INFO

Foreningen af Interne Revisorer
Nummer 88 | December 2024 | 29. årgang

Minitema: Global Internal Audits Standards

Finanstilsynets nye strategi

Læs vores spændende interview med Louise Mogensen, den nye direktør for Finanstilsynet

Assurance mapping

Et værktøj, der illustrerer fuldstændigheden af de kontroller og assuranceaktiviteter, som udføres på tværs af alle væsentlige risikotyper

Vision 2035 ● CIA ● Whistleblowing ● Risk Management

INFOs redaktion

Ansvarshavende redaktør
CIA, CISA
Birgitte Rousing Svenningsen
BDO Statsautoriseret revisionsaktieselskab
☎ 30 65 41 30 ✉ bisve@bdo.dk

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

Senior Internal Audit Manager
Sherko Mesbah
Nordea
☎ 55 46 68 89 ✉ sherko.mesbah@nordea.com

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

Næste nummer
INFO 89 udkommer i april 2025.
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
Pixabay

Redaktionens adresse

Foreningen af Interne Revisorer (IIA Denmark)
Att.: Seniorspecialist Glenn Thunø
Intern revision, Nykredit
Sundkrogsgade 25
2150 Nordhavn

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

Mette Andersen, Bestyrelsesmedlem IIA, Intern revisionschef Lån & Spar Bank, statsautoriseret revisor

Kære Alle

Jeg har glædet mig til at skrive denne leder. Vi har nemlig nogle spændende artikler til jer – også i dette nummer af INFO.

Jul og nytår nærmer sig med hastige skridt, og jeg antager, at der er travlt hos jer, ligesom der er hos mig og mine kollegaer, med at få lukket opgaverne på årets revisionsplan.

Dette årsskifte markerer en stor ændring for os interne revisorer. Det er jo efterhånden ingen overraskelse, men det føles alligevel som om, en epoke er slut, og en ny starter, nu hvor de internationale IIA standarder, som vi har kendt og arbejdet med en hel del år, bliver erstattet af nye standarder til januar. Og januar … det er jo altså lige om lidt. Måske I har det ligesom jeg og tænker: ”har jeg helt styr på ændringerne og, hvad betyder de nye standarder reelt for mig og mine kollegaer” ?

Ud over disse tanker er der for mit eget vedkommende særligt én ting i de nye standarder, som jeg både er meget begejstret for, men som absolut også vil medføre ændringer for både mig, mine kollegaer og for vores chefer i Revisionsudvalget og bestyrelsen. Det drejer sig om kravet om, at der skal udarbejdes en strategi for Intern revision. Vi er en lille revisionsfunktion bestående af 4 medarbejdere inklusiv mig selv. Der har aldrig eksisteret en strategi for Intern revision hos os. Men det kommer der til i 2025. Jeg har allerede været i dialog med formanden for vores bestyrelse og revisionsudvalg og begge synes, at det er en fremragende ide, at vi får udarbejdet en sådan. Jeg glæder mig til at arbejde videre med en sådan strategi. Og heldigvis viste det sig, at det, som jeg finder allermest strategisk vigtigt for vores funktion, også er det, som Revisionsudvalget og bestyrelsen finder vigtigst: At vi er en værdiskabende Intern revision med gode relationer i organisationen. Dette vil blive hjørnestenen vores nye strategi for Intern revision, som vi skal udarbejde lige om lidt.

En status på de nye Global Standards, standardernes krav til en strategi for Intern revision og meget mere om indholdet af de nye standarders domæne IV og V, kan I læse om i dette nummer af INFO. Jeg kan desuden henvise til tidligere udgivelser af INFO fra i år, hvis I gerne vil genopfriske det væsentligste fra de nye standarders domæne I til III.

I denne udgave af INFO er det blandt andet også muligt at læse artikler om 2 medlemmers erfaringer med at blive CIA-certificeret; hvordan en organisation kan udarbejde en assurance-mapping for de 3 forsvarslinjers arbejde samt et par artikler på engelsk omkring ”The Internal Audit Foundation’s Vision 2035 report” og ”Internal Audit’s Role in Risk Management”. Der er desuden nogle artikler af særlig relevans for interne revisorer i den finansielle sektor, herunder et spændende interview med Finanstilsynets direktør Louise Mogensen.

Rigtig god læselyst.

Glædelig jul og godt nytår !

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 2025. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iia.dk.

Prisoverrækkelsen vil ske på IIA's årsmøde i maj/juni 2025. Bedømmelsesudvalget består af Kim Klarskov Jeppesen (CBS) og Birgitte Rousing Svenningsen (BDO).

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

Interview med Louise Mogensen, Finanstilsynet

Af Lars Maagaard og Lars Geisler, Nykredit

I starten af november havde vi fornøjelsen af at interviewe direktør Louise Mogensen, der tiltrådte som direktør for Finanstilsynet i september 2023. Louise Mogensen har således siddet i stolen i lidt mere end et år, og vi var derfor bl.a. nysgerrige på, hvad der havde været hendes primære prioriteter som nytiltrådt direktør. Det blev til en god snak om Finanstilsynet, deres fremtidige strategi og fokusområder, risikobilledet og generelle udviklingstendenser. Endvidere berørte vi også Finanstilsynets stigende fokus på 2nd line funktioner samt tilsynets vurdering af Intern revision som funktion generelt, herunder behovet for opdatering af den gældende revisionsbekendtgørelse.

Som ny direktør er der meget at sætte sig ind i. Finanstilsynet har godt 450 medarbejdere, herunder 23 kontorchefer. Tilsynet har mange opgaver, bl.a. blev der i 2023 behandlet omkring 12.000 sager. En stor driftsopgave, som inkluderer tilladelser og godkendelser. "Det har været et intenst år. Det som har fyldt meget for mig, har været at lære huset at kende. Det er ikke noget, som man lige hurtigt kan overskue". Det er dog trods alt ikke alle 12.000 sager, som Louise Mogensen har været involveret i. Kun de væsentlige.

Ny strategi for Finanstilsynet

Finanstilsynets strategi "*Finanstilsynets strategi 2025*" er fra 2020, og hviler på fire ben: En robust finansiel sektor, En ordentlig finansiel sektor, Et tilsyn og regelsæt, der afspejler samfundets udvikling og Et fagligt og effektivt finanstilsyn. Louise Mogensen kunne afsløre, at hun har prioriteret at udarbejde en ny strategi, som planlægges offentliggjort kort før jul, og løftede sløret for lidt af indholdet:

"En ting, som jeg har prioriteret, er, at lave en ny strategi. Det har vi brugt relativt meget tid på her i år. Det har været en relativ fredelig periode for mig som direktør, hvor der ikke har været store finansielle kriser, bortset fra nogle enkelte sager, som har krævet opmærksomhed for mig. Skal man have en strategi, når man er myndighed og har et fast mandat?

Der er en stor stabilitet omkring vores kerneopgave: om at føre tilsyn og hjælpe til med lovregulering. Vi har også en lovfæstet informationsforpligtelse. Vi skal selvfølgelig fortsat arbejde for en robust og stabil sektor. Det er kommet for at blive. Men der er nogle ting, som er under forandring. Verden står ikke stille. Det gør Finanstilsynet heller ikke. Det gør risiciene eller måden hvorpå, hvordan vi skal håndtere dem, heller ikke. Det er det, som vi prøver at adressere med den nye strategi.

Kapitalmæssigt er den finansielle sektor blevet en mere robust sektor, men i forhold til nogle af de operationelle risici, er vi i stigende grad bekymret. Vi er som tilsyn generelt bekymret, men med den nye strategi vil vi lægge ekstra kræfter i den operationelle robusthed. Altså de ikke-finansielle risici. Der er mange usikkerheder: geopolitiske, handelspolitiske, men selvfølgelig også på it-området. Noget af det kan have finansielle implikationer, men andet ikke, men det kan komme til at stoppe virksomhederne. Styring af de klassiske finansielle risici, som f.eks. kapital- og likviditetsområdet, er mere modent".

Endvidere vil tilsynet have fokus på den komplekse og detaljerede regulering, som har medført, at de finansielle virksomheder står et bedre sted i forhold til finanskrisen. Men reguleringen vurderes også at være blevet meget omfangsrigt og for komplekst, hvilket kan bevirke, at det kan være svært for virksomhederne at være risikobaserede og have fokus på det væsentligste.

"Hele lovkomplekset er virkelig blevet omfangsrigt. Det er svært for virksomheder at have fokus på det væsentligste, og det er svært at føre tilsyn med. Vi skal være risikobaseret og have fokus på det væsentligste, men når der er så meget lovgivning, kan man godt risikere at overse noget. Det er det, som jeg er lidt bekymret for. Det er i tråd med regeringen, som selv har det som målsætning at se nærmere på lovreguleringen. Vi skal være sikker på, at værdiskabelsen står i mål med de byrder, som vi påfører. Det er vigtigt for mig at understrege, at det ikke handler om at lempe eller slække på kravene. Vi taler om forenkling."

Det er en dagsorden, som Finanstilsynet også vil forfølge internationalt, og det vurderes, at det er et godt tidspunkt at påvirke denne dagsorden set i lyset af udmeldinger fra den nye EU-kommission, samt den øgede fokus

på Europas fremtid og konkurrencekraft generelt, hvor der bl.a. er rejst nogle flag i Mario Draghis rapport. Louise Mogensen erkender dog, at det bliver meget svært, for der er rigtig meget EU-regulering, og langt hovedparten af reguleringen i den finansielle sektor er fastsat af EU. Tilsynet vil også være optaget af forenkling af den nationale regulering.

"Vi vil i virkeligheden gerne gøre det nemt for virksomhederne at gøre det rigtigt."

Den teknologiske udvikling med bl.a. anvendelse af Gen-AI er også omfattet af Finanstilsynets nye strategi. Finanstilsynet står i bund og grund i samme situation, som vi som intern revisionsfunktion står over for: At kunne forstå den måde, som virksomhederne anvender teknologien på og hvilke nye risici, som det indebærer.

"I den nye AI-Act er der valgt nogle områder ud, som er vurderet som særligt kritiske: det er inden for livsforsikring og kreditgivning. Så hvis virksomhederne anvender AI på de forretningsområder, så har vi er særlig tilsynsopgave. Men det er virksomhederne ikke begyndt på endnu. Det er mere på lidt ufarlige områder, men det kan komme. Og derfor er det selvfølgelig noget, som vi skal være opmærksom på. Vi forventer, at virksomhederne forstår risici ved anvendelsen heraf, og vi skal kunne føre tilsyn med det."

Finanstilsynet vil også se på, hvordan den ny teknologi kan anvendes til at forbedre egne processer.

"Det er ikke noget nyt, at vi ønsker at blive bedre til at kunne drive databaseret tilsyn. Det vil vi fortsat være optaget af: Hvad kan vi gøre for at være endnu mere målrettet? Vi vil være rigtig gode til vores stikprøver. AI kan hjælpe med at gøre det endnu mere målrettet. Det vil gøre det lettere for hovedparten af virksomhederne, som gør det rigtige."

Der er også et mål for Finanstilsynet at forbedre kommunikation og indgå i dialog med virksomheder og andre interessenter.

"I forbindelse med en inspektion må man gerne udfordre tilsynet. Nogle gange er vi ikke klar over, hvor meget vi egentlig beder om. Ved en dialog kan man snakke sig tilrette og måske finde en anden løsning. Jeg opfordrer derfor til dialog, og man får snakket sammen. Man risikerer, at der bliver leveret så meget, at man mister overblikket. I en presset hverdag tænker man måske: vi sender bare det hele. Vi har ikke som mål at overraske nogen. Vi vil prøve at arbejde på en mere åben måde omkring hvordan vi tilretter tilsynet på."

Generelle udviklingstendenser

I forhold til generelle udviklingstendenser for finansielle virksomheder kommer Louise Mogensen tilbage til fokus på de ikke-finansielle risici, særligt i forhold til de stigende krav i håndteringen af it-risici.

"Opgraderingen af lovkrav for IT-sikkerhed har flyttet sig meget. Nu skal vi til at føre tilsyn efter DORA, som træder i kraft pr. 17. januar 2025. Det er EU's svar på den trussel, som vi står over for. Det bliver en kæmpe opgave at skulle føre tilsyn efter det. Det afspejler den risiko, der er. Vi har nok klassisk tænkt, at det kun var trusler, som kom udefra. Der er en større bevidsthed om, at der også er en risiko med medarbejdere. Der kan også være trusler indefra. Når vi tester robustheden, så er det udgangspunktet, at trusler kan komme alle steder fra. I den relation er det ikke så vigtigt, hvordan systemerne bliver lagt ned. Mere hvad man så vil gøre, når der indtræffer en hændelse. Det fylder meget. Vi har hidtil af gode grunde haft fokus på den klassiske finansielle robusthed, det kommer vi også fortsat til at have fokus på, men der vil være en opgradering med it-sikkerheds tilsyn fremover."

Disse risici vil givet kræve nogle andre kompetencer hos både virksomhederne og Finanstilsynet, hvilket Louise Mogensen er enig i, som også kommer ind på udfordringen med rekruttering generelt:

"Det er rigtigt. Der er brug for medarbejdere med nye kompetencer. Der vil være en naturlig opbygningsperiode. Det er svært at tiltrække medarbejdere. Alle kæmper om de samme kompetencer. Vi kan ikke tilbyde den højeste løn. Vi kan tilbyde et meget stort ansvar. Vi kan tilbyde et tværgående sektorkendskab. Og et stort purpose om at gøre noget godt for samfundet. Det er den palette, som vi arbejder inden for. Vi har en stolt og lang tradition for at uddanne medarbejdere til den finansielle sektor. Og det er også en del af robustheden i sektoren. Vi håber, at de husker noget af det, som de har lært herinde. Det sker heldigvis også, at vi får nogle fra sektoren til Finanstilsynet, som søger væk og vil prøve noget andet. Nogle gange synes medarbejderne, at de arbejder med et "smalt" område. Det kan godt være, at de fik en større lønpakke, men har arbejdet med et meget afgrænset område."

2. og 3. forsvarslinjes arbejde

Det opleves, at Finanstilsynet i stigende omfang er begyndt at interessere sig for arbejdet i 2. og 3. forsvarslinje. Til dette siger Louise Mogensen:

"Alle forsvarslinjer udfører et vigtigt arbejde. Vores fokus har i de senere år været på anden forsvarslinje. Det er nyere funktioner. Der har været en opbygningsperiode, en modenhedsproces. Intern revisions rolle har historisk

"Vi vil i virkeligheden gerne gøre det nemt for virksomhederne at gøre det rigtigt."

været forankret i lovgivningen i mange år: Uafhængighed i forhold til, at intern revision refererer til bestyrelsen.

Det har gjort, at Finanstilsynet har haft lidt mere fokus på 2nd line. Vi er ret optaget af, at 2nd line skal kende sin rolle. 3rd line skal være uafhængige. Det er lidt mere udfordrende for 2nd line, at de ikke har samme uafhængighed, som intern revision har. Vi kan se, at der er stor variation på, hvordan man indretter 2nd line funktionerne. Det med at have en vis ensartet tilgang til nogle grundlæggende ting vil være godt. Vi prøver i virkeligheden på at give dem lidt mere power, så tilsynet kan være lidt mere hjælpsomme, hvis der er nogle, som føler sig lidt klemte."

I forhold til intern revision har Finanstilsynet noteret sig, at praksis i mange interne revisionsfunktioner i Danmark har ændret sig fra finansiel revision til hovedvægt på operationel revision.

"Der er jo en rolle, som har forandret sig noget. Det er en vigtig rolle, som vi jo er enormt glade for. I forhold til ekstern revision har intern revision tilegnet sig intern viden, som er forankret i virksomhederne, hvilket er til gavn for direktion og bestyrelse. I hele arbejdet om at opnå en robusthed og en ordentlighed, så er det en vigtig funktion. Jeg kan godt fornemme, at der stadig er en forskel på, hvilken rolle intern revision har. Rollen har forandret sig, og gør det løbende."

Revisionsbekendtgørelsen

Revisionsbekendtgørelsen for finansielle virksomheder har fejret 9 år fødselsdag i sin nuværende form. Sprogbruget i bekendtgørelsen relaterer sig mere til finansiel revision, og afspejler ikke udviklingen i praksis. I forhold til udsigten til en opdatering af bekendtgørelsen inden for de kommende år, siger Louise Mogensen:

"Revisionsbekendtgørelsen skal genlæses igen i forhold til, at verdenen har forandret sig, og måden hvorpå ting fungerer på. Den vil vi også rigtig gerne opdatere, men ud fra et risikobaseret tilsyn og hvor mange ressourcer vi har, så har den 'hængt' lidt. Det bliver nok ikke i 2025. Vi deler opfattelsen af, at bekendtgørelsen er moden til en opdatering. Det kommer. Der er lidt mismatch i forhold til de rammer, som står i bekendtgørelsen, og den måde, som I arbejder på i dag."

Louise Mogensen CV

(fra Finanstilsynets hjemmeside)

Tiltrådt som direktør i Finanstilsynet september 2023

Uddannet cand.polit fra Københavns Universitet

Erhvervserfaring fra den finansielle sektor bl.a.:
Direktør i Forenet Kredit
Vicedirektør i Finans Danmark
Kontorchef i Erhvervsministeriet
Kontorchef i Nationalbanken

Erfaring med læsning af CIA

Trine Møller Ovesen, Senior Internal Audit Manager, GIA, Nordea

Iben Nøhr Nielsen, Senior Audit Manager, GIA, Danske Bank

Intro

Certified Internal Auditor (CIA) er den eneste globalt anerkendte certificering for interne revisorer.

Som beskrevet i artiklen "The Certified Internal Auditor is changing" (INFO 86), vil både pensum og eksamen blive ændret i løbet af 2025 som følge af de nyligt opdaterede IIA standarder.

Der er to måder hvorpå man kan opnå en CIA certificering; Enten ved at bestå den tredelte CIA eksamen eller ved at bestå CIA Challenge Exam, der dog forudsætter Certified Internal Systems Auditor (CISA) certificering.
I denne artikel vil vi gennemgå vores personlige erfaringer ved at bliver CIA certificeret.

Trine Møller Ovesen, Senior Internal Audit Manager, GIA, Nordea

Jeg tog den traditionelle tredelte CIA eksamen, Der er valgfrihed i forhold til hvilken rækkefølge du tager eksamen.

Min motivation for at forfølge en CIA certificering var drevet af følgende to faktorer:

1. En personlig ambition relateret til min forretningsmæssige baggrund forud for min ansættelse i GIA. Jeg ville gerne have et formelt bevis på min teoretiske kunnen i forhold til intern revision.
2. Et strategisk fokus på at øge certificeringsratioen i min afdeling.

Vi arbejder ikke ens, og sådan tænker jeg også det gælder i forhold til at forfølge drømmen om en CIA certificering.

Selv arbejder jeg rigtig godt med en skarp deadline, så inden jeg gik i gang med at læse til hhv. 1., 2., og 3. eksamen, bookede jeg min eksamensdato. Typisk 1-1½ måned frem i tid. Så vidste jeg, hvad jeg havde at arbejde med og kunne dedikere mig selv til en fokuseret indsats i den periode.

På grund af det strategiske fokus betaler GIA i Nordea for bøger, eksamensomkostninger og eksamensforberedende kursus. Jeg benyttede mig derfor af Gleim's CIA eksamensforberedende kursus online og fulgte modulerne stepvis.

Typisk læste jeg de fleste aftener i perioden, når der var ro på "hamsterhjulet". Det var hårdt men tilfredsstillende, hver gang jeg havde gennemført et modul. Forud for hver eksamen var min mand også sød at tage en weekend væk hjemmefra med vores 3 børn, så jeg kunne dedikere mig 110% til eksamenslæsningen. GIA i Nordea betaler også 10 fridage i forbindelse med forberedelsen, hvilket jeg også gjorde brug af.

Min erfaring er, at nogle af de emner der fyldte meget i det eksamensforberedende kursus ikke fyldte tilsvarende meget til eksamen. Derfor vil jeg anbefale at notere sig, hvor meget hvert område vægter og sørge for at selv områder der synes små, får den rette opmærksomhed.

Man siger ofte "it takes a village to raise a child". Tilsvarende vil jeg påstå, at det (næsten) også kræver en landsby at blive CIA certificeret. En meget stor del af indsatsen skal du selvfølgelig lægge selv. Jeg var ret transparent omkring mit forløb, inklusive op- og nedture, og opbakningen fra familie, venner, kolleger osv. mens jeg jagtede CIA certificeringen, var guld værd.

Iben Nøhr Nielsen, Senior Audit Manager, GIA, Danske Bank

Jeg havde faktisk planlagt den traditionelle tredelte eksamen, men da et vindue åbnede for den såkaldte Challenge Exam, blev jeg fristet og efter flere overvejelser blev det denne jeg gik efter.

Fordelene ved en Challenge Exam som jeg ser det:

1. Du kommer hurtigere igennem forløbet.
2. Du skal op til færre eksamener (1 i stedet for 3).
3. Du skal op i et mindre pensum.

Så i det hele taget lyder det jo bare som win-win-win situation, men da jeg skulle op til eksamen, ramte virkeligheden også ift. at du skal op i pensum i 3 bøger og ikke kun op i en bog ad gangen! Selvom IT-delen fra bog 3 er udenfor pensum (anset som dækket af CISA eksamen) til Challenge Exam og selvom antallet af spørgsmål selvfølgelig er reduceret fra hver bog, kan du få spørgsmål inden for alle bøgerne til denne ene eksamen. Så det er et forholdsvist stort pensum.

Jeg blev nødt til at tage nogle fridage op til eksamen, hvor jeg primært læste i bøgerne og tog en hel del noter.

Jeg tror på, at læring holder bedre såfremt man ikke kun læser, men også får det "gennem kroppen" ved at tage håndskrevne noter. Forud for det havde jeg sammen med en kollega fra Litauen fulgt en større læseplan med oplæsning af pensum og gennemgang af tilhørende test spørgsmål. Desværre kom vi begge i problemer med læseplanen, da den travle sæson ramte med årsafslutningen i januar og vi senest skulle til eksamen i februar. Så selvom der umiddelbart er mange wins ved dette approach, er der også nogle andre tidsmæssige begrænsninger, som man skal være opmærksom på mht. tilmelding, afholdelse af eksamen samt evt. re-eksamen.

Jeg nåede også at være med på et af IIA Danmarks forberedelseskurser til blot 300 kr., til den første del af pensum. Desværre kunne de andre kurser ikke passe ind i forhold til de "åbne vinduer" for Challenge Exam for mig. Mit indtryk fra første kursus er dog meget positivt og havde jeg ikke haft tilgangen med Challenge Exam, havde jeg også klart tilmeldt mig de andre forberedelseskurser.

Jeg synes, at jeg havde haft god alsidig forberedelse, men da jeg sad til eksamen, synes jeg alligevel at spørgsmålene var noget anderledes og ikke i den lette ende. Jeg var noget usikker på, om jeg havde bestået efter eksamen og blev ovenud lykkelig, da resultatet var bestået.

At blive CIA certificeret har været et mål for mig i lige så mange år, som jeg har arbejdet indenfor revision (læs: mange). Så at jeg fik godkendt at tage certificeringen og lykkedes med den føles bare virkeligt godt.

I Danmark er CIA ikke noget der giver lønløft, eller så vidt vides ikke påkrævet for visse stillinger, og i Danske Bank bliver vi heller ikke målt på ratioen af certificeringer, så for mig var det udelukkede et personligt udviklingsmål.

Selvom jeg dagene lige op til eksamen fortrød lidt, at jeg tog vejen til at blive CIA gennem Challenge Exam, er jeg i dag glad for det, da jeg måske ellers stadig ville være i gang med at læse op til en eksamen i dag.

Årshjulet for CIA er som nævnt mere restriktivt for Challenge eksamen og ser ud som følger:

- "Application window: April - September
- First Attempt Testing Windows: June, August, November, or February
- Once your application is approved, please note you have 180 days to register, schedule, and sit for the exam."

https://www.theiia.org/en/promotions/certifications/qisa/qisa-cia-challenge-exam/Apply/

Yderligere information om Challenge Exam kan findes her:

https://www.theiia.org/en/promotions/certifications/qisa/qisa-cia-challenge-exam/

Fælles betragtninger

Vi var begge overraskede over, hvor kompliceret ansøgningsprocessen er. Der er adskillige trin i processen for den tredelte CIA, som skal bekræftes fx uddannelse, anbefaling, relevant erhvervserfaring mv. For Challenge Exam er der noget mindre dokumentation der skal indsendes, da CISA-certifikatet dækker dette, dog var processen stadig besværlig, og man skal være meget opmærksom på at ens IIA-profil stemmer helt overens med ens pas i forhold til fornavne og efternavn.

Vi har ingen konkrete opgørelser over vores forberedelsestid, men IIA angiver et vejledende tidsforbrug til den tredelte eksamen på 130 timer fordelt på hhv. 40 + 40 + 50 timer per eksamen, hvilket er vurderet til at ligge markant i underkanten af det reelle tidsforbrug.

https://www.theiia.org/globalassets/site/certifications/certified-internal-auditor/cia-brochure_2024.pdf

For Challenge Exam findes der en anslået forberedelsestid på 1-2 timer 3 til 5 dage om ugen i ca. 2-3 måneder, hvilket jo er meget bredt, og den anslåede tid for Challenge Exam ligger nok et sted derimellem.

https://ipasstheciaexam.com/cia-exam-difficulty/

Afslutning

Da det ikke var muligt for os at få et billede sammen til brug for artiklen, har vi i stedet fået AI (Shutterstock) til at genere et billede af "os" med vores eksamensbeviser. Og ja, man vil måske ikke helt kunne genkende os på baggrund af det AI genererede billede, men til gengæld pynter det.

I øvrigt får du ikke et fysisk certifikat tilsendt mere: Efter bestået eksamener får du en e-mail der beskriver hvordan du kan købe det og få det indrammet, men det er pænt dyrt. Du kan dog printe det gratis i CCMS og som bevis på dine anstrengelser og din præstation, kan du også få et gratis "emblem" til din LinkedIn profil.


IIA Årsmøde 2025
21.5-22.5.2025
Cornwell
H.C. ANDERSEN
ODENSE
Sæt allerede nu kryds i kalenderen

Minitema:
Global Internal Audit Standards

De nye Global IIA Standarder, som vores moderorganisation offentliggjorde i januar i år, er gældende fra januar 2025.

Hvad betyder det for dig?

Læs om:

- **Status på standarderne**
- **Domain IV – Styring af intern revision betyder også, at vi skal have en strategi for vores funktion**
- **Domain V – Fokus på ledelsessystemet, risikostyring og kontrolprocesserne gennem hele processen for de enkelte revisionsopgaver**

God læselyst

Status på Global Standards

Bestyrelsesmedlem i IIA, Birgitte Rousing Svenningsen, BDO Internal Audit Services, CIA, CISA

Indledning

IIA Global offentliggjorde i januar 2024 de nye standarder for intern revision, som er gældende fra 9. januar 2025.

Formålet med opdateringen af standarderne har været at forbedre strukturen på standarderne og gøre dem mere tidsaktuelle. Formålet har således ikke været at ændre drastisk på god skik inden for intern revision.

I INFO 86 gennemgik jeg de væsentligste ændringer i domain III. Dette blev efterfulgt af, at jeg i INFO 87 gennemgik de væsentligste ændringer i domain I og II. I dette nummer af INFO slutter jeg af med en gennemgang af de væsentligste ændringer i domain IV og V.

Ud over artiklerne har IIA Global også offentliggjort en række dokumenter, videoer og webinars, som kan hjælpe den enkelte med at få et overblik over bestemmelserne i de nye IIA-standarder.

Topical Requirements

Et af de nye tiltag i forbindelse med de nye IIA standarder, er emnespecifikke standarder – de såkaldte "Topical Requirements".

Den første, som vedrører Cyber Security, blev udsendt i høring i april 2024. Høringsfristen var 3. juli 2024. Vi har siden gået og ventet på den endelige udgave. IIA Global har udsat udgivelse flere gange senest til første kvartal 2025, så vi må vente lidt endnu.

Undervejs har der også været forskellige udmeldinger om, hvilke andre emner der vil blive udarbejdet emnespecifikke standarder for.

Det seneste nye herom er, at der på IIA Globals hjemmeside står, at der i 2025 forventes at blive udsendt emnespecifikke standarder i høring for:

- Tredje parts risici
- Kultur
- Business Resiliency.

Dette kan selvfølgelig ændre sig mange gange endnu, men jeg kan kun opfordre alle til at holde lidt øje med IIA Globals hjemmeside, idet disse emnespecifikke standarder er obligatoriske at følge, hvis man vil slå sig op som en intern revisionsafdeling, der følger best practice.

Domain IV – Styring af intern revision betyder også, at vi skal have en strategi for vores funktion

Bestyrelsesmedlem i IIA, Birgitte Rousing Svenningsen, BDO Internal Audit Services, CIA, CISA

Indledning

Domain IV i de nye IIA-standarder omhandler den "interne" ledelse af revisionsafdelingen. Dette skal ikke forveksles med domain III, som omhandler ledelse og styring af den interne revisionsafdeling i forhold til samarbejdet med bestyrelsen, revisionsudvalget og direktionen.

Principle 9 – Plan Strategically
The CAE plans strategically to position the internal audit function to fulfill its mandate and achieve long-term success.

Principle 10 – Manage Resources
The CAE manages resources to implement the internal audit function's strategy and achieve its plan and mandate.

Principle 11 – Communicate Effectively
The CAE guides the internal audit function to communicate effectively with its stakeholders.

Principle 12 – Enhance Quality
The CAE is responsible for the internal audit function's conformance with the Global Internal Audit Standards and continuous performance improvement.

Jeg vil i denne artikel gennemgå nogle af de centrale regler i domain IV herunder beskrive de væsentligste ændringer i forhold til de nuværende IPPF-er.

Den mest markante ændring i forhold til tidligere er, at der stilles krav om, at den interne revision udarbejder en strategi. Det er uddybet nedenfor.

Princip 9

Princip 9 indeholder regler om strategisk planlægning, og princippet er opdelt i 5 underprincipper:

1. Forståelse af virksomhedens ledelsessystem, risikostyring og interne kontroller
2. Udarbejdelse af strategi for intern revision

3. Udarbejdelse af revisionsmetodik
4. Udarbejdelse af revisionsplan
5. Koordination med andre assuranceleverandører.

Forståelse af virksomheden
Kravet om forståelse af virksomhedens ledelsessystem, risikostyring og interne kontroller er ikke et nyt krav. Der stod for eksempel tidligere i IPPF 2010-2, at revisionschefen skulle opnå en forståelse af virksomhedens strategi, mål, tilknyttede risici og risikostyringsproces. Man skal dog være opmærksom på, at der vedrørende virksomhedens ledelsessystem står, at revisor skal overveje, hvordan virksomheden:

- Fastsætter strategisk mål og træffer strategiske og operationelle beslutninger
- Fører tilsyn med risikostyring og kontroller
- Fremmer en etisk kultur
- Leverer effektiv præstationsstyring og ansvarlighed
- Strukturerer sine ledelses- og driftsfunktioner
- Kommunikerer risiko- og kontroloplysninger i hele organisationen
- Koordinerer aktiviteter og kommunikation mellem bestyrelsen, interne og eksterne assuranceleverandører og ledelsen.

Forståelse af virksomhedens ledelsessystem spænder således ud over at få en kopi af virksomhedens organisationsplan. Jeg har specielt bidt mærke i, at revisor skal forholde sig til, hvordan virksomheden fremmer en etisk kultur. Dette fremhæver, at virksomhedens kultur er et vigtigt element og dermed et element, som den interne revisor skal dække med sin planlægning og revisioner.

Strategi for intern revision
Kravet om, at den interne revision skal udarbejde en strategi for revisionsafdelingen, er nyt. Nogle interne revisionsafdelinger har allerede en strategi, men min erfaring er, at hovedparten af de interne revisionsafdelinger i

Danmark ikke har en strategi. Nogle har en revisionsstrategi, som beskriver strategien og målene for revisionen, men ikke strategien for den interne revisionsafdeling.

Man kan med rette stille spørgsmålet, om hvilken værdi en strategi har, når de fleste revisionsafdelinger nu i mange år har levet uden en strategi, og når vi ved, at vi i Danmark har en del revisionsafdelinger bestående af kun en medarbejder. En af fortalerne for en strategi, er den tidligere præsident for IIA Global Richard Chambers. Når han skriver om værdien af en strategi, refererer han til følgende citat af Yogi Berra: "Hvis du ikke ved, hvor du skal hen, ender du et andet sted". Det, kan man vel kun sige, er kloge ord. Med udgangspunkt heri giver det også mening, at man udarbejder en strategi, selv om man er en én-mands afdeling, idet man via strategien kan afstemme med bestyrelsen, revisionsudvalget, direktionen, ekstern revision og andre interessenter, hvilken retning man skal gå, og hvor man skal hen. En strategi kan således give værdi for alle revisionsafdelinger uanset størrelse.

Det næste spørgsmål er, hvordan man udarbejder en strategi, og hvad strategien skal indeholde. Det vil i nogen grad være afhængigt af den enkelte interne revisionsafdeling, idet strategien skal hænge samme med virksomhedens strategi.

Der er dog også en del vejledning at finde. Her vil jeg fremhæve:

- IIAs vejledning "Developing the Internal Audit Strategic Plan"
- "Blueprint for Developing a Strategic Plan" fra AuditBoard.

IIAs vejledning beskriver processen for udvikling af en strategi. Processen opdeles i syv faser, som vist i **Figur 1** nederst på siden.

Audit Board (dvs. bl.a. Richard Chambers) anbefaler stort set samme proces, hvilket kan ses af **Figur 2** på næste side.

Fælles for begge modeller er, at strategien skal resultere i definition af nogle målbare nøgleinitiativer, som baner vejen for, hvor man vil hen. Alt i alt synes jeg, at der er god vejledning at hente hos IIA og relaterede organisationer, så jeg tænker, at det bare er at komme i gang med tankerne om, hvor din afdeling skal hen.

Revisionsmetodik og revisionsplan
Kravene til revisionsmetodik og revisionsplan er ikke nye. Man skal dog være opmærksom på, at man skal dokumentere, at man overholder kravene, hvilket for eksempel for revisionsmetodik, kan være via dokumentation for løbende opdatering af metodikken og dokumentation for uddannelse af medarbejderne i metodikken. For revisionsplan kan dokumentationen være revisionsplanen i sig selv, men også for eksempel en nedskreven metode for risikovurdering og håndtering af væsentlige ændringer.

Koordination med andre assuranceleverandører
Det sidste underprincip under princip 9 stiller krav om koordination med andre interne og eksterne assuranceleverandører, herunder at den interne revision overvejer at bygge på arbejde udført af de øvrige assuranceleverandører såsom compliance, risikostyring og ekstern revision.
Dette er ikke nyt, og dog! Standarden oplister følgende eksempler på koordinering:

- Afstemme omfang og timing af planlagt arbejde
- Aftale ensartet teknikker, metoder og terminologier
- Give adgang til hinandens (revisions)instrukser og rapporter
- Anvende ledelsens risikostyringsinformationer til fælles risikovurdering
- Oprette et fælles risikoregister og liste af risici
- Kombinere resultater og konklusioner i fælles rapportering.

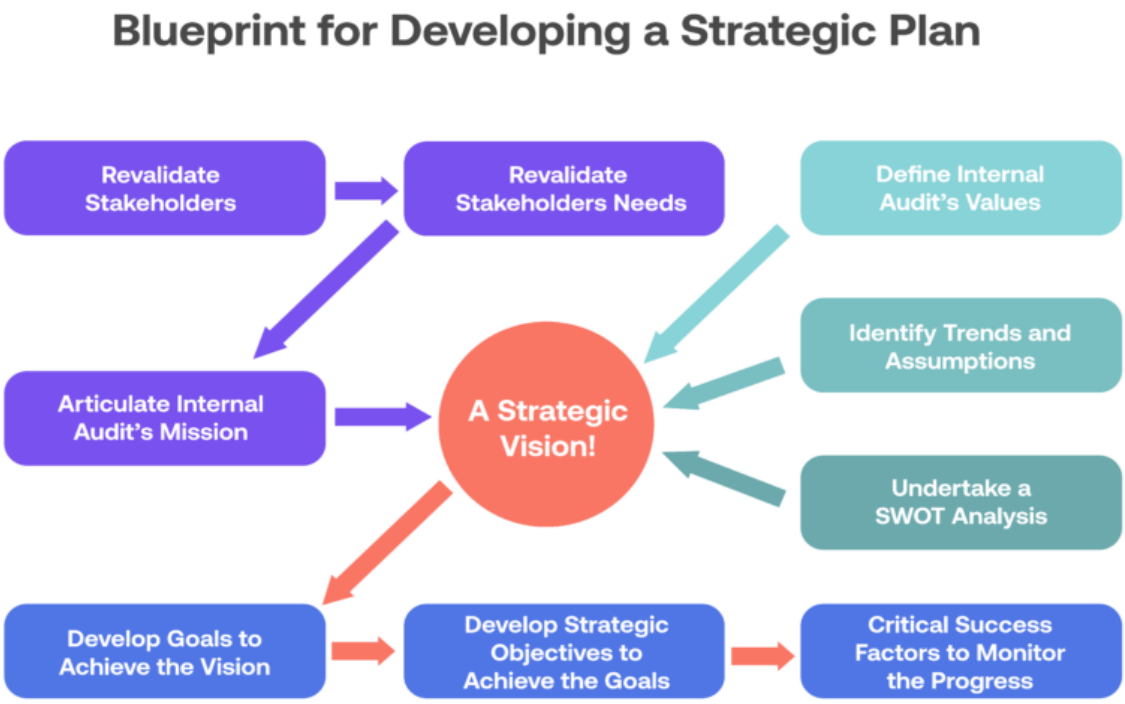
Min erfaring er, at det er forskelligt, hvor meget indsatserne fra de forskellige forsvarslinjer er koordineret. Mange har sikkert et fælles risikoregister og en fælles risikotaksonomi. Men jeg tænker, at det er de færreste, som har en fælles rapportering, og jeg tror også, at flere revisorer har svært ved at sluge den ide, for er det muligt at lave en fælles rapportering og samtidig som intern revision at bevare sin uafhængighed? Jeg forstår bekymringen, men på den anden side tror jeg også, at rapportmodtagerne (dvs. bestyrelsen, revisionsudvalget, direktionen osv.) vil elske at modtage en fælles rapportering. Jeg tror derfor, at det er et af de tiltag, som vi alle skal arbejde med for at sikre, at vi stadig er relevante for vores virksomhed. Det kræver dog, at vi tænker smart og får lavet en rapporteringsproces og -skabelon, som gør, at vores uafhængighed ikke kompromitteres.

Princip 10

Princip 10 vedrører styring af ressourcer. Princippet er underopdelt i 3 underprincipper:

Figur 1: IIAs proces for udvikling af en strategi for intern revision

Figur 2: AuditBoards proces for udvikling af en strategi for intern revision



1. Budget
2. Personalestyring
3. Teknologiske ressourcer.

Der er ikke ret meget nyt i disse principper. Der lægges vægt på, at budgettet godkendes af bestyrelsen, hvilket stemmer godt overens med den øgede vægt på samarbejdet med bestyrelsen, revisionsudvalget og direktionen i domain III.

Personalestyring
Princippet "personalestyring" omfatter rekruttering, udvikling og vedligeholdelse af medarbejdere herunder vurdering af, hvilke ressourcer der er behov for. Dette inkluderer også overvejelser, om man udelukkende skal anvende interne ressourcer. Der er en tendens til, at man i Danmark i højere grad end tidligere anvender eksterne konsulenter, som en del af sit team for på den måde at kunne dække specielle ekspertområder eller sikre sig fleksibilitet. Hvis man gør det, skal man være opmærksom på, at man også for disse ressourcer skal kunne dokumentere overholdelse af IIA standardernes krav. Det betyder blandt andet, at revisionschefen skal kunne fremvise en skriftlig kontrakt med leverandøren og CV på de enkelte konsulenter, således at revisionschefen kan dokumentere, at han/hun har vurderet, at konsulenternes kompetencer er tilstrækkelige.

Teknologiske ressourcer
Det sidste underprincip vedrører teknologiske ressourcer. Revisionschefen skal sikre og løbende revurdere, at den interne revisionsafdeling har tilstrækkelige teknologi til at understøtte revisionsprocessen. I tilfælde af, at den interne revision ikke har den nødvendige teknologi til rådighed, skal revisionschefen informere bestyrelsen om, hvilke begrænsninger det giver.

Generelt synes jeg, at det er interessant, at standarderne nævner teknologi, som et særskilt punkt. Der nævnes intet om, at man som revisionschef skal sikre, at medarbejderne har tilstrækkelige kontorfaciliteter såsom lyse lokaler, gode borde og stole. Dette understreger vigtigheden af teknologi, og at interne revisorer ikke kan udføre sin revision uden teknologiske hjælpemidler.

Det er dog op til revisionschefen at vurdere, hvor avancerede disse hjælpemidler skal være. Er det nok med Microsoft Office produkter, eller skal man have AI-værktøjer til rådighed? Det må afhænge af den enkelte revisionsafdelings aktiviteter og kompetencer og er derfor et forhold, som revisionschefen skal analysere og vurdere. Herunder bør revisionschefen vurdere, om revisionsafdelingen har brug for nogle eksterne konsulenter eller oplæring af sine medarbejdere i brugen af værktøjerne, fx dataanalyseværktøjer.

Når det er besluttet, og de nødvendige penge er afsat i budgettet, er det også vigtigt at inddrage virksomhedens IT-afdeling og/eller IT-sikkerhedsafdeling for at sikre, at den af intern revision anvendte teknologi overholder virksomhedens IT sikkerhedsstandarder.

Princip 11

Princip 11 vedrører effektiv kommunikation. Min erfaring er, at konflikter typisk opstår som følge af manglende eller uklar kommunikation, så man kan ikke understrege for meget, hvor vigtigt effektiv kommunikation og dermed princip 11 er. Princippet er opdelt i fem underprincipper vedrørende:

1. Opbygning af samarbejde med interessenter
2. Effektiv kommunikation
3. Kommunikation af resultater
4. Rettelse af fejl og mangler i kommunikationen
5. Rapportering af ledelsens godkendelse af risici.

Overordnet set er det ikke nye principper. Jeg vil dog fremhæve nogle få af kravene.

Regelmæssig, løbende kommunikation med ledelsen

Først og fremmest understreges det, at regelmæssig, løbende kommunikation mellem bestyrelse, topledelse og den interne revisionsafdeling er essentiel, idet det bidrager til en fælles forståelse af virksomhedens risici. Standarderne angiver, at revisionschefen bør indgå i virksomhedens kommunikationskanaler (dvs. fx ledelsesrapportering og mødereferater) for at holde sig ajour med væsentlige udviklinger og planlagte aktiviteter, der kan påvirke virksomhedens mål og risici. Revisionschefen bør også deltage i møder med bestyrelsen og centrale ledelsesudvalg såvel som møder med den øverste ledelse og grupper, der rapporterer direkte til den øverste ledelse.

Min erfaring er, at praksis i Danmark er forskellig på dette område. I nogle virksomheder deltager revisionschefen som observatør i mange møder og modtager hovedparten af virksomhedens ledelsesrapportering. I andre virksomheder er revisionschefens involvering begrænset.

Der er ingen tvivl om, at man som ledelse af en virksomhed får det bedste ud af den interne revision, hvis man har samme opfattelse af virksomhedens risikobillede, hvilke man kun har, hvis revisionschefen har de samme oplysninger om virksomhedens aktiviteter og risici som ledelsen. Derfor bør revisionschefen, som standarderne angiver, deltage i ledelsesmøder og modtage ledelsesrapportering.

Når det er sagt, er der også behov for en balancegang, idet revisionsafdelingerne i Danmark generelt er små, og det er vigtigt, at den interne revision ikke anvender alt sin tid på håndtering af interessenterne og informationsindsamling. Der skal jo også være tid til revision. Konklusionen er altså, at ledelsen bør invitere revisionschefen til alle relevante møder og tilbyde at distribuere alt relevant ledelsesrapportering til revisionschefen, hvorefter revisionschefens opgave er at prioritere på fornuftig vis.

Effektiv kommunikation

Det andet underprincip "effektiv kommunikation" foreskriver, at kommunikationen skal være præcis, objektiv, klar, kortfattet, konstruktiv, fuldstændig og rettidig. Dette er en gengivelse af den tidligere standard 2420-1 og dermed ikke et nyt krav, men en god liste at skrive ind i sin revisionsmetodik, og også have som et punkt i kvalitetssikringen.

Overordnet konklusion

Det tredje krav, som jeg vil fremhæve i forbindelse med princip 11, er kravet om kommunikation af resultater. Her har jeg bidt mærke i to ting:

1. Krav om rapportering af mønstre og trends
2. Skabelon/struktur for rapportering af konklusion på organisationsniveau.

Der er således krav om, at den interne revision ikke udarbejder rapportering vedrørende de enkelte revisionsopgaver. Man skal også vurdere, om der er nogle generelle mønstre eller trends på tværs af revisionerne. Dette kunne for eksempel være, at den samme "root cause" har medvirket til svagheder på flere områder. For eksempel, hvis "root cause" er manglende ledelsesfokus på kontroller.

For så vidt angår konklusion på organisationsniveau, angiver standarderne, at sådanne rapporteringer skal indeholde:

- Resume af anmodningen om konklusionen
- Beskrivelse af kriteriet for konklusion (altså hvad har man målt op mod)
- Omfang og afgrænsning
- Resume af, hvilken information konklusionen bygger på
- Angivelse af, om konklusionen bygger på arbejde udført af andre "assuranceprovidere".

Hvis man er intern revision i en finansiel virksomhed, skal man være opmærksom på, at §29-erklæringen må betragtes som en konklusion på organisationsniveau, og at revisionsprotokollen derfor skal indeholde et afsnit med ovennævnte information for, at man overholder IIA standarderne. Det samme gælder, når interne revision generelt udarbejder perioderapportering, hvor der konkluderes på det overordnet niveau af governance, risikostyring og interne kontroller.

Princip 12

Det sidste princip i domain IV omhandler forbedring af kvaliteten. Princippet er opdelt i tre underprincipper:

1. Intern kvalitetsvurdering
2. Præstationsmåling
3. Overvågning og forbedring af udførelsen af revisionsopgaverne.

Dette princip skal ses i sammenhæng med princip 8 i domain III, som udstikker regler for bestyrelsens overvågning af den interne revision og dermed også indeholder regler om kvalitet og ekstern kvalitetsvurdering.

Princip 12 omhandler det interne arbejde omkring kvalitet. Den helt overordnet bestemmelse er, at revisionsche-

fen er ansvarlig for, at den interne revision overholder IIA Standarderne og løbende forbedrer kvaliteten af arbejdet. Den interne revision skal have en intern kvalitetsvurderingsproces, hvilket næppe er nyt for nogle.

KPI-er
Mere interessant er underprincippet om præstationsmåling, som i stor udstrækning hænger sammen med kravet om en strategi for intern revision jf. princip 9. Revisionschefen skal definere KPI-ere, og de skal hænge sammen med den interne revisions strategi og funktionsbeskrivelse, og skal tage højde for ønsker og forventninger fra bestyrelsen og direktionen.

Nogle danske revisionsafdelinger har allerede KPI-er, mens andre har haft, men er gået fra det. Den helt store udfordring i forhold til KPI-er er, at få defineret nogle målbare og retvisende KPI-er.

Jeg har set både gode og dårlige KPI-er. Der er flere interne revisionsafdelinger, som måler på antallet af lukkede revisionsanbefalinger og filosofien bag det er, at forretningen med glæde følger den interne revisors anbefalinger, hvis anbefalingerne er relevante. Jeg har dog også oplevet dette forhold målt, som andelen af revisionsanbefalinger der ikke er lukket inden for fristen. Altså en KPI, som hed:

$$\frac{\text{Ikke lukkede revisionsanbefalinger inden for fristen}}{\text{Åbenstående revisionsanbefalinger}}$$

Målet var, at andelen var så lille som muligt. Ulempen ved denne KPI er, at tallet bliver forbedret jo flere revisionsanbefalinger, man giver (set fra den interne revision) eller jo flere revisionsanbefalinger, man får (set fra forretningens side).

Idet det er svært at definere KPI-er, ser jeg det som en fordel, at præstationsmåling er kommet med som et krav i standarderne, idet det alt andet lige betyder, at IIA Global udviklinger flere værktøjer til hjælp til udvikling af retvisende KPI-er. Standarden i sig selv bringer den første vejledning, idet den angiver, at KPI-erne for eksempel kunne omfatte:

- De udførte revisioners dækning af intern revisions ansvarsområde
- Andel af revisionsbefalinger der vedrører virksomheders væsentlige mål
- Andel af revisionsanbefalinger og action planer lukket
- Andel af organisationens nøgle risici og kontroller dækket af de udførte revisioner
- Kundetilfredshed
- Andel af planlagte revisioner, som er gennemført
- Balance mellem assurance og rådgivningsopgaver
- Resultatet af ekstern kvalitetsvurdering
- Andel af uddannelsesaktiviteter gennemført i forhold til den interne revisions strategi
- Andel af medarbejdere med en professionel certificering.

Jeg synes, at det er nogle interessant eksempler, men ikke udtømmende. Personligt synes jeg at det kunne være spændende at måle på balancen mellem assurance og rådgivningsopgaver, idet det kunne være grobund for en drøftelse med bestyrelsen/revisionsudvalget om, hvordan denne fordeling bør være. Jeg mangler dog nogle KPI-er, som måler den interne revisions anvendelse af teknologi. Som nævnt ovenfor under princip 10, er det vigtigt, at revisionschefen tager stilling til den interne revisions behov for teknologiske værktøjer, hvorfor jeg også tænker, at en KPI i relation hertil vil være relevant.

Afslutning
Samlet set giver domain IV et samlet overblik over de mange pligter, revisionschefen har for at sikre, at den interne revision er mest effektiv og mest værdiskabende. De fleste krav er ikke nye, men i flere tilfælde indeholder de mere vejledning end tidligere. Nyt er kravet om en strategi for intern revision og kravet om præstationsmåling. IIA Global har allerede udgivet flere værktøjer, som hjælper os på vej til at overholde de nye krav.

Domain V – Fokus på ledelsessystemet, risikostyring og kontrolprocesserne gennem hele processen for de enkelte revisionsopgaver

Birgitte Rousing Svenningsen, bestyrelsesmedlem IIA, BDO Internal Audit Services, CIA, CISA

Indledning

Domain V i de nye IIA-standarder vedrører revisionsprocessen og den egentlige udførelse af revisionsopgaverne. Hvor de fire første domæner mest vedrører revisionschefer, så bør alle interne revisorer sætte sig godt ind i bestemmelserne i domain V.

Overordnet set består domain V af følgende 3 principper:

Principle 13 – Plan Engagements Effectively
Internal auditors plan each engagement using a systematic, disciplined approach.

Principle 14 – Conduct Engagement Work
Internal auditors implement the engagement work program to achieve the engagement objectives.

Principle 15 – Communicate Engagement Results and Monitor Action Plans
Internal auditors communicate the engagement results to the appropriate parties and monitor management's progress toward the implementation of recommendations or action plans.

Som man kan se ud af de tre principper, fastlægger de regler for en traditionel revisionsproces bestående af planlægning, udførelse og rapportering. De tre faser kan jf. standarderne være overlappende.

De tre principper gælder for både assurance- og rådgivningsopgaver (efterfølgende benævnte "revisionsopgaver"). Standarderne er ikke som tidligere opdelt i standarder for assuranceopgaver (nummeret med A) og standarder for rådgivningsopgaver (nummeret med C). I de tilfælde, hvor enkelte standarder ikke er gældende for rådgivningsopgaver, er det for eksempel nævnt, at der ikke er krav om udarbejdelse af en formaliseret risikovurdering for en rådgivningsopgave, hvis det ikke er relevant.

Jeg vil i denne artikel gennemgå nogle af de centrale regler i domain V herunder beskrive de væsentligste ændringer i forhold til de nuværende IPPF-er.

Princip 13

Princip 13, som vedrører planlægning af de enkelte revisionsopgaver, fremhæver, at første trin er at forstå årsagen til, at opgaven er inkluderet i revisionsplanen. Denne forståelse er essentiel for at kunne fokusere på det vigtige i revisionen, dvs. risiciene for revisionsområdet i forhold til virksomhedens strategi og mål.

Princip 13 består af 6 del-principper. Det foreskrives, at den interne revisor skal:

1. Kommunikere effektivt i løbet af hele revisionen
2. Vurdere risiciene relateret til revisionsområdet
3. Fastlægge og dokumentere formål og omfang af revisionsopgaven
4. Identificere kriterier, som kan anvendes som grundlag for revisionen
5. Fastlægge behovet for ressourcer til revisionsopgaven herunder hvilke kompetencer, der er nødvendige
6. Udarbejde en revisionsinstruks for revisionen.

I forhold til de tidligere standarder er det nyt, at standarderne fastsætter regler for løbende kommunikation under revisionsopgaverne. Men processen, som de 6 del-principper foreskriver, er ikke ny. Det nye er mere, at der er lagt vægt på kommunikation og afstemning med den reviderede part, som beskrevet nedenfor.

Afstemning af risikovurdering
Ud over opstart- og afslutningsmøde og løbende kommunikation under revisionen kræver de nye IIA-standarder, at den interne revisor drøfter resultatet af sin risikovurdering for det enkelte revisionsområde med den reviderede part. Formålet med dette er at sikre, at den interne revi-

sor fokuserer på de rette områder under revisionen og derved bliver mest relevant for virksomheden.

Udarbejdelse af risikovurdering
Den interne revisors risikovurdering er grundlæggende og central for den enkelte revisionsopgave. De nye IIA-standarder angiver, at den interne revisor for det enkelte revisionsområde skal indhente pålidelig og relevant information om:

- Virksomhedens strategi, mål og risici
- Risikotolerance
- Risikovurderingen som understøtter revisionsplanen
- Ledelsessystem, risikostyring og kontrolprocesser
- Rammeværktøjer, vejledninger og andre kriterier (som beskrevet nedenfor under "identifikation af kriterier").

Jeg synes, at der specielt er to ting, som er spændende i denne oplistning.

Den første er, at man skal identificere virksomhedens risikotolerance, hvis en sådan er fastlagt. Jeg vil i den forbindelse anbefale, at man starter med at identificere virksomhedens risikoappetit (dvs. den risiko, som virksomheden er villig til at acceptere for at opnå sine mål).

Hvis virksomheden har fastlagt en risikoappetit for revisionsområdet, er næste trin at identificere, om virksomheden tillige har fastlagt en risikotolerance (dvs. den accepterede/maksimalt mulige afvigelse fra risikoappetitten). Min erfaring er, at mange virksomheder ikke har fastlagt sin risikoappetit og risikotolerance, og hvis man har, er det ikke for alle revisionsområder. Hvis risikoappetitten og/eller risikotolerancen mangler, er kommunikation og afstemning af risikoniveauet med virksomhedens ledelse yderst væsentligt.

Det andet område under risikovurdering, som jeg vil fremhæve, er, at den interne revisor skal, som en del af sin risikovurdering, opnå forståelse af ledelsessystemet, risikostyringen og kontrolprocesserne for det enkelte revisionsområde. Her understreges således, at den interne revisors fokus er på ledelsessystemet, risikostyringen og de interne kontroller.

De nye standarder er en kærkommen lejlighed til at tjekke, om man i sin risikovurdering for de enkelte revisionsområder dækker ovennævnte områder. Man kan jo passende indrette sin skabelon for risikovurderingen efter ovennævnte liste.

Fastlæggelse af formål og omfang
I forbindelse med formål og omfang lægger de nye IIA-standarder ligeledes op til mere koordination med den reviderede part end de tidligere standarder, idet det foreskrives, at den interne revisor skal drøfte begrænsninger i at gennemføre det planlagte omfang med den reviderede part.

Det er formuleret således:

> Scope limitations must be discussed with management when identified, with a goal of achieving resolution. Scope limitations are assurance engagement conditions, such as resource constraints or restrictions on access to personnel, facilities, data, and information, that prevent internal auditors from performing the work as expected in the audit work program.

Dette betyder, at den interne revisor skal have defineret en proces for, hvordan afdelingen håndterer forhindringer, såfremt den reviderede part ikke leverer det ønskede materiale eller på anden vis hindrer gennemførelsen af revisionen.

En anden vigtig bestemmelse vedrørende fastsættelse af formål og omfang er, at standarderne kræver fleksibilitet, således at formål og omfang af revisionsopgaven kan justeres løbende under revisionen, hvis der identificeres behov herfor. Et sådant behov kan opstå på baggrund af ny viden, men er som udgangspunkt ikke tiltænkt, som en justering af omfanget udelukkende på baggrund af, at den interne revisor har været langsom, syg eller lignende.

Identifikation af kriterier
Den sidste ting, som jeg vil fremhæve vedrørende planlægningen, er del-princip 4, som angiver, at den interne revisor skal identificere relevante kriterier for revisionsområdet. Kriterierne findes for eksempel i:

- Interne politikker og forretningsgange
- Lovgivning og kontrakter
- Rammeværktøjer og standarder
- Organisatorisk practices
- Forventninger baseret på designet af en kontrol
- Procedurer, som ikke er formaliseret.

Som udgangspunkt fastsættes kriterierne (reglerne) af ledelsen. Den interne revisors opgave er at vurdere, om kriterierne er tilstrækkelige, og om den faktiske tilstand er i overensstemmelse med kriterierne. Såfremt ledelsen ikke har defineret klare og tilstrækkelige kriterier, skal den interne revisor indgå i en dialog og aftale med ledelsen om kriterierne for revisionsområdet, således at der er enighed om kriterierne, før revisionen påbegyndes. Dette er en kærkommen regel, idet det forebygger konflikter i slutningen af revisionen i forbindelse med observationer og anbefalinger. Min erfaring er dog, at den interne revisor ofte springer dette trin over, idet det er tidskrævende.

Princip 14

Princip 14 omhandler udførelsen af revisionsopgaverne og indeholder 6 del-principper. Den interne revisor skal:

1. Indhente information
2. Analysere informationen
3. Evaluere observationer
4. Beslutte om der skal gives anbefalinger

5. Udarbejde en samlet konklusion
6. Dokumentere revisionsopgaven.

Overordnet set er der intet nyt i disse del-principper, men jeg vil dog fremhæve nogle enkelte forhold nedenfor.

Identifikation af "root cause"
I forbindelse med observationer (dvs. forskelle mellem kriterie og faktisk tilstand) foreskriver standarderne, at den interne revisor identificerer "root cause", dvs. den egentlige årsag til den konstaterede svaghed.

Min erfaring er, at de fleste interne revisioner allerede opererer med begrebet "root cause", men det er også min erfaring, at mange interne revisorer ikke får identificeret den korrekte "root cause". Faren i dette er, at man heller ikke får defineret den korrekte revisionsanbefaling/ action plan, hvorfor det konstaterede problem ikke bliver løst.

Der er typisk to faldgruber i forhold til identifikation af "root cause".

Den ene er, at den reelle "root cause" ikke bliver identificeret, fordi den interne revisor ikke har lavet en tilstrækkelig analyse. Jeg har set eksempler på, at den interne revisor har identificeret "root cause", som den umiddelbare årsag til svagheden, men ikke har søgt længere tilbage. Den interne revisor kunne for eksempel have konkluderet, at manglende udførelse af en kontrol skyldes, at kontrollen ikke er formaliseret (dvs. ikke beskrevet i en forretningsgang). I dette tilfælde har den interne revisor konkluderet, at "root cause" er manglende forretningsgang. Dette vil ofte dog ikke være "root cause", fordi kontrollen bliver ikke udført blot, fordi den bliver beskrevet. Den interne revisor bør derfor i sådanne tilfælde undersøge årsagen til den manglende kontrol dybere. Årsagen kunne være manglende ressourcer eller bare generelt en manglende fokus og prioritering af kontroller. Det er derfor mere sandsynligt, at "root cause" i stedet for er manglende ressourcer eller manglende kontrolkultur.

Den anden faldgrube er anvendelse af en drop-down liste. En drop-down liste for "root cause" har den fordel, at det er lettere at lave statistikker og identificere tendenser, men har den ulempe, at listen ikke altid er udtømmende og derfor kan føre til, at den reelle "root cause" ikke bliver identificeret. Man skal derfor være påpasselig med at lave en drop-down liste for "root causes". I hvert fald vil jeg anbefale, at man altid har en "øvrig" kategori, således at en drop-down liste ikke forhindrer, at den korrekt "root cause" bliver identificeret.

Jeg ved godt, at man er under tidspres, når man udarbejder rapportering, og derfor sommetider springer over, hvor gæret er lavest, hvilket er meget naturligt. Jeg vil dog kraftigt anbefale, at man prioriterer at få identificeret de rigtige "root causes", det vil sige, at man allokerer mere tid til rapporteringsfasen, idet der ellers er en risiko for, at man ikke får sat den rigtige forbedring i gang, hvilket kan være yderst omkostningstungt for virksomheden.

Afgivelse af revisionsanbefalinger
Det andet forhold, som jeg vil fremhæve vedrørende princip 14 og del-principperne, er, at der ikke længere er krav om, at den interne revisor afgiver revisionsanbefalinger. Det var et krav i de tidligere standarder. De nye standarder giver tre muligheder:

- Give anbefalinger
- Anmode ledelsen om action planer
- Samarbejde med ledelsen om at udarbejde action planer.

Spørgsmålet om man skal give revisionsanbefalinger eller ej, har været diskuteret i branchen i mange år. Jeg synes derfor, at det er godt, at det nu er blevet frivilligt. Umiddelbart er det lidt af en smagssag.

Argumentet for revisionsanbefalinger er, at det er via anbefalingerne, at den interne revisor giver værdi og medvirker til forbedringer.

Argumentet imod revisionsanbefalinger er, at den interne revisor via revisionsanbefalingerne bliver en del af beslutningsprocessen og som følge heraf mister sin uafhængighed.

Modargumentet for det sidste er, at revisionsanbefalingerne skal være passende generiske. Hertil kan man spørge, om generiske revisionsanbefalinger giver værdi, idet generiske revisionsanbefalinger ofte bliver en omformulering af observationen, som for eksempel: "Forretningsgang X er forældet, idet den ikke er opdateret siden 2005". "Vi anbefaler, at forretningsgang X opdateres".

Min personlige holdning er, at man i stedet for skal fokusere på risikoen ved svagheden og "root cause", og når man har defineret disse, enten anmode ledelsen om action planer eller udarbejde action planer i samarbejde med ledelsen.

Dokumentation af revisionsopgaven
Det sidste forhold, som jeg vil kommentere under princip 14, er reglerne om dokumentation. Reglerne er ikke nye men væsentlige. Der skal foreligge dokumentation af analyser, vurderinger og indsamlede informationer. Dokumentation skal være tilstrækkelig til, at en anden person kan genudføre revisionen og nå til samme konklusion.

Reglen er, som vi kender den. Men den øgede anvendelse af dataanalyse, AI mv. i de interne revisionsafdelinger stiller nye spørgsmål til, hvilken dokumentation der skal opbevares. Hvis man for eksempel anvender dataanalyse, må det antages, at dokumentationen som minimum skal indeholde selve dataanalysen og de underlæggende data. Den bør nok også i visse tilfælde indeholde en verbal beskrivelse af, hvorledes dataene er analyseret. Ved brug af AI kan dokumentationen være endnu sværere, fordi man ikke altid kan dokumentere, hvordan AI-en er kommet frem til sit resultat.

Desuden skal det bemærkes, at der i standarden lægges vægt på, at de enkelte dokumenter såvel som arkiveringen af disse er struktureret og systematisk, hvilket kræver gode skabeloner og arkiveringsregler.

Proces for håndtering af konflikter
Ud over ovennævnte er der for flere af del-principperne implementeret nye regler om, at den interne revision skal have procedurer for håndtering af uoverensstemmelser med den reviderede part.

Det er et vigtigt forhold, idet der selvfølgelig kan opstå konflikter som følge af, at intern revision og den reviderede part kan have forskellig opfattelse af risici og best practice, hvorfor en proces for, hvordan sådanne situationer løses og der opnås en fælles forståelse, er væsentlig.

Princip 15

Det sidste princip omhandler rapporteringsfasen inkl. opfølgning. Princippet er opdelt i 2 del-principper. Disse angiver, at den interne revisor skal:

1. udarbejde en endelig rapportering for revisionsopgaven
2. bekræfte at ledelsen har implementeret revisionsanbefalingerne/action planerne.

Revisionsrapporter
Der er ikke krav om et bestemt format af revisionsrapporteringen. Man kan således anvende både Word og PowerPoint, og strukturen på rapporteringen er ligeledes frivillig. Der er dog krav om, at rapporteringen som minimum indeholder:

- Et afsnit om at den interne revisor har overholdt IIA-standarderne
- Formål, omfang og afgrænsning
- Observationer, væsentligheden af disse og prioritering
- Konklusion, herunder konklusion på effektiviteten af ledelsessystemet, risikostyringen og kontrolprocesserne for revisionsområdet.

Det er min erfaring, at de fleste danske interne revisionsafdelinger allerede inkluderer hovedparten af disse områder. Jeg tror dog, at det er de færreste, som i revisionsrapporterne for de enkelte revisionsopgaver har et afsnit om overholdelse af IIA-standarderne.

Endvidere er det min erfaring, at ikke alle konkluderer på effektiviteten af ledelsessystemet, risikostyringen og kontrolprocesserne for det enkelte revisionsområde. Revisionscheferne bør sikre, at disse forhold tilføjes i revisionsrapporterne fremadrettet.

Opfølgning
Princippet vedrørende opfølgning på revisionsanbefalinger/action planer er ikke nyt. IIA-standarderne kræver, at den interne revisionsafdeling har en defineret proces, som minimum beskriver processen for:

- Forespørgsel om status på implementeringen
- Risikobaseret opfølgning på implementeringen
- Opdatering af status på anbefalingerne.

Det skal bemærkes, at standarderne kræver, at den interne revisor indhenter forklaring fra ledelsen, hvis implementeringen er forsinket, og at den interne revisor informerer den øverste ledelse om forsinkelser.

Afslutning

Samlet set stiller Domain V ikke nogen krav, som er væsentlige forskellige fra kravene i de tidligere standarder. Det er ikke overraskende, idet formålet med ændringen af revisionsstandarderne ikke er at ændre noget i den generelle interne revisionspraksis, men derimod at opdatere standarderne så de bliver tidsaktuelle.

Det, jeg dog vil anbefale, at man lægger mærke til, er, at standarderne er bygget op om det grundlæggende element, at formålet med intern revision er at vurdere effektiviteten af ledelsessystemet, risikostyringen og kontrolprocesserne i relation til det enkelte revisionsområde.

Som jeg ser det, er de nye IIA-standarder en kærkommen lejlighed til, at man gennemgår sin revisionsproces og kigger indad – ikke fordi, jeg mener, at det er afgørende at overholde standarderne. Det er ikke et formål i selv. Man skal kigge indad og reflektere over, om man overholder standarderne for på denne måde at blive endnu bedre, mere effektiv og mere værdiskabende for den virksomhed, man arbejder for.

INFO-redaktion – hvervning

Hvorfor være medlem af redaktionen?

Fra tid til anden sidder du formentlig med faglige spørgsmål om f.eks. nye lovkrav, trends eller ændringer i praksis, som kan være komplekst at tilgå i en travl hverdag. Som en del af redaktionen vil du få mulighed for at få svar på din nysgerrighed, og du er formentlig ikke den eneste interne revisor, som sidder med de spørgsmål.

Hvad kræver det?

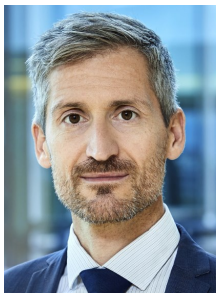
Redaktionen drøfter, hvilke emner som kan være interessante for vores profession, og forsøger herefter at finde relevante forfattere til at skrive artikler. Det er ikke tanken, at redaktionsmedlemmer skal skrive artikler til bladet.

Redaktionsmøder finder sted 3 gange om året og er af typisk 2 timers varighed. Der kræves ikke fysisk tilstedeværelse. Endvidere afholdes statusmøder 3 gange om året af 30-60 min. varighed.

Kom og vær med til at vi som forening fortsat fremover kan udgive vores medlemsblad INFO til gavn for alle dine kollegaer i branchen.

IIA Denmark

Overblik med assurance-mapping



Martin Tripax, Director, Deloitte

Indledning

Det er velkendt, at intern revision har snitflader til kontrolfunktionerne[1] i 2. forsvarslinje, og hvis de ikke håndteres, kan det medføre uhensigtsmæssigheder for organisationen. Det kan være i form af dobbeltarbejde, områder, som ikke bliver dækket af en kontrolfunktion, og en generel dårlig oplevelse for de områder af organisationen, der bliver kontrolleret.

Findes der en 1. forsvarslinje, som udfører kontrolaktiviteter af tilstrækkelig kvalitet, kan kontrolfunktionerne til en vis grad bero på dette arbejde, og der vil så være behov for at håndtere snitfladerne mellem alle tre forsvarslinjer. Det gælder ligeledes i forhold til ekstern revision og eventuelle myndigheder, som udfører grundig kontrol. Dette er særligt udtalt i den finansielle sektor, hvor 1. og 2. forsvarslinje er veludbyggede og udfører omfattende kontrolaktiviteter.

Denne artikel beskriver problemstillingen og kommer med forslag til, hvordan den kan håndteres via såkaldt "assurance-mapping". Med henblik på at sætte dette i perspektiv, vil artiklen adressere den europæiske Digital Operational Resilience Act (DORA), som finansielle virksomheder skal efterleve fra januar 2025, og hvordan assurance-mapping kan hjælpe i den forbindelse. Fordelene er mange, herunder mere effektiv risikostyring og allokering af ressourcer samt overblik over kontrolmiljøets dækning / fuldstændighed.

Artiklen tager udgangspunkt i den finansielle sektor, men det er mit håb, at læsere der arbejder udenfor sektoren, kan få inspiration til at håndtere de nævnte udfordringer i en tid, hvor det ikke kun er den finansielle sektor, som har fokus på at forbedre risikostyring og compliance.

Problemstillingen

De fleste organisationer står overfor et risikolandskab, der udvikler sig løbende og på mange områder er blevet mere komplekst. Årsagerne er mange, herunder en stigende mængde lovkrav, digitalisering og et mediebillede, der øger risikoen for skade på omdømmet. Det medfører, at der bruges flere ressourcer på kontroller og på at sikre, at disse er effektive. Som følge heraf ønsker ledelsen og bestyrelsen i højere grad at blive betrygget i, at alle væsentlige risici bliver håndteret, og dette gøres så omkostningseffektivt som muligt. Det bemærkes i den forbindelse, at risikoen for manglende efterlevelse af lovkrav, altså compliancerisikoen, er en risikotype, som intern revision i den finansielle sektor skal forholde sig til, selvom det er compliancefunktions kerneansvar.

Når der indføres nye kontroller i 1. forsvarslinje, og de eksisterende bliver mere formaliserede, så giver det arbejde til de kontrolfunktioner i 2. og 3. forsvarslinje, som skal overvåge og rapportere på kontrollernes effektivitet. Det kan føre til overlap, f.eks. ved, at man tester de samme kontroller og i forsøget på at undgå dette, kan der være områder, som 2. og 3. forsvarslinje ikke dækker.

Det kan være nødvendigt at teste de samme kontroller og gennemgå de samme områder, da kontrolfunktionernes ansvarsområder overlapper, men i de tilfælde er det vigtigt, at funktionerne er koordineret, så de kontrollerer de samme områder i 1. forsvarslinje på forskellige tidspunkter eller med et forskelligt scope eller ultimativt i en samlet indsats. Tilsvarende hvis der findes flere funktioner i 2. forsvarslinje, så skal de koordinere internt. Sidst men ikke mindst, så kan det være nødvendigt, at 2. og 3. forsvarslinje planlægger deres arbejde i forhold til ekstern revisions arbejde og eventuelle inspektioner udført af myndigheder.

Findes der en moden 1. forsvarslinje, som tester sine kontroller med en grad af funktionsadskillelse, har det betydning for, hvad 2. og 3. forsvarslinje skal kontrollere og hvor dybt. Der er altså tale om prioritering ud fra en residualrisikobetragtning.

De finansielle virksomheder er i fuld gang med at forberede sig til DORA, der stiller krav om bla. et rammeværk for it-risikostyring, kontroller samt klare roller og ansvar, herunder en uafhængig kontrolfunktion. Det vil sige, at funktioner med ansvar for at udføre kontroller i 1. forsvarslinje samt funktioner såsom Chief Information Security Officer (CISO), databeskyttelsesrådgiveren, risikostyringsfunktionen og compliancefunktionen skal koordinere deres arbejde.

Der er derfor overhængende risiko for, at virksomhedernes kontroller og kontrolfunktioner er ukoordinerede og ultimativt ikke kan betrygge ledelsen og bestyrelsen i, at alle væsentlige risici bliver håndteret, og at dette gøres så omkostningseffektivt som muligt. Assurance-mapping, som beskrives nedenfor, er derfor et relevant værktøj, der kan anvendes i forbindelse med implementeringen af DORA og i den løbende efterlevelse af DORA (fra januar 2025 og frem).

Assurance-mapping

Assurance-mapping er et værktøj, der illustrerer fuldstændigheden af de kontroller og assuranceaktiviteter, som udføres på tværs af alle væsentlige risikotyper.

Anvendelsen af assurance mapping

Man kan anvende assurance-mapping proaktivt til at fordele og koordinere opgaver mellem funktionerne, og det

kan anvendes i den løbende overvågning af kontrolmiljøets dækning.

Fordelene ved at anvende assurance-mapping proaktivt er, at organisationen på baggrund af sin risikovurdering, kan beskrive, hvordan det samlede kontrolmiljø på tværs af de tre forsvarslinjer skal sættes op med fokus på omkostningseffektivitet og assurance. I forbindelse med f.eks. implementeringen af DORA, vil det være et værdifuldt værktøj, som derved bliver input til udarbejdelsen af politikker, procedurer, operating models og procestegninger, da assurance-mapping giver et overskueligt overblik over, hvem der skal gøre hvad i den daglige drift.

Fordelene ved at anvende assurance-mapping løbende er, at det:

1) Giver et overskueligt overblik over kontrolmiljøets dækning, som kan anvendes over for direktionen og bestyrelsen.

2) Danner udgangspunkt for forbedringer i kontrolmiljøet med fokus på omkostningseffektivitet, fuldstændighed og effektive kontroller.

3) Bruges i den løbende koordinering af årsplaner og aktiviteter imellem kontrolfunktionerne.

4) Anvendes overfor myndigheder, som udfører tilsyn, f.eks. Finanstilsynet, samt overfor ekstern revision og demonstrerer derved, at organisationen forstår sit samlede kontrolmiljø.

Udformningen af et assurance-map
I det viste eksempel i **Figur 1** herunder, er organisationens risici opdelt i otte forskellige risikotyper på niveau 1, som er blevet vurderet i forhold til deres iboende risiko. På skalaen Ingen, Lav, Middel eller Høj (herefter I, L, M eller H), er det angivet i hvilken grad kontroller og assuranceaktiviteter dækker de otte risikotyper set på tværs af organisationen. I parentes er angivet den ønskede dækning på de områder, hvor dækningen ikke er god nok. Det er bevidst, at der ikke anvendes farverne grøn, gul og rød, da de indikerer, at noget er godt og noget ikke er godt. Pointen med L, M og H er, at organisationen skal forholde sig til, om man ønsker L, M eller H på det pågældende område. Bogstavet I vil altid kræve en forbedring, da området ellers skal farves sort, hvilket indikerer at ingen aktiviteter er påkrævet.

I praksis vil man som oftest bryde risikotyperne ned i niveau 2, og bryde organisationen yderligere op og derved opnå et mere granulært assurance-map. Med niveau 2 henvises der til organisationens risikotaksonomi, som uddybes senere i artiklen.

Organisationen skal have defineret kriterier for, hvad der er henholdsvis L, M og H for at kunne arbejde med et assurance-map. Senere i denne artikel vil forudsætningerne for at kunne arbejde med assurance-mapping bliver udfoldet.

It- og sikkerhedsrisiko som et eksempel
I ovenstående assurance-map er farverne dog ikke helt tilfældigt placeret for så vidt angår risikotypen "it- og sikkerhed". Farverne her er tænkt til at illustrere, hvordan det kan se ud, når en organisation skal håndtere risici relateret til digital operationel resiliens og samtidig håndtere de compliancerisici, som er et resultat af DORA (DORA vedrører digital operationel resiliens).

Farverne indikerer, at hele organisationen, bortset fra finans og compliancefunktionen, skal forbedre deres dæk-

Figur 1: Eksempel på et assurance-map

Riskotype – Niveau 1	Iboende risiko	1. Forsvarslinje						2. Forsvarslinje		3. Forsvarslinje	4. Forsvarslinje
		Forretning I	Forretning II	Forretning III	Drift	IT	Finans	Risikostyring	Compliance	Intern revision	Ekstern revision
Strategisk	4	M	M	M	L	L	M	M		M	
Bæredygtighed	3	I (M)	L (M)	I (M)			L (H)	L		H	L
Operationel	5	H	M (H)	H	H	M	H	M		M	L
Compliance	5	M (H)	H	M (H)	M	M	H	L	M (H)	M	L
It- og sikkerhed	5	I (L)	I (L)	I (L)	M (H)	M (H)		I (H)		L (H)	L
Data	5	L	L	I (L)	M	M	H	M		L (M)	
Finansiel kriminalitet	3	I (L)	I (L)	L	L	L		L	M	L	
Adfærd	4	M (H)	M (H)	H	M	M	L	L	H	M	

I Ingen dækning | L Lav dækning | M Middel dækning | H Høj dækning | Ikke relevant | Parentes: Angiver ønsket dækning

Note: Dette assurance-map er lavet til illustration, hvorfor farverne er tilfældigt placeret.

ning af risikotypen "it- og sikkerhed". Ikke på grund af DORA, men på grund af den stigende iboende risiko fra f.eks. cyber-angreb. Compliancefunktionen skal ikke dække den risikotype, da funktionen skal dække DORA som en del af risikotypen "compliance". Det kan virke banalt for en intern revisor, men det er min erfaring, at mange af vores stakeholders i 1. og 2. forsvarslinje har svært ved at forstå forskellen på de to risikotyper, der jo i denne kontekst begge relaterer sig digital operationel resiliens. Assurance-mapping er et af værktøjerne, som man kan bruge til at opnå fælles forståelse mellem forsvarslinjerne og med fælles forståelse, er der grundlag for koordinering og assurance.

Sidst men ikke mindst, så kan man udlede af det viste assurance-map, at intern revision skal øge sin dækning af risikotypen "it– og sikkerhed" i en fart, da den ikke kan bero på risikostyringsfunktionen eller 1. forsvarslinje. Tilsvarende kan intern revision justere sin dækning ned, når disse har opnået en tilstrækkelig dækning af risikoen.

Forudsætninger for at anvende assurance-mapping

Alle organisationer af en vis størrelse kan på ad-hoc basis arbejde med assurance-mapping som et værktøj til at opnå forståelse mellem kontrolfunktionerne og koordinere deres aktiviteter. Det er min erfaring, at man kan opnå stor værdi, hvis man har et whiteboard og de rigtige folk i et lokale i 3-4 timer.

Skal man derimod arbejde med assurance-mapping løbende og have fuld værdi, så kræver det en struktureret tilgang og nogle forudsætninger, som skal være opfyldt:

1) Ansvarsfordelingen mellem forsvarslinjerne
Roller og ansvar mellem de tre forsvarslinjer skal være anerkendt på tværs af organisationen, da det ellers vil være umuligt at blive enige om den ønskede kontroldækning på et givet område. Ønsket kontroldækning er illustrereret i parentes i ovenstående assurance-map.

2) Kategorisering af risici
Organisationen skal have en risikotaksonomi, altså en kategorisering af sine risici på niveau 1, som herefter er brudt op på niveau 2 og eventuelt også niveau 3. Taksonomien skal afspejle organisationens iboende risikoprofil, og den skal være accepteret på tværs af organisationen.

3) Forståelse af væsentlige risici
Risikotaksonomien kan ikke stå alene, og organisationen skal derfor have en forståelse for sine væsentligste risici, og disse skal være kategoriseret ved hjælp af taksonomien.

4) Forståelse af kontroller og vurdering af disse
Der skal være en fælles forståelse for, hvad der er en kontrol og hvordan man vurderer effektiviteten af en kontrol og effektiviteten af det samlede kontrolmiljø.

5) Vurdering af kontrollernes dækning
For at kunne vurdere kontrollernes dækning, skal organisationen have defineret kriterier for, hvad der er henholdsvis Lav, Medium og Høj dækning. Det er min erfaring, at graden af dækning ikke kan kvantificeres, hvorfor selve vurderingen vil bero på en kvalitativ tilgang.

6) Løbende opdatering af et assurance-map
Det er ressourcekrævende at opbygge et assurance-map, og værdien ligger i høj grad i den løbende opdatering, så det bliver et værktøj til ledelse og styring. Opdateringen er ikke specielt ressourcekrævende, men det er vigtigt, at der afsættes tid til det. Ligeledes er det vigtigt, at et assurance-map har en ejer, der er "accountable" for opdateringen. Om ejeren er i 1., 2. eller 3. forsvarslinje er for mig at se uden betydning, så længe alle tre forsvarslinjer er enige om, at de er "responsible" for at holde det opdateret. Ansvarsfordelingen kan med fordel forankres i en politik, der er bestyrelsesgodkendt.

Sammenfatning

IIA har i 2018 skrevet en Practice Guide om assurance-mapping, og værktøjet er således ikke nyt. Mig bekendt er der ikke mange organisationer i Danmark, som anvender værktøjet løbende, og det skyldes måske, at de ovennævnte forudsætninger ikke har været på plads.

Efterhånden som risikostyring og compliance bliver formaliseret og dokumenteret i større danske organisationer, så mener jeg, at assurance-mapping bør overvejes. Det er tidskrævende, og forudsætningerne skal være opfyldt, men selvom de ikke er helt opfyldt, så kan det alligevel give mening at gå i gang. Arbejdet med udarbejdelse af assurance-mapping er nemlig en givtig proces, som kan fremme en fælles forståelse på tværs af organisationen og sikre, at de sidste forudsætninger kommer på plads.

Proaktiv anvendelse af assurance-mapping i forbindelse med implementering af lovkrav eller andre store projekter, stiller ikke de store krav om modenhed, og det vil ligeledes være en givtig proces, som i sig selv kan fremme modenheden.

Intern revision kan med fordel anvende metoden fra assurance-mapping ved revision af større projekter, f.eks. organisationens implementering af lovgivning. For så vidt angår DORA er det nok for sent at være proaktiv, men det er ikke for sent i forhold til f.eks. AI-Forordningen. Intern revisions rolle kunne i den forbindelse være at forholde sig proaktivt til kontrolmiljøets fremtidige dækning og foreslå assurance-mapping, som et værktøj 1. forsvarslinje kan tage i anvendelse i forbindelse med udarbejdelsen af f.eks. politikker, procedurer, operating models og procestegninger.

Noter

[1] I denne artikel anvendes "kontrolfunktioner" som en samlebetegnelse for intern revision og funktionerne i 2. forsvarslinje.

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.

www.InternalAuditor.org

www.theiia.org

The Institute of Internal Auditors

Elevating Impact

Whistleblowerordning set i et praktisk perspektiv

Christel Breum, Head of Group Compliance, Tryg Forsikring A/S

Mette Rubæk Christensen, Senior Compliance Officer, Cand.jur., Tryg Forsikring A/S

Indledning

De seneste år har whistleblowing været et fokus hos lovgiverne og i virksomheder, som har skulle implementere de nye regler. Flere større virksomheder har oplevet en stigning[1] i antallet af indberetninger, men også i medierne, har whistleblowersager trukket overskrifter om eksempelvis hvidvask.

De nye regler om whistleblowing trådte i kraft i Danmark den 17. december 2021, og formålet bag den nye regulering var at styrke håndhævelsen af EU-retten ved fastsættelse af minimumsregler, der skal sikre et højt niveau af beskyttelse af whistlebloweren.

I denne artikel ønsker vi at sætte fokus på de overvejelser og udfordringer, der kan være forbundet med, at whistleblowerordninger i den finansielle sektor både er underlagt sektorregulering (fx lov om forsikringsvirksomhed/lov om finansiel virksomhed) og reglerne i lov om beskyttelse af whistleblower (herefter whistleblowerloven). Først vil vi give en kort introduktion til reglerne samt pligten til etablering af interne og eksterne whistleblowerordninger.

Bemærk at "whistlebloweren" i det efterfølgende, vil være benævnt "indberetteren".

1. Hvor reguleres whistleblowerordninger

Den første formelle lovgivning om whistleblowerordninger for finansielle virksomheder blev indført i Danmark i 2014, og før dette tidspunkt kunne whistleblowerordninger etableres med tilladelse fra Datatilsynet. Reglerne i lovgivningen for finansielle virksomheder - med senere ændringer - gælder fortsat i dag og stiller krav om, at en finansiel virksomhed skal stille en uafhængig og selvstændig kanal til rådighed for deres ansatte, hvor der kan indberettes om overtrædelser og potentielle overtrædelser af den finansielle regulering.

Efterfølgende er whistleblowerdirektivet implementeret i dansk ret ved vedtagelsen af whistleblowerloven. Da der er tale om et minimumsdirektiv, kan dette være implementeret forskelligt i EU-landene, hvilket kan give anledning til flere udfordringer for selskaber, der har virksomhed i flere EU-lande. Med den nye whistleblowerlov blev der bl.a. indført formelle sagsbehandlingsregler i forhold til indberetningerne, så det sikres, at sagerne behandles inden for rimelig tid, og at indberetter bliver informeret. Men også regler, som sikrer indberetter, der indberetter i god tro, en absolut beskyttelse mod repressalier.

Det er også væsentligt at have for øje, at andre regler kan påvirke sagsbehandlingen af indberetningerne i whistleblowerordningerne. Et eksempel er databeskyttelsesreglerne, som kan føre til, at personen, der er blevet indberettet om, i nogle tilfælde skal informeres om, at der er gennemført en undersøgelse af vedkommende, men også andre helt grundlæggende rettigheder, som retten til at blive glemt og indsigt.

2. Hvem skal have en whistleblowerordning - hvor kan de findes?

Finansielle virksomheder vil som udgangspunkt være forpligtet til at tilbyde en whistleblowerordning til de ansatte, og med den nye whistleblowerlov vil mange andre arbejdsgivere også være forpligtet til at etablere en whistleblowerordning, hvis de har 50 eller flere ansatte, jf. **Figur 1** på næste side.

Et krav om etablering af eksterne whistleblowerordninger i alle EU-landene er også indført med whistleblowerdirektivet, og i Danmark er den nationale eksterne whistleblowerordning forankret hos Datatilsynet.

Eksterne ordninger er imidlertid ikke en ny opfindelse, da der allerede i 2014 blev etableret en ekstern whistleblowerordning hos Finanstilsynet.

3. Krav og overvejelser i forhold til en whistleblowerordnings set-up

Hvem skal kunne anvende ordningen?

Den enkelte arbejdsgiver skal beslutte, hvorvidt whistleblowerordningen kun skal stilles til rådighed for ansatte, eller om den også skal stilles til rådighed for eksterne, som har skaffet sig adgang til oplysninger om overtrædelser i forbindelse med deres arbejdsrelaterede aktiviteter. Det kan fx være tidligere ansatte, aktionærer, medlemmer af bestyrelsen eller leverandører.

Koncernfællesordninger – i Danmark og EU

En koncernfællesordning er en samlet whistleblowerordning, som omfatter alle koncernens selskaber og/eller filialer. Når en koncern alene er etableret i Danmark, har man mulighed for at oprette en koncernfællesordning, eller der kan etableres selvstændige whistleblowerordninger i hvert af selskabets danske virksomheder. Hvilken løsning der skal vælges, må bero på, hvilket set-up, der er mest enkelt at benytte for de ansatte, herunder tilgængeligheden og hvordan behandlingen af sagerne sker mest hensigtsmæssigt.

Figur 1: Krav til etablering af whistleblowerordning

I en koncern med selskaber og/eller filialer og ansatte i flere EU-lande er det ikke lige så enkelt at tage stilling til samme spørgsmål, da det ikke nødvendigvis er lovligt at etablere en koncernfælles whistleblowerordning i alle EU-lande. Problemstillingen om lovligheden af koncernfællesordninger skyldes, at whistleblowerdirektivet er implementeret forskelligt i de enkelte EU-lande. Nationale særregler kan derfor give anledning til juridiske og operationelle udfordringer i internationale koncerner.

Et eksempel herpå er, at det i Danmark er muligt at etablere koncernfællesordninger, hvorimod dette ikke er muligt i samme omfang i Sverige. Dette betyder, et dansk etableret selskab med filialer i flere EU-lande, vil skulle fortage en juridisk vurdering af, om den enkelte filial kan omfattes af en koncernfællesordning, eller om der skal etableres flere selvstændige ordninger i de enkelte EU-lande.

Anonymitet
Forsikringsselskaber er forpligtet til at tilbyde en whistleblowerordning, som sikrer, at indberetninger kan foretages anonymt. Dette giver selvfølgelig en særlig god beskyttelse af indberetter, men for whistleblowerenhedens undersøgelser, kan anonymiteten give flere praktiske udfordringer i forhold til undersøgelse af det indberettede forhold.

Eksempelvis kan der være en risiko for, at whistleblowerenhedens undersøgelser utilsigtet kan føre til, at personer som inddrages i opfølgningen på sagen, vil kunne regne ud, hvem der er indberetter, da whistleblowerenheden ikke kender indberetterens identitet, og derfor ikke har mulighed for at tage højde herfor.

Kravet om muligheden for anonym indberetning i den finansielle lovgivning kan, som ovenfor anført, i nogle situationer give visse udfordringer ift. undersøgelsen af en sag. En veloplyst anonym indberetning kan dog danne grundlag for en videre undersøgelse. Vores generelle anbefaling er at opfordre den som indberetter, til at give sig til kende, og at indberetteren giver whistleblowerenheden mulighed for at kontakte vedkommende for yderligere informationer via virksomhedens whistleblowersystem. I langt de fleste tilfælde er det vores erfaring, at også anonyme indberettere ønsker at være med til at oplyse sagen yderligere, hvis der ikke er tilstrækkelig information i indberetningen.

Dokumentation
Kravet om skriftlig dokumentation for opfølgning på en indberetning i Lov om forsikringsvirksomhed går videre end sagsbehandlingsreglerne i whistleblowerloven. Den skriftlige dokumentation for opfølgning kan fx bestå i opbevaring af relevant mailkorrespondance, interne undersøgelsesrapporter eller anden dokumentation i form af en skriftlig gennemgang af udbetalinger eller lignende. Rent praktisk er det vores erfaring, at det er en god idé løbende at dokumentere, hvad der skal undersøges, og hvordan undersøgelsen påtænkes gennemført. Der kan med

fordel anvendes templates tilpasset sagens kompleksitet. På den måde kan man løbende vurdere, om forholdene i indberetningen er undersøgt tilstrækkeligt, eller der er behov for yderligere undersøgelser og i sidste ende få be-eller afkræftet det indberettede forhold.

4.Den operationelle håndtering af sagerne i en whistleblowerenhed

Screening

Alle nye sager screenes indledningsvis med henblik på at afklare, om indberetningen er omfattet af ordningen, kan afvises som ikke værende omfattet af ordningen eller om det kræver yderligere undersøgelser for at afklare dette. Det er vores erfaring, at der indberettes en del sager i sidstnævnte kategori, da formuleringen af henvendelserne nødvendiggør en nærmere undersøgelse.

Når disse nærmere undersøgelser foretages i sager, hvor der er tvivl om, hvorvidt der er tale om en whistleblowersag – er det vores erfaring, at det er vigtigt, at indberetter informeres herom for at undgå, at indberetter er i vildfarelse om, at indberetningen er omfattet af whistleblowerordningen.

Når en indretning ikke omfattes af ordningen, er det vigtigt at afstemme med indberetter, hvorvidt henvendelsen må sendes til fx Human Ressources eller til virksomhedens klageansvarlige, for at få afklaret indberetters problem eller bekymring. Grunden til dette er, at der kan være en årsag til, at indberetter har valgt whistleblowerordningen, og at de sædvanlige eskalationsveje ikke blev valgt i første omgang.

Opfølgning

Ved opfølgningen på en indberetning, er det nødvendigt at være opmærksom på den lovbestemte tavshedspligt i whistleblowerloven, der gælder for indberetterens identitet og for indholdet af selve indberetningen. Indholdet af indberetningen kan deles, når det sker som led i whistleblowerenhedens undersøgelse af en indberetning. Det er derfor vigtigt dels ikke at inddrage for mange i undersøgelsen og dels at sikre, at de som involveres, forstår at de er underlagt den lovbestemte tavshedspligt. Indberetters identitet kan kun deles med andre uden for whistleblowerenheden, hvis indberetter har givet samtykket til dette, eller videregivelsen sker til en anden offentlig myndighed for at imødegå overtrædelser, eller med henblik på at sikre berørte personers ret til et forsvar.

Feedback

Forpligtelsen til feedback til whistlebloweren er essentiel, og vi oplever, at der ofte er et stort behov for at sikre, at indberetterens bekymring tages alvorligt og at kommunikation gives i øjenhøjde. I feedbacken skal der også tages hensyn til beskyttelsen af den eller de personer, der er indberettet om, da de også beskyttes af de databeskyttelsesretlige regler.

Balancen mellem på den ene side at give indberetter konkret feedback og på den anden side at iagttage hensynet til den, der er indberettet om, kan føre til, at indberetter kan opleve feedbacken som overfladisk. Derfor er det en god idé løbende at forventningsafstemme og italesætte overfor indberetter, at det ofte ikke vil være muligt at give feedback om eventuelle konkrete sanktioner af hensyn til beskyttelsen af de øvrige involveredes rettigheder.

Repressalier

Virksomheder skal opfordre til, at interne ordninger benyttes fremfor en ekstern ordning i de situationer, hvor indberetter er betrygget i, at overtrædelsen kan håndteres effektivt i den interne ordning, og indberetter vurderer, at der ikke er risiko for repressalier.

En måde at sikre en betryggende håndtering er, at indberetter kan fravælge, at en eller flere medlemmer af whistleblowerenheden, skal kunne se indberetningen. Dette vil være relevant, hvis indberetter vurderer, at medlemmer af whistleblowerenheden, kan være involveret i overtrædelsen. Dette er måske særligt relevant i virksomheder, som ikke har en uafhængig compliancefunktion til håndtering af sagerne, eller benytter et eksternt advokatkontor til at screene og/eller håndtere sagerne.

Opfordringen til brug af den interne ordning ændrer ikke på, at virksomheden naturligvis også skal informere om, at indberetter også kan anvende eksterne ordninger.

For en whistleblowerenhed er det vigtigt at fastholde sit fokus på forbuddet mod repressalier, også i tiden efter, at en undersøgelse er afsluttet. Det omfatter eksempelvis opmærksomhed på organisationsændringer eller nedlukning af aktiviteter. Når sådanne forandringer foretages i en organisation, vil disse ofte blive håndteret af ansatte, der ikke er en del whistleblowerenheden, og de personer har derfor helt naturligt ikke kendskab til, om ændringerne vil komme til at berøre en person, som har indberettet.

For at undgå misforståelser, er det derfor vigtigt, at whistleblowerenheden inden for rammerne af fortrolighed og de databeskyttelsesretlige regler har en løbende dialog med Human Ressources om ændringer i organisationen og eventuelle konsekvenser heraf.

Whistleblowerenhedens sammensætning
Ved sammensætningen af whistleblowerenheden skal det sikres, at der er uafhængighed til den daglige drift. Det kan derfor i en finansiel virksomhed være en fordel at have compliance med i whistleblowerenheden, da compliance i sit daglige arbejde skal have en armslængde til forretningen, ikke må træffe beslutninger om forretningsmæssige løsninger, kender til reglerne og er vant til at arbejde under fortrolighed. Det kan ligeledes være en fordel at have et medlem af bestyrelsen med i whistleblowerenheden for at sikre forankring i det øverste ledelseslag.

5. Afrunding

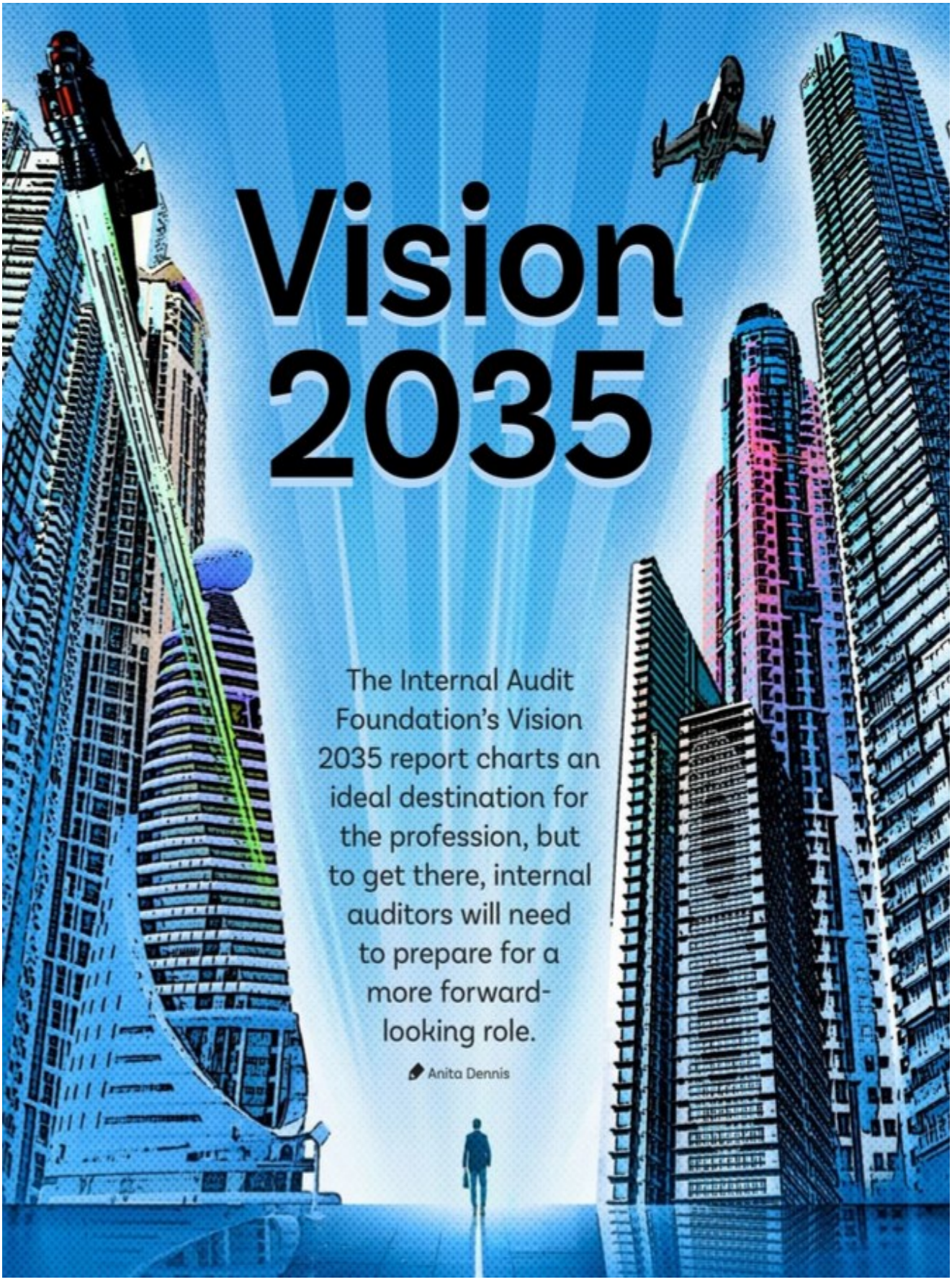
Overordnet kan der i en whistleblowerordning indberettes på mange forskellige områder. Det betyder, at whistleblowerenhedens undersøgelser vil kræve stor indsigt i og viden om virksomheden og de regler, virksomheden er underlagt, for fx at kunne inddrage de korrekte personer i opfølgningen på sagen, med henblik på endelig be- eller afkræftelse af det indberettede forhold.

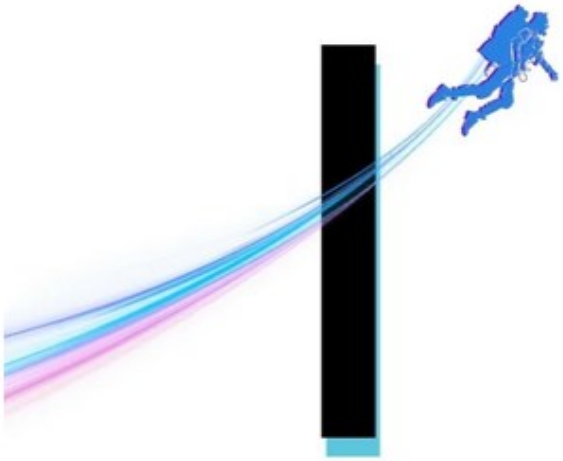
Whistleblowerordninger kan bidrage positivt til at afdække ulovlige forhold og give værdifuld viden om virksomhedens kultur. Men ordningen kan ikke træde i stedet for en kultur, hvor alvorlige og saglige forhold kan adresseres af medarbejderen via de sædvanlige kanaler uden frygt for konsekvenser.

Det er vigtigt, at whistleblowerenhederne har en robust proces og en struktur for at gennemføre deres undersøgelser, da dette vil være med til at styrke tilliden til whistleblowerordningerne. De seneste år er der set en stigning i antallet af whistleblowersager hos flere af de største virksomheder i Danmark, og området der kan indberettes om, er blevet langt bredere end tilfældet er i de sektorregulerede ordninger. Dertil kommer, at der har været stort fokus i virksomhederne på at informere medarbejderne om de nye regler.
Det kan ikke udelukkes, at virksomhedernes whistleblowerenheder i den næste tid vil modtage indberetninger om forhold, som ikke tidligere har været behandlet i regi af virksomhedens whistleblowerordning. Dette skyldes, at de forhold, der kan indberettes om med ikrafttrædelsen af den nye whistleblowerlov er blevet langt flere. Det betyder, at nye typer af sager kan finde vej til virksomhedernes whistleblowerordninger, og disse sager kan betyde, at der skal laves tilpasninger i processen for undersøgelse af sagerne, som muligvis skal tilrettelægges på en anden måde, end sager vedrørende overtrædelse af den finansielle regulering. Fokus må derfor forventes at skulle rettes mod at forfine og afklare, hvordan nye områder skal undersøges på tilstrækkelig vis.

Noter

[1] Stor stigning i antallet af whistleblower-indberetninger i C25-virksomheder og Antallet af whistleblower-indberetninger i C25-virksomheder fortsætter med at stige | PwC.


Vision 2035
The Internal Audit Foundation's Vision 2035 report charts an ideal destination for the profession, but to get there, internal auditors will need to prepare for a more forward-looking role.
Anita Dennis



n the coming years, the internal audit profession is expected to face rapid, ongoing, and extensive change driven by emerging technologies, new business models, and disruptive trends. Against this backdrop, The IIA's Internal Audit Foundation recently completed a landmark project to answer two compelling questions about the profession's future:

- What *will* the internal audit profession be in 2035?
- What *should* the internal audit profession aspire to become by the year 2035?

The centerpiece of this initiative, Internal Audit: Vision 2035–Creating Our Future Together, is a comprehensive research project that gathered insights from internal auditors and stakeholders across professional levels, global business environments, and industries (see "A History of Transformation"). The completed report, released in July, provides a clear-eyed view of where the profession stands today and what steps can help it elevate its impact in the future.

Vision 2035 maps out a future in which internal auditors move firmly into their roles as strategic advisors who provide unique, holistic perspectives to their organizations, while enhancing their assurance role. According to the report, in the coming years, they will leverage virtual and augmented reality, quantum computing, and advanced analytics to offer evidence-based assurance and forecast future trends. Internal auditors across all levels, industries, and organization types will have the abilities and stakeholder support they need to confidently address new risks and changing audit environments.

"In today's rapidly evolving landscape, it is crucial for the internal audit profession to embrace technological advancements and emerging risks to sustain our profession's relevance and influence," says IIA President and CEO Anthony Pugliese. "Vision 2035 underscores the importance of adapting as a profession to ensure internal audit remains a vital part of helping the organizations that we support succeed."

Becoming the Strategic Advisor

Looking ahead, Vision 2035 survey participants see internal auditors enhancing their role as independent, objective strategic advisors who provide tremendous value to their organizations. In fact, more than half of respondents say being seen as trusted advisors is one of the most exciting aspects of the profession. And, three out of four say the chance to add value is the most exciting facet.

Participants say they expect the advisory services that define the strategic advisor role will become a larger part of their job in the future. They say they expect the percentage of time internal auditors devote to advisory services will rise from 24% today to 41% in 2035, while time spent on assurance services will drop from 76% to 59%.

"The allocation of time spent from an internal audit perspective will change dramatically by 2035," says Theo Bunting, a Nashville, Tenn.-based audit committee chair at NiSource and Unum Group and former group president at Entergy Corp. "The foundational elements of the work won't change, but the area of focus and skill sets will." Internal audit is positioned to increase value through more advisory services because it can see across the entire organization, but the function will have to take its observations a step further.

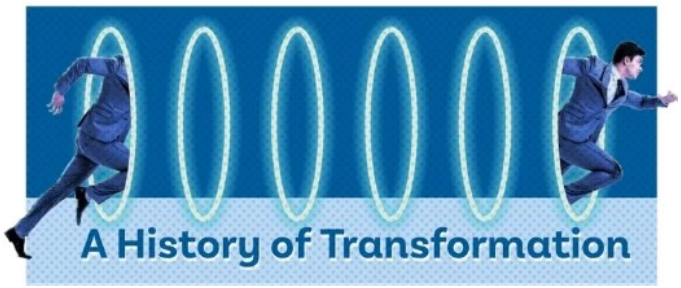
"Internal auditors are very comfortable saying they've taken a sample and that it doesn't comply with a certain policy," says Sandy Pundmann, executive vice president, chief audit and risk officer at Warner Bros. in New York. "But they need the confidence to recommend new policies, agendas, or capabilities to the chief information officer or business unit or strategy leader. They have to be the truth tellers so they can influence the appropriate leaders to take steps that will achieve the organization's business objectives, mitigate risks, or address new challenges or opportunities."

Independence is always a key concern for the internal audit team, says Kimberly Ellison-Taylor, founder and CEO of KET Solutions LLC in the Washington, D.C. area. Being a part of a project implementation team and then auditing the completed project would be inappropriate. However, internal auditors can identify and advise on relevant leading practices that can be used in strategies and making decisions. "In today's complex and ever-changing business environment, we need wide-ranging expertise and perspectives. Internal audit is a value-added stakeholder, and it would be a misstep to exclude it."

Changing Mindsets

Misperceptions about internal auditors' role and skills could hinder their advancement into a new role. Half of Vision 2035 respondents report being misunderstood or undervalued is the top challenge for the profession. Many say internal auditors often are seen as having a policing role (48%), while far fewer report they are viewed as change agents (21%) or strategic (19%).

The profession is already adapting its approaches to emerging expectations. "The purview of internal audit has increased enormously," says Mervyn King, a former judge



The internal audit profession has a long history of evolving to meet changing stakeholder and regulatory demands. The Vision 2035 initiative is part of this history, undertaken at a time when emerging technologies and a range of global business and geopolitical trends are driving seemingly relentless change.

The Internal Audit Foundation conducted the project's research in several phases, using multiple approaches to ensure a thorough understanding of the profession and its future. It began with foundational research that extensively examined internal auditing and its potential future. The subsequent qualitative research phase involved in-depth interviews and focus groups with more than 500 participants from around the world, including internal auditors, audit committee members, executives, and other stakeholders.

Researchers also analyzed social media data, industry and academic literature, visioning publications, and trend reports. Finally, an online survey conducted in eight languages involved roughly 6,500 participants, which included internal auditors, audit committee members, educators, students, and other internal stakeholders.

of the Supreme Court of South Africa who drafted the widely used King Report on Corporate Governance. Once a hindsight profession focused on pointing out what has gone wrong, today internal audit also is a foresight profession. "Internal audit is the oil that ensures the machine runs smoothly," he says. "If internal audit is not functioning properly, you have a problem."

An organization's ability to fully appreciate internal audit's value depends in part on its culture. Organizations with a continuous improvement culture are less likely to view internal audit as a team that exists to find fault and more likely to welcome it as a critical element of the operational excellence, performance, and risk management processes, Ellison-Taylor says.

"Supportive leadership who see internal audit as more than compliance, as well as a speak-up culture, reduce the stigma of 'findings,'" she explains. "Tone from the top is critical in ensuring the organization sees internal audit as valuable team members." She notes that CEOs can encourage a more positive perception of internal audit by highlighting its value and impact in management meetings and organizationwide communications.

To engage senior leaders, CAEs need to proactively inform them about the internal audit function's capabilities. "There's education that needs to take place in the C-suite," Bunting says. "Leaders need to understand that a good defense when faced with a regulatory, code of conduct, or other investigation is a strong, robust internal audit function."

Senior management should view the CAE as a strategic executive who brings insights on process, control, and risk to the executive team, Pundmann adds. "It's not only about protecting value, but about helping shape value creation and risk mitigation for the future," she says.

Burzin Dubash, chief operating officer at Ankur Capital in Mumbai, points out that "the scope of the audit depends on the budget, but audit budgets often have no correlation to the actual business risk that the company is facing." An appreciation of internal audit's role, then, is important because it may lead to more adequate funding. Available resources should reflect risk as well as potential advisory opportunities that internal audit insights can provide.

Harnessing Technology

Participants in Vision 2035 agree that an ideal future for the profession will rely on using and auditing advanced and emerging technologies. To make that happen, internal audit must seize opportunities to improve and participate in technology innovations. For example, while 74% of internal auditors say artificial intelligence (AI) is most important for the ideal future, 52% say they are not involved in AI activities today.

Digital technologies in general, and AI in particular, are becoming embedded tools in areas such as procurement, recruiting, production, sales, distribution, and quality control, Dubash notes. "The focus on technology needs to increase significantly," he says, including time spent on technology in audits. The tools to address risks are now digital, and those risks include new threats to cybersecurity, data integrity, and privacy that technology, itself, can introduce.

Internal audit must be actively involved in the planning stage for new technologies, Pundmann says, ensuring that new systems are built for purpose and not simply corrected after they go live. "Internal audit can advise on whether the right authorizations and controls are in place," she explains. She likens the internal auditor to an electrician who is called in to inspect a building's wiring before the drywall goes up.

Upskilling for New Expectations

"As the focus of audit committees changes and businesses focus more on risk, culture, technology, and innovation, internal audit has to be able to evolve, as well," Bunting says. Over the next decade, current approaches to educating and recruiting internal auditors are expected to evolve, he notes. In addition, training and recruitment

will expand beyond accounting skills to include technology, AI, and business advisory capabilities, according to Vision 2035 participants.

Internal auditors also must understand how to address new sustainability reporting protocols required by evolving regulatory mandates or stakeholder expectations. To do so, audit functions will need expertise with nonfinancial assets and the organization's impact on the economy, society, and environment.

"Internal audit is absolutely critical in the organization's move away from the primacy of the shareholder to a focus on other stakeholders," King explains. "It has to deal with how the product impacts on society."

Although internal auditors may have a basic understanding of these new risk areas, Dubash questions whether that is sufficient to inspire trust with process owners. To strengthen internal audit functions, he recommends they develop competency frameworks that outline how to recruit, compensate, and retain people with solid skills outside the financial arena. That framework should include a career path that enables auditors to shift to another function if they choose.

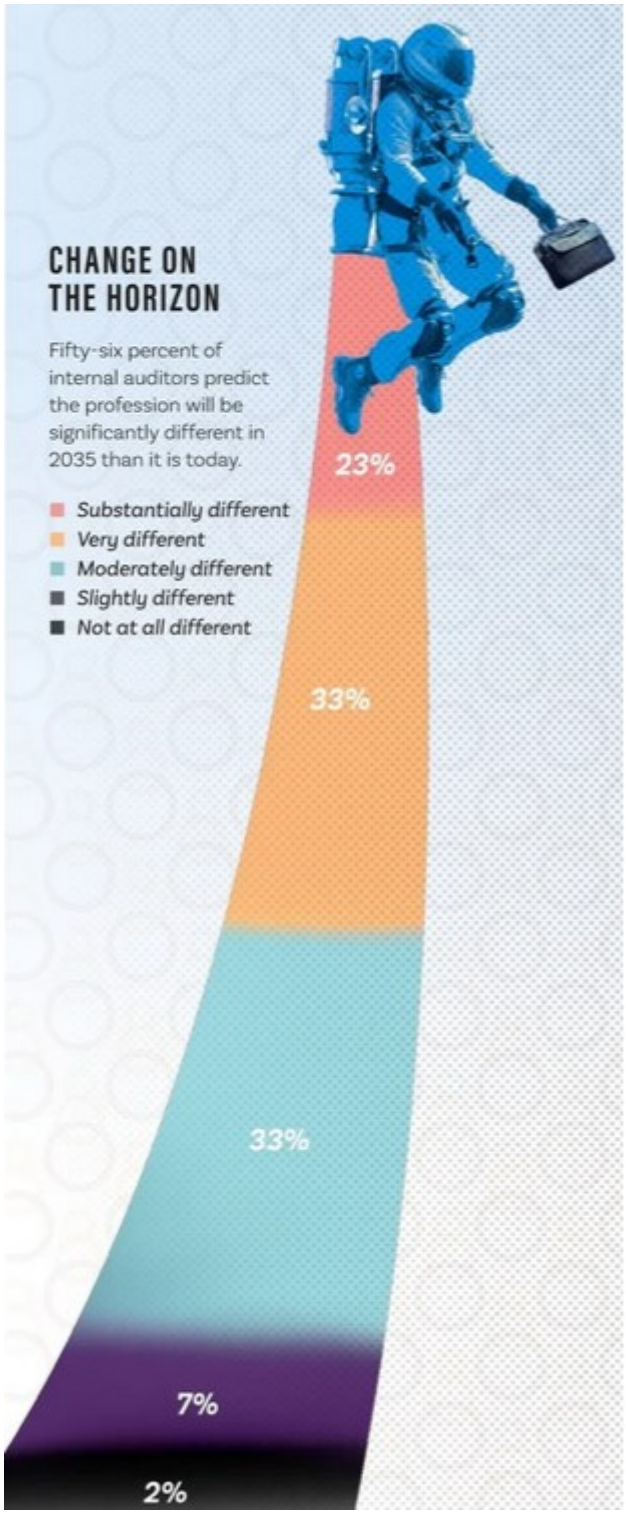
Training options and mentoring opportunities also need to be expanded so these team members can advance their knowledge, Dubash says. "If auditors are not skilled in applying judgment, they won't be taken seriously as risk advisors," he notes. In addition, internal audit functions can enhance their capabilities by collaborating with or leveraging talent from other functions.

Most of all, internal auditors over the next decade will be called on to effectively manage change. According to survey participants, adaptability and learning agility are among the most important competencies today (56%) and will remain so in the future (48%).

Keys to the Future

The Vision 2035 report sets out an inspiring future for the profession, one in which internal auditors help drive change in their organizations through foresight and independent assurance and advice. Yet to reach their potential, internal auditors must start now by leveraging technology and enhancing skills.

As internal auditors stand at a turning point, the profession and its stakeholders already hold the keys to future success, the report notes. These include internal audit's expertise in providing independent assurance and advice, its holistic understanding of the organization, and its familiarity with the needs of stakeholders. Vision 2035 gives the profession the direction it needs to take its next best step forward.



Anita Dennis is a freelance writer based in New Jersey.

This article was reprinted with permission from the August 2024 issue of Internal Auditor (Ia), published by The Institute of Internal Auditors, Inc., www.theiia.org.

Internal Audit's Role in Risk Management

The move to more advisory work isn't without challenges.

Matt Kelly Rheya Tanner

Everything needs to adapt to changing conditions or die, and internal audit functions are no exception to that rule. So perhaps it's no surprise that we hear a lot these days about internal audit teams doing more to help their organizations manage risk.

Yes, to a certain extent, internal audit functions have always helped their organizations manage risk — but only in the regimented routines of providing assurance. Internal auditors test business processes to see how well they work, document weaknesses, recommend improvements, and issue reports. That's it.

That's no longer enough, and everyone knows it. Consider The Internal Audit Foundation's Internal Audit: Vision 2035 report released in July, which expressly calls for internal audit to do more risk advisory work, helping organizations to identify emerging risks and design business processes that keep those risks in check from the start. That report put into writing what internal audit thinkers have been saying for years.

"The journey hasn't been an overnight one," says Tom McLeod, chief risk officer at Yellow Canary, a software firm in Australia, and who previously ran internal audit or risk assurance functions at numerous large Australian

companies. "It's been one where there's a long realization that auditing isn't just about delivering reports; it's about delivering value."

A wise idea? Absolutely. It helps organizations navigate today's complicated business environment and makes the internal audit function more valuable to management, which never hurts.

That said, making such a shift skillfully is no easy feat. Boards, management teams, and internal audit leaders, alike, need to proceed carefully.

Advisory By Popular Demand

First, we should be clear that providing more advisory services is something most internal auditors want to do. According to Vision 2035 (which polled some 7,000 internal audit professionals around the world), internal auditors expect the time spent on assurance services will fall from 76% today to 59% by 2035, while time spent on advisory work rises from 24% to 41%.

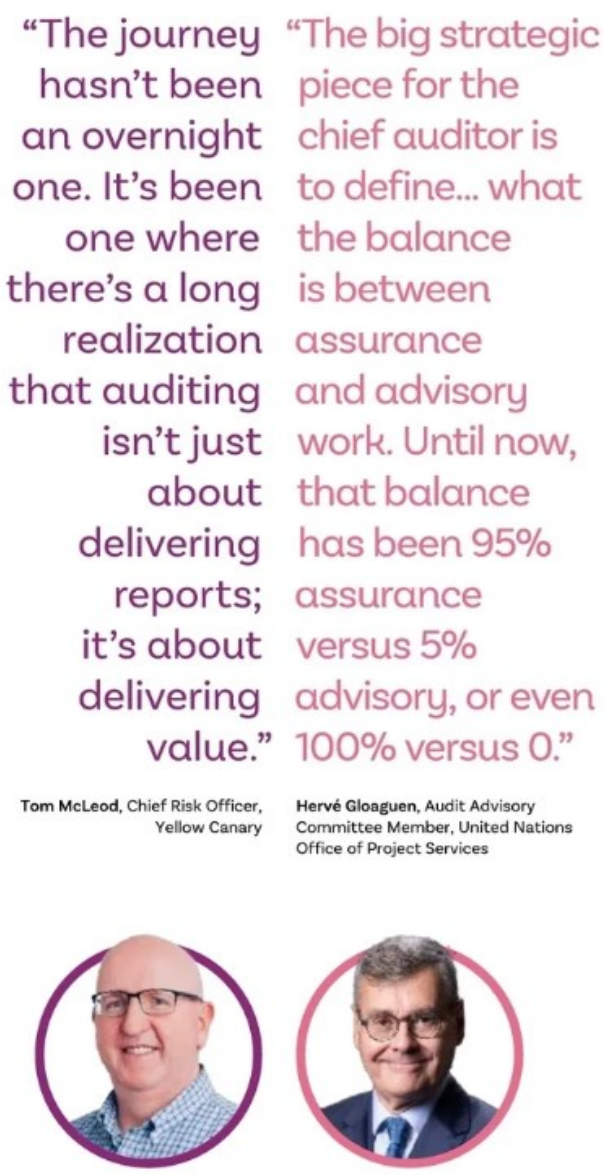
Moreover, internal auditors like the prospect of more risk advisory work. Seventyfive percent of respondents say they're excited about adding value to the organization; 57% say they're excited about improving risk management. That enthusiasm is the raw material necessary for internal audit functions to make the leap into more risk advisory work.

The challenge is to strike the right balance between traditional assurance work and more modern risk advisory duties. Corporate boards and CAEs will need a clear understanding of what that balance can be given the internal audit team's resources and capabilities.

"The big strategic piece for the chief auditor is to define with the board, and in particular with the chair of the audit committee, what the balance is between assurance and advisory work," says Hervé Gloaguen, who sits on the audit advisory committee of the United Nations Office of Project Services. "Until now, that balance has been 95% assurance versus 5% advisory, or even 100% versus 0."

Now consider how to determine that balance. The audit committee would need to weigh the traditional assurance duties that internal audit still needs to fulfill (say, the annual financial audit or any data security audits the organization might need to undergo), versus the emerging risks that shouldn't be ignored but don't neatly line up with assurance or compliance obligations (such as the risks of artificial intelligence or environmental, social, and governance issues).

Don't forget the practical constraints, either. For example, does the internal audit team have the right technology to tackle emerging risks? Does it have the right people with the right skills? Probably not; 96% of Vision 2035 respondents say experienced internal auditors will need to increase their technology skills to remain relevant. And, what about staffing levels and budgets?



Those details matter, Gloaguen warns. "People are struggling today just to do the assurance and audit work — before they even begin to think about doing risk advisory work."

Even if the audit committee and internal audit do reach a consensus on balancing advisory and assurance work, we still have one other object in this three-body problem: management.

Risk Advisory vs. Risk Management

The peril here is that management might interpret "internal audit provides risk advisory help" as "internal audit owns risk management." Those are not the same things.

One can't blame management teams for trying this maneuver. Successful business operations today are much more about managing risk on an ongoing basis than they ever were before. Management teams know that, but their risk management efforts so far don't seem to be very impressive. According to the 2024 State of Risk Oversight Report from North Carolina State University, only 30% of companies say they have a strong enterprise risk management function.

The other 70% are still working on it — and in that case, because internal audit already has a solid grounding in risk management, why not give the CAE that responsibility? Indeed, some very large organizations — T-Mobile, Warner Bros. Discovery, and New York Presbyterian Hospital, to name only a few — have internal audit and risk management functions led by one person.

McLeod himself has been in that predicament. He once had the title of chief audit and risk officer, and a board director point-blank asked him, "You're the chief audit and risk officer; why don't you own more of those risks?" including cybersecurity and physical security.

Shoving internal audit into a second-line role, with direct responsibility for risk management, is decidedly not the risk advisory work described earlier. It threatens internal audit's objectivity and independence. It leaves internal audit in a weird place organizationally, reporting directly to both senior management (which, let's remember, does oversee the second line) and to the audit committee, as usual.

To guard against that bad risk management habit, audit committees will need to pay close attention to how senior management wants to run risk management.

"It's kind of an empty space, which department is really taking care of risk management," Gloaguen says. "The way through this is not a shortcut through internal audit. It's to build real muscle and teeth for the risk management function."

That means the audit committee should have a conversation with internal audit leaders and the management team to identify a feasible plan for how internal audit helps others manage risk, but not shoulder that burden directly.

Internal audit leaders, meanwhile, must be "completely transparent" with business chiefs talking about their role as a risk advisor rather than risk owner, McLeod says. "You can't do this by stealth. Set up an environment that's completely transparent and that talks about ownership and what advisory really means."

That's advice all internal audit teams should take to heart — and take a lot sooner than 2035.

Matt Kelly is editor and CEO of RadicalCompliance.com, an independent blog about audit, compliance, and risk management. He welcomes feedback at mkelly@radicalcompliance.com.

This article was reprinted with permission from the October 2024 issue of Internal Auditor (Ia), published by The Institute of Internal Auditors, Inc., www.theiia.org.


Embracing Change,
ELEVATING STANDARDS
TORONTO
save the date • July 14-16, 2025
IIA INTERNATIONAL CONFERENCE

Systemrevisionsbekendtgørelsen

Nils B. Christiansen, Associate Partner, EY

Indledning

Jeg vil i denne artikel beskrive ændringerne til systemrevisionsbekendtgørelsen og deres indvirkning på systemrevisors og erklæringsmodtagernes arbejde samt forventninger til den fremtidige udvikling.

I forbindelse med opdateringen af systemrevisionsbekendtgørelsen, blev der etableret en arbejdsgruppe bestående af intern revision fra nogle af datacentralerne, samt FSR, hvor eksterne revisorer, der deltog i revision af systemrevisionserklæringerne, ligeledes deltog.

Denne artikel tager udgangspunkt i det arbejde som denne arbejdsgruppe udførte med henblik på at udarbejde en opdateret model for systemrevisionserklæringer i henhold til den opdaterede systemrevisionsbekendtgørelse.

Den nuværende systemrevisionsbekendtgørelse[1] blev vedtaget den 22. december 2022, og er gældende for systemrevisionserklæringer der påbegyndes den 1. januar 2023 eller senere.

De systemrevisionserklæringer der er udarbejdet for 2023 er således udarbejdet efter den opdaterede systemrevisionsbekendtgørelse.

Systemrevisionsbekendtgørelsen er gældende for fælles datacentraler, it-operatører af detailbetalingssystemer samt datacentraler, der udfører både væsentlig it-drift og it-udvikling for den fælles betalingsinfrastruktur.

Formålet med ændringerne der kom ind i den nuværende systemrevisionsbekendtgørelse var at:

- Tydeliggøre at erklæringsområdet for systemrevisionserklæringen er system-, data- og driftssikkerheden hos datacentralen i forhold til it-sikkerhed, herunder forhold fra ledelsesbekendtgørelsens[2] bilag 5.
- Tydeliggøre hvilke it-risici de tilknyttede pengeinstitutter skal være opmærksom på i forhold til outsourcing til datacentralerne.

Væsentligste ændringer fra tidligere

De væsentligste nyskabelser ved den opdaterede systemrevisionsbekendtgørelse er:

1. Erklæringen skal medtage relevante krav fra Ledelsesbekendtgørelsens bilag 5 (§8, stk. 2)
2. For hvert kontrolmål i erklæringen skal der anføres en konklusion med en af kategorierne (§8, stk. 3)
   a. Betryggende
   b. Betryggende, men med behov for nogle forbedringer
   c. Ikke betryggende
3. Erklæringen skal indeholde en selvstændig oplistning af kontroller der er eller har været, ineffektive (§8, stk. 4)
4. Datacentralens ledelse skal udarbejde en ledelsesredegørelse der skal indeholde en beskrivelse af (§21, stik. 1)
   a. Ledelsens vurdering af kontrolsvagheder og afledte risici for tilknyttede pengeinstitutter
   b. Hvordan datacentralen håndterer de identificerede kontrolsvagheder
   c. Hvilke kompenserende kontrol- og sikringsforanstaltninger de tilknyttede pengeinstitutter kan implementere for at imødegå kontrolsvagheder
5. Revisor skal afgive en udtalelse om ledelsens redegørelse (§21, stk. 2).

Relevante krav fra ledelsesbekendtgørelsens bilag 5

Med opdateringen af systemrevisionsbekendtgørelsen og kravet om at erklæringen skulle omhandle alle relevante krav fra Ledelsesbekendtgørelsens bilag 5, var der behov for at ændre indholdet af systemrevisionserklæringerne.

Kort inden ikrafttrædelsen af systemrevisionsbekendtgørelsen blev ISO 27001 / ISO 27002 opdateret til 2022 version. De fleste systemrevisionserklæringer for datacentraler er udarbejdet i henhold til ISO 27001/2 standarderne som kontrolrammeværk.

Da der i forvejen var behov for at opdatere indholdet af systemrevisionserklæringerne for at kunne medtage alle

relevante krav fra Ledelsesbekendtgørelsens Bilag 5, var det oplagt at udarbejde en ny struktur hvor den opdaterede ISO 27001/2 standard og kravene fra Ledelsesbekendtgørelsen blev sammenkædet. De datacentraler der anvender ISO 27001/2 som kontrolrammeværk havde i forvejen en forventning om at overgå til ISO 27001/2 2022 versionen.

Ledelsesbekendtgørelsens bilag 5 indeholder 108 krav, og de fleste af kravene fra Ledelsesbekendtgørelsens bilag 5 kunne direkte relateres til kontroller i ISO 27001/2 standarderne. Enkelte krav er så detaljeret at der er behov for etablering af særlige kontroller til disse krav.

Disse mere detaljerede krav er oprettet som separate kontroller, men stadig mappet til en ISO kontrol der var mest relevant. Disse ekstra kontroller der går udover ISO27001/2 standarderne er markeret med 'a', 'b', 'c' etc. alt efter hvor mange ekstra detaljerede kontroller der var relevante at medtage.

I ledelsesbekendtgørelsen er der derudover en række krav indenfor 'It-strategi', 'it-risikostyringspolitik' og 'implementering af it-risikostyringspolitikken' som ikke kan mappes til tilsvarende eller tilnærmelsesvis tilsvarende kontroller i ISO 27001/2:2022.

For disse 3 områder er der i stedet oprettet særskilte kontrolmål og underliggende kontroller. Disse har typisk fået kontrolnumre der ligger udenfor kontrolnumre fra ISO27001/2 standarderne, dvs. det er kontroller der har kontrolnr. 1.xx, da ISO 27001/2 standarden starter med kontrolnr. 5.01.

Af den samlede oversigt over kontrolmål, kontroller, udførte testhandlinger og resultat af tests er der typisk for hver kontrol også anført hvilket krav fra ledelsesbekendtgørelsens bilag 5 kontrolaktiviteten er linket til.

Det er ikke alle kontrolaktiviteter der er linket til Ledelsesbekendtgørelsen, da der medtaget kontrolaktiviteter der ikke er påkrævet efter Ledelsesbekendtgørelsens bilag 5, eksempelvis styring af aktiver, HR og fysisk sikkerhed.

Konklusion pr. Kontrolmål
I en ISAE 3402 rapport anføres normalt kun en samlet konklusion for hele erklæringsemnet i revisors erklæring. Med opdateringen til systemrevisionsbekendtgørelsen er der nu krav om at der for hvert enkelt kontrolmål anføres en konklusion i en af 3 kategorier:

1. Betryggende
2. Betryggende, men med behov for nogle forbedringer
3. Ikke betryggende

Der er i systemrevisionsbekendtgørelsen ikke anført nogle definitioner af hvad der skal medføre en af de 3 konklusioner.

Idet der i systemrevisionsbekendtgørelsen ikke er defineret hvad der medfører de 3 konklusioner, var der i arbejdsgruppen enighed om at anvende en enkelt 'matematisk' vurdering, således at alle erklæringer vil have samme grundlag for konklusionerne uafhængig af systemrevisor.

Blandt systemrevisorerne for datacentralerne er der enighed om at:

Betryggende anvendes når der ikke er anført nogle afvigelser til de pågældende kontrolmål.

Betryggende med behov for nogle forbedringer anvendes når der er konstateret afvigelser til en eller flere af kontrollerne for det pågældende kontrolmål, men uden at der er taget forbehold for kontrolmålet.

Ikke betryggende anvendes hvis systemrevisor har taget forbehold for kontrolmålets opnåelse.

Typisk er denne konklusion pr. kontrolmål medtaget i en tabel i eget afsnit under kapitlet i systemrevisionserklæringen med kontrolmål, kontrolaktiviteter, testhandlinger og resultat af tests (typisk kapitel 4). Dette afsnit indeholder også ofte oplistningen af kontroller der er eller har været ineffektive (se nedenfor).

Selvstændig oplistning af kontroller der er eller har været ineffektive
Det tredje nye element der er kommet til med opdateringen af systemrevisionsbekendtgørelsen er et krav om at der i erklæringen medtages en selvstændig oplistning af kontroller der er, eller har været, ineffektive.

Dette betyder at uanset om afvigelse er afhjulpet eller ej inden erklæringsperioden udløb, så skal den medtages i oplistningen. Dette krav medfører redundant information, da information om en kontrol er, eller har været, in effektiv allerede fremgår af resultat af test i kapitlet med kontrolmål, kontrolaktiviteter, testhandlinger og resultat af test.

Kontrolaktiviteter der var omtalt i forrige års systemrevisionserklæring vil typisk altid være medtaget i indeværende års erklæring med oplysning om hvornår afvigelsen er afhjulpet. Tilsvarende vil afvigelser der er opstået i erklæringsperioden have information om hvornår afvigelsen er opstået, og evt. afhjulpet hvis den også er afhjulpet indenfor erklæringsperioden.

Afsnittet med den selvstændig oplistning af kontroller der er, eller har været, ineffektive giver således en opsummering af resultat af tests for de kontroller der er, eller har været, ineffektive, således at modtagerne af erklæringen hurtigere kan få et overblik over dette.

Datacentralens ledelsesredegørelse
Dette er den største nyskabelse i systemrevisionsbekendtgørelsen, og også det afsnit der er mest tidskrævende i forbindelse med afgivelse af systemrevisionserklæringen.

Ledelsesredegørelsen kan enten være en integreret del af systemrevisionserklæring (typisk løsning), men kan også være et separat dokument ved siden af selve systemrevisionserklæringen.

Såfremt ledelsesredegørelsen er et separat dokument, er der krav om at det skal fremsendes til de tilknyttede pengeinstitutter samtidig med selve systemrevisionserklæringen fremsendes til de tilknyttede pengeinstitutter.
Af denne årsag er ledelsesredegørelsen typisk et særskilt afsnit i systemrevisionserklæringen.

Systemrevisionserklæringerne er øget betragteligt i omfang, og det kan primært tilskrives afsnittet med ledelsesredegørelsen, da dette afsnit er ret omfattende.

I ledelsesredegørelsen skal datacentralens ledelse udarbejde en redegørelse hvor de for alle de identificerede kontrolsvagheder (afgivelser) skal omtale:

Ledelsens vurdering af kontrolsvagheden og dens afledte risiko for pengeinstitutterne
Dette er et centralt afsnit i systemrevisionserklæringerne. Her skal datacentralens ledelse give sin vurdering af kontrolsvagheden. Det er ikke tilstrækkeligt blot at anføre lav/mellem/høj risiko. Afsnittet skal give en tilstrækkelig vurdering af kontrolsvaghederne og de afledte risici.

Hensigten med dette afsnit er, at modtagerne af erklæringen, tilknyttede pengeinstitutter, bedre kan forstå og forholde sig til afvigelserne, herunder bedre kan forstå hvilke risici afvigelserne medfører for pengeinstituttets it og drift.

Informationen i dette afsnit er centrale for modtagerne, og tiden der medgår til at udarbejde dette afsnit skal ikke undervurderes. Derfor vil det være en fordel for datacentralen løbende i året at udarbejde dette afsnit, således at processen startes allerede når afvigelsen er konstateret.
Eksempelvis kan der som del af afslutningerne af de enkelte områder, hvor der opnås enighed om de enkelte observationer, at der samtidig hermed formuleres vurderingen af kontrolsvagheden mv.

Hvordan datacentralen har håndteret den identificerede kontrolsvaghed
I forlængelse af ovenstående omkring vurdering af risici, skal datacentralens ledelse også omtale hvordan kontrolsvagheden er håndteret, eller er i gang med at blive håndteret.

Her skal datacentralen beskrive de tiltag eller handlingsplaner der er taget for at afhjælpe kontrolsvagheden. For de kontrolsvagheder der er afhjulpet skal omtalen beskrive hvordan kontrolsvagheden blev afhjulpet og hvornår.
Beskrivelsen bør også indeholde beskrivelse af hvad datacentralen har udført for at reducere risikoen forbundet med kontrolsvagheden til et for de tilknyttede pengeinstitutter acceptabelt niveau.

For de kontrolsvagheder der endnu ikke er fuldt afhjulpet skal der beskrives en kombination af hvilke handlingsplaner der er lagt for afhjælpningen, samt status for disse.

Hvilke kompenserende kontrol- og sikringsforanstaltninger de tilknyttede pengeinstitutter kan implementere
Dette afsnit kan ses som tillæg til de allerede eksisteren-

de afsnit omkring komplementerende kontroller hos pengeinstitutterne. I dette afsnit skal datacentralen beskrive hvilke kontrol- og sikringsforanstaltninger som pengeinstitutterne selv kan udføre for at afhjælpe kontrolsvagheden eller reducere risikoen forbundet med kontrolsvagheden til et acceptabelt niveau.

Revisors udtalelse om ledelsens redegørelse
Systemrevisor skal afgive en udtalelse om ledelsens redegørelse.

Systemrevisor skal således ikke foretage en revision af ledelsens redegørelse, men alene gennemlæse ledelsens redegørelse og sikre, at der ikke er fejlagtige og modstridende informationer i redegørelsen i forhold til det som systemrevisor er blevet bekendt med som del af sin revision.

Hvis ledelsens redegørelse er integreret i systemrevisionserklæringen, så vil revisors udtalelse være en del af selve revisors erklæring, hvor udtalelsen medtages på samme måde som revisors udtalelse om ledelsesberetningen i påtegningen på et årsregnskab.

Hvis ledelsens redegørelse er et separat dokument, skal systemrevisor udarbejde en udtalelse til dette separate dokument.

Brug af systemrevisionserklæringen

Som modtager af systemrevisionserklæringen er der nu flere informationer de tilknyttede pengeinstitutter og de interne og eksterne revisorer for pengeinstitutterne skal forholde sig til.

Vurdering af ledelsens udtalelse og revisors erklæring
Som altid bør man starte med at gennemgå og vurdere ledelsens udtalelse og revisors erklæring, med henblik på at vurdere scope af erklæringen samt om der evt. måtte være fremhævelse af forhold der er relevante for pengeinstituttet, eller om der er forbehold i erklæringen.

Vurdering af beskrivelsen
Dernæst bør man som modtager af systemrevisionserklæringen gennemgå beskrivelsen for at sikre, at beskrivelsen og derved erklæringen dækker over de systemer mv. som man forventer og har behov for at få afdækket.

Herudover skal man i forbindelse med vurderingen af beskrivelsen forholde sig til om beskrivelsen giver information der er behov for i forhold til at kunne vurdere kontrolmiljøet hos datacentralen for at kunne sikre, at pengeinstituttet efterlever krav til system-, data- og driftssikkerhed.

Særligt beskrivelsens afsnit omkring komplementære kontroller skal have fokus, da der her vil være omtalt kontrolaktiviteter man selv som brugerorganisation skal have implementeret, og som skal fungere effektivt, for at datacentralens kontroller vil fungere effektivt. Som intern og ekstern revisor for pengeinstituttet skal det sikres pengeinstituttet har designet og implementeret kontroller svarende til de komplementære kontroller datacentralen har identificeret, og at de har fungeret effektivt.

Da revisionen udføres inden systemrevisionserklæringen er afsluttet og endelig, vil intern og ekstern revision i pengeinstituttet ofte basere sin revision på sidste års komplementære kontroller.

Vurdering af kontroller og kontrolafvigelser
Herefter bør man som modtager af erklæringen foretage en gennemgang af hvilke kontrolaktiviteter datacentralen udfører, og selv foretage en vurdering af om kontrolaktiviteterne er tilstrækkelige for at afdække de risici man selv har identificeret, og om det er tilstrækkeligt i forhold til pengeinstituttets system-, data- og driftssikkerhed.

Hvis det vurderes at kontrolaktiviteterne ikke er passende til at afdække de risici der er identificeret, så skal man enten selv implementere kontroller til at afdække risici, eller som minimum reducere risikoen til et acceptabelt niveau. Alternativt kan man indgå dialog med datacentralen om hvorvidt erklæringen fremadrettet bør medtage supplerende kontrolaktiviteter.

Når kontrollerne er vurderet, skal man efterfølgende forholde sig til de afgivelser systemrevisor har konstateret.
Indledningsvis skal man vurdere om afvigelsen vedrører systemer / tjenester som er relevant for pengeinstituttets egen regnskabsaflæggelse og system-, data- og driftssikkerhed.

Hvis afvigelsen vedrører systemer / tjenester der er relevant for pengeinstituttet, skal pengeinstituttet vurdere hvilken indvirkning afvigelsen har på pengeinstituttets egen regnskabsaflæggelse og system-, data- og driftssikkerhed, og så enten udføre kompenserende kontrolaktiviteter lokalt, eller rapportere at der er ineffektive kontrolaktiviteter, hvorefter der så bør foretages substantive tests for at reducere risikoen til et acceptabelt niveau.

Gennemgang af datacentralens ledelsesredegørelse
Det nye element i systemrevisionserklæringerne, datacentralens ledelsesredegørelse, er hvor man som modtager af erklæringen bør sætte ind i forhold til vurderingen af erklæringen.

Datacentralens ledelsesredegørelse vil hjælpe modtager pengeinstituttet med at identificere risici og indvirkningen på pengeinstituttet, da datacentralen kommer med sin vurdering af risici og indvirkning, som måske afviger fra pengeinstituttets egen initielle vurdering.

Datacentralens ledelsesredegørelse kommer også med inspiration til hvilke komplementerende kontrolaktiviteter pengeinstituttet kan udføre for at enten afhjælpe risikoen, eller reducere den til et acceptabelt niveau.

Herudover skal man som modtagende pengeinstitut også bruge datacentralens ledelsesredegørelse til at vurdere om datacentralens handlingsplaner for at afhjælpe afvigelsen er tilstrækkelige, eller om man som tilknyttet pengeinstitut har behov for at stille yderligere krav til af-

hjælpningen, eller hastigheden hvorpå afhjælpningen forventes gennemført.

Fremtiden

Opdateringen af systemrevisionsbekendtgørelsen var meget drevet af at systemrevisionserklæringerne skulle medtage relevante krav fra ledelsesbekendtgørelsens bilag 5.

Med de kommende regler omkring NIS2 og DORA vil der formentligt ske en ny opdatering af systemrevisionsbekendtgørelsen og/eller ledelsesbekendtgørelsens bilag 5, og derved opdatering af krav til systemrevisionserklæringens indhold. Muligvis vil Ledelsesbekendtgørelsens bilag 5 helt udgå, da der er mere detaljerede krav i DORA der måske vil blive henvist til i stedet.

I forhold til regulering, så er fællesejet datacentraler ikke omfattet af DORA, men er i stedet omfattet af NIS2.

Med de overordnede krav der er i NIS2, og indholdet af de nuværende systemrevisionserklæringer, vil der formentligt ikke være behov for at medtage yderligere oplysninger eller kontroller i systemrevisionserklæringerne fremadrettet.
De noget mere omfattende og detaljerede krav i DORA, vil formentligt medføre at de tilknyttede pengeinstitutter vil have behov for yderligere information for at kunne efterleve DORA og kravet omkring monitorering af forsyningskæden.

De primære fællesejede datacentraler i Danmark (Bankdata, BEC, SDC og JN Data) har igangsat arbejdet med at identificere behovet for yderligere rapportering i henhold til DORA, og en model for hvordan dette kan gøres. Arbejdet er lige igangsat, så der er pt. ikke noget oplæg til hvordan DORA kan blive indarbejdet i systemrevisionserklæringerne.

Afslutning

Med den nuværende systemrevisionsbekendtgørelse er der kommet en del nye elementer til, som både påvirker systemrevisor ved gennemførelse af revisionen til systemrevisionsbekendtgørelsen, men også påvirker modtagerne af systemrevisionserklæringen.

Den største ændring er datacentralens redegørelse hvormed der gives meget mere information i systemrevisionserklæringen end hidtil.

Som systemrevisor er der derved mere information hvor det skal sikres at der er en sammenhæng til den foretagne revision.

Som modtager af systemrevisionserklæringen vil man modtage mere information, således at der vil være et større og bedre grundlag til at foretage sin risikovurdering og vurdering af system-, data- og driftssikkerhed, samt at man som modtager af de nye systemrevisionserklæringer med datacentralens redegørelse, modtager mere information omkring sikkerheden af de it systemer der er outsourcet, samt hvordan serviceleverandøren arbejder med at styrke informationssikkerheden.

De øvrige nyskabelser er primært etableret for at skabe bedre overblik for modtagerne af erklæringerne.

Den opdaterede systemrevisionsbekendtgørelse har således medført lidt mere man skal udføre, både som afgivende systemrevisor og som modtagende intern og ekstern revisor i pengeinstitutterne.

Noter

[1] BEK nr 1581 af 22/12/2022
[2] BEK nr. 1103 af 30/06/2022

Nye medlemmer

Nye medlemmer i IIA fra 30.09.2024 - 8.12.2024

A.P. Møller-Mærsk
Nolubabalo Mbophane
Arpan Prasad
Natasha Rajcomar

Bankdata
Mie Kathrine Holdt

BEC
Lasse Arenholt Rosengaard

Deloitte
Claus Brix Flensberg

EIFO
Selma Onurlu

Middelfart Sparekasse
Mai-Britt Soo

Nordea
Sean Spalding
Dmitrijs Hodoss

PenSam
Vanja Skougaard

PwC
Annalena Beierke

Saxo Bank
Reece Hamilton

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.

18.12.2024: Virtuelt: Finanstilsynet, Julemøde
8.4.2025: Temadag for den finansielle sektor
21.5-22.5.2025: IIA Årsmøde 2025, Comwell, Odense
10.1.2025: Mød en Intern Revision: Carlsberg
16.1.2025: Business Ethics in Theory and Practice

"Bagsmækken"

Foreningens adresse

Foreningen af Interne Revisorer (IIA Denmark)
Intern revision
Nykredit
Sundkrogsgade 25
2150 Nordhavn

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

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, CIA, CFSA
Christoffer Max Jensen
Arbejdernes Landsbank
☎ 21 12 52 41 ✉ cmj@al-bank.dk

Kasserer
Revisionschef, CIA
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
BDO Statsautoriseret revisionsaktieselskab
☎ 30 65 41 30 ✉ bisve@bdo.dk

Chief Internal Auditor
Mie Kristine Bolt Therkelsen
Nordea Kredit Realkreditaktieselskab
☎ 40 61 28 11
✉ mie.kristine.bolt.therkelsen@nordea.com

Intern Revisionschef
Lars Maagaard
Nykredit
☎ 61 62 18 90 ✉ lma@nykredit.dk