INFO

Foreningen af Interne Revisorer

Nummer 84 | September 2023 | 28. årgang

Kunstig intelligens

Revisorerhvervets snarlige død?

Koncernrevision

Etablering af fælles koncernrevision i Arbejdernes Landsbank

Cyberrisiko • ESG • Besvigelser

INFOs redaktion

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

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

IT Auditor
Stine Juhl-Hansen
Danfoss
☎ 28 34 57 37 ✉ stine.juhl-hansen@danfoss.com

Intern revisor, CIA, CRMA
Kim Nehls
DSB
☎ 24 68 18 77 ✉ kine@dsb.dk

Internal Audit Manager
Avelina Francoise Lykkegaard Nielsen
Nordea
☎ 31 54 07 05
✉ avelina.francoise.lykkegaard.nielsen@nordea.com

Director
Martin Tripax
Deloitte
☎ 91 56 93 90 ✉ mtripax@deloitte.dk

Næste nummer
INFO 85 udkommer i december 2023.
ISSN: 1903-7341 (Elektronisk version).

Indlæg til INFO
Har du en god idé til en artikel eller har lyst til at skrive en artikel kan du skrive til redaktionen@iia.dk

Artikler i INFO påskønnes med en vingave og giver CPE-point.

Forsidefoto
UnknownNet

Redaktionens adresse

Foreningen af Interne Revisorer (IIA Denmark)
Att.: Seniorspecialist Glenn Thunø
Intern revision, Nykredit
Kalvebod Brygge 1-3
1780 København V

redaktionen@iia.dk

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

Morten Bendtsen, Direktør, CIA,
Intern revision, Alm. Brand Group

Velkommen til INFO 84
Som bestyrelsesformand for IIA Danmark deltog jeg i den globale konference for IIA (IIA Global) i Amsterdam den 7. til 9. juli 2023. Der deltog deltagere fra 115 Affiliates.

En vigtig del er at udbygge netværk med IIA Global - på tværs af lande - og allerede fra starten så jeg flere kendte ansigter :-).

I år lykkedes vi med at skabe kontakt til IIA Global med henblik på at give merit til statsautoriserede revisorer i forhold til CIA. Det er en omfattende proces som Lars Maagaard og jeg har startet op, og vi forventer et positivt resultat og et kommende udbud i 2024. Det er vores strategi, at CIA også kan markedsføres via FSR og dermed at vi kan komme bredere ud.

Desværre er der isoleret set ikke mulighed for merit med Cand.merc.aud.

Ellers var hovedemnerne på konferencen:

- Vision 2035
- New Credentialing Pathway
- IPPF Evolution Project and it's Topical Requirements
- Global Operating Model
- Legal and Regulatory Framework Position Paper.

Jeg vil fremhæve, at der som del af IPPF kommer en række supplerende tekniske standarder, bl.a. indenfor områderne ESG, Cyber og Fraud Risk. Standarderne bliver obligatorisk og forventes udgivet i Q4 2024.

IIA Global er opmærksomme på, at CIA står foran en fornyelse og der åbnes op for at del 3 kan erstattes af en række godkendte specialiseringer, fx indenfor offentlig revision, it eller den finansielle sektor.

De løbende workshops gav mig anledning til at notere et behov for, at vi i bestyrelsen arbejder på at promote og udbyde credentials. Der udbydes i dag 6 emner, alle af høj aktualitet, fx ESG, Cyber sikkerhed og Fraud.

Yderligere blev det tydeligt, at vi som forening bør arbejde på at kunne udbyde eksternt review, hvilket er afgørende for at opretholde fagets troværdighed på længere sigt.

Og så til bladets indhold. Vi får denne gang fem artikler indenfor forskellige emner:

- Christoffer Max Jensen fortæller om sit arbejde med at danne en koncernrevision i AL efter deres opkøb i Vestjysk Bank.
- Brugen af kunstig intelligens vinkles i forhold til revision og stiller spørgsmålet om det kan blive revisionsfagets snarlige død!
- Og vi får to spændende artikler i relation til Cyberrisiko.

God læselyst og husk næste årsmøde den 11. til 12. juni 2024 i København.

Nyt fra redaktionen

Birgitte Rousing Svenningsen, bestyrelsesmedlem IIA, CIA, CISA

Det er med stor glæde, at jeg kan byde velkommen til Martin Tripax fra Deloitte i redaktionen. Martin er uddannet jurist og har en baggrund fra både EY og Danske Bank. Han har de seneste år arbejdet en del med operationelle risici, herunder arbejdet sammen med flere interne revisionsafdelinger. Jeg forventer derfor, at Martin med sin baggrund kan bidrage med viden om såvel lovgivningen som intern revision og operationelle risici. Jeg ser rigtigt meget frem til at arbejde sammen med Martin.

I samme omgang har Christian Barrett valgt at udtræde af redaktionen. Christian er rykket videre i sin karriere til Deloittes CFO services, hvorfor han ikke længere har samme finger på pulsen om, hvad der sker inden for intern revision. Det er årsagen til, at han har valgt at udtræde af redaktionen. Jeg vil gerne sige Christian stor tak for den indsats, han har ydet i redaktionen. Christian har bidraget med mange artikler om ny lovgivning og forordninger og ikke mindst artikler om tips og tricks, så vi alle kan blive bedre og mere effektive.

Er du også en af de personer, som har fingeren på pulsen? Eller har du nogle emner, som du synes, at vi mangler at berøre, er du meget velkommen til at kontakte os. Vi vil altid gerne have flere redaktionsmedlemmer, og vi vil altid gerne have gode emner til artikler.

Bliv en aktiv del af IIA!!!!

Vær med til at sætte dagsordenen for den fremtidige udvikling af intern revision.

Skriv artikler, deltag i udvalg og netværksgrupper. Læs mere på foreningens hjemmeside www.iia.dk, eller send en mail til kontakt@iia.dk.

IIA PRISEN

Prisopgave om intern revision

IIA Prisens formål er at fremme kendskabet til intern revision blandt studerende på cand.merc.aud. og andre relevante kandidatuddannelser samt tilskynde disse til at skrive kandidatafhandlinger inden for intern revision. Prisen er en præmie på

25.000 kr.

For at komme i betragtning til IIA Prisen skal kandidatafhandlingen have opnået karakteren 7, 10 eller 12 og enten handle direkte om intern revision eller indeholde væsentlige elementer, hvor emnets relevans for intern revision diskuteres. Det er eksempelvis i orden at indsende en afhandling om corporate governance til IIA prisen, hvis afhandlingen har en ikke uvæsentlig grad af fokus på intern revisions rolle i virksomhedens ledelse. Det samme gælder for eksempel for opgaver om risikostyring og interne kontroller, som pr. definition er intern revisions øvrige hovedområder.

Ansøgningen indsendes elektronisk til iiaprisen@iia.dk og skal indeholde:

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

Ansøgningsfristen er 15. januar 2024. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iia.dk.

Prisoverrækkelsen vil ske på IIA's årsmøde i maj 2024. Bedømmelsesudvalget består af Kim Klarskov Jeppesen (CBS) og Birgitte Rousing Svenningsen.

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

IIA Denmark

Etablering af fælles koncernrevision - med udgangspunkt i Arbejdernes Landsbanks overtagelse af en større andel af aktierne i Vestjysk Bank

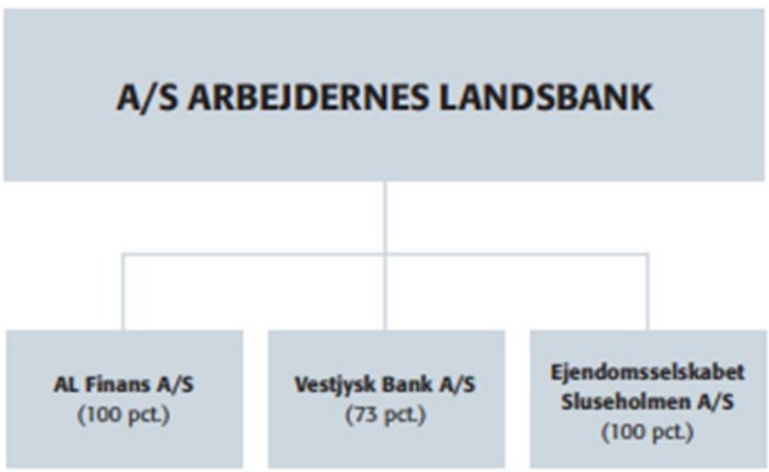
Christoffer Max Jensen, Koncernrevisionschef Arbejdernes Landsbank koncernen,Næstformand i bestyrelsen IIA, CIA, CFSA

Efter Arbejdernes Landsbank (AL) i sommeren 2021 opkøbte en større andel af aktierne i Vestjysk Bank (VB), blev AL udpeget som en del af landets systemisk vigtige finansielle institutter (SIFI), og VB blev et datterselskab i AL koncernen.

Som led heri besluttede bestyrelsen at oprette en ny koncernrevision, omfattende de to interne revisioner i AL og VB, og ansætte mig som koncernrevisionschef med henblik på at etablere en koncernrevision. Koncernrevisionen blev derfor formelt etableret den 1. april 2022 som en fusion af de to interne revisioner, der i AL bestod af 9 medarbejdere, og koncernrevisionschefen, og VB, der bestod af tre medarbejdere.

Revisionschefen for AL varetager endvidere hvervet som revisionschef for Grønlandsbanken, der har outsourcet den interne revision til AL. Grønlandsbanken er udpeget som SIFI på et individuelt grundlag.

Figur 1: Koncernstruktur



Konstruktionen med ejerskabet af VB er grundlæggende ret speciel, da AL er en unoteret finansiel virksomhed, mens VB er en børsnoteret finansiel virksomhed, med ca. 27% af de børsnoterede aktier i cirkulerende mængde. I forhold til etableringen af en koncernrevision medfører det en kompleksitet i forhold til den måde, man normalt ville styre en bankkoncern på hvor moder oftest ejer 100% af de underliggende døtre, og derved ofte etablerer fuld kontrol med selskabet i form af egen bestyrelse mv. Koncernstrukturen er anført i **Figur 1** nederst på siden.

Ved etableringen af en koncernrevision har jeg derfor ikke kunne spejle mig 100 pct. i, hvordan jeg selv tidligere har grebet det an, eller eksempelvis hvordan mine kolleger i sektoren har grebet det an. Vi har derfor skulle finde vores egen vej til, hvordan etableringen af en koncernrevision skulle se ud, og henad vejen sikre en effektiv og værdiskabende koncernrevision, der kan betrygge bestyrelsen i hvorvidt koncernen har etableret et tilstrækkeligt og betryggende kontrolmiljø.

Samtidig har koncernrevisionen skulle etableres med de respektive individuelle krav til intern revision i både AL og VB, samt øvrige datterselskaber. De individuelle krav til revisionen af bankerne er primært forankret i, at de to banker stadig forretningsmæssigt er to individuelle enheder med deres individuelle forretningsmodeller, individuelle bestyrelser, individuelle tilsyn fra Finanstilsynet mv. Vi har derfor ikke kunne implementere en koncernløsning på samme måde som det er implementeret i en række andre finansielle koncerner. Primært på grund af ejerstrukturen, samt det forhold, at ikke alle funktioner er etableret som koncernfunktioner. Det skaber et stadigt behov for individuelle forhold.

Tilgangen var, efter de indledende drøftelser med koncernbestyrelsen og -direktionen, at vi indledningsvist ville fokusere på følgende forhold, som jeg efterfølgende vil beskrive hvordan vi har grebet an. Det skal bemærkes, at forandringer tager tid – og oftest meget længere tid end man initialt sætter af.

Her er det min erfaring at det kræver en vis tålmodighed. Det skal også tilføjes, at vi efter lidt over et år som koncernrevision endnu ikke er på plads, og stadig arbejder med flere områder af implementeringen. Denne del kommer jeg afslutningsvist tilbage på. Men som nævnt – forandringer tager tid.

Det indledende fokus var på afklaring – og efterfølgende implementering - af nedenstående, der dog bestemt ikke er udtømmende for etableringen, da implementeringen jo også indeholder helt basale handlinger som at skabe relationer med stakeholders, skabe relationer mellem medarbejderne, skabe arbejdsglæde, udvikling mv.

- Governancestruktur for – og praktisk etablering af - koncernrevisionen
- Koncernrevisionens formål og opgaver
- Samarbejde med ekstern revision
- Metode, processer, templates, systemer og rapporteringer
- Kompetencer, medarbejdere og budget
- Strategi for koncernrevisionen.

Governancestruktur for – og praktisk etablering af - koncernrevisionen

Som led i etableringen af en koncernrevision, er der en række praktiske forhold afledt af lovgivningen og revisionsbekendtgørelsen, der skal håndteres. Det primære var koncernrevisionschefens fit and proper godkendelse, der dog var sket forud for ansættelsen.

Herudover følger det af kravene i revisionsbekendtgørelsens §25, stk. 1, at den person, der er udpeget som revisionschef, skal være revisionschef i alle de virksomheder, der er i koncernen. Det vil sige, at vi i praksis skulle sikre, at de tidligere revisionschefer "fratrådte" deres stilling som revisionschef over for Finanstilsynet, og jeg tiltrådte i de to banker. Det virker lidt omstændeligt, men er et krav fra Finanstilsynet i henhold til revisionsbekendtgørelsen.

Herudover skulle vi have etableret koncernrevisionen formelt i de respektive bestyrelser. Grundet ejerstrukturen og det forhold, at de to banker har to fuldstændig uafhængige bestyrelser, valgte vi at etablere en vicerevisionscheffunktion i VB, som er dækket af den tidligere revisionschef. Dette sikrede også vores fysiske tilstedeværelse i banken, komiteer og bestyrelses- samt udvalgsmøder, hvor disse i mange tilfælde endnu ikke var tilrettet i forhold til koncernen og havde en række fælles mødedatoer. Herudover sikrer det også, at vi har en dygtig daglig leder til funktionen i VB, der står for dag-til-dag-styringen af intern revision i VB.

Sidst skulle vi have opdateret de lovmæssige dokumenter efter revisionsbekendtgørelsen – funktionsbeskrivelsen og revisionsaftalen - for hver af de to banker. Kravet er naturligt at dette først etableres i moderselskabet (AL), og herefter tiltrædes af hvert af datterselskaberne.

Koncernrevisionens formål og opgaver

En væsentlig del af etableringen af koncernrevisionen og tiltrædelsen som koncernrevisionschef var at afklare intern revisions formål og opgaver, udover de forhold der følger af revisionsbekendtgørelsen og anden lovgivning, bekendtgørelser og vejledninger. Det vil sige generelt fokus på at afstemme forventninger med bestyrelse og ledelse i koncernen, og efterfølgende afstemme dette med de underliggende selskaber i koncernen således, at det sikres at koncernbeslutninger implementeres ensartet.

Intern Revision i såvel AL som VB havde i mange år påtegnet årsrapporten, og finansiel revision havde i mange år været en væsentlig del af revisionsplanen. Jeg, bestyrelsen og direktionen havde dog sammenfaldende ønsker om et større fokus på operationel revision, hvor det var vurderingen, at koncernrevisionen i højere grad kunne skabe værdi for banken og bestyrelsen. Vi meldte derfor allerede ved etableringen af koncernrevisionen i april 2022 ud, at 2022 ville være det sidste år hvor Intern Revision ville påtegne årsrapporten.

Vi kunne have valgt allerede at stoppe med påtegningen med det samme. Det var dog et bevidst ønske fra min/vores side, at vi kunne bruge kalenderåret 2022 til at sammensætte den bedste og mest effektive arbejdsdeling for den finansielle revision i samarbejde med ekstern revision. Derfor valgte vi, at Intern Revision påtegnede årsrapporten for 2022, som det sidste år. Beslutningen om at stoppe med at påtegne årsrapporten skal i henhold til revisionsbekendtgørelsen tillige meddeles til Finanstilsynet – dette for alle finansielle institutioner hvor intern revision påtegner årsrapporten.

Som led i at fastlægge den mest effektive arbejdsdeling i relation til det finansielle regnskab, har vi for 2023 og fremadrettet, aftalt med ekstern revision, at Intern Revision er den primære revisor, både i forhold til kontrolbaseret revision og substanstest, for så vidt angår Kreditområdet samt Fondsområdet, herunder også finansielle instrumenter.

Baggrunden herfor var, at det var vores vurdering at de to områder, er væsentlige risikoområder i banken, hvor vi ved den løbende revision af det interne kontrolsystem, risikostyring, ledelses- og bestyrelsesrapportering mv., i forvejen udfører et stort omfang af revisionsarbejde, og at vi ved denne opdeling vil undgå et for stort overlap i mellem vores og ekstern revisions arbejde, samtidig med at vi skaber værdi for banken.

Samarbejde med ekstern revision

Samarbejdet med den generalforsamlingsvalgte eksterne revision blev som led i etableringen af koncernrevisionen,

og den strategiske ændring ved at intern revision fra 2023 ikke længere påtegner årsrapporten, ændret betragteligt, og dette har medført opdatering i revisionsaftalen, som følger af revisionsbekendtgørelsen. Arbejdsdelingen er i dag langt mere simpel, og fællesområderne færre. Vi ser dog stadig revisionen af banken som en fælles opgave, som vi løbende koordinerer, men blot en opgave hvor vi løser hver vores områder, og hvor ekstern revision på en række områder koordinerer mere direkte med banken, i stedet for gennem os. Det har også effektiviseret processerne for banken, os og ekstern revision.

I forhold til eksekvering af den operationelle revisionsplan, er der som led i etableringen af koncernrevisionen indgået aftaler med eksterne konsulenter/revisorer, som vi kan anvende på de områder hvor intern revision ønsker at udvide kompetencerne eller ikke selv har kompetencen, og en del af revisionens budget er allokeret hertil. Dette er særligt på specialistområder som IT, kapitalområdet, ESG, modeller samt øvrige dele af risikostyringsområdet, hvor vi indtil videre har anvendt specialister.

Metode, processer, templates, systemer og rapporteringer

Vi har fra starten ønsket at ensrette metoder, processer, rapporteringer mv. Målet har været over tid at sikre en ensretning således, at grundlaget og revisionsmetoden for den rapportering vi afgiver til direktion, revisionsudvalg og bestyrelse, er det samme.

Et af de områder vi har brugt mest tid på ved implementeringen, har været at drøfte, gennemgå, opdatere, ensrette og implementere en fælles revisionsplan, en revisionsmetode med fælles templates, og fælles rapporteringer. Herunder hvordan vi sikrer vores kvalitet indadtil i vores egne processer, og samtidig leverer tilstrækkelig og retvisende rapportering til revisionsudvalg og bestyrelse, i forhold til revisionsudvalgsrapportering og bestyrelsesprotokollater, samt rapportering til den daglige ledelse i form af revisionsrapporter og management letters.

En væsentlig ændring i vores metode er, at vi fra 2023 har implementeret et revisionsunivers, der dækker bankens 12 primære risikoområder. Risikoområderne er udvalgt ud fra et revisionsmæssigt perspektiv, og er de områder, som vi vurderer, er de væsentlige og risikofyldte områder i koncernen, og indeholder de største risici for koncernen. Efter implementeringen heraf, er 2. linie funktionerne checket ind i samme risikounivers, hvorved vi på koncernniveau anvender samme taxonomi når vi beskriver og rapporterer på risici. De 12 risikoområder danner også grundlag for vores afrapportering til direktion og bestyrelse.

Vi har for 2023 etableret en fælles revisionsplan for koncernen, der er den første plan, der beskriver Intern Revisions overgang til operationel revision, uden påtegning af årsregnskaberne. Alle opgaver er koncernrevisionens – dvs. vores fælles opgaver, uanset om de udføres i AL, VB eller et af de øvrige selskaber. Herudover er der fra foråret 2023 etableret en fælles revisionsmetode, templates, kvalitetssikring og rapporteringer – både dag-til-dag-rapporteringer i form af revisionsrapporter og management letters, samt rapportering til revisionsudvalg og protokollat til bestyrelsen.

Vores revisionsproces er dog stadig meget manuel, hvilket udfordrer projektstyringen og sikkerheden i, og dokumentationen af, kvalitetssikringen. Denne del kan vi først endelig løse ved implementeringen af et revisionssystem, og vi har derfor i foråret 2023 opstartet en proces med at undersøge potentielle revisionsværktøjer, der forhåbentlig skal ende ud i en systemimplementering primo 2024.

Kompetencer, medarbejdere og budget

En væsentlig del af leveringen af revisionsplanen og det vi har lovet bestyrelsen og ledelsen i koncernen, er afhængig af, at vi har et tilstrækkeligt budget, og har de rette medarbejdere og kompetencer i koncernrevisionen.

Budgettet drøfter vi løbende med ledelsen, revisionsudvalget og bestyrelsen, og der har ikke her været de store ændringer, udover at vi har justeret imellem antal revisorer og budget til at insource konsulenter/specialister, på de områder hvor vi ikke selv har haft kompetencerne eller tilstrækkelige ressourcer til at revidere et område. Dette generelt set for at sikre, at vi altid reviderer de væsentligste risici, og ikke kun de risici vi har kompetencer til.

Ændringen af Intern Revisions fokus væk fra påtegning og over mod primært at levere operationel revision, gjorde også at vi skulle revurdere de kompetencer vi skulle have i Intern Revision for at kunne afdække de identificerede risici. Samtidig skulle vi også sikre at vi har/havde de kompetencer, der skal sikre at vi er fit-for-purpose fremadrettet.

Her var vi fra starten godt stillet kompetencemæssigt, idet der både i AL og VB var – og er – flere revisorer med mange års revisionserfaring, herunder flere års erfaring med revision af finansielle institutioner. En ændret strategi kan dog påvirke dette, og som led i den ændrede strategi over imod operationel revision, har der været medarbejdere, der på helt forståelig vis, ikke så sig selv som en del af den nye strategi, og derfor valgte at søge væk.

Med henblik på at sikre den rette sammensætning af kompetencer, har vi ud fra de væsentlige risikoområder (fra planlægning/risikovurdering) lavet en mapping af de nødvendige kompetencer i koncernrevisionen. Dette har

vi brugt til at vurdere de nødvendige kompetencer, men ligeledes de områder hvor vi forventer at skulle insource kompetencer udefra. Vi har nu fået bragt hovedparten på plads, og forventer endeligt at være på plads kompetencemæssigt ved udgangen af 2023.

Strategi for koncernrevisionen

Med henblik på at skabe en fælles koncernrevision, og en retning og strategi for koncernrevisionen, har vi også arbejdet på en fælles strategi for hvad koncernrevisionen skal stå for, den kultur vi ønsker, hvordan vi arbejder sammen og skaber arbejdsglæde og udvikling. Det vil sige generelt den strategi vi vil have for vores fælles arbejde og udvikling fremadrettet. Denne del arbejder vi stadig ihærdigt med, men vi må erkende at vi for en stor del helt naturligt har prioriteret den faglige udvikling og leveringerne til ledelserne og bestyrelserne.

Hertil har der også været en relativ stor turnover af medarbejdere fra den tidligere interne revision i AL, og samtidig udfordringer med endeligt at kunne samle koncernrevisionen som enhed i forhold til adgange, autorisationer mv. på tværs af bankerne og selskaberne. Denne del er nu i al væsentlighed bragt på plads og vi kan arbejde videre med vores interne strategi, kultur og retning for 2023 og frem.

Afslutningsvist vil jeg vurdere, at vi er kommet langt på det første år. Især i forhold til fælles metoder, arbejdsgrundlag, dokumentation, kvalitet og rapporteringer. Den feedback vi modtager fra vores primære stakeholders, er positiv. Men der er stadig en række projekter der skal arbejdes videre med, i en verden hvor risici og den teknologiske udvikling flyver afsted.

Vi har som tidligere nævnt et projekt omkring implementering af et revisionssystem. Herudover skal vi i 2024 komme betydeligt længere med et projekt på continuous monitoring og generelt at få implementeret dataanalyse mere effektivt i vores revisionsproces, så vi kan bruge de kompetencer vi har på data mere effektivt.

Hertil skal vi også – som pilotprojekt - arbejde med at give plads til en større metodefrihed, for at se om det åbner for nye metoder til at opnå et tilstrækkeligt revisionsbevis på den mest effektive måde. Oveni det, tror jeg at kravene til vores rapportering over tid vil bevæge sig, og at vi skal arbejde henimod metoder for smartere rapporteringer mv. Mulighederne og projekterne er mange, og vi er kun lige begyndt.

IIA Årsmøde 2024 11.-12.6.2024
på Comwell Copenhagen Portside

Sæt allerede nu kryds i kalenderen!

Er der behov for øget fokus på besvigelsesrisici?

Julia Thomassen, statsautoriseret revisor og certified fraud examiner (CFE), EY Forensic & Integrity Services

Hanny Ammal, EY Forensic & Integrity Services, Data analytics and eDiscovery

Introduktion

I Danmark er vores samfund i et vist omfang baseret på tillid. Et tillidsbaseret samfund kan skabe en følelse af ærlighed, pålidelighed og gennemsigtighed. Denne tillidsbaserede tilgang kan have udfordringer i relation til trusler fra besvigelser.

I Danmark har virksomhedernes kontrolforanstaltning, i større omfang end resten af verden, været baseret på tillid til udvalgte nøglepersoner. Den udbredte opfattelse af at mennesker handler i god tro, kan medføre en mangel på opmærksomhed relateret til mulighederne for besvigelser. Derudover kan den tillidsbaserede holdning medføre, at man ikke er tilstrækkeligt forberedt på at håndtere de forskellige former for besvigelser[1].

En anden faktor der spiller ind, er et generelt lavere niveau af ekstern kontrol i tillidsbaserede samfund. I Danmark er der fx ikke revisionspligt for mindre virksomheder og den tillidsbaserede holdning og det reducerede niveau af kontrol kan skabe en situation med mindre overvågning og åbne døren for potentielle trusler fra besvigelser.

Undersøgelser viser, at forebyggelse gør en afgørende forskel når det kommer til de tab som virksomhederne lider på baggrund af besvigelser og bedrageri, men hvordan sikrer virksomhederne at de konstant er et skridt foran de kreative besvigelsesmetoder? Og hvordan beskytter virksomhederne bedst muligt deres integritet og omdømme, når verden konstant er foranderlig?

Tendenser viser ændringer til risikobilledet

Den generelle udvikling i besvigelser har været præget af stigende kompleksitet i takt med udviklingen i teknologi og den stigende digitalisering. Den teknologiske udvikling og digitaliseringen har medført en stigning i cyberkriminalitet, herunder phishing og ransomware. Men selvom vi ser en stigning i de eksterne trusler, har virksomhederne fortsat udfordringer med besvigelser begået af interne medarbejdere.

Undersøgelser viser, at op mod halvdelen af alle virksomheder har været udsat for en besvigelsessag, og at det koster virksomhederne en ikke uvæsentlig andel af omsætningen når de rammes af besvigelser. Og her er der ikke taget højde for uopdagede besvigelsessager.

Kriser og ændringer til verdensøkonomien kan åbne op for nye muligheder for svindel, og de seneste år har været præget af en række udfordrende begivenheder. Disse begivenheder kan have haft indflydelse på forskellige virksomheders drift og risikobillede, herunder Corona krisen og den usikre økonomiske situation i verden.

Den nuværende klimakrise har desuden medført mere og omfattende regulering og rapportering på området for ESG og sustainability. Den nuværende regulering er til dels umoden og der indføres stadig nye direktiver og incitamentet til at manipulere med oplysninger og rapportering vedrørende ESG øges dag for dag, og der er stadig større og større pres fra virksomhedens ejere og ledelse.

Denne situation kan skabe et incitament for manipulation og uærlig rapportering relateret til ESG. Presset fra både samfundet, ejere og ledelse om at opfylde ESG-kravene kan friste nogle til at præsentere forbedringer eller bæredygtige tiltag, der måske ikke er fuldt ud i overensstemmelse med virkeligheden.

Disse tendenser stiller krav til virksomhederne om at være opmærksomme på ændringer i risikobilledet og være agile i vurderingen af hvilke forebyggende tiltag der kan have god effekt på imødegåelsen af besvigelser.

Har virksomhederne udfordringer med håndteringen?

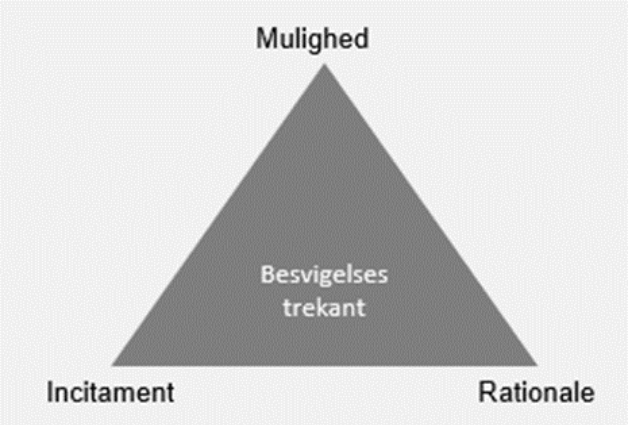
Bekæmpelse af svindel er en kontinuerlig udfordring og nye tendenser opstår i takt med udviklingen, særligt udviklingen indenfor teknologi, men også ved ændringer i økonomiske og samfundsmæssige forhold.

En af de store udfordringer i forbindelse med håndteringen af besvigelsesrisici er at være på forkant med udvik-

lingen. Det er vigtigt at virksomhederne har for øje at risikobilledet konstant forandrer sig i takt med bl.a. den teknologiske udvikling og udviklingen i økonomien og samfundet. Besvigelsesmetoderne tilpasser sig løbende udvikling og lovgivning og det er derfor essentielt i kampen mod besvigelser, at virksomhederne medtager en vurdering af besvigelsesrisici i den løbende risikovurdering, implementerer et stærkt kontrolmiljø, opbygger en stærk etisk kultur samt uddanner og oplyser medarbejdere.

I vurderingen af udviklingen indenfor besvigelser og den etablerede kontrolforanstaltning, er det en god ide at være opmærksom på elementerne i den velkendte besvigelsestrekant:

1. Mulighed
   - Der skal være en mulighed for at begå besvigelsen, det kan fx være mangler i interne kontroller
2. Incitament/pres
   - Der indgår en form for pres eller motivation for at begå besvigelser, det kan fx være økonomiske problemer eller pres fra ledelsen
3. Rationale
   - Handlingen skal kunne retfærdiggøres fx ved at overbevise sig selv om at det er berettiget eller acceptabelt at begå besvigelser



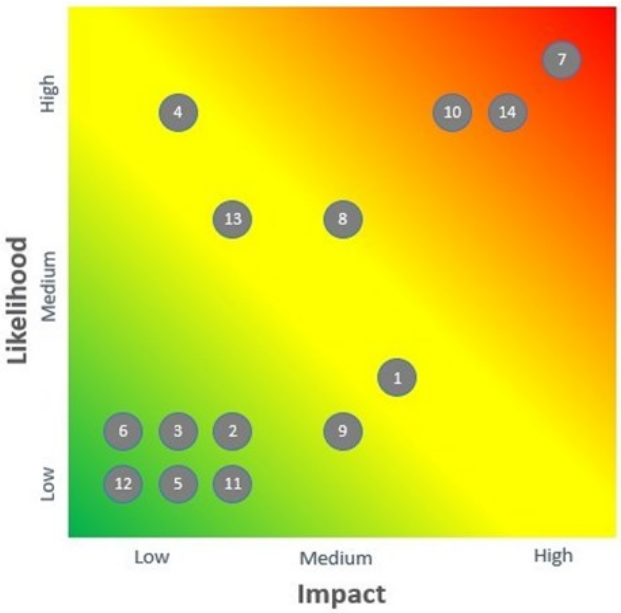
Virksomheder kan benytte besvigelsestrekanten som et praktisk værktøj i vurderingen af besvigelsesrisici. Ved at analysere hver af de tre elementer, kan virksomheder forstå de mulige motivationer for svigagtig adfærd og styrke interne kontroller og forretningsgange.

Løbende risikovurdering af besvigelser

Indeholder virksomhedens løbende risikoanalyse en vurdering af risikoen for de forskellige og relevante typer af besvigelser? Har virksomheden taget stilling til hvordan de fordeler deres ressourcer i forhold til de identificerede besvigelsesrisici? Har virksomheden løbende vurderet de kontroller der er relevante i forhold til den besvigelsestrussel de står overfor?

Ovenstående spørgsmål kan hjælpe virksomhederne i arbejdet med at forebygge besvigelser. Særligt vigtigt er det, at man løbende vurderer hvilke besvigelsesrisici man som virksomhed står overfor og tager stilling til om disse risici har forandret sig. Denne vurdering har nemlig direkte effekt på hvor godt eventuelle forebyggende kontroller og tiltag fungerer. En ændring af risikobilledet for besvigelser kan medføre, at de implementerede procedurer og kontroller ikke er tilstrækkelige.

Virksomheder kan eventuelt indarbejde en risikoanalyse for besvigelser i deres løbende risikovurdering.



Håndteringen og vurderingen af besvigelsesrisici kan evt. indeholdes i følgende tre kategorier:

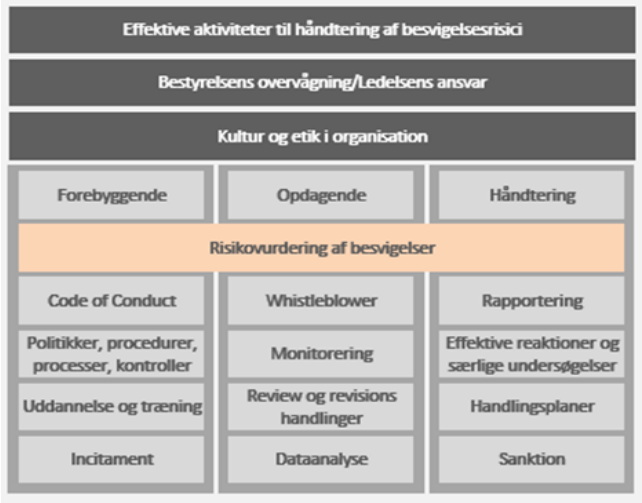
1. Forebyggende
2. Opdagende
3. Håndtering

Den forebyggende aktivitet kan omfatte en risikovurdering af den iboende risiko for relevante områder. Drøftelsen og identifikation af risikofyldte områder bør inddrage et bredt udvalg af relevante medarbejdere fra hele virksomheden, for at sikre en holistisk risikovurdering.

Samtidig kan virksomheden identificere relevante politikker, forretningsgange og kontroller, og vurdere disse i henhold til den opdaterede risikovurdering. Ligeledes er det vigtigt, at alle medarbejdere modtager den relevante og nødvendige uddannelse og træning, ligesom code of conduct og kulturen i virksomheden kan være vigtige brikker i vurderingen af risikoen for besvigelser.

Den opdagende del af analysen kan indeholde dataanalyser og tests, der udføres på relevante datagrundlag (se særskilt afsnit om dataanalyse). Dataanalysen kan danne grundlag for udvælgelse af forhold og transaktioner til gennemgang. Yderligere kan der fx. foretages en stikprø-

vevis kontrol af relevante forretningsgange og interne kontroller som udvælges på baggrund af den udførte risikovurdering. Kontrollen kan bl.a. teste om forretningsgange og kontroller er effektive og udføres korrekt. Man kan også udføre en test der er særligt rettet mod om virksomheden er underlagt den nødvendige funktionsadskillelse ved risikofyldte forretningsgange.



I tillæg til ovenstående er det vigtigt at nævne, at størstedelen af bedragerisager på globalt plan opdages på baggrund af tips (whistleblower etc.). Undersøgelser viser, at hele 42% af de undersøgte sager er opdaget på baggrund af et tip. Virksomheder kan derfor med god effekt etablere de nødvendige rapporteringskanaler samt sikre at rapportering af uregelmæssigheder ikke har konsekvenser. Ligeledes kan virksomhederne sørge for tilstrækkelig træning og uddannelse af medarbejderne i tilgængeligheden og brugen af etablerede rapporteringskanaler.

Som opfølgning og reaktion på risikoanalysen kan virksomheden fastsætte tiltag til reduktion af de identificerede besvigelsesrisici. Der kan bl.a. udarbejdes konkrete handlingsplaner for væsentlige områder samt forslag til forbedringer af forebyggende og opdagende kontroller.

Når "shit hits the fan" og virksomheder bliver ramt af en besvigelses- eller bedragerisag, så er det vigtigt at have det rigtige beredskab, der sikrer en effektiv og hurtig reaktion på forholdet. Det kan være bekosteligt at blive ramt af en besvigelsessag og det kan være skadeligt for virksomhedens omdømme, integritet og økonomi. Omkostningen kan dog begrænses hvis virksomheden er forberedt og tager de rigtige skridt i forhold til at reagere effektivt og rettidigt på forholdet.

Ovenstående eller andre effektive øvelser kan med fordel løbende opdateres med henblik på at sikre at etablerede kontrolforanstaltninger fortsat er effektive og har den oprindelige tiltænkte effekt, nemlig at mitigere risikoen for at virksomheden rammes af besvigelser.

Dataanalyse – en kraftfuld allieret

Effektiv dataanalyse hjælper virksomheder og interne revisorer med at skabe et stærkere kontrolmiljø og styrke virksomhedens risikostyring, så den er bedre rustet til at håndtere truslerne fra bedrageri og svindel.

For at maksimere effektiviteten af dataanalyse i besvigelsessager, kan interne revisorer med fordel afklare følgende trin inden selve analysen udføres:

1. **Definer et mål**
   - Klart definerer mål og omfang af dataanalyseprocessen i forhold til besvigelsesrisiciene og på baggrund af virksomhedens risikovurdering.

2. **Dataindsamling**
   - Sikre, at alle relevante datakilder er tilgængelige og indsamlet på en struktureret måde.

3. **Datasanering**
   - Forberede data til analysen ved at fjerne eventuelle redundanser, fejl eller inkonsekvenser.

4. **Analysemetoder**
   - Vælg de mest relevante analyseteknikker og værktøjer til at opdage uregelmæssigheder og svig.

5. **Samarbejde**
   - Samarbejd med IT-afdelingen og tekniske eksperter for at sikre korrekt implementering af dataanalyseværktøjer.

Undersøgelser viser, at 16% af de sager der undersøges opdages af Intern Revision. Interne revisorer spiller derfor en afgørende rolle i at opdage og forebygge uregelmæssigheder, men med den stigende kompleksitet og omfang af moderne forretningsdata, er det afgørende for interne revisorer at have de rette værktøjer til at afsløre potentielle besvigelser og besvigelsesmetoder.
Dataanalyse giver virksomhederne og interne revisorer redskaberne til at opdage potentielle uregelmæssigheder og mønstre i store datamængder, som ellers ville være vanskelige at identificere gennem traditionelle metoder. Her er nogle måder, hvorpå dataanalyse kan være behjælpelig i opdagelse og afdækning af besvigelsessager:

Identifikation af potentielle uregelmæssigheder: Ved at analysere store datamængder kan dataanalyse bruges til at identificere mønstre, afvigelser og usædvanlige transaktioner, der kan være tegn på besvigelser. For eksempel kan der identificeres gentagne beløbstransaktioner eller uregelmæssigheder i konti, som indikerer potentiel svindel.

Relationel analyse: Dataanalyse giver mulighed for at undersøge relationer mellem data fra forskellige kilder. Det kan afsløre usædvanlige forbindelser mellem leverandører, ansatte eller andre parter, der kan være involveret i besvigelser.

Kontrol med identitetsbesvigelser: Dataanalyse kan hjælpe med at overvåge adgang og brug af systemer og identificere eventuelle unormale mønstre, der kan indikere identitetsbesvigelser eller uautoriseret adgang.

Analyse af kommunikationsdata: Gennem analyse af e-mails, chats og andre kommunikationsdata kan dataanalyse afsløre mistænkelige dialoger eller mønstre, der peger på svigagtig aktivitet.

Dataanalyse er en vigtig allieret grundet den stigende digitalisering og den voksende datamængde. Dataanalyse er et vigtigt værktøj i arbejdet med opdagelse af besvigelser så omfanget og tidshorisonten af besvigelsen kan reduceres.

Afsluttende bemærkninger

Er der så et behov for øget fokus på besvigelser? Potentialet for besvigelser vokser i hvert fald i takt med digitaliseringen og de teknologiske muligheder, og samtidig peger pilene i retning af, at det kan være en bekostelig affære hvis man først bliver ramt af en besvigelse. Konsekvenserne spænder fra alt mellem økonomisk tab til tab af omdømme og retlige konsekvenser.

Virksomheder kan derfor med fordel tænke vurderingen af besvigelser og behovet for kontrolforanstaltninger ind i deres overordnede risikovurdering af forretningen. I takt med digitaliseringen og udviklingen i teknologien, herunder AI, opstår der også nye muligheder for virksomhederne for hurtigt og effektivt at analysere store mængder data. Mængden af data fortsætter med at stige og disse værktøjer er vigtige allierede i kampen mod besvigelser.

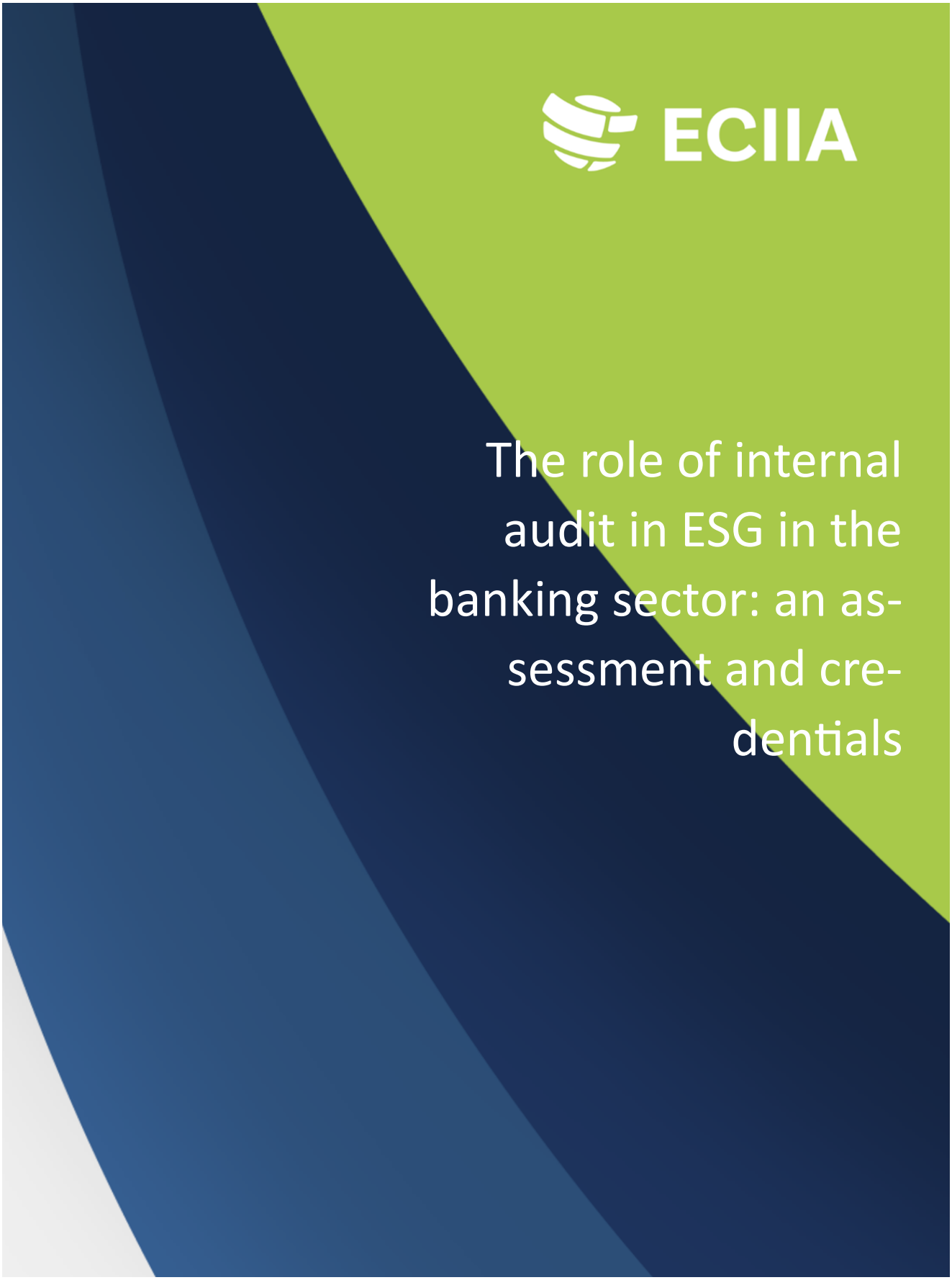
En forebyggende tilgang kan således ikke kun hjælpe virksomhederne med at beskytte økonomien, men også virksomhedernes omdømme og integritet.

Noter

[1] Besvigelse refererer til handlinger, hvor en person forsætligt misbruger sin stilling eller beføjelser til at opnå økonomisk gevinst gennem ulovlige eller bedrageriske handlinger. Det kan inkludere tyveri, forfalskning, korruption, og andre former for finansielle overtrædelser. Besvigelser kan blandt andet have alvorlige konsekvenser og store byrder for virksomheden, herunder tab af penge, skade på omdømme, og retsforfølgning af de involverede.

Kilder

ACFE (Association of Certified Fraud Examiners) 2022. Occupational Fraud 2022: A Report to the Nations
EY 2022. Tunnel Vision or the Bigger Picture? Global Integrity Report 2022


ECIIA
The role of internal audit in ESG in the banking sector: an assessment and credentials

PART 1: The role of internal audit in ESG in banking

1. Introduction

"Climate change is one of the biggest challenges facing the world today. Banks can and must play a critical role in aligning economic growth with positive social and environmental impact, ensuring a just transition towards the low-carbon economy of the future. Internal Audit (IA) is in the position to add real value in this learning process.

The European Regulators have issued new regulations and guidance on ESG: the Sustainable Finance Taxonomy, the CSRD, accompanied by the draft European Sustainability Reporting Standards (ESRS), the ECB "Guide on Climate–related and Environmental Risks" as well as an overview of good practices for climate-related and environmental risk management, the Corporate Sustainability Due Diligence Directive (CSDDD, draft), to name a few key ones. The Security Exchange Commission (SEC) recently also announced it plans to integrate climate change risks into mainstream financial reporting requirements.

IA is well positioned to help businesses navigate this fast-changing world of ESG regulations and stakeholder expectations.

In a field that is in constant motion and where national and international standards are still in flux, both assurance and advisory services can add real value. In this respect, development of Internal Audit skills and capabilities is a critical lever for the Entity to respond adequately to these big changes. A sound education in ESG themes and identifying common audit approaches on the matter, also through a specific "ESG audit Certification", will significantly support the ESG goals and objectives.

2. IA and ESG in general

Although many ESG areas of the organization might not yet be mature enough for assurance audits, there is a high demand and regulatory expectations for this. The risk of not taking action from an internal audit perspective is that the control environment to support the ESG strategy of the banks may not be designed or operating effectively.

In this interim phase, where ESG management is still maturing, IA can perform audits to evaluate the organization's ESG maturity. In certain cases IA can also help an organization progress through advisory services.

Assurance services

In these early days IA can assess the ESG path to maturity defined by banks, and the related actions taken towards achieving that plan. In doing so, IA can:

- Raise awareness at Board and senior management level about ESG priorities, gaps and implications (including greenwashing risk) and serve as a sounding board as management designs their program;
- Review how ESG risk factors (including transition and physical climate risks) have been identified and assessed in all business lines and verify & encourage the development of control activities to mitigate ESG risks;
- Verify & encourage the development of designed & documented standard processes;
- Benchmark controls against best practice, regulatory expectations to validate their maturity.

Other key areas for ESG assurance services are:

Reviewing the ESG Governance Structure and Oversight

IA can assess the governance structure and ESG oversight by reviewing:

- If risk management procedures are clearly defined and management understands how ESG impacts its respective business operations;
- If roles and responsibilities are clearly established across the 3 lines of defence and understood throughout the organization to ensure a sound ESG control environment and to monitor ESG issues, including the formation of an ESG committee consisting of cross-functional executive members; and
- Policy and procedure manuals to help communicate the company's ESG strategy, goals and specific processes and activities throughout the organization to mitigate ESG risks.

Evaluating the ESG Risk Management Framework and the adequacy of Impact Assessments and Stress Tests

IA should review the organization's existing frameworks and standards, ranking, measurement protocols, and reporting to ensure they are reasonable, being followed, consistent with industry recommended frameworks, regulatory expectations and comparable with similar entities. For instance, in the case of banks, IA can confirm if the organization is adhering to the updated risk appetite and ESG guidelines to prevent financing clients and sectors that are high-profile polluters or are exposed to high climate risk. In addition, IA should assess how ESG risks are embedded in the overall credit risk management framework.

Additionally, IA can evaluate the design and operating effectiveness of management's performance of periodic impact assessments and organization-wide stress tests to ensure ESG risk scenarios are plausible, and capital and liquidity implications are monitored and remediated. Also, regulators are increasing their requirements over stress test exercises as exemplified by the recent climate risk stress testing exercise required for banks by the European Central Bank (ECB). IA can monitor the organization's progress in the exercise and highlight any potential major areas of attention.

Validating ESG Goals
ESG goals can be validated through measurement of the gap between expected and actual performance and, based on that, by assessing whether goals are realistic and measurable. Goals should also be included in the company's strategic objectives and be a regular item on Board meeting agendas. IA can also complement this assessment through benchmarking: this can help the organization identify where it stands compared to peers and identify the amount of improvement possible.

Where the entity has adhered voluntarily to initiatives like for example NetZero Banking Alliance, IA can ensure that there is a regular follow up on the objectives and controls on the measurement of performance against these objectives, specifically when they are publicly disclosed.

Reviewing ESG Reporting
One of the most critical areas for IA to play a role is in validating the relevancy, accuracy, completeness and timeliness of management's ESG financial (when not covered by external audits) and non-financial reporting metrics in public disclosures. To avoid unsubstantiated claims that could be considered greenwashing and adversely impact the organization's reputation.

IA can review the materiality assessment data gathering process used for building the metrics and can also challenge the use of specific metrics over others which might be more relevant for external investors and other stakeholders and reflecting company's strategic objectives. To ensure the reporting is focused on what is material. Examples of material/relevant topics for banks could be the bank's exposure to fossil fuel and other high emitting sectors, its progress in reducing the bank's footprint through its operations, supply chain and financing portfolio, and the impact of the offered sustainable investments.

Assurance reviews could also be performed to prevent reputational risk on financial products or services labelled as "Green" or "Sustainable", with a view to ensure they effectively comply with taxonomy and other legislative requirements and the information provided to customers reflects adequately the sustainability of the product.

Audit on ESG Risk Models
Recently, Environmental, Social, and Governance score modelling gained significant attention as a framework for evaluating the sustainability impact of companies. The banking industry is facing increased regulatory scrutiny in this context, and the IA plays an essential role in ensuring the accuracy and reliability of ESG score models.

Defining and quantifying a score, able to reflect the ESG impact of a company, leads to several methodological challenges for any European Bank, from collecting and analysing a broad and new type of data/information to developing and reviewing of the underlying processes.
In this context, an Audit Model Risk assessment can help in enhancing the transparency and credibility of ESG scores, across the Bank and to the Supervisor, by providing an independent assurance on the methodological approach used in the calculation.
Among other, the accuracy, completeness, and consistency of data and information collected should be verified. This includes checking the integrity of data sources, evaluating the methodologies and expert-based assumptions, and assessing the appropriateness of disclosures.

Furthermore, IA should evaluate the effectiveness of the internal controls in collecting, processing, and reporting ESG-related data accurately considering the three lines of defence, and the model's life cycle as well. According to this, IA should assess whether the banks' internal controls are designed effectively to identify, mitigate, and report ESG-related risks and opportunities.

In summary, IA has a relevant role in relation to the review of the new ESG scores and related Bank's processes that should always be aligned with the bank's strategies and with the evolution of the regulatory framework. It provides assurance on the accuracy and reliability of ESG data, assesses the effectiveness of internal controls, enhances the transparency and credibility of ESG scores, and helps banks identify areas for improvement.

Advisory services
On the advisory side, IA can support the organization in implementing ESG requirements. Regulators in many jurisdictions have increased their focus on ESG risks with initiatives related to climate change, executive pay, diversity and inclusion, working conditions, human trafficking, and product content, among others. These jurisdictions have mandated or encouraged greater disclosure of sus-

tainability practices and risks, and several major stock exchanges are instituting similar requirements. For this reason, such topics cannot be ignored by IA, as the stakes are simply too high, with pressure exerted by regulators, investors, customers, third-party affiliates, and society at large.

Implementing the requirements in practice is difficult due to lack of expertise in specific ESG topics and of standardized approaches within the industry. IA could help organizations moving in the right direction by:

- Collaborating with Legal and Compliance to validate ESG reporting disclosures comply with applicable regulations. For example, IA can create an inventory of ESG disclosure requirements to identify what disclosures are required, by which agencies / regulators / governments; Advising on developing specific internal controls in relation to the identified requirements; advising on ESG governance due to IA's holistic understanding of risk across the organization; and more generally
- Challenging the current way things are done from a risk and control perspective
- Performing business monitoring, facilitating knowledge sharing with different internal stakeholders.

Internal vs external audit on ESG

While the internal and external audit functions could complement each other, their purposes and areas of focus differ. The Institute of Internal auditors (IIA) emphasizes that the two functions do not compete or conflict; rather, they both contribute to effective governance. In general, Internal auditors take a holistic view of their organization's governance, risk, and control systems (in other words, primarily non-financial information), while external auditors are either concerned with the accuracy of business accounts and the organization's financial condition and its regulatory compliance.

With regard to ESG, IA can provide the independent internal assurance needed for trustworthy ESG disclosures and help to ensure the existence and effectiveness of internal controls on ESG risks and their continuous monitoring processes across the organization. External auditors provide third party assurance services by endorsing the integrity of non-financial (ESG-related) public disclosures and ensuring they align with financial information in external reporting to investors and stakeholders. External auditors can also help to perform a benchmark to compare the entity with competitors and ESG best practices in the financial sector.

While the purpose, focus, and outcomes of their fieldwork may vary, internal and external auditors often share information to avoid duplication and improve audit coverage. In fact, IA can leverage the external auditor's comments / findings on areas included in their review and vice versa.

Challenges faced by IA

According to the 2021 ECB comparative study on the state of climate and environmental (C&E) risk management in the banking sector[1], institutions are increasingly integrating C&E risks into their three lines model. However, "the integration of C&E risks into the third line remains rare, as only about 15% of institutions have explicitly considered these risks in their internal audits or reviews. In some cases, internal audit functions have performed a dedicated audit of the compliance of institutions' practices with their internal policies and with regulations applicable to C&E risks."

The low level of Internal audit engagements on C&E risks, and more in general on ESG, might indicate that IA functions face challenges in the way they approach ESG. This may be due to Internal auditors' lack of awareness or understanding of ESG risks and the operational and financial implication to the organization.

Another challenge for IA is to identify responsible parties within the organization. ESG has become such a pervasive topic that every function within the organization will cover ESG related topics to a certain extent. Often, Investor Relations, Finance, Strategy, Legal, Compliance, Risk Management and front-office functions will be involved in ESG.

However, who ensures the effective coordination among these groups? And, most importantly, who ensures effective governance around ESG within the organization?

Effective coordination among these groups and a focal point of responsibility is critical to progress. These challenges become even more evident for multinational banks, where a sound coordination is expected between Head Office and subsidiaries or foreign branches. Also, the different regulatory expectations and requirements in different countries, create additional complexity in the management of ESG risks and, as consequence for IA. Translating the organizational set up of the bank in terms of ESG into the audit universe and ensuring a complete audit coverage for the global organization is one of the key challenges for internal auditors.

Furthermore, as Kaplan and Ramanna (2021)[2] comprehensively discuss, ESG's sub-components are not homogenous. They in fact rely on different indicators, language, and measurement. For instance, environmental issues can be measured in inputs and outputs, while governance issues often rely on compliance- or process-measures, that require a considerable level of judgment and contextualization to be interpretable. Neither inputs nor outputs are easily determined.

And last but not least, social issues are more hybrid and probably pose even greater challenges for their measurement, than environmental and climate-related issues. The consequence of this is that not all issues can and should be audited through the same process in the same audit engagement. Also, this suggests that different expertise is needed to review and judge the correct and fair repre-

sentation of the underlying information.

Another challenge that IA functions are facing is the low level of maturity of ESG regulations and business practices, which may delay business decisions on strategic and compliance risks. At the same time, in the European Union we are witnessing an enormous increase of new regulations aiming to address ESG and greenwashing risks.

This forces organizations to develop new processes, set of controls and policies, and above all, obtain the right data to fulfill the regulatory requirements (e.g. CSRD). The availability and accuracy of ESG perhaps poses even greater challenges: does the organization have the right ESG data; is that accurate, relevant and sufficient to provide information that correctly depicts the organization's ESG efforts, without incurring into greenwashing? These are all questions that IA functions can and should address in their assurance reviews over, for instance, ESG reporting. It is clear there is a need for Internal auditors to be trained on ESG risk solutions. By developing knowledge IA can add value and partner with management to identify and establish effective ESG controls, develop audit work programs and verify that reported ESG program outcomes are supported by evidence of performance.

Addressing ESG risks can no longer be postponed due to other priorities: IA has a clear responsibility to highlight both emerging risks and exposures that are not being mitigated or properly addressed by the company, including ESG risks.

PART 2: ESG internal audit in practice: the experience of European Banks

The IA journey on ESG

There are many opportunities - and a few important challenges - for IA to play a valuable role in ESG management. Likewise, there are various ways of approaching the topic from an audit perspective.

In the following the steps are set out which have been taken within IA of an European Bank to date. The experiences can be a helpful starting point for others.

Allocation of responsibilities

In 2020, the Bank IA function started the journey to develop an audit approach to include the ESG risks in the audit oversight. The primary focus was on mapping and assessing the impact of ESG regulatory developments and requirements, however the complexity and width of the ESG topic warrants a more holistic approach. This resulted in the decision to create a specific dedicated audit team with central ownership on ESG risk that started in 2021.

Considering that climate change and environmental issues are likely to increase in importance over the next years, the audit team was built with people that collectively possess the skills and knowledge required for their involvement in these areas. This expertise has been achieved by completing specific trainings and internationally recognized certifications on the topic, but also, by onboarding in the audit team experienced people that worked before in Sustainability related functions within the Bank.

This allocation of clear responsibilities within the third line enables the team to develop a standard audit approach globally, to cultivate specialist knowledge and skill set to perform audits on these risks and challenge the business, and to be on top of the evolving regulatory landscape. Additionally, from a client perspective, having dedicated staff for sustainability topics facilitates the development of stakeholder relationships and alignment with business.

Audit universe split

IA is in the process of aligning the audit priorities, the audit universe and audit plan, with the Bank's strategic Sustainability priorities. The materiality analysis that is disclosed in the Annual Report provided relevant insights on the material matters.

As starting point, IA split the audit universe between two main areas: Responsible Business and ESG Risk. Responsible Business comprises the offer of sustainable products for Retail and Wholesale banking clients. ESG Risk includes the risk related activities, like climate risk management, specific environmental and social risk frameworks, ESG reporting activities and compliance with specific Sustainability regulatory requirements. The definition and breakdown of the audit universe was done bearing in mind that it would be evolving over time, as sustainability related activities and requirements will also evolve in the organization.

Definition of audit universe and coverage of ESG risks

When defining the audit approach coverage, one of the main challenges faced was to set up the audit work at the correct level (group level or local level). There are regulatory developments, like the ECB Guide on Climate and Environmental risks, that are impacting entities at consolidated level; also, the ESG information is disclosed in the annual report at Group level.

However, there are other regulations, like Sustainable Finance Disclosures Regulation (SFDR), or specific frameworks for performing the environmental and social due diligence on clients, that have an impact on the different entities across the Bank. To ensure that key ESG risks are sufficiently addressed in the audit work, IA decided on a combination of both global and local coverage. Local coverage for specific implementations on the different business units, also depending on the maturity level. And global coverage for group-wide topics such as Sustainability Reporting or Climate Stress Testing.

Global versus local

Although most of the regulatory initiatives were launched at European level, IA is aware that there could be additional local regulatory developments in the different jurisdictions where the bank operates. In order to ensure that these local regulatory specificities related to Sustainability are followed-up and integrated in the corresponding audit entity, in the next year IA envisions to set-up a virtual sustainability network made of auditors located across the main subsidiaries and the central team to build together this overview.

This network will help the audit function to maintain a tracker of local ESG regulations and establish potential impact of the local regulatory requirements on audit work. At the same time, knowledge will flow from Group Audit to local audit teams,

Combining assurance and advisory

The Bank's IA function mainly focuses on providing assurance. Nevertheless, they recognize the different levels of maturity of the ESG elements in the organization and would like to adapt their role to this reality. Besides the standard assurance work done on the existing (ESG) processes already running in the bank, IA uses specific limited assurance, or non-assurance reviews where useful and practical (mainly based on the level of maturity of processes reviewed)

Another key part of IA's advisory role relates to business monitoring activities. These are carried out through a combination of regular meetings with main stakeholders and the attendance to the relevant committees and forums in the bank. Business monitoring plays a relevant role in the ability to support the implementation of the bank's Sustainability Strategy.

For this purpose, IA developed a stakeholder relationship matrix, assigning specific auditors to key areas/ stakeholders, and using knowledge gained via the interaction with other IA teams, via for example the Sustainably Internal Audit Forum, which comprise more than 30 internal audit functions from different banks, established by Corporate Audit Team at the beginning of 2021.

The forum has become a reference of knowledge in the industry, as for example, allowed a voluntary group of 9 leading banking institutions to develop for the first time, a Climate Risk Audit program based on the ECB Guide on Climate and Environmental Risk, and the Supervisory Statement (SS3/19) on Enhancing Banks' and Insurers' Approaches to Managing the Financial Risks from Climate Change, issued by the PRA in 2019.

These forums will continue in 2023 and beyond and invite any interested financial institution to join.

Creating awareness on ESG within IA

Considering the transversal nature of the ESG risks across the entities, it is relevant that all auditors get an understanding of the basic elements of Sustainability and related risks. For that purpose, apart from the planned virtual sustainability network with auditors located in main subsidiaries, the bank ESG audit team provides awareness trainings for the rest of auditors in the bank.

Spreading knowledge on this topic can help all IA teams to identify and embed ESG risks in their audits adequately. With this purpose, a series of internal webinars are planned every year, open to all internal auditors across the bank, where the ESG audit team provides insight on different topics, shares the latest developments from within the organization, main regulatory requirements and the results of last audits done on the topic. Furthermore, all people joining IA in the bank get a dedicated Sustainability risks training session, as part of the standard new joiners on-boarding training.

Finally, as a key additional step to create awareness on ESG across all IA teams in the bank, specific training sessions for senior management of the Corporate Audit Team were organized.

Those sessions were mainly delivered by senior sustainability experts within the bank, together with external consultants, to provide all Audit Heads the foundations of Sustainability concepts, understanding of the bank sustainability strategy, priorities, risks and ongoing developments.

Work Program

Noting the lack of a standard or benchmark yet on how to perform ESG audits, the German Institute of Internal Audit has developed a practice guide. It is based on regulatory risk management requirements for the banking sector and approaches the ESG topic from different directions. It may serve as audit catalogue or checklist consisting of various modules. On the basis the individual IA function may create an audit program tailored to the specific level of maturity of the topic within the organization, the purpose of the audit (e.g. governance audit, product specific audit) and for instance the specific audit approach[3].

Conclusion

The relevance of ESG risks for companies requires the involvement of the IA function to support the bank's response to these material challenges. The ESG territory is still developing and there are many (regulatory) uncertainties and challenges, but this cannot be used as an excuse/limitation for IA functions not to get involved and support organizations on their pathway towards a sustainable future.

ABOUT ECIIA

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and the Mediterranean basin.

The mission of ECIIA is to be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union, its Parliament and Commission and any other appropriate institutions of influence. The primary objective is to further the development of corporate governance and internal audit through knowledge sharing, key relationships and regulatory environment oversight.

ABOUT ECIIA BANKING COMMITTEE

ECIIA set up a Banking Committee in 2013 with Chief Audit Executives of the largest European Banks, supervised by the ECB. The mission of the ECIIA Banking Committee is: "To be the consolidated voice for the profession of Internal Audit in the Banking sector in Europe by dealing with the Regulators and any other appropriate institutions of influence at European level and to represent and develop the Internal Audit profession as part of good corporate governance across the Banking Sector in Europe ». ECIIA represents around 55.000 internal auditors and around 15.000 are active in the banking sector.

THANK YOU

The paper describes the results of discussions amongst the ECIIA Banking Committee members and we want to thank the Committee members for their input.

A big thanks as well to the redaction team: Jessica de Boer, Elena Durante and Sara Gonzalez, ESG Risk Audit at ING and Patrizia Biermann and Daniel Krömer, ESG Risk Audit at Commerzbank for their support.

Notes

[1] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202111guideonclimate-relatedandenvironmentalrisks~4b25454055.en.pdf

[2] Kaplan, RS and Ramanna, K (2021) How to Fix ESG Reporting, Forthcoming Harvard Business Review.
See DIIR website : DIIR_ESG-Leitfaden_Banken.pdf

[3] See DIIR website : DIIR_ESG-Leitfaden_Banken.pdf

Kunstig intelligens, revisorerhvervets snarlige død? Om kunstig intelligens i revision – muligheder og begrænsninger!

Rolf Elm-Larsen[1], Political scientist specialised in accounting and auditing

Indledning

Nyhedsmedierne har på det seneste annonceret "døden" for en række professioner så som jurister, journalister, tekstforfattere, kunstmalere, komponister og også for revisorerhvervet. Baggrunden for denne ex ante "dødsattest" er lanceringen af en række nye programmer, som markedsføres som kunstig intelligens (AI)[2].

Den engelske matematiker Allan Turing opstillede allerede i 1950 et kriterium for, hvornår man kunne tillægge en maskine menneskelig intelligens eller evnen til at tænke. Det er tilfældet, hvis en maskines svar i en samtale ikke på nogen måde kan skelnes fra et menneskes svar på det samme spørgsmål.

Enhver - der har forsøgt sig med en dialog med de offentligt tilgængelige chatbots - vil have oplevet, at rigtig formulerede spørgsmål giver fornuftige svar, mens upræcise og dunkle spørgsmål giver kryptiske svar. Nutidens chatbot respons er ofte, som den svenske digter Tegner udtrykker med, at *"det dunkelt sagda är det dunkelt tänkta"*. Næppe det matematikeren Allan Turing forstod ved kunstig intelligens.

Det er derfor heller ikke unaturligt at tillægge maskiner udstyret med kunstig intelligens menneskelige egenskab og evner, herunder også destruktive intentioner, der vil kunne skade eller endog udrydde menneskeheden selv. Det er især tilfældet, når man undlader at analysere og opnå en forståelse af, hvad kunstig intelligens reelt er, og hvordan det virker i professionel kontekst.

Det er denne artikels intention at åbne og se på indholdet i maskiner, der fremtræder som havende intelligens, omend den er kunstig. Gennem denne analyse er det hensigten at undersøge, om hvorvidt AI-systemer rent faktisk udgør en trussel mod revisorerhvervets eksistens eller undergang. Men artiklens intention er ikke at være et "maskinstormer" indlæg, men den er et forsøg på at give nogle bud på, hvor i revisionsprocessen computere udstyret med programmer for kunstig intelligens kan fungere som et adækvat værktøj for menneskeligt intelligente revisorer, og under hvilke forudsætninger kunstig intelligens kan bidrage til kvaliteten af revisionen.

Hvad er kunstig intelligens?

I Danmarks nationalleksikon - Lex.dk - defineres kunstig intelligens (KI) som computerprogrammer og maskiner, der efterligner et eller flere aspekter af den menneskelige intelligens forstået som evnen til abstrakt tænkning, analyse, problemløsning, mønstergenkendelse, sprogbeherskelse og -forståelse, fornuftig handling og lignende.

Når definitionen går på IT-fænomener, der forsøger at kopiere menneskelig intelligens i bredeste forstand, bliver den bred og abstrakt. Den er bedst egnet til beskrivelse af forskningsfeltet kunstig intelligens, men den er velegnet når det drejer sig om konkrete eksisterende systemer og systemer, som er under aktuel udvikling.

Både OECD og EU har, som led i begyndende regulering af AI området, opstillet definitioner, der er mere operationelle og mere præcise i deres afgrænsning af kunstig intelligens.

OECD definerede i 2019 begrebet i sine anbefalinger for anvendelsen af kunstig intelligens som et maskinbaseret system, der for et sæt af menneskeligt definerede mål kan foretage forudsigelser, anbefalinger eller beslutninger, der påvirker virkelige eller virtuelle miljøer, og som er designet til at fungere med forskellige niveauer af autonomi.

Det er en definition, der kan bistå mennesket med specifikke processer, så som forudsigelser og beslutninger med en grad af uafhængighed fra menneskelig intervention. Det er nok autonome maskinbaserede computersystemer, men det er mennesket, der er i kontrol med hvad systemet skal bruges til ved fastsættelsen af målene. OECD's definition på AI er en bred, teknisk neutral og brugbar definition i en politisk kontekst, selvom den dermed bliver mindre præcis, og til dels gør det vanskeligt at identificere virkelighedens AI-systemer.

Siden EU-kommissionen fremsatte sit forslag til forordning om KI, har der politisk både i EU-Parlamentet og EU's Ministerråd, været arbejdet intensivt med at få en brugbar definition, der kunne lægges til grund for lovgivningsarbejdet. I juni 2023 var man nået frem til følgende definition:

"System med kunstig intelligens" (AI-system): et maskinbaseret system, der er designet til at fungere med en varierende grad af autonomi, og som med eksplicitte eller implicitte mål kan generere output såsom forudsigelser, anbefalinger eller beslutninger, der påvirker de fysiske eller virtuelle miljøer.

Der er nu en stor fællesmængde mellem OECD's og EU-definition på AI. Dog fremhæver OECD's definition, at det er mennesket, der fastlægger målene for de maskinbaserede AI systemer. Det indebærer, at det er mennesker,

som har ansvar for AI systemernes autonomi. Forskellen skal dog ses i den sammenhæng, at EU-lovgivningen netop stiller et veldefineret ansvar for brugen af AI-systemer.

EU-definitionens formål skal relateres til forordningens dobbelt målsætning om at beskytte EU's borgeres grundlæggende rettigheder samt at opretholde et effektivt indre marked. I den kontekst er definitionen relevant for denne artikel, da revision som tjenesteydelse er omfattet af reguleringen af det indre marked.

Der findes to former for kunstig intelligens. For det første systemer, som bygger på symbolsk struktur, og de kan være enten logisk sekventielle eller hierarkiske. Den anden form er konnektive strukturer, der både kan være serielle og parallelle "neurale netværk", der med deres databaser af erfaringer og observationer kan foretage mønstergenkendelse.

Ekspertsystemer, der bygger på en faglig logik og regler, hører til den første type af kunstige intelligens systemer, mens de nu alment tilgængelige og delvis gratis chatbots er eksempler på den sidstnævnte type.

En analyse af emnet kunstig intelligens og revision må fokusere mere specifikt på metoder og teknikker ved AI for at kunne afgøre muligheder og begrænsninger ved kunstig intelligens i revisionen. I denne artikel vil jeg for reelt at kunne identificere AI systemer forudsætte, at systemerne indeholder en logisk sekventiel struktur til behandling af viden/data og/eller databehandling efter et kognitivt paradigme, der gør mønsterkendelse mulig. Det er en nødvendig afgrænsning, når man skal se på de aktuelle muligheder for praktisk anvendelse af kunstig intelligens.

Kommende EU-regulering af kunstig intelligens

Den kommende EU-forordning om anvendelsen af digital AI bygger på to søjler dels ansvarlighed og dels transparens. Forordningen stiller krav om, at AI-systemer klassificeres efter deres risiko, samt at der stilles krav om transparens, åbenhed og gennemskuelighed for AI-systemer. Forordningen skelner også mellem AI-systemer, hvor risikoen er uacceptabel. Systemer med uacceptabel risiko (manipulation af udsatte mennesker, social klassifikation af fysiske personer, biometrisk identifikation) bliver forbudt, mens systemer, der har højrisiko, løbende skal evalueres. Til alle andre AI-systemer er der et krav om transparens til applikationerne. Det påhviler dem, der har ejerskabet og systemansvaret.

Begrebet revision og kunstig intelligens

Efter gældende internationale revisionsstandarder[3] er revisionens formål gennem en proces at nå frem til en udtalelse om, hvorvidt et regnskab i alle væsentlige henseender er udarbejdet i overensstemmelse med gældende regnskabsramme[4].

Med andre ord er finansiel revision en systematisk proces, der skal lede frem til en konklusion, om at et regnskabsmateriale opfylder de kriterier, der er indeholdt i et givet sæt af regler for regnskabsaflæggelse. Revisionsprocessen skal sikre, at regnskabet er aflagt i overensstemmelse med de forskrifter, regler, koder og mønstre, der er indeholdt i den regnskabsmæssige ramme.

Meget forenklet sagt vil revisionsprocessen kunne udføres ved at se, om regnskabet i al væsentlighed har de samme mønstre og koder som fastsat i regnskabsrammen. Stillet op på den måde er der tale om, at revisor ved en sådan maskinel proces vil kunne få svar på, om regnskabet er aflagt efter regnskabsrammen.

Imidlertid skal revisoradfærd – revisionen - være karakteriseret af en række specifikke egenskaber, så som professionel skepsis og bedømmelser, der bygger på en forståelse af virksomheden og tilstrækkeligt revisionsbevis baseret på en bedømmelse af væsentlighed og risiko. Den logiske konsekvens af dette er, at det ikke er tilstrækkeligt, at revisor indlæser regnskabet i et AI-system, som en chatbot, og beder maskinen om at producere en revisionspåtegning. En sådan brug af et AI-system vil derfor ikke umiddelbart sikre en revisionsfaglig evaluering af for eksempel virksomhedens fremtidige levedygtighed (going concern), effektiviteten eller hensigtsmæssigheden af ledelsens etablerede risikovurdering og interne kontrolsystemer, eller revisorers vurdering af sammenhængen mellem en separat ledelsesberetning og regnskabet.

På den baggrund synes en forudsigelse om revisorerhvervets forestående død at være uden hold i virkeligheden. Det er øjensynligt alene varsler taget i kaffegrums. Derimod kan kunstig intelligens med stor sandsynlighed medvirke til en teknisk udvikling og effektivisering af revisionen.

Brugen af AI i revision

Eksisterende magtstrukturer indbygges i AI-systemernes koder, derudover indbygges de juridiske regler for regnskab og regnskabsaflæggelse. Dermed kan regneskabsreglerne omsættes til mønstre, der udgør vidensdatabasen, hvor i regnskabsreglerne er formaliseret. De eksisterende magtstrukturer, som regnskabsreglerne er et udtryk for, er således ind lagret i AI-systemer, der anvendes i regnskab og revision.

Revision er en sammenholdelse af et regnskab med de normale mønstre af regler og koder for regnskabsaflæggelse. I AI-tidsalderen kan revision reduceres til et spørgsmål om, hvorvidt et regnskab matcher de kode mønstre mv., som er sat op i databasen over regnskabsregler. Er der tale om match, vil regnskabet principielt kunne forsynes med en blank påtegning, mens det ved afvigelser fra mønstrene i databasen for regnskabsregler mv. skal have en påtegning med karakteren af bruddet på regnskabsreglerne

Når regnskab og revision ses som et mønster af koder, giver det mulighed for en gruppe af professionelle, at sikre sig den dominerende rolle i den proces, der skriver

databasens koder. Den oversættelse giver koderne mulighed for at fortolke reglerne indenfor regnskab og revision, så det varetager de interesser, der (u)bevidst styrer deres adfærd.

AI-systemerne, som bygger på den konnektive tilgang, bygger ikke på en logisk sammenhæng mellem orden, men alene på en statistisk sammenhæng mellem sidestillede ord og sætninger. Konsekvensen er, at der ikke nødvendigvis er tale om, at AI-systemer generer udsagn, der har en mening, og selv om udsagnene har en mening, er de ikke nødvendigvis sande.

I modsætning til et menneske kan en AI-applikation skrive et løgnagtigt udsagn uden at rødme eller blive afsløret af en løgnedetektor. Med andre ord behøver AI-systemers "deep learning" ikke at afspejle en revisions faglig logik, men alene den frekvens som ord og sætninger er sammenstillet. En væsentlig potentiel fejlkilde for generelle "audit failures", hvis sådanne systemer eventuelt anvendes i revisionspraksis.

Aktuel brug af kunstig intelligens i revision

Det er svært at få etableret et overblik over den aktuelle brug af kunstig intelligens i revisionspraksis. En væsentlig kilde, som indhold i de store revisionsfirmaers hjemmesider, er primært fastlagt ud fra forretningsmæssige hensyn, hvilket gør dem svært brugbare til en nøgtern kortlægning af deres brug og overvejelser af anvendelsen af kunstig intelligens i revisionsprocessen.

Tabel 1 herunder viser, at alle de fire største revisionsbrands er engageret i udviklingen og brugen af kunstig intelligens for at effektivisere revisionen. Det gøres ud fra meget forskellige tekniske principper og formål. Der er øjensynlig ikke enighed mellem firmaerne om, hvor og hvordan den kunstige intelligens på nuværende tidspunkt kan bidrage til den faglige udvikling af revisionsarbejdet.

Automatisering af revisionsprocessen

Ved udførelsen af revisionen, er der opgaver af gentagne karakter, som før og stadig i dag udføres af revisorer og deres medhjælpere. Nu er det muligt at udføre disse opgaver ved brug af computere med et sæt af forprogrammerede tommelfingerregler. Det kan være programmer, der er skrevet på baggrund af de instrukser, som ledende revisor tidligere har formuleret til revisorassistenter til brug ved gennemgangen eller skanningen af store mængder af bilag og transaktioner. Dette arbejde genereres i dag gennem en maskindialog med særlige revisionssoftwarelister det materiale, som revisor skal viderebearbejde og vurdere. Denne type af automatiseringsprogrammer giver revisor svar på en række elementære spørgsmål bedre end kohorter af revisorassistenter, fordi computeren ikke har menneskelige svagheder som uopmærksomhed fx ved skanning af transaktioner af kontokort eller bilagsmateriale.

Det er imidlertid omdiskuteret, om disse typer programmer kan klassificeres som kunstig intelligens[5]. Det vil være nærliggende, fordi algoritmen i disse systemer indeholder de erfaringsbaserede regler, som de erfarende revisorer bruger ved introduktionen af de mindre erfarende nyansatte revisorassistenter. Den form for kunstig intelligens indeholder uden tvivl de lavthængende frugter set i forhold til systemer, der bygger på mønstergenkendelse eller fuzzy-logik mv.

Regelbaserede systemer formaliserer den professionelles revisors viden og vurderinger - både eksplicitte og implicitte. Sådanne systemer kræver, at lærebøger formaliseres og erfarende revisorer interviewes, så deres ikke-formaliserede viden ekspliciteres. Det kræver evnen til at

Tabel 1. De fire største revisionsfirmaers brug af AI i revisionsprocessen

Revisions-firma	AI Application	Aktivitet	Funktion
KPMG	"Clara"	Uddrager afvigelser fra både struktureret og ustruktureret regnskabsmateriale.	Identifikation af forhold med væsentlig risiko for fejl information.
EY	"Document Intelligence Platform"	Review af kontrakter med henblik på efterfølgende professionel bedømmelse.	Effektiviserer revisionsarbejdet, så revisorer kan koncentrere sig om revisionsfaglige spørgsmål.
Deloitte	"Argus"	Udtrækker nøgle- informationer fra andre elektroniske dokumenter og sammenholder dem med standarddokumenter.	Identifikation af, om regnskabsmaterialet indeholder væsentlig fejlinformation, som indgår i regnskabets registreringer.
PwC	"GL.ai"	Identifikation af afvigelser i hovedbogen (general ledger), som en professionel revisor vil identificere under sin analyse af regnskabet.	Identifikation af transaktioner i selve regnskabet.

Primære kilde: Cory Ng and John Alarcon: Artificial Intelligence in Accounting. Practical Application, Routledge 2021, p. 26 ff

klarlægge og præcisere den tavse viden som erfarne og rutinerede revisorer betjener sig af i deres virke.

Ved mønstergenkendelse etableres der relationer mellem observationer, hvor disse danner et billede af et givet fænomen. Denne form for KI kræver store databaser for at kunne identificere mønstre i relationerne, som så kan danne grundlag for dannelse af definitionen af et givent fænomen.

I **Tabel 2** er der på grundlag af de forskellige faser i revisionsprocessen forsøgt givet en oversigt over eksempler på, hvorledes artiklens forfatter ser, at kunstig intelligens kan anvendes i revisionsarbejdet. De to hovedtyper af kunstig intelligens kan bidrage på forskellig måde til revisionsarbejdet, men det må nok antages at potentialet ligger i brugen af de regelbaserede systemer på kort sigt. Imidlertid er der et stort fremtidigt potentiale i systemer, som bygger på mønstergenkendelse mv., hvilket dog kræver opbygning af store databaser.

Den kunstige intelligens begrænsninger

Den virkelige menneskelige intelligens, som revisorer betjener sig af i deres professionelle virke, har en række egenskaber, som det ikke per definition er muligt at transformere til formaliserede instrukser til computere.

Det særlige ved den menneskelige erkendelse er, at den kan hente indsigt og løsninger ved at forskyde eller transcendere sin egne erkendelsesgrænser på den anden side

Tabel 2. Eksempler på anvendelsesmuligheder af AI systemer i revision

Revisions-processen	ISA	Regelbaseret	Mønstergenkendelse
Klientaccept	210	Formalisering af firmaets normer for klientaccept på baggrund af den potentielle kundes data.	Match mellem potentielle klienter og mønstre for god virksomhedsledelse og særligt god regnskabspraksis.
Planlægning	300	Analyse af virksomhedens nøgletal med henblik på identifikation af nøgleområder for revisionen.	Kan virksomhedens finansielle karakteristika og strategier matche de mønstre og billeder, der kan genereres. På hvilke punkter afviger klienten fra normen.
Risikovurdering	315	Ekspertsystemer med formaliserede regler for betingelser for potentielle risici. Regler for sammenhæng mellem risici og interne kontroller.	På baggrund af analyser af mønstre og afvigelser fra norm evalueres risikoniveauet ved revisionen.
Væsentlighed	320	På baggrund af alternative modeller for beregning af væsentlighedsniveau kan skabes indsigt fra forskelligt perspektiv, der kan skabe grundlag for accept eller forkastelse af om regnskabet som givende et retvisende billede.	På grundlag af database over, hvad revisorer betragter som væsentlige, kan genkendes mønstre for væsentlighedskriterier.
Besvigelser	240	Væsentlige afvigelser i regnskabstal og ledelsens tilsidesættelse af centrale forretningsgange og interne kontrol.	Identifikation af mønstre karakteristisk for bedrageri, fx Ponzi skema.
Revisionshandlinger		Tommelfingerregler for udvælgelse af transaktioner, der kan påvirke om regnskabet giver et retvisende billede.	Sikre compliance med den regnskabsramme som virksomheden anvender.
Revisions dokumentation	500	Regler og normer for tilstrækkeligt og passende revisionsbevis.	Vurdering af om den indsamlede dokumentation matcher normale mønstre for revisionsdokumentation.
Vurdering af going concern	560	Regnskabsanalytiske tommelfingerregler fx om likviditetsberedskab, indregning af aktiver.	Støtte til revisors vurdering af going concern ved særlige sproglige mønstre i ledelsens egen vurdering af going concern.
Udformningen af revisionserklæring	700	Revisionsstandarden indeholder slutningsregler for udformningen af revisionserklæringen: hvilke typer af væsentlige regnskabsfejl medfører (ikke) modificerede erklæringer.	Database, som etablerer et netværk, der kombinerer observationer med betydning for revisionskonklusionen og særligt erklæringer med forbehold mv.

af sig selv. Den kan med andre ord bruge det metafysiske til at danne ny indsigt, hvorved mennesket flytter grænserne for sin egen erkendelse: Gøre det metafysiske til fysisk real eksisterende viden. Vi bruger det ikke-erkendte til at flytte erkendelsens grænser ind i metafysikkens ukendte territorium. Heureka er det øjeblik, hvor den menneskelige erkendelse forstår og formulerer problemet. Så følger løsningen, og der er vundet ny indsigt og viden.

Som alle andre professioner har revisor erhvervet et sæt af ikke-eksplicit formulerede normer, koder og praksisser. Der er tale om tavs viden. Den faglige praksis er kontekst baseret, og uden at erhvervet har gjort betingelser og forudsætninger for revisionspraksis eksplicitte. Den type af viden har en maskine ingen reel mulighed for at tilegne sig. Det er kun fagprofessionelle individer.

Den menneskelige intelligens omfortolker løbende den eksisterende viden til nye indsigter. Intet fag – heller ikke revision – er statisk. Vores tankevirksomhed udvikler sig dialektisk, hvor nye indsigter udfordrer gamle, så der skabes nye fagkundskaber, der er en syntese af modsætninger i den eksisterende viden. Denne intellektuelle proces er ikke inkluderet i den kunstige intelligens.

AI er blot et supplement eller en delmængde af den rigtige medfødte menneskelige intelligens, der er grundlaget for en profession som revisorerhvervet og dets eksistens rationale og formål.

To typer sammenfatning og en konklusion

Artiklen er en sammenstilling af to typer af intelligens: kunstig og menneskelig. Derfor også to ulige sammenfatninger, som forfatteren bringer på en ultrakort formel i en afsluttende konklusion.

Revisionsfaglig sammenfatning
Artiklen leder frem mod følgende overordnede faglige pointer:

- Grundlæggende består computere og maskiner, der betjener sig af "kunstig intelligens", af menneskeskabte algoritmer og databaser, hvis indhold er defineret af mennesker. Det fastlægger dermed den kunstige intelligens grænser især i forhold til den menneskelige intelligens, herunder den professionelle revisor.

- Revision er et professionelt domæne, der ligger uden for den kunstige intelligens grænser, fordi den menneskelige intelligens er en forudsætning for revisors professionelle skepsis og bedømmelse af virksomheders ledelsesaflagte finansielle regnskab.

- Maskiner med kunstig intelligens har et potentiale til at øge kvaliteten af revisionen på de felter i revisionsprocessen, hvor der er tale om, at revisor anvender tommelfingerregler, og hvor det er muligt at foretage mønstergenkendelse.

- Revisionserhvervet har et særligt ansvar for, at de kunstige intelligenssystemer, som udvikles til brug i revision, lever op til de grundlæggende værdier for revisionsbranchen transparens og effektiv risikovurdering.

Når alt den "kedelige" og "knastørre" revisor- og IT-logik standser, har den "kunstige intelligens" - jeg har studeret på for at skrive denne artikel – dog et "menneskeligt" glimt i øjet i sin egen sammenfatning på et af mine formulerede spørgsmål. Den "kunstige intelligens" får derfor lov til at afslutte artiklen.

Chatbotens selvironiske sammenfatning
Under mit arbejde med denne artikel har jeg naturligvis også brugt en gratis chatbot (www.chat.openai.com). Et af svarene indikerede AI systemernes egne grænser:

" However, it's important to note that while AI can greatly enhance the audit process, human judgment remains essential, especially in situations where interpretation of accounting standards requires context, experience, and understanding of the specific business and industry. AI should complement, rather than replace, the expertise of auditors in evaluating compliance with the chosen accounting framework."

Måske har ChatGPT haft adgang til at læse Dreyfus & Dreyfus bog fra 1986: "Mind over Machine" og at gengive bogens stadig gyldige filosofisk begrunde synspunkt! Muligvis har chatbot'en måske allerede luret mig, så den taler mig efter munden som en anden dårlig sælger, der skal få mig til at købe et abonnement på applikationen. Den er jo kun gratis for at lokke mig til at blive så afhængig, jeg køber et abonnement på deres betalingsversion af AI-applikationen!

Da jeg spurgte, hvilke kilder ChatGPT havde til synspunktet, fik jeg et uspecifikt generelt svar, som blot påviste behovet for det menneskelig væsens intellektuelle evner til kritisk tænkning. Aksiomet om, at kunstig intelligens ækvivalerer det menneskelige intellekt, er brudt. Fremtiden er nok snarere den analoge verdens innovative og kritiske tænkning understøtter og styrer AI-systemerne. Revisor har fået en ny opgave i at styre og kontrollere de nye "kunstige intelligente" applikationer ansvarligt og korrekt ind i revisionsprocessen på en for brugerne af revisors tjenesteydelsers transparent måde.

Konklusion
På ultrakort formel er artiklens konklusion:

> **AI er kolde algoritmer uden revisions faglig indsigt eller identitet.**

Litteratur

Crawford, Kate: *Atlas of AI*. Yale University Press. 2021
Dreyfus, Hubert L. & Stuart E. Dreyfus: *Mind over machine. The Power of Human Intuition and Expertise in the Era of the Computer*. Free Press 1986

Ng, Cory and John Alarcon: *Artificial Intelligence in Accounting. Practical Applications*. Routledge 2021
Polanyi, Michael: *The Tacit Dimension.* University of Chicago Press 1966
Tegnér, Esaias: "*Epilog vid magisterpromotionen 1820*". Febus är förnuftets gud Apollo.
Alan M. Turing: Computing Machinery and Intelligence. *Mind. A Quarterly Review of Psychology and Philosophy.* Vol. LIX. No. 236. October 1950. pp. 433 - 460
Yde, Iben; Thomas G Nielsen og Rasmus Dahlberg (red): *Smart krig. Militær anvendelse af kunstig intelligens*. Djøf Forlag 2021

Andre kilder

IAASB:
https://eis.international-standards.org/standards/iaasb/2020

European Parliament: Artificial intelligence act (proposal). November 2021

Europa Kommissionen: Forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens https://www.eu.dk/samling/20211/kommissionsforslag/KOM(2021)0206/forslag/1773316/2410668.pdf
BILAG til Forslag til Europa-Parlamentets og Rådets forordning: om fastsættelse af harmoniserede regler om kunstig intelligens (retsakten om kunstig intelligens) og ændring af visse eu-retsakter https://www.eu.dk/samling/20211/kommissionsforslag/KOM(2021)0206/forslag/1773316/2410670.pdf
De Faste Repræsentanters Komité (1. afdeling) Rådet Bruxelles, den 25. november 2022
https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/da/pdf

Ændringer vedtaget af Europa-Parlamentet den 14. juni 2023 om forslag til Europa-Parlamentets og Rådets forordning om harmoniserede regler for kunstig intelligens (retsakten om kunstig intelligens) og om ændring af visse af Unionens lovgivningsmæssige retsakter (COM (2021) 0206 – C9-0146/2021 – 2021/0106(COD))
https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_DA.pdf
OECD: Recommendation of the Council on Artificial Intelligence
https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449
Danmarks Nationalleksikon:
www.lex.dk

Noter

[1] Artiklen er ikke skrevet af en chatbot, men af forfatteren selv med samme metoder som tidligere bidrag til dette tidsskrift. Chatbot'en "OpenAI" er anvendt på samme måde, som jeg benytter Google.
[2] Artiklen anvender den engelske forkortelse for kunstig intelligens "AI" alene på grund af det danske sprogs spændstighed i daglig brug.
[3] ISA 200 Overall Objectives of The Indepedent Auditor and The Conduct of an Audit in Accordance with International Standards on Auditing, A.1
[4] Der er tale om en definition, som er laveste fællesnævner for begrebet "revision" og som i mange jurisdiktioner har andre og supplerende egenskaber knyttet og integreret i sig.
[5] Ng, Cory and John Alarcon: Artificial Intelligence in Accounting. Practical Application, Routledge 2021, p. 36 ff

Gør dig selv den tjeneste - Gå ind og oplev Internal Auditor Magazine.

Er du ligeså glad for Ia (Internal Auditor) magasinet som os, så er det gratis tilgængeligt i en digital udgave via hjemmesiden InternalAuditor.org eller direkte via app til både iOS og Android. Så uanset hvor du er, så har du adgang. Bemærk dog at du først skal anmode om adgangen via dine medlemsoplysninger på www.iia.dk.

Artiklernes indhold er nu også linket til emner, så ønsker du viden inden for bl.a. Governance, Risk, Compliance eller Fraud – så er det virkelig nemt.

Ia magasinet er kåret som den førende kilde der leverer det mest relevante indhold til erhvervet Intern Revision i realtime, og med flere platforme og 24/7 adgang, er det lettere end nogensinde at holde trit med det udviklingen indenfor feltet intern revision.

Den digitale udgave af Ia er en fuld replikeret version af magasinet, så du kan se hele udgaver og bladre mellem siderne - ligesom den trykte udgave. Du finder en række navigationsværktøjer til at gennemse artikler samt bonusvideoindhold parret med udvalgte funktionsartikler.

Arkivet for den digitale udgave går tilbage til februar 2004 og er fuldt søgbare så du kan udnytte dets robuste søgefunktion for at identificere artikler af interesse.

Hvilken betydning har cybersikkerhed risikostyringen for revisor?

Michael Clement, Partner, PwC

Bo Petersen, Partner, PwC

Indledning

PwC's seneste cybercrime-survey viser, at 51 % af de virksomheder, som deltog i undersøgelsen, har oplevet en eller flere cybersikkerhedshændelser inden for det seneste år. Den viser også, at kun for 45 % af de deltagende virksomheder er der den rette balance mellem cybertrusler og investeringer i cybersikkerhed, og det er kun 22 %, der mener at have tilstrækkelige cyberkompetencer. Endvidere viser undersøgelsen, at kun i 39 % af virksomhederne er cybersikkerhed en fast del af bestyrelsens årshjul.

Der er ikke tvivl om, at der kommet en øget fokus på cyberrisici og cyberrisikostyringen i mange virksomheder, herunder i bestyrelser og direktioner, og Bestyrelsesforeningen har fx i april 2023 udgivet en omfattende vejledning og anbefalinger til styrkelse af strategiske cyberkompetencer og er dermed med til at understøtte, at cyberrisici kommer på agendaen og får den rette fokus hos ledelsen.

Cyberrisici har traditionelt ikke være det store fokusområde for revisor, især ikke i forhold til årsregnskabet, men i takt med at truslerne er øget, og der konkret har være sager i både ind- og udland, som har haft betydelig påvirkning på virksomheders drift og regnskab, er der også kommet en øget fokus fra revisor. Mens ekstern revision oftest vil have fokus på cyberrisici i forhold til risikoen for væsentlige fejl og mangler i årsregnskabet og til dels going concern, vil mange interne revisioner også have fokus på den operationelle risiko i forhold til virksomhedens forretning.

Betydning for årsregnskabet

ISA 315 (ajourført), der trådte i kraft for revision af årsregnskaber efter 15. december 2021, introducerer også cyberrisici som et element revisor skal være opmærksom på i sin planlægning af revisionen af årsregnskabet. Cyberrisici skal inddrages i planlægningen og vurderingen af kompleksiteten af it-anvendelsen, i forhold til dens betydning for at der opstår væsentlige fejl eller mangler i årsregnskabet.

Operationel risiko i forhold til virksomhedens forretning

Ved vurdering af cyberrisicienes indvirkning på virksomhedens forretning, vil det være naturligt at have fokus på, hvilke konsekvenser forskellige typer af vellykkede cyberangreb kan have for virksomhedens forretning, alt efter i hvor høj grad disse kan påvirke virksomhedens drift.

Eksempelvis: Foregår salg via nethandel? Er virksomhedens produktion følsom over for it-anvendelse? Har virksomheden "opskrifter", patenter o.l. som er vitale og ikke bør komme til andres kendskab?

Hvad er god risikostyring med fokus på cyberrisici?

Uanset om der er tale om fokus på revision i forbindelse med årsregnskabet og/eller operationelle risici, vil virksomhedens risicistyring på cyberrisiko-området have betydning for revisors vurderinger og planlægning.

Cyberrisikovurderingen bør i princippet følge samme model som virksomhedens øvrige risici, herunder:

1. Har virksomheden en fast proces for vurdering af risici, og er de medarbejdere, der udfører denne, kompetente?
2. Er der udpeget en ansvarlig for risikovurderinger i virksomheden, og har denne de fornødne kompetencer til at facilitere risikovurdering og den fornødne indsigt i virksomheden til sparring og vurdering af svar fra forretnings- /procesansvarlige?
3. Findes der beskrevne politikker og procedurer for risikovurdering?
4. Er der foretaget en struktureret risikovurdering på følgende områder:
   a. Hvad er de vigtigste aktiver for virksomhedens drift og overlevelse?
   b. Hvilke cybertrusler er der for disse aktiver?
   c. Hvilke sårbarheder har virksomheden i forhold til cybertruslerne?
   d. Hvad er sandsynligheden for, at en cybertrussel forekommer?
   e. Hvad er konsekvensen, hvis dette sker?
   f. Hvilke tiltag har virksomheden gjort for at imødegå truslerne?
5. Er cyberrisici en fast del af virksomhedens analyse?
6. Inkluderer analysen også eventuelle outsourede områder?
7. Indgår cyberrisici som en del af ledelsesrapporteringen til direktionen og bestyrelsen?
8. Har risikovurderingen en kvalitet, som gør, at revisor kan tage udgangspunkt i denne for sine egne vurderinger?

Er cyberrisici en del af virksomhedens risikostyring, og indgår de på lige fod med andre risici for virksomheden, vil det alt andet lige styrke revisors arbejde og forståelse for, hvilke risici der er for virksomheden, og dermed også, hvilken indflydelse disse har på såvel årsregnskabet som på operationelle forhold.

Revisor bør opnå en forståelse for virksomhedens cyberrisici, og hvilken betydning de har. Vi gennemgår nærmere i nedenstående afsnit de fokusområder, som intern og ekstern revisor kan have, og efterfølgende kommer vi nærmere ind på, hvordan revisor kan opnå forståelse for virksomhedens cyberrisici.

Fokuspunkter for både ekstern og intern revision

Som nævnt ovenfor er der typisk to indgangsvinkler til fastlæggelse af scope for vurdering af cyberrisici; betydning for årsregnskabet eller virksomhedens operationelle forhold.

Fokus i forbindelse med årsregnskabet

I forbindelse med revisors revision af årsregnskabet er hovedfokus jo risikoen for, at der opstår væsentlige fejl og/eller mangler i årsregnskabet, og hvordan disse risici reduceres til et acceptabelt niveau.

I denne sammenhæng er omdrejningspunktet ISA 315, der i punkt A174 omtaler cyberrisiko:

A174: Omfanget og arten af de relevante risici, der opstår ved brugen af it, varierer afhængigt af arten og karakteristikaene af de identificerede it-applikationer og andre aspekter af it-miljøet. Gældende it-risici kan opstå, når enheden bruger eksterne eller interne tjenesteudbydere til identificerede aspekter af sit it-miljø (f.eks. outsourcing af hosting af sit it-miljø til en tredjepart eller brug af et shared servicecenter til central styring af it-processer i en koncern). Gældende risici, der opstår ved brug af it, kan også identificeres i forbindelse med cybersikkerhed. Det er mere sandsynligt, at der vil opstå flere risici ved brugen af it, når omfanget eller kompleksiteten af automatiserede applikationskontroller er højere, og ledelsen i højere grad stoler på disse kontroller for effektiv behandling af transaktioner eller effektiv vedligeholdelse af integriteten af underliggende information.

Bilag 5 til ISA 315 omfatter overvejelser til forståelse af informationsteknologi (IT), herunder cyberrisiko i punkt 4 og 19:

Punkt 4
Kompleksiteten af sikkerheden over it-miljøet, herunder sårbarheden af it-applikationer, databaser og andre aspekter af it-miljøet over for cyberrisici, især når der er webbaserede transaktioner eller transaktioner, der involverer eksterne grænseflader.

Punkt 19
Revisors overvejelse af uautoriseret adgang kan omfatte risici relateret til uautoriseret adgang fra interne eller eksterne parter (ofte omtalt som cybersikkerhedsrisici). Sådanne risici påvirker ikke nødvendigvis finansiel rapportering, da en virksomheds it-miljø også kan omfatte it-applikationer og relaterede data, der adresserer drifts- eller compliancebehov. Det er vigtigt at bemærke, at cyberhændelser normalt først sker gennem perimeter- og interne netværkslag, som har en tendens til at være længere væk fra it-applikationen, databasen og operativsystemerne, der påvirker udarbejdelsen af regnskabet. Hvis der er identificeret oplysninger om et sikkerhedsbrud, overvejer revisor derfor normalt, i hvilket omfang et sådant brud har potentialet til at påvirke regnskabsaflæggelsen.

Det betyder, at revisor skal opnå en forståelse for, hvilke cyberrisici virksomheden har, i forhold til i hvilket omfang og på hvilken måde virksomheden anvender it, og vurdere betydningen for årsregnskabet. I den forbindelse vil det være naturligt, at revisor undersøger, hvordan virksomheden har tilrettelagt sin vurdering af cyberrisici og imødegåelse heraf (risikostyring). Hvis virksomheden har konstateret egentlige hændelser i forbindelse med cyberangreb, vil revisor i forhold til årsregnskabet være nødt til at forholde sig til, om angrebet har haft konsekvens for de systemer og data, som har betydning for årsregnskabet.

Fokus i forbindelse med operationelle forhold

Såfremt formålet med revisionen er operationelle forhold, risici i den forbindelse og afdækning heraf, vil scopet typisk have fokus på forhold, som ikke kun påvirker årsregnskabet, men også omfatter virksomheden mere generelt, eller hvor fokus er specifikke forhold, som ønskes afdækket fx i forhold til lovgivning.

Der er aktuelt en øget regulering i gang i forhold til virksomhedernes fokus på og forebyggelse af cyberrisici. Fx træder NIS2-direktivet i kraft fra den 18. oktober 2024, hvilket vil omfatte en række virksomheder, som er defineret som hørende under kritisk infrastruktur, og den 17. januar 2025 træder DORA i kraft (Digital operationel modstandsdygtighed i den finansielle sektor).

Herudover er SEC's nye regelsæt om "cyberoplysningspligt" trådt i kraft per 26. juli 2023, hvor der er krav om, at omfattede virksomheder skal oplyse om deres cyberrisikostyring, og -goverance som en del af rapporteringen, og væsentlige cybersikkerhedshændelser skal rapporteres i løbet af fire arbejdsdage.

Vi skal ikke komme nærmere ind på disse reguleringer, men de har alle stor fokus på cyberrisici og vil nok også mange steder være et naturligt fokusområde for en operationel revision. Det kan enten være, fordi virksomheden er direkte underlagt NIS2 eller DORA-krav, eller fordi virksomheden er leverandør til en kunde, som er underlagt disse regelsæt.

Hvis man skal foretage en revision af operationelle risici i forhold til cyberrisici, er der nogle rammeværker, som revisor kan tage udgangspunkt i, hvis ikke virksomheden selv har valgt en metodik til fastlæggelse af cyberrisici. Fx har CIS (Center for Internet Security) opstillet et rammeværk omfattende *"Critical Security Controls are a prioritized set of actions for cybersecurity that form a defense-in-depth set of specific and actionable best practices to mitigate the most common cyber attacks"*, også kaldet CIS18.

IIA har også udgivet en audit guide "assessing cybersecurity risk", som revisor kan tage udgangspunkt i. Denne giver en guide til revisor om relevante risici og trusler i forhold til cybersikkerhed og omfatter også en vurdering af virksomhedens governance / risikostyring i forhold til cybersikkerhed.

Praktiske forhold for revisor

Når revisor skal opnå en forståelse for virksomhedens sikring i relation til de identificerede cybersikkerheds-risici, bør revisor indledningsvis foretage en vurdering af, om virksomheden har identificeret de cyberrisici, der måtte være relevante for den aktuelle virksomhed. Denne vurdering skal foretages med udgangspunkt i virksomhedens aktiviteter og natur, men det bør som minimum sikres, at følgende er omfattet:

1. Risici for uautoriseret adgang til netværk og operationelle systemer
2. Risici for databrud, som kan relateres til uautoriseret adgang til applikationer med kritiske data (fx finansielle transaktioner, personoplysninger etc.)
3. Risici for tab af data eller manglende mulighed for at få adgang til data
4. Risici for nedbrud af forretningskritiske systemer
5. Risici som følge af utilstrækkelige eller manglende politikker og procedurer.

I forbindelse med denne vurdering kan revisor også vurdere, om virksomhedens procedure for identificering og vedligeholdelse af væsentlige informationsaktiver er tilstrækkeligt implementeret, herunder at der sker behørig klassificering og prioritering af beskyttelse af disse informationsaktiver, samt at der sker løbende overvågning af, at dette til stadighed er tilstrækkeligt. Et væsentligt element i denne vurdering omfatter den organisatoriske forankring af ansvaret for cybersikkerheds-risici til sikring af, at der er en entydig ansvarsfordeling, at der findes tilstrækkelige kompetencer til at varetage opgaverne, samt at der sker løbende rapportering herpå til ledelsen.

Såfremt virksomheden har været udsat for cybersikkerhedshændelser, bør revisor endvidere sikre sig, at virksomheden har foretaget den nødvendige oprydning efterfølgende – både operationelt og finansielt – samt at der er foretaget en tilstrækkelig root-cause-undersøgelse af hændelsen og implementeret tilstrækkelige sikkerhedsforanstaltninger, til sikring imod at tilsvarende hændelser skal opstå, omfattende såvel et it-sikkerhedsmæssigt som et finansielt perspektiv.

Revisor bør desuden sikre sig, at der er etablerede procedurer til at opdage sikkerhedshændelser (incident management-procedurer), samt at disse procedurer omfatter identificering og prioritering af cybersikkerhedshændelser, hvor der sker behørig og rettidig rapportering af disse hændelser til relevante parter i virksomheden.

Revisor bør herefter foretage en designmæssig vurdering af virksomhedens implementerede sikkerhedsforanstaltninger med henblik på at identificere eventuelle mangler i designet samt identificere relevante nøglekontroller til operationel test af effektivitet, som skal indarbejdes i den samlede revisionsplan.

Opsummering

Cyberrisici er blevet så almindeligt relevant for alle typer og størrelser af virksomheder, at det er blevet en nødvendighed for revisor at foretage en vurdering af virksomhedens cyberrisici og cyberrisikostyring som en del af revisionsplanlægningen.

Revisor bør sikre sig, at virksomheden har en tilstrækkelig og dækkende risikovurdering af cyberrisici og har designet og implementeret de nødvendige kompenserende kontrolforanstaltninger til at afdække de relevante cyberrisici, uagtet om revisor har sin primære fokus på årsregnskabet eller på de operationelle forhold. Revisor må endvidere vurdere, om der er behov for indarbejdelse af konkrete revisionshandlinger i revisionsplanen for at kunne afdække, om virksomheden har implementeret effektive kontroller til afdækningen af cyberrisici, og om disse har været effektive.

Forstå hvordan en hacker arbejder

Dennis Perto, Cyber Defense Tech Lead, Conscia A/S

Da flere efter årsmødet 2023 har udtrykt interesse for Dennis Pertos 10-punkts liste med anbefalinger, har vi lokket ham til at udgive dem som artikel her i bladet. Vi håber I finder nedenstående relevant og vil bruge det i jeres security audits.
Stine Juhl-Hansen, IT-auditor, Danfoss

Forstå hvordan en hacker opererer

Disse anbefalinger er lessons learned fra et virkeligt Conti ransomware event. Anbefalingerne er ikke komplette, ej heller i prioriteret rækkefølge. Der vil være andre mitigerende kontroller som passer din virksomhed bedre.

Med udgangspunkt i listen, vil jeg personligt starte med de punkter som ikke har noget med teknisk gæld at gøre. Afdæk din virksomheds angrebsflade, find ud af hvor I er sårbare og også hvilke aktører der har interesse, midler og kompetence til at udføre et angreb på jer.

Dernæst en "gratis" øvelse - få synliggjort hvilke sikkerhedsprodukter I har, samt lav en proces for hvem der til hver en tid har ansvaret for at vurdere det væld af sikkerhedsalarmer I dagligt modtager fra selv samme produkter. De fleste virksomheder har rigeligt med teknik implementeret, men det bliver så sjældent brugt i dagligdagen på trods af de store konsekvenser det kan have at blive "hacket".

Når disse to punkter er udført, har I er formidabelt grundlag for at kigge på al den tekniske gæld der er i jeres infrastruktur. Teknikken er ikke installeret forkert i tidernes morgen, men truslerne har udviklet sig siden da, og nu er der brug for en ordentlig gennemgang og opstramning.

Anbefalinger

1. **Mistænksomme logins**
   MFA (Multi Factor Authentication) kan være med til at besværliggøre uautoriseret adgange. Mange benytter i dag sms-koder eller en authenticator app.

2. **Always on VPN**
   Er det nødvendigt at VPN er på hele tiden?
   Er det nødvendigt at der tildeles fuld adgang?
   Benytter vi least privilege princip?

3. **Credential Access**
   Er de systemer vi benytter moderne og opdateret software?

4. **Gamle systemer**
   Er der legacy systemer der er nået end-of-life og ikke længere kan opdateres isoleret på netværket?
   Er antimalware opdateret til at kunne fange de nyeste trusler?

5. **Malware via Excel**
   Man har set angreb udnytte sårbarheder i office pakken. Derfor er det vigtigt at afinstallere unødvendig software. Eks. Hvorfor er der excel på en Domain Controller?

6. **Elevering af rettigheder**
   Husk aldrig at gemme eller videresende password i klar tekst. Eks. Skriv dem ikke i description feltet i Active Directory.
   Husk lange passwords til service accounts og benyt least privilege.

7. **Adgang til virtualiseringshost**
   Det anbefales at adgangen ikke tildeles gennem Active Directory (AD). Hvis AD er kompromitteret, så kan angriberne nemmere ødelægge mere.

8. **Adgang til backup**
   Også her anbefales det ikke at tildele adgang gennem AD. Sørg for at have en kontinuerlig kopi opbevaret Off premise og immutable.

9. **Overvågning af alarmer!**
   Det nytter ikke at have fine alarm systemer hvis der ikke tages action på alarmerne. Det er her det er vigtigt at få justeret strømmen af alarmer der modtages. Hvis der er for mange, så drukner de ansvarlige og vigtig info ang. igangværende angreb vil blive overset.

10. **Afdæk din angrebsflade**
    Det er vigtigt at I ved hvor I er sårbare, og også hvilke aktører der har interesse, midler og kompetence til at udføre et angreb på jer.

Nye medlemmer

Nye medlemmer i IIA fra 11.4.2023 - 14.9.2023

A.P. Møller-Mærsk
Lotte Petersen

Arbejdernes Landsbank
Malthe Kaplan-Christensen
Anne Birgitte Jørgensen

ATP
Jannick Vindahl Madsen
Louise Hedmann Jacobsen

BDO
Christoffer Roldsgaard

Betri Banki
Durita Sjúrðardóttir Wiberg
Terji Skaalum Jacobsen

Carlsberg Breweries
Seng Hoe Lee

Danmarks Nationalbank
Søren Græsborg

Deloitte
Tommy Schormand Johansen
Sabrine Skovgaard Ording
Bryndís Símonardóttir
Tobias Volck Hybholt
Lars Hillebrand

Energistyrelsen
Jesper Alex Jørgensen

Folkekirkens Nødhjælp
Nancy Zhang

Forsvarsministeriets Interne Revision
Lone Elisabet Holm
Beinta Lund
Marius Stremilowski

Hempel
Yulin Zhao

Jyske Bank
Marie Juhl Hansen
Stephanie Hartje Krüger
Alexander Vonebjerg-Grundholm

Københavns Kommune
Pernille Bay

Landbrugsstyrelsen
Morten Heinrichsen
Eric Van Leenen
Clara Nyegaard-Signori
Ivan Léon Sihr
Kim Bonde Jensen
Peter Bonne Rasmussen

Lån & Spar Bank
Kasper Arvé Jensen

Nets
Falentin Eliaz Valentino Jørgensen

Novo Nordisk
Yousef Al-Sadi
Emil Borup
Thomas Guerrero
Christopher Wang
Diana Feodotov

Nykredit
Zayn Awan

PwC
Natascha Krebs Hartvich

Rigspolitiet
Fadia Hermanstad
Kim Størup

Ringkjøbing Landbobank
Frederikke Skov Tagmose

Saxo Bank
Anna Simonova

Skatteministeriet
Annette Kirstine Skov Pedersen

Sparekassen Kronjylland
Stephanie Drægert

Sparekassen Sjælland-Fyn
Gustav Frederik Pedersen

Skandinaviska Enskilda Banken
Kristina Balandienė

Solar
Julie Børgesen Hansen

Sydbank
Jørgen Bak

Sønderjysk Forsikring
Dennis Kjerside Mariager

Tryg
Simon Stegmann Quvang

UNOPS
Odette Fuentes Urrutia

Ørsted Services
Zsuzsanna Kugler
Charlotte Bonvarlet

”Bagsmækken”

Foreningens adresse

Foreningen af Interne Revisorer (IIA Denmark)
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, CIA, Nordea GIA - Nordea Finance
☎ 31 18 38 01 ✉ heino.hansen@nordea.com

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.

Kommende kurser mv.

02.10.2023: CIA Part 1 Virtual Training - Day 1,2,3 and 4
03.10.2023: Kursus for pengeinstitut og realkreditrevisorer
06.11.2023: Kursus for forsikringsrevisorer
23.11.2023: Mød en Intern Revision
09.04.2024: Temadag for den finansielle sektor
11.6-12.6.24: IIA Årsmøde 2024

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

Formand
Direktør, CIA
Morten Bendtsen
Alm. Brand Group
☎ 35 47 47 47 ✉ abmobn@almbrand.dk

Næstformand
Koncernrevisionschef
Christoffer Max Jensen
Arbejdernes Landsbank
☎ 21 12 52 41 ✉ cmj@al-bank.dk

Kasserer
Revisionschef
Per G Ventzel
ATP
☎ 41 47 30 25 ✉ pevn@atp.dk

Bestyrelsesmedlemmer
Intern Revisionschef
Mette Andersen
Lån & Spar Bank
☎ 33 78 21 66 ✉ meta@lsb.dk

Partner
Kristian Ehrenreich Hansen
Deloitte
☎ 30 93 50 03 ✉ krhansen@deloitte.dk

Audit Director, Senior Vice President
Claus Sonne Linnedal
Danske Bank
☎ 45 12 77 89 ✉ clli@danskebank.dk

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

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

Strategisk Partner, CIA
Tobias Zorde
Nordea
☎ 21 18 54 97 ✉ tobias.zorde@nordea.com

Intern Revisionschef
Lars Maagaard
Nykredit
☎ 21 18 54 97 ✉ lma@nykredit.dk

Finanstilsynet søger revisorer og økonomer med interesse for bæredygtighed

Vil du være med til at sikre en høj kvalitet af forsikringsselskabers og pensionskassers bæredygtighedsoplysninger? Vi har to ledige stillinger i vores kontor for Reassurance og Skadesforsikring, hvor du kommer til at bidrage til en bæredygtig økonomisk udvikling i EU

Området for bæredygtighedsregulering er i rivende udvikling. Vi er i fuld gang med at implementere bæredygtighedsreglerne fra EU´s Corporate Sustainability Reporting Directive (CSRD). De nye regler stiller høje krav til forsikringsselskabernes og pensionskassernes rapportering om bæredygtighed. De nye regler skal bidrage til, at pengestrømmene i EU kanaliseres derhen, hvor de giver den mest bæredygtige økonomiske udvikling. Baggrunden for reglerne er bl.a. et mål om klimaneutralitet i EU i senest 2050.

Jobbet
Du skal føre tilsyn med de helt nye regler for forsikringsselskabers og pensionskassers bæredygtighedsoplysninger i deres årsrapporter. Du vil arbejde sammen med kollegaer, som har lavet implementeringen af bæredygtighedsdirektivet i de danske regler. Du vil naturligt få en rolle i forhold til tilsynet med den øvrige del af selskabernes årsrapporter og i arbejdet med regnskabs- og revisionsreglerne, herunder reglerne for den interne revision i finansielle virksomheder.

Vi arbejder også for at sikre samfundets tillid til skadesforsikringsselskaberne bl.a. ved at vurdere, om skadesforsikringsselskabernes forretningsmodeller er holdbare. Dette arbejde bliver du også en del af. Vores ambition er, at vi opdager eventuelle faresignaler så tidligt som muligt, så vi i samarbejde med selskabet kan finde den rigtige løsning for at sikre kunderne. Du vil også komme med på virksomhedsbesøg hos selskaberne, hvor vi i dialog med de ledende medarbejdere undersøger, om selskabernes forretningsmodel fortsat lever op til lovens krav. Du får også mulighed for at deltage i internationale arbejdsgrupper.

I løbet af de første 14 dage hos os gennemgår du sammen med andre nystartede en introduktion til Finanstilsynet, ligesom du får en bred introduktion til opgaverne i vores kontor. Herefter får du opgaverne i stigende sværhedsgrad, i takt med at du kan løfte dem.

Om dig
Du skal være cand.merc.aud, cand.merc.fir, cand. scient.pol, can.merc.oecon, cand. oecon, cand.polit eller have anden relevant samfundsøkonomisk uddannelse og have lyst til at arbejde med de nye regler for bæredygtighedsrapportering og lære om selskabernes forskellige forretningsmodeller og de risici, der er forbundet med dem.

Du bliver motiveret af at kunne få indflydelse på vigtige samfundsopgaver og har en åben og positiv tilgang til forskelligartede opgaver indenfor dit felt. Det er afgørende, at du har gode samarbejdsevner, da vi sjældent løser opgaverne alene. Det er en fordel, hvis du har relevant erfaring fra f.eks. revisions- eller regnskabsarbejde, fra ESG-området, fra den finansielle eller offentlige sektor. Når vi er på virksomhedsbesøg i selskaberne, har hele holdet ansvar for inspektionen, så det gør ikke noget, hvis du også har lyst til at påtage dig rollen som inspektionsleder et par år efter din ansættelse.

Hvis du kan se dig selv i ovenstående, så vil vi meget gerne høre fra dig.

Finanstilsynet
Hvis du bliver vores nye kollega, så bliver du en del af Finanstilsynets kontor for Reassurance og Skadesforsikring. Vi er 23 kolleger/medarbejdere, som primært er økonomer, jurister, aktuarer og revisorer, der er vant til at sparre med hinanden i et fagligt stærkt miljø.

Kontoret for Reassurance og Skadesforsikring er ansvarligt for at sikre, at skadesforsikringsselskabernes forretningsmodeller er holdbare og lever op til lovens krav. Vi har også ansvaret for revisionsområdet for bank og forsikring, for regnskabsreglerne for forsikring og for certificeringsordningen af statsautoriserede revisorer.

Ansættelsesvilkår
Din ansættelse sker efter gældende overenskomst mellem AC og Finansministeriet. Afhængig af din erfaring og kompetencer bliver du ansat som fuldmægtig, special- eller chefkonsulent. Det er en forudsætning for at arbejde i Finanstilsynet, at du kan fremvise en straffeattest.

Som medarbejder i Finanstilsynet har du flekstidsordning, betalt frokostpause, kantineordning, massageordning og renseriordning. Vi har også en række medarbejderforeninger bl.a. funktionel træning, løb, skak og vin.

Spørgsmål?
Har du spørgsmål, er du velkommen til at kontakte kontorchef Birgitta Nielsen på tlf. 61 93 07 27 el. bin@ftnet.dk.

Oplysninger om løn- og ansættelsesvilkår kan du få ved at henvende dig til vores HR Rekrutteringspartner Iben Rolsted Schulin Zeuthen på tlf. 91 33 70 80.

Sådan ansøger du
Send din ansøgning via vores elektroniske ansøgningssystem på finanstilsynet.dk senest søndag den 1. oktober 2023. Husk at uploade dit CV, eksamensbeviser og andre relevante bilag sammen med din ansøgning. Vi tager ikke ansøgninger i betragtning, der er blevet indsendt på anden vis.

Vi opfordrer alle interesserede uanset alder, køn, religion eller etnisk tilhørsforhold til at søge stillingen. Du kan læse mere om Finanstilsynet på www.finanstilsynet.dk – særligt under rubrikken "Karriere". Du kan også finde os på LinkedIn ved at søge på Finanstilsynet Danmark.