process Mining kort fortalt

PM er et dataanalytisk værktøj til blandt andet at evaluere og/eller visualisere en proces. Ved hjælp af software baserer PM sig på data, der udtrækkes fra forskellige typer af informationssystemers hændelseslogfiler (på engelsk event logs) og andre hændelsesregistre, som er relevante. Denne metode gør det muligt at analysere de eksisterende processer, baseret på netop disse logfiler, som udtrækkes fra forskellige systemer såsom: Enterprise Resource Planning (ERP), Supply Change Management og E-commerce-systemer. Eksempler på forskellige typer af processer er, blandt andet, indkøbsordrer og betalinger, godkendelsesprocedurer i forbindelse med ydelse af lån, IT-change management samt forskellige typer af sagsbehandlinger, eksempelvis foretaget i et shared service center.

Forberedende aktiviteter og overvejelser

Indledningsvis skal fremhæves to centrale forberedende aktiviteter og overvejelser, som kræver begrænsede ressourcer og kan give stærke indikationer på, om det kan skabe værdi i den specifikke situation at anvende PM.

1. Inspektion og klargøring af data

Datakvalitet er en er essentiel faktor i forberedelserne og vurderingen af, om det er muligt at anvende PM. Det er derfor nødvendigt at kontrollere de aktuelle logfiler for at vurdere, om de nødvendige data er tilgængelige og fuldstændige.

2. Forsøg at forstå processen i store træk

Hvis det er muligt, så anbefales det at få et grundigt kendskab til, og forståelse af, processen i store træk – inklusive processens målsætninger og forventede output. Som ved andre revisionsprojekter er det også en god idé at inddrage procesejer(ne) for at forstå hvilke politikker og generelle procedurer, der er relevante for processen, alt afhængig af projektets omfang.

Disse indledende øvelser forventes at give en indikation af, om det er relevant at anvende PM eller ej. Det kan for eksempel vise sig, at datagrundlaget ikke er tilgængeligt eller er ufuldstændigt, og/eller en række procedurer i processen forløber autonomt og ikke registreres i de eksisterende systemer. Sådanne observationer bør rapporteres til ledelsen. Derudover kan det også være en indikation på, at den interne revisor bør overveje andre metoder og handlinger i forbindelse med revisionsprojektet.

Anvendelsesmuligheder

Når de indledende aktiviteter er udført, blandt andet via klargøring og inspektion af data, og procesforståelsen er på plads, da kan PM-processen påbegyndes. I denne artikel tages der udgangspunkt i tre typiske PM-analyseformer for at give et indblik i PM's praktiske anvendelsesmuligheder i forhold til interne revisionsprojekter.

Analyse 1: Fastlæggelse af den eksisterende proces

Udgangspunktet for fastlæggelsen af en eksisterende proces er hændelseslogs, der består af spor som følger hinanden. Analysen har til formål, baseret på hændelseslogs, at konstruere en model, som bygger på det minimum af spor, der skal til for at vise processen fra start til slut. På denne måde er det muligt at identificere væsentlige svagheder i designet af processen, og identificere risiciene for at processens målsætninger ikke opnås.

Case – Proceskendskab og integration på tværs i en organisation

I denne case betragter vi en organisation, der hovedsagligt er vokset via opkøb, hvilket har bevirket en stigende proceskompleksitet. Inden opkøbet var det generelle kendskab til processerne i organisationen mangelfuldt, og den eksisterende procesdokumentation var forældet.

Målsætningen var at skabe en forståelse af processerne, med det formål at harmonisere disse på tværs af landegrænser i de opkøbte enheder.

Der blev foretaget et udtræk af organisationens hændelseslogfiler fra de forskellige systemer, hvorefter processerne blev visualiseret, og optimeringsmulighederne blev identificeret. Organisationen modtog for første gang et komplet overblik samt dokumentation for processerne svarende til realtid. Dette bevirkede, at organisationen fik et indblik i, hvorfor de opkøbte enheder performede forskelligt.
Således kunne intern revision identificere og rapportere uhensigtsmæssige forhold i processen. Den interne revisionsrapport blev efterfølgende brugt som input til en handlingsplan, med det formål at få de forskellige processer bedre integreret på tværs i organisationen.

Analyse 2: Fit-GAP-analyse

I en Fit-GAP-analyse sammenlignes den fastlagte model for en given proces med den samlede og fuldstændige population af hændelseslogs for den valgte periode. Derefter analyseres uoverensstemmelserne mellem hændelserne og modellen, og de identificerede risici vurderes med udgangspunkt i de fastsatte målsætninger og acceptable risikotolerancer for processen.

Ved at analysere, hvad der i virkeligheden skete, og hvad der burde være sket, kan PM opdage (u)ønskede afvigelser i udførelsen af processen samt indikere afvigelser i henhold til ønskede kontroller.

Case – Transparens i indkøbs- og betalingsprocesser

I denne case betragter vi en organisation, som producerer luksusvarer til detailhandlen. Organisationen havde identificeret et behov for at skabe transparens i de eksisterende processer vedrørende indkøb og betalinger samt processen vedrørende de skattemæssige forhold. Organisationen ønskede at få et værktøj til at skabe transparens og samtidig monitorere effektiviteten af processerne og overholdelsen af de interne kontroller.

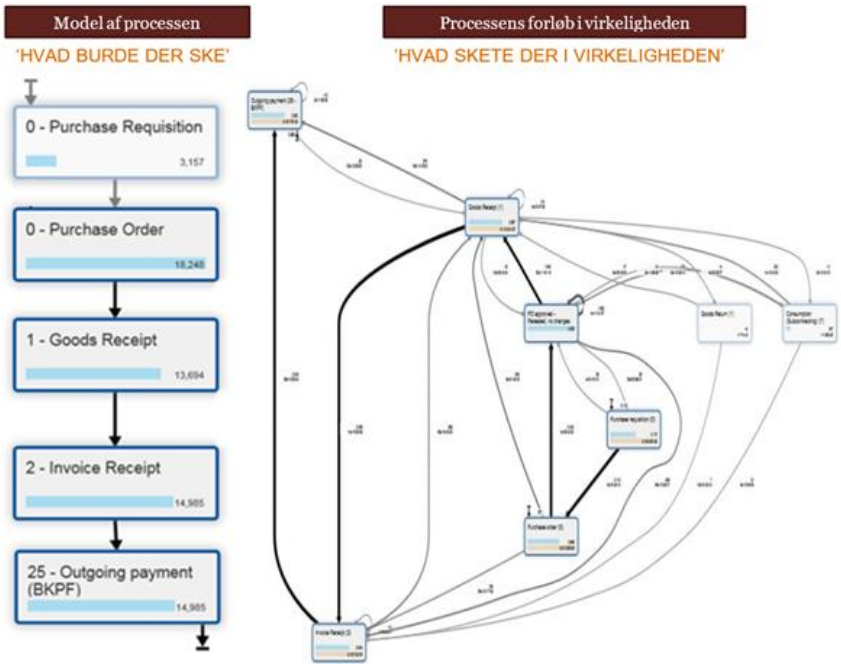
Data blev udtrukket fra flere end 20 forskellige enheder i organisationen over en periode på omkring et år. Visualiseringen af processen viste, at flere betalinger blev ændret manuelt før, og kort tid efter, at betalingen blev effektueret. **Figur 1** herunder er en visualisering af processen som er skabt ved brug af PM. Figuren viser, hvordan processen burde forløbe sammenlignet med hvordan processen i virkeligheden forløb.

Konsekvenserne af de manuelle ændringer blev analyseret, og processen blev sammenlignet med andre interne processer for at forstå niveauet af standardiseringen af processerne og effektiviteten af processernes forløb. Dette indblik medførte, at organisationen efterfølgende implementerede en arbejdsplan for at adressere de væsentligste risici ud fra en prioriteret betragtning, samt udarbejdede KPI i forbindelse med den forsatte monitorering af processen.

Analyse 3: Effektivisering

Effektiviseringsanalysen kan anvendes, når der er udarbejdet en foregående model for processen, og når det faktiske hændelsesforløb for processen er visualiseret. Analysen kan bidrage med nye typer af information, for eksempel forarbejdningsomkostninger, cyklus- eller ventetider (sagsbehandlingstider), omkostninger, godkendelser mv.

Figur 1: Visualisering af processen som er skabt ved brug af PM



Målet for denne type analyse er at fremhæve, hvordan den givne proces præsterer og efterfølgende identificere mulige forbedringsforslag.

Case – Identifikation af mulighederne for at forbedre og automatisere processen i forbindelse med udarbejdelsen af forsikringspolicer

I denne case betragter vi et forsikringsselskab. Ved brug af PM blev det synligt, at den eksisterende proces for udarbejdelse af forsikringspolicer var anderledes, end den selskabet selv havde forståelsen af. I nogle tilfælde blev end ikke de interne retningslinjer overholdt. Derudover identificerede analysen, at de fastsatte KPI'er for processen ikke var retvisende i forhold til det faktiske forløb af processen og det tilhørende datagrundlag. Som følge heraf, blev alle dele af processen, som ikke overholdt de interne retningslinjer, elimineret. Endvidere blev det identificeret, at en specifik proces vedrørende tildeling af sager imellem de ansatte kunne automatiseres ved brug af Robotic Process Automation, hvilket svarede til en besparelse på op til flere fuldtidsansatte over en periode på et år.

Konklusion

Som tidligere beskrevet er PM et analytisk værktøj, der har til formål at opdage og/eller overvåge eksisterende processer for på den måde at identificere eksisterende risici, svagheder og ineffektive elementer af en eller flere processer. Som beskrevet i de tre cases, er PMs anvendelsesmuligheder mange, og ikke begrænset af industri eller branche.

Kom godt i gang

PM kan give en mere nuanceret og detaljeret indsigt i en proces sammenlignet med andre metoder. Men før du giver dig i kast med at anvende PM bør du som minimum overveje følgende: Er dit datagrundlag fuldstændigt og tilgængeligt, og har du forståelse for den aktuelle proces?

Anvendelsen af PM har følgende fordele:

- **Fuldstændighed:** Alle transaktioner testes i en given periode, og du er derfor ikke afhængig af at finde nålen i høstakken.
- **Kommunikation:** Øjeblikkelig og kontinuerlig visualisering af processen og dets hændelsesforløb.
- **Besvigelser:** Øger mulighederne for at identificere besvigelser ved at belyse alle afvigelser i en proces.
- **Monitorering:** Når revisionsprojektet er afsluttet, kan PM fortsat anvendes som en del af monitoreringen af ledelsens opfølgende aktiviteter og efterfølgende skabe kontinuerlig assurance.

Afslutningsvis skal det nævnes, at der er flere virksomheder, som tilbyder softwareløsninger, der understøtter PM, men disse er oftest forbundet med en investeringsomkostning. Et alternativ er at afprøve mulighederne og fordelene ved en proces via en stand-alone-analyse fra en ekstern konsulent.

PM som et dataanalytisk værktøj er kommet for at blive. I fremtiden vil PM medvirke til at fastholde interne revisorer som betroede rådgivere og skabe værdi for deres interessenter.

Outsourcing - fortsat et hot emne

Birgitte Rousing Svenningsen, CIA, CISA

Indledning

EBA – European Banking Authority – udsendte i juni et udkast til nye retningslinjer for outsourcing. EBA er et lovkontor under EU. EBA har mandatet til at underkende de lokale myndigheder, hvis disse ikke på passende vis regulerer banksektoren. Planen er, at de nye retningslinjer træder i kraft 30. juni 2019.

Retningslinjerne kommer til at gælde for banker og betalingsformidlere, men hvis man ser på de nuværende retningslinjer fra 2006, kan man se, at bl.a. den danske outsourcingsbekendtgørelse for finansielle virksomheder og Solvency II Direktivet for forsikringsselskaber kraftigt er inspireret af retningslinjerne fra EBA. Retningslinjerne er derfor også relevante for interne revisorer og andre, som arbejder i andre typer finansielle virksomheder.

Retningslinjerne beskriver nogle grundlæggende principper for outsourcing, hvorfor jeg også mener, at de kan anvendes og være til stor gavn for interne revisorer uden for den finansielle sektor.

Grundlæggende princip

Basalt set er det grundlæggende princip, at ledelsen fortsat har det fulde ansvar for aktiviteterne – også selv om de er outsourcet til et andet selskab. Dette gælder uanset om det andet selskab er et eksternt selskab eller et selskab i samme koncern.

Dette princip er uændret. Til trods herfor er der fortsat virksomheder, som har udfordringer med håndtering heraf, og som ikke har en strømlinet outsourcingsproces. Årsagen hertil er formodentlig, at outsourcing ofte bunder i et ønske om at spare penge, hvorfor ekstra omkostninger til specielt løbende overvågning af de outsourcede aktiviteter i mange lederes øjne synes overflødig.

Som nævnt bevarer ledelsen det fulde ansvar for de outsourcede aktiviteter, hvorfor man kan undre sig over, at ledere ofte føler sig fuldt ud trygge ved at have et andet firma til at udføre en service uden nogen form for overvågning heraf (egen kontrol). Kunne man fx forestille sig, at en leder er ansvarlig for en service, hvor medarbejderen, som udfører servicen, sidder i et lukket lokale, som lederen aldrig besøger og hvor lederen i stedet én gang om året beder en revisor om at besøge teamet for at se, om alt foregår, som det skal? Det er i princippet det, som sker, hvis ledelsen udelukkende understøtter sit ledelsesansvar med en årlig revisorerklæring. Normalt vil en leder overvåge teamet mere, hvorfor det også giver mening, at man skal overvåge outsourcede aktiviteter, når man fortsat har det fulde ansvar.

Der er dog nogle ledelser, som endnu ikke har forstået, hvorfor vi som interne revisorer fortsat har en opgave med at uddanne ledelsen og informere om risiciene ved outsourcing. Denne kontinuerlige påvirkning og holdningsbearbejdelse skal ske før de nye retningslinjer (såvel som de nuværende) kan anvendes. Derfor ser jeg stadig outsourcing som et hot emne.

Et andet forhold, som tillige gør, at outsourcing er et hot emne, er, at den teknologiske udvikling bevirker, at det bliver mere og mere almindeligt at anvende cloud løsninger. Man kan måske drive det så langt, at det i mange tilfælde vil være ansvarsløs ledelse ikke at anvende cloud løsninger. Jeg vil derfor også nedenfor komme nærmere ind på problemstillinger i forbindelse med cloud løsninger.

Outsourcingsprocessen

Retningslinjerne foreskriver, at virksomheden skal have en outsourcingspolitik, som sikrer en tilstrækkelig håndtering af de outsourcede aktiviteter. Herudover angiver retningslinjerne, at der er følgende delprocesser:

1. Forundersøgelse
   - Vurdering af væsentligheden af de outsourcede aktiviteter
   - Due diligence
   - Risikovurdering
2. Kontraktfasen
3. Overvågning

Endvidere lægger retningslinjerne specielt vægt på, at der er tilstrækkelige exit strategier.

Der er umiddelbart intet nyt i outsourcingsprocessen. Når jeg alligevel finder udkastet til de nye retningslinjer interessant og nyttigt, er det fordi de detaljerede retningslinjer giver vejledning i forhold til nogle af de spørgsmål, jeg gennem tiden har fået fra ledelsen eller andre interne revisorer. Specielt i forhold til definition af væsentlig out-

sourcing, indhold af outsourcingskontrakter, koncernintern outsourcing og cloud løsninger synes jeg, at retningslinjerne giver nogle anvendelige svar. Jeg vil derfor i resten af artiklen fokusere på disse områder. Jeg vil også involvere dansk lovgivning.

Definition af væsentlig outsourcing

Gennem årene har jeg fået en del spørgsmål, om hvilke aktiviteter den danske outsourcingsbekendtgørelse omfatter. Outsourcingsbekendtgørelsen anvender termen "væsentlige aktivitetsområder". På grund af implementeringen af Solvency II Direktivet for forsikringsselskaber, blev outsourcingsbekendtgørelsen i relation til forsikringsselskaber ændret 1. januar 2018, hvorefter "kritiske og vigtige operationelle funktioner" er omfattet af bekendtgørelsen, for så vidt angår forsikringsselskaber. I forbindelse med ændringen skrev Finanstilsynet i sit høringsbrev, at "vedrørende forståelsen af kriterierne "kritisk/vigtig", så vurderes disse at være udtryk for et væsentlighedskrav svarende til det, der i dag gælder for finansielle virksomheders outsourcing af aktivitetsområder". Hvorvidt der anvendes termen "væsentlig" eller "kritisk/vigtig" synes derfor ikke afgørende.

Men hvordan skal væsentlig/kritisk/vigtig fortolkes? Udkastet til retningslinjerne skriver følgende herom - se **Figur 1** herunder (tallene/punktnumrene refererer til EBA retningslinjerne).

Der er således en lang liste af overvejelser, man bør gøre sig. Konklusionen vil fortsat afhænge af den enkelte virksomheds aktiviteter, og af hvorledes den enkelte virksomhed ønsker at fortolke retningslinjerne.

Figur 1: Udkast til retningslinjer

49. Institutions and payment institutions should always consider a function as critical or important for the purpose of outsourcing:
a. where a defect or failure in its performance would materially impair:
i. their continuing compliance with the conditions of their authorisation under Directive 2013/36/EU , Regulation (EU) No 575/2013, Directive (EU) 2015/2366 and Directive 2009/110/EC and their regulatory obligations;
ii. their financial performance; or
iii. the soundness or continuity of their banking and payments services and activities;
b. when operational tasks of internal control functions are outsourced; or
c. when they intend to outsource banking or payment services requiring authorisation by a competent authority.

51. When assessing whether or not an outsourcing arrangement is critical or important, i.e. it concerns a critical or important function, institutions and payment institutions should take into account at least the following criteria:
a. whether the proposed outsourcing arrangement is directly connected to the provision of banking or payment services for which they are authorised;
b. the potential impact of any disruption or outage of the outsourcing arrangement on their:
i. short and long-term financial resilience and viability, including, if applicable, its assets, capital, costs, funding, liquidity, profits and losses;
ii. business continuity and operational resilience;
iii. operational risk, including conduct, information and communication technology (ICT), legal and reputational risks;
iv. where applicable, recovery and resolution planning, resolvability and operational continuity in a resolution situation.
c. the potential impact of the proposed outsourcing arrangement on their ability to:
i. identify, monitor and manage all risks;
ii. comply with all legal and regulatory requirements; and
iii. conduct audits regarding the outsourcing arrangement;
d. the potential impact on the services provided towards its clients;
e. taking into account other outsourcing arrangements, the institution's and payment institution's aggregated exposure to the same service provider or the cumulative impact of outsourcing arrangements in the same business area;
f. the size and complexity of any business area affected;
g. the possibility of the proposed outsourcing arrangement to be scaled up at the discretion of either party without replacing or revising the underlying agreement;
h. the ability to transfer the proposed outsourcing arrangement to another service provider, if necessary or desirable, both, contractually and in practice, including the estimated difficulties, costs and timeframe for doing so ('substitutability');
i. the ability to reintegrate the outsourced function into the institution or the payment institution, if necessary or desirable;
j. the protection of data and the potential impact of a confidentiality breach or failure to ensure data availability and integrity on the institution or the payment institution and their clients, including but not limited to Regulation 2016/679.

Man kan kun gætte på, hvordan de nye retningslinjer vil påvirke fremtiden. Et gæt kunne være, at flere virksomheder i fremtiden vil betragte outsourcet lønadministration som "væsentlig" på grund af størrelsen af lønudgiften (punkt f) og på grund af fortroligheden af oplysningerne (punkt j). Dette vil også være en logisk udvikling, idet ledelsen ud fra en risikobetragtning burde være interesseret i en tæt og systematisk opfølgning på en outsourcet lønadministration.

Outsourcingskontrakter

Grundlæggende kan de fleste serviceleverandører levere, hvad man beder om, men hvis det ikke er fastsat i kontrakten, vil det ofte være forbundet med ekstra omkostninger, hvorfor en fyldestgørende outsourcingskontrakt er fundamental for en god outsourcing. Den danske outsourcingsbekendtgørelse, Solvency II regler for forsikringsselskaber og EBAs udkast til nye retningslinjer lister alle minimumskrav til outsourcingskontrakter. Kravene er forskellige og for at give et overblik har jeg i **Tabel 1** herunder sammenlignet kravene i retningslinjerne med outsourcingsbekendtgørelsen. Af hensyn til at skabe et overblik har jeg ikke sammenlignet med Solvency II reglerne (tallene/punktnumrene refererer til henholdsvis EBA retningslinjerne og outsourcingsbekendtgørelsen).

Tabel 1: Sammenligning af krav til outsourcingskontrakter i EBA retningslinjerne og outsourcingsbekendtgørelsen

EBA	Outsourcingsbekendtgørelsen
63a) a clear description of the outsourced function;	1) En klar afgrænsning af de outsourcede opgaver.
63b) the start and end dates of the agreement, including notice periods;	
63c) the governing law of the outsourcing arrangement;	
64g) termination rights as further specified in Section 10.4;	
64b) the agreed service levels, which should include precise quantitative and qualitative performance targets for the outsourced function that allow timely monitoring in a manner that appropriate corrective action can be taken without undue delay if agreed service levels are not met;	2) En klar beskrivelse af de krav, som leverandøren skal opfylde og hvorfra ydelsen bliver leveret.
64d) the respective parties' financial obligations;	
	3) Krav om at leverandøren skal udføre de outsourcede opgaver rettidigt og i overensstemmelse med de aftalte krav.
64e) whether the service provider should take mandatory insurance against certain risks and, if applicable, the cover of the insurance requested;	
64c) the reporting obligations of the service provider to the institution or payment institution, including the communication by the service provider of any development that may have a material impact on the service provider's ability to carry out effectively the critical or important function in line with the agreed service levels and in compliance with applicable laws and regulatory requirement;	4) Krav om at outsourcingsvirksomheden skal underrettes straks om enhver udvikling, som i væsentlig grad kan forringe leverandørens nuværende eller fremtidige evne til eller muligheder for at udføre de outsourcede opgaver.
64f) requirements to implement and test business contingency plans;	
	5) Krav om at leverandøren skal rapportere om opgavens udførelse til outsourcingsvirksomheden. Kravene skal definere rapporteringens indhold, kvalitet og hyppighed.
64a) the right of the institution or the payment institution to monitor the service provider's performance on an ongoing basis;	

Tabel 1 (fortsat): Sammenligning af krav til outsourcingskontrakter i EBA retningslinjerne og outsourcingsbekendtgørelsen

EBA	Outsourcingsbekendtgørelsen
63f) where relevant, provisions regarding the accessibility, availability, integrity, privacy and safety of relevant data, as further specified in Section 10.2;	6) Krav om at leverandøren skal beskytte personoplysninger samt andre oplysninger, der ved lov er gjort fortrolige. Denne beskyttelse skal også gælde efter outsourcingskontraktens ophør.
63e) the location(s) where the critical or important function will be provided and/or where relevant data will be kept, including the possible storing locations, and processed and the conditions to be met, including a requirement to notify the institution or the payment institution if the service provider proposes to change the location(s);	
63g) the obligation of the service provider to cooperate with the competent authorities of the institution or the payment institution, including other persons appointed by them;	7) Krav om at leverandøren forpligtes til at give Finanstilsynet, outsourcingsvirksomheden og dennes revisorer alle nødvendige oplysninger angående de outsourcede opgaver.
63h) the unrestricted right of institutions, payment institutions and competent authorities to get any information needed with regard to the outsourcing and to access and audit the service provider as further specified in Section 10.3	
64j) for institutions, a clear reference to the national resolution authority's powers, especially to Articles 68 and 71 of Directive 2014/59/EU (BRRD), and in particular a description of the "substantive obligations" of the contract in the sense of Article 68 of that Directive.	8) Krav om at Finanstilsynet kan få oplysninger om den outsourcede aktivitet ved enten, at Finanstilsynet eller en repræsentant, der optræder på Finanstilsynets vegne, mod behørig legitimation får adgang til leverandøren.
64i) a clear statement that in the event of insolvency or discontinuing of business operations by either party the relevant data will be made available irrespective of the occurrence of the default;	9) Krav om at leverandøren ved outsourcingsaftalens ophør, uanset ophørsgrund, loyalt og hurtigst muligt skal medvirke til, at opgaven enten overgår til en anden leverandør eller tilbageføres til outsourcingsvirksomheden. Leverandøren skal forpligtes til at levere de outsourcede ydelser, indtil der er sket endelig overdragelse.
64h) provisions that ensure the access to data that are owned by the institution or the payment institutions in case of the insolvency of the service provider;	
63d) whether the sub-outsourcing of a critical or important function is permitted and if so, the agreement should ensure that the sub-outsourcing is subject to conditions specified in Section 10.1;	10) Krav om at outsourcingsvirksomheden skal godkende leverandørens eller underleverandørens eventuelle videreoutsourcing af de outsourcede opgaver.

Som det ses af **Tabel 1** indeholder EBA retningslinjerne flere krav til outsourcingskontrakter, som ikke indgår som krav i den nuværende danske lovgivning. Flere af dem er interessante. Jeg vil her særligt fremhæve:

- Hvorvidt leverandøren skal tegne visse forsikringer (64e)
- Krav om implementering af beredskabsplaner og test heraf (64f)
- Outsourcingsvirksomhedens ret til løbende at overvåge leverandørens performance (64a).

Punktet med forsikringer er interessant, fordi det i et vist omfang kan reducere omfanget af overvågning, idet ledelsen (som har det fulde ansvar) kan argumentere for, at risiciene er afdækket af forsikringer. Det kan derfor være en måde, hvorpå ledelsen kan holde omkostningerne nede.

På nuværende tidspunkt foreskriver outsourcingsbekendtgørelsen, at outsourcingsvirksomhedens procedurer skal sikre, at outsourcing ikke er til hinder for gennemførelse af outsourcingsvirksomhedens beredskabsplaner, men der er ikke et krav om, at det er stadfæstet i outsourcingskontrakten. I praksis er det dog således, at den bedste måde at sikre det på er, at der indgår krav i kontrakten herom. Jeg ser det derfor som en forbedring og en hjælp til både outsourcingsvirksomheden og den interne revisor, at de nye retningslinjer decideret stiller krav herom.

Det sidste forhold, som jeg har fremhævet, "Retten til løbende overvågning" er ligeledes en forbedring i forhold til tidligere retningslinjer. Løbende overvågning har også tidligere været et krav, men at sikre, at det indgår i outsourcingskontrakterne vil betyde, at der bliver færre, som efter indgåelse af en kontrakt står tilbage uden mulighed for at udføre løbende overvågning. Dette ses i dag, fordi nogle virksomheder ikke tænker på overvågning i forbindelse med kontraktindgåelsen, og fordi nogle leverandører ikke er interesseret i løbende overvågning foretaget af eksterne parter.

Ud over ovennævnte krav stiller EBA retningslinjerne også en række krav til outsourcingskontrakten i tilfælde af videreoutsourcing. Dette er også en interessant ændring, idet videreoutsourcing bliver mere og mere almindeligt og absolut ikke gør tingene nemmere at overvåge. I **Figur 2** nedenfor er gengivet kravene til outsourcingskontrakter, som indeholder videreoutsourcing.

Koncernintern outsourcing

Koncernintern outsourcing er også et forhold, hvor jeg gennem årene har modtaget en del spørgsmål. I den finansielle branche ser vi mere og mere finansielle koncerner – altså koncerner, som har flere forskellige finansielle produkter (fx bank, forsikring og realkredit). Da disse aktiviteter ikke må drives i samme selskab, består koncernen af flere forskellige juridiske selskaber. Koncernerne ønsker dog ofte at drive visse funktioner (fx IT eller regnskabssystemer) fælles for at opnå en synergieffekt. Dette er naturligt og forståeligt. Derved opstår formelt koncernintern outsourcing. Da koncernerne ofte også drives som ét selskab med fælles ledelse osv., kan det i visse tilfælde være svært at forstå, at sådanne fælles aktiviteter betragtes som outsourcing og skal følge virksomhedens outsourcingsproces. Forholdet gælder både for rene danske koncerner men også for udenlandske koncerner med danske datterselskaber. Ved sidstnævnte skal væsentlige aktiviteter leveret af moderselskabet betragtes som outsourcing.

Dette dilemma fjernes ikke med de nye EBA retningslinjer. Det pointeres, at retningslinjerne skal følges såvel af koncernen som af hvert enkelt juridiske selskab. Baggrunden er, at det enkelte selskabs ledelse har det fulde ansvar for aktiviteterne, og derfor også skal inkludere dem i sin risikovurdering. Herunder peger retningslinjerne på, at koncentrationsrisikoen (dvs. risikoen som følge af afhængighed af få leverandører) som minimum skal vurderes.

Hvis alle enkeltstående juridiske selskaber i koncernen skal overholde outsourcingsreglerne og dermed udføre

Figur 2: Krav til outsourcingskontrakter, som indeholder videreoutsourcing

65. The outsourcing agreement should specify whether or not sub-outsourcing of critical or important function is permitted. If so, it should:
a. specify any types of activities that are excluded from sub-outsourcing;
b. specify the conditions to be complied with in the case of sub-outsourcing;
c. specify that the service provider is obliged to oversee those services that it has subcontracted in order to ensure that all contractual obligations between the service provider and the institution or the payment institution are still met;
d. require the service provide to obtain prior approval from the institution and the payment institution before sub-outsourcing data subject to the GDPR;
e. include an obligation for the service provider to inform the institution or the payment institution of any planned sub -outsourcing, or material changes thereto, in particular where that might affect the ability of the service provider to meet its responsibilities under the outsourcing agreement. This includes planned significant changes to the subcontractors and the respective notification period;
f. the notification period to be set under point (e) should allow the outsourcing institution and payment institution to carry out a risk assessment of the proposed changes before the changes come into effect;
g. ensure, where appropriate, that the institution or the payment institution has the right to object against intended sub-outsourcing or that an explicit approval is required;
h. ensure that the institution or payment institution have the contractual right to terminate the agreement in case of undue sub-outsourcing, e.g. where the suboutsourcing materially increases the risks for the institution and the payment institution or where the service provider sub-outsources without notifying the institution or the payment institution.

tilstrækkelig overvågning, kan det blive en tidskrævende proces for det leverende selskab. Retningslinjerne peger derfor på, at man kan have en central overvågningsfunktion. En sådan overvågningsfunktion skal være uafhængig af den leverende enhed, og det er vigtigt at ledelsen i hvert enkelt selskab modtager tilstrækkelig rapportering omkring den foretagne overvågning. Min erfaring er, at nogle koncerner anvender mange ressourcer på at argumentere for, at et fælles regnskabssystem driftet af moderselskabet eller en fælles IT drift ikke er outsourcing. I stedet for at indgå i en sådan diskussion og anvende ressourcer herpå, bør man som revisor pege på simple løsninger såsom en fælles overvågning. Det kræver dog en opbakning fra hele koncernen, hvilket kan være svært at få, hvis man sidder i et datterselskab af en udenlandsk koncern og dermed som intern revisor har begrænset kontakt til koncernledelsen.

Cloud løsninger

Som nævnt ovenfor anvender flere og flere virksomheder cloud løsninger. Det kan være til opbevaring af kundedata, transaktionsdata eller mindre løsninger såsom en bestyrelsesportal eller et system til at modtage ansøgninger i forbindelse med rekruttering.

Det har gennem årene været diskuteret, om sådanne cloud løsninger er outsourcing og dermed omfattet af outsourcingslovgivningen. Basalt set anser EBA retningslinjerne en cloud leverandør som en hvilken som helst anden leverandør. Dvs. at cloud løsninger er outsourcing og væsentlig/kritisk/vigtig outsourcing, hvis cloud løsningen anvendes til noget, som anses som væsentligt/kritisk/vigtigt jf. ovennævnte definition. Der er dog forskelle, idet der er særlige risici tilknyttet cloud løsninger, hvorfor EBA retningslinjerne stiller yderligere krav til outsourcing via cloud løsninger. Retningslinjerne angiver således, at registeret over outsourcede aktiviteter for cloud løsninger skal indeholde information om typen af cloud (public/private/hybrid/community). Endvidere skal registeret indeholde oplysninger om, hvor data opbevares.

Vedrørende den obligatoriske overvågning af cloud løsninger foreskriver retningslinjerne, at denne fokuserer på databeskyttelse, lokalitet, sikkerhedsforhold og koncentrationsrisiko.

Intern revisions rolle

Ud over retningslinjer for outsourcing og styring heraf, stiller EBA retningslinjerne også krav til intern revisions rolle. Revisionsplanen skal således baseret på en risikovurdering indeholde kritisk/vigtige outsourcede aktiviteter. Den interne revision skal som minimum fastslå/påse:

- At virksomhedens outsourcingsproces inkl. outsourcingspolitikken er korrekt og effektivt implementeret i overensstemmelse med lovgivningen, ledelsens risikoappetit og beslutninger i øvrigt.
- At virksomhedens vurdering af, hvilke aktiviteter der er kritiske/vigtige er tilstrækkelig, af høj kvalitet og effektiv.
- At virksomhedens risikovurdering af outsourcingsaftalerne og -leverandørerne er tilstrækkelig, af høj kvalitet og effektiv, samt at virksomhedens risici bevares inden for ledelsens risikoappetit.
- At leverandørens risikoappetit, risikostyring og kontrolprocedurer er i overensstemmelse med outsourcingsvirksomhedens strategi.
- At virksomhedens ledelsesorganer (governance bodies) er passende involveret.
- At der er passende overvågning og styring af outsourcingsaftalerne.

Intern revision har således efter EBAs opfattelse en omfattende opgave i forhold til outsourcing. Mest nyskabende i forhold til den nuværende praksis i Danmark er formodentlig det faktum, at intern revision skal sikre, at virksomhedens risici fortsat er inden for ledelsens risikoappetit og i overensstemmelse med virksomhedens strategi. Intern revision skal således ikke udelukkende fokusere på kontroller og overholdelse af lovgivningen. Dette er i overensstemmelse med IIAs generelle anbefalinger og udviklingen inden for faget intern revision.

Konklusion

EBA retningslinjerne er som nævnt på nuværende tidspunkt i udkast. Der er en høringsproces i gang, og de kan derfor forventes at blive justeret – men sandsynligvis i mindre grad.

Uanset hvad kan jeg kun opfordre til at læse udkastet til retningslinjerne. De giver svar på nogle af problemstillingerne i forbindelse med outsourcing og beskriver den interne revisions rolle og man kan derfor finde input og inspiration i retningslinjerne, uanset om man er intern revisor i en bank, en anden finansiel virksomhed eller en virksomhed uden for den finansielle sektor. Retningslinjerne kan også anvendes som input til ledelsen, compliancefunktioner mv. i de virksomheder, der har udfordring med tilstrækkelig håndtering af outsourcing. Hvis denne artikel har vakt din interesse, kan udkastet til retningslinjerne findes her:

https://www.eba.europa.eu/documents/10180/2260326/Consultation+Paper+on+draft+Guidelines+on+outsourcing+arrangements+%28EBA-CP-2018-11%29.pdf

Nye medlemmer

Nye medlemmer i IIA fra 6.4.2018 – 3.9.2018

A.P. Møller – Maersk
Frank Thy
Rubirosa Cruz

BDO
Iben Larsen

Danske Bank
Ali Dalan
Kristina Birk Thomsen
Jacob Eggers Rasmussen
Christopher Pommergaard

Deloitte
Maria Foged
Kristian Ehrenreich Hansen
Kristine Løgsted Rasmussen

Jutlander Bank
Eva Falck Ørndrup

Jyske Bank
Tobias Hald

KPMG
Berk Akbay
Christoffer Kock Petersen

Københavns Kommune
Derya Gokcen
Helle Lund Jørgensen

Nordea
Roger Coen
Natalia Brøns-Poulsen

Novo Nordisk
Adriana del Valle Cajal
Carla Amodeo

Skandinaviska Enskilda Banken
Kenneth Wiberg

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

02.10.2018 Kursus for Forsikringsrevisorer
29.11.2018 Temadag for den finansielle sektor
25.04.2019 Kursus for pengeinstitut– og realkreditrevisorer
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 Auditor 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

CIA, CISA
Birgitte Rousing Svenningsen
☎ 30 65 41 30 ✉ Birgitte.Rousing@svenningsen.eu

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