INFO

Foreningen af Interne Revisorer
Nummer 85 | December 2023 | 28. årgang

Intern Revision som springbræt

3 personer deler deres erfaringer med at tage skridtet fra Intern Revision til første eller anden linje

DORA

Bliv klogere på Digital Operational Resilience Act - og hvad den kommer til at betyde for den finansielle sektor

CSRD • ESG • NIS2 • AI • Root Cause Analysis

INFOs redaktion

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

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

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

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

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

Næste nummer
INFO 86 udkommer i april 2024.
ISSN: 1903-7341 (Elektronisk version).

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

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

Forsidefoto
UnknownNet

Redaktionens adresse

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

redaktionen@iia.dk

Synspunkter, der kommer til udtryk i medlemsbladet, behøver ikke nødvendigvis at svare til bestyrelsens opfattelse eller være udtryk for foreningens officielle standpunkt.

Indhold

Nyt fra bestyrelsen

Referater fra bestyrelsesmøder lægges på foreningens hjemmeside umiddelbart efter mødernes afholdelse. Du kan her løbende holde dig opdateret på bestyrelsens arbejde på hjemmesiden under "Nyheder".

www.iia.dk

Leder

Claus Sonne Linnedal, Audit Director, Senior Vice President, Danske Bank

Velkommen til et nyt nummer af INFO …

… hvor du kan få indblik i ny områder samt "tanke viden op" fra vores branche. I IIA's bestyrelse har vi de sidste par år arbejdet på at gøre vores fælles forening endnu mere slagkraftig og dermed sikre en fremtidig stærk og robust intern revisionssektor til glæde for både vores branche men også for samfundet omkring os.

Men hvad er det IIA skal tilbyde i fremtiden? og hvilken rolle har bestyrelsen, udvalgene og os alle som medlemmer?

Helt grundlæggende rummer IIA en enorm mængde viden og metode, som vi alle har glæde af i forbindelse med vores daglige arbejde. Dette kan vi blandt andet læse om i INFO tre gange om året. Derudover udbydes en lang række certificeringer og vi stiller træning samt konferencer til rådighed til meget konkurrencedygtige priser. Og så er IIA et netværk, der består af os alle sammen og den viden vi samler har kun værdi når der er en afsender, en modtager og en snitflade, hvor den kan anvendes.

IIA er derfor både dig og mig! Vi er afhængige af hinanden og for at det skal være mest muligt frugtbart og produktivt, skal der være balance i relationerne. Det er cirka den samme historie I hører nede i svømmeklubben og ovre til fodbold. Det fungerer kun hvis vi alle arbejder sammen og giver en smule af os selv til fællesskabet. Der er heldigvis en lang række af vores medlemmer der er formidable til at få nye ideer og producere information til træning, konferencer og vores nyhedskanaler. Men hvis vi er flere til at dele arbejdet imellem os, bliver det langt mere attraktivt for den enkelte og vi slider ikke ildsjælene op.

Spørg ikke kun hvad IIA kan gøre for Dig men også hvad Du kan gøre for IIA!

I dette nummer stiller vi blandt andet skarpt på hvordan Intern revision kan være springbræt til andre og alternative karriereveje. Vi er alle klar over, at man som intern revisor besidder nogle værktøjer og metoder og opsamler en del viden, som er særdeles værdifuld i mange andre sammenhænge. Vi ser det blandt andet i 2 LoD – risk and compliance. Vi skal derfor være i stand til at træne og producere endnu flere interne revisorer for at opfylde dette behov i fremtiden.

Vi har også et indlæg om Intern Revisions rolle ift. ESG og CSRD rapportering. Og assurance og erklæringsarbejde indenfor NIS2 er også et varmt emne i nogle segmenter, mens det er DORA der er øverst på agendaen i den finansielle sektor.

For bare et år siden var der ikke mange der talte om AI.

Men med GenAI og ChatGPT er der opstået nogle helt nye muligheder, som både skaber nye perspektiver og muligheder, men også åbner op for nye risici. Der findes både de generiske AI værktøjer som er åbne for alle via apps, men dertil ser vi en tiltagende tendens til at de store virksomheder opbygger egne GenAI services baseret på standardværktøjer i markedet. Det bliver ikke kedeligt at følge denne udvikling og vi har også et indlæg om AI forordningen i INFO.

Så sæt dig tilbage i stolen og se frem til en inspirationspause i godt selskab mens du venter på julegaverne.

Glædelig jul og godt nytår!

Nyt fra redaktionen

Birgitte Rousing Svenningsen, bestyrelsesmedlem IIA, Revisius Consulting, CIA, CISA

Redaktionen og bladet er intet uden de frivillige kræfter, som redaktionsmedlemmerne bidrager med. Jeg er derfor glad for den tid, som Lars Geisler, Kim Nehls, Avelina Nielsen og Martin Tripax har lagt i at samle artiklerne til dette nummer af INFO. Stor tak til jer alle.

Stort tak til Kim og Stine

En særlig tak skal lyde til Kim Nehls, som efter 4 år i redaktionen har valgt at sige farvel til redaktionen for at bruge mere tid på studier. Kim har over årene været inspireret af de ting, som lægger os alle på læberne lige nu. Om det så har været ESG, Green-washing eller Chat-GPT, så har Kim på imminent vis fundet forfattere som har delt deres ekspertviden med os læsere.

I enkelte tilfælde har Kim endda taget førertrøjen på og selv spidset pinden, og endelig har Kim været vores trofaste spion og opsamlet artikler af særlig interesse fra IIA Global's blad Internal Auditor. På den måde har vi som danske medlemmer haft en let adgang til de mest spændende artikler fra vores moderorganisation. Vi vil i redaktionen komme til at savne Kim, men vi vil også ønske ham god læselyst med sine studier.

Jeg vil også benytte lejligheden til at sige tak for det arbejde som Stine Juhl-Hansen har lagt i redaktionsarbejdet.

Stine har forladt redaktionen, idet hun fremover vil stå i spidsen for den årlige IT Sikkerhedskonference, som arrangeres i samarbejde mellem IIA, ISACA og FSR.

Vi vil i redaktionen også komme til at savne Stine, som med sin baggrund har bidraget med ideer til aktuelle IT-artikler, og som med sit store netværk har skabt kontakten til mange interessante forfattere. Selv om vi er ærgerlige over, at Stine er trådt ud af redaktionen, er vi glade for, at hun vil lægge sine kræfter i arrangering af IT Sikkerhedskonferencen.

Med Stines bidrag og erfaring fra at arrangere konferencer for SheLeads, er vi sikker på, at IT Sikkerhedskonferencen også de kommende år vil omfatte aktuelle og spændende emner med kompetente foredragsholdere.

Er redaktionsarbejdet noget for dig?

Nu har vi sagt farvel til Kim og Stine. Det har været en fornøjelse af have dem med i redaktionen og sidder du og har lyst til at bidrage med nogle få timer til redaktionsarbejdet, hører vi gerne fra dig.

Vi er en lille gruppe og vi synes selv, at vi har det hyggeligt og er med til at påvirke agendaen inden for intern revision. Som udgangspunkt skriver vi ikke artikler selv, men kigger os rundt efter aktuelle emner og får eksperter til at skrive artiklerne herom til gavn for vores medlemmer. På den måde hjælper vi os selv og vores kollegaer til at lære nyt.

Se mere om vores arbejde og hvordan du bliver en del af det på næste side.

Vi ser frem til at høre fra dig.

Bliv en aktiv del af IIA!!!!

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

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

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

De nye IIA revisionsstandarder er lige på trapperne

Birgitte Rousing Svenningsen, bestyrelsesmedlem IIA, Revisius Consulting, CIA, CISA

Du husker måske, at jeg i april 2023 skrev, at IIA's revisionsstandarder var under ændring og på daværende tidspunkt var sendt i høring. De 10 væsentligste ændringer, som var foreslået, var:

- Nyt navn
- Ny struktur
- Nyt afsnit i hver standard
- Nyt formål med intern revision
- Nye etiske standarder
- Nye standarder for forholdet mellem bestyrelsen og revisionschefen
- Nye krav til kvalitetssikring
- Speciel fokus på den offentlige sektor
- Øget fokus på interessenter og offentlighedens interesse
- Nye begreber og opdateret ordliste.

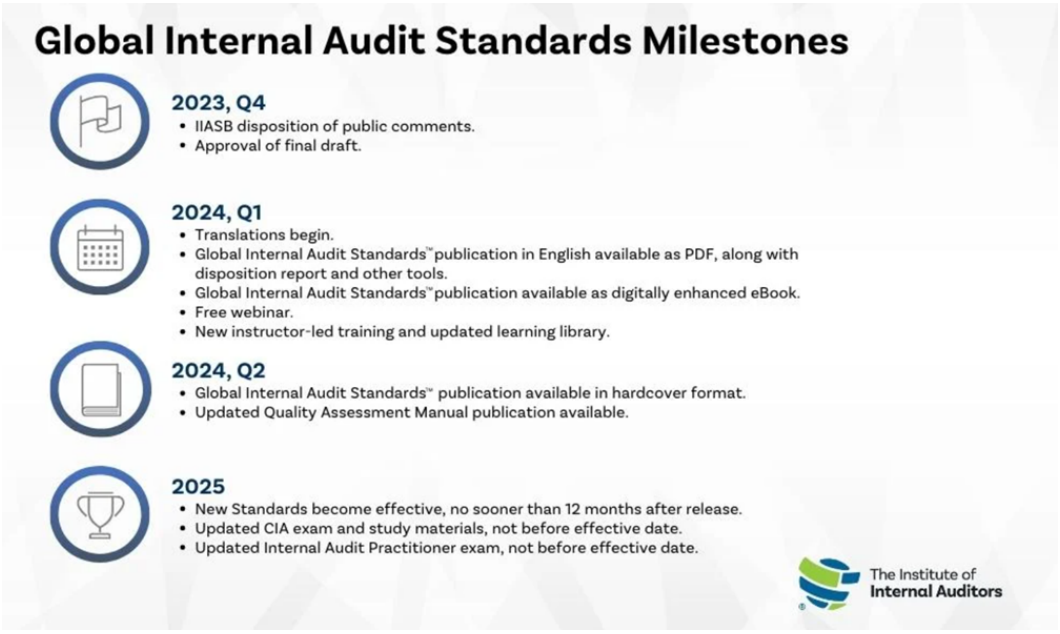
Se yderligere beskrivelse af de enkelte ændringer i INFO 83.

Selv om IIA modtog 19.000 kommentarer til standarderne fra 1.612 personer, skal man ikke forvente, at de endelige standarder bliver væsentlige forskellige fra udkastet. Kommentarerne vedrørte primært:

- Manglende anvendelse af ordet "must"
- Uklare krav til eksterne kvalitetsvurderinger
- Vag formulering af formålet med intern revision
- Manglende krav til efteruddannelsestimer og kompetencer i intern revision
- Manglende definition af direktionens ansvar i forhold til intern revision, hvorimod kravene til bestyrelsen var formuleret for direkte
- Uklar sondring mellem intern revisions mandat og funktionsbeskrivelsen for intern revision
- Forvirring om passende mål for intern revision
- Manglende adskillelse af kravene til "assurance" og rådgivningsopgaver
- Uklare krav til intern revision om at komme med anbefalinger på løsning af observationerne
- Uklare krav til rating af overordnet resultat og de enkeltstående observationer
- Uklare krav til overordnet konklusion i den endelige afrapportering.

Planen er, at IIA udgiver de nye standarder i januar 2024 på engelsk. I første omgang vil det være en elektronisk udgave af standarderne, men de forventes udgivet i bogform i marts 2024. Der forventes justeringer på ovenstående 11 områder, men ikke noget revolutionerende i forhold til udkastet.

Alt i alt bliver det spændende at se, hvor meget de nye standarder kommer til at påvirke vores hverdag. Derfor hold øjne åbne i januar og læs de nye standarder, når de bliver tilgængelige. Jeg har nedenfor indsat IIA's tidsplan for udgivelsen af standarderne. Vi vil også i kommende numre af INFO vende tilbage og dykke mere ned i ændringerne.



IIA PRISEN

Prisopgave om intern revision

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

25.000 kr.

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

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

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

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

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

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

Med implementering af CSRD-direktivet er væsentlige forandringer inden for bæredygtighedsrapportering på vej

Lars Fermann, Partner, Head of Climate & Sustainability Service, EY

Indledning

CSRD-direktivet medfører nye og væsentligt mere omfangsrige og komplekse krav til bæredygtighedsrapportering, som gælder for regnskabsår, der starter 1. januar 2025 eller senere for regnskabsklasse C stor. De store børsnoterede virksomheder med mere end 500 ansatte skal allerede implementere reglerne for regnskabsår, der starter 1. januar 2024 eller senere.

I henhold til lovudkastet er formålet med CSRD-direktivet at forbedre virksomheders bæredygtighedsrapportering for derigennem bedre at udnytte potentialet i at få virksomhederne i EU til at bidrage til opnåelse af målene i EU's Green Deal og FN's Verdensmål. Arbejdet med bæredygtighedsrapportering vurderes at være centralt for erhvervslivets grønne omstilling, og det er vigtigt, at bæredygtighedsrapporteringen bliver troværdig og anvendelig for investorer, långivere, kreditorer m.fl.

Målet er, at investorer, långivere og andre interessenter bedre kan vurdere virksomhedernes bæredygtighed og kanalisere finansiering og efterspørgsel i retning af de mest bæredygtige virksomheder.

Overordnede krav i bæredygtighedsdirektivet

CSRD-direktivet (bæredygtighedsdirektivet) sætter de overordnede krav til den nye bæredygtighedsrapportering. Det fremgår af CSRD-direktivet, at kravene skal udfyldes med egentlige bæredygtighedsstandarder, der skal fastsætte de detaljerede krav til virksomhedernes bæredygtighedsrapportering. EFRAG (European Financial Reporting Advisory Group) har på vegne af EU-Kommissionen fået til opgave at udarbejde udkast til de europæiske bæredygtighedsstandarder (ESRS-standarderne).

De nye krav adskiller sig væsentligt fra den praksis, der findes i dag, og vil kræve væsentlige nye processer og ressourcer for de omfattede virksomheder. Bæredygtighedsrapporteringen omfatter bl.a. detaljerede krav til virksomhedernes rapportering om klima og miljø, menneske- og arbejdstagerrettigheder og andre sociale forhold samt ledelsesmæssige forhold. Virksomhederne kan blive omfattet af mere end 1100 kvantitative og kvalitative datapunkter og er dermed underlagt væsentligt udvidede og standardiserede oplysninger om en række bæredygtighedsforhold i forhold til de nuværende krav.

Som en yderligere nyskabelse skal revisor fremadrettet afgive en erklæring om bæredygtighedsrapporteringen med i første omgang begrænset sikkerhed, hvor der efter de gældende regler alene kræves en udtalelse baseret på et såkaldt konsistenstjek. Bæredygtighedsdirektivet indebærer således ikke kun ændringer til årsregnskabsloven, men også ændringer i bl.a. revisorlovgivning.

Det må forventes, at danske virksomheder skal anvende ressourcer i form af såvel løbende administrative omkostninger samt omkostninger til at gennemføre "omstilling" til ny rapportering, indsamling af data m.v. Det har også været fremført, at hastigheden, hvormed virksomhederne skal foretage denne "omstilling", pålægger virksomhederne en relativ stor byrde.

Hvordan implementeres de nye krav til bæredygtighedsrapportering i dansk lov?

Ændringer til årsregnskabslovens § 99a implementerer bæredygtighedsdirektivet i årsregnskabsloven. Dette skal sikre, at rammerne for bæredygtighedsrapporteringen så vidt muligt er gengivet i årsregnskabsloven.

ESRS-standarderne skal derimod ikke implementeres i årsregnskabsloven. Disse vedtages af EU-Kommissionen ved en delegeret retsakt og er dermed direkte gældende i medlemsstaterne.

Virksomhedernes pligt til at rapportere efter de til enhver tid gældende standarder for bæredygtighedsrapportering tilvejebringes ved at indføre bestemmelser, der direkte henviser til de delegerede retsakter, som løbende vedtages af EU-Kommissionen. Dette reducerer behovet for løbende at ændre i årsregnskabsloven som følge af ændringer til ESRS-standarderne.

Bæredygtighedsstandarder (ESRS-standarder)

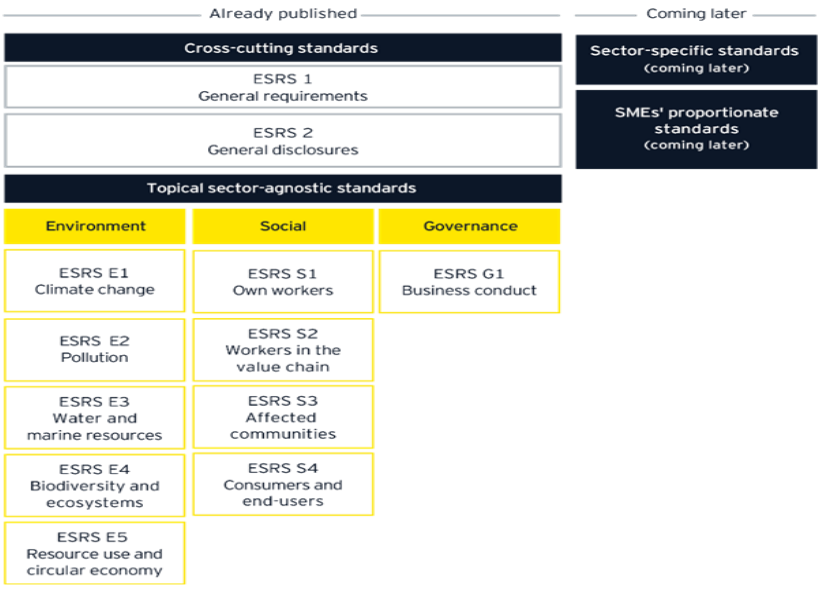
De europæiske bæredygtighedsstandarder (ESRS'erne), fastsætter det nærmere indhold af de oplysninger, som virksomhederne skal rapportere om. Det første sæt af standarder (12 i alt) blev vedtaget af EU-Parlamentet i juli 2023 og finder anvendelse for alle virksomheder omfattet af CSRD-direktivet. Standarderne omfatter såkaldte "cross cutting"-standarder (ESRS 1 og ESRS 2), og standarder inden for "Environment" (ESRS E), "Social" (ESRS S) og "Governance" (ESRS G). Derudover er sektorspecifikke standarder under udarbejdelse - se **Figur 1** på næste side.

De nye krav medfører, at de omfattede virksomheder som en del af en særskilt sektion i ledelsesberetningen skal rapportere ifølge ESRS'erne. Af de 12 ESRS'er er kun ESRS 1 og ESRS 2 obligatoriske. ESRS 1 omfatter

ingen rapporteringskrav, men beskriver ESRS'ernes arkitektur, grundlæggende begreber og fastsætter generelle krav til udarbejdelse og fremlæggelse af bæredygtighedsrelaterede oplysninger, herunder kravene til dobbelt væsentlighed som grundlag for bæredygtighedsrapportering. ESRS 2 er obligatorisk for alle omfattede virksomheder, og fastsætter oplysningskrav vedrørende de oplysninger, som virksomheden skal fremlægge på et generelt plan på tværs af alle bæredygtighedsspørgsmål. ESRS 2 indebærer konkrete rapporteringskrav vedrørende områderne styring, strategi, virkning, risiko- og mulighedsstyring samt parametre og mål. Denne ESRS giver et dybdegående indblik i emner som 'risikostyring og intern kontrol med bæredygtighedsrapportering', 'strategi, forretningsmodel og værdikæde' og 'interessenternes interesser og synspunkter'. Indeholdt i ESRS 2 er der 12 generelle rapporteringskrav med +125 tilhørende kvalitative og kvantitative datapunkter.

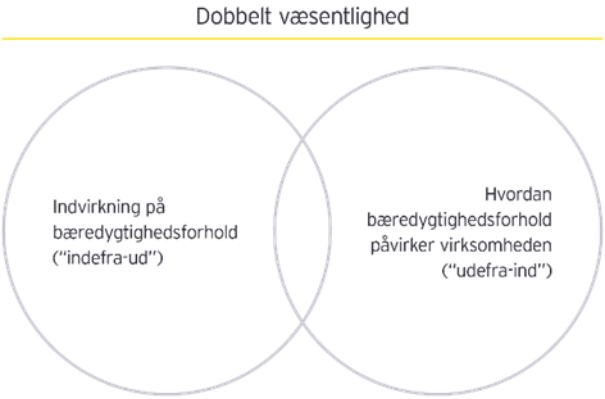
De resterende 10 ESRS'er er emnespecifikke, og dækker miljømæssige (Environmental, E), sociale (Social, S), og ledelsesmæssige (Governance, G) standarder. Der er fem miljømæssige standarder, fire sociale og en ledelsesmæssig. De 10 standarder omfatter 37 under-emner og 73 under-under emner. Indeholdt i de 10 emnespecifikke standarder er der desuden 70 rapporteringskrav med +900 tilhørende kvantitative og kvalitative datapunkter.
Den helt store forskel mellem de tværgående standarder, ESRS 1 og ESRS 2, og de emnespecifikke standarder, er at virksomheder kun skal rapportere på de emnespecifikke standarder, i tilfælde af at de er vurderet væsentlige baseret på princippet om dobbelt væsentlighed. Alle virksomheder skal dermed ikke nødvendigvis rapportere på alle +900 datapunkter.

Figur 1. De europæiske bæredygtighedsstandarder (ESRS'erne)



Dobbelt væsentlighed

Med lovudkastet bliver det en pligt for virksomhederne at anvende det dobbelte væsentlighedsprincip, som er en metode til at forstå virksomhedens indvirkning på bæredygtighedsforhold ("indefra-ud"), og hvordan bæredygtighedsforhold påvirker virksomhedens udvikling, resultat og situation ("udefra-ind"). Resultatet af virksomhedens dobbelte væsentlighedsvurdering er bestemmende for de oplysningskrav, som virksomheden skal medtage i sin redegørelse om bæredygtighed ud fra ESRS-standarderne.



Virksomheder skal altså foretage en væsentlighedsvurdering, for at identificere de væsentlige virkninger, risici og muligheder der skal rapporteres. Dobbelt væsentlighed har to dimensioner: virkningens væsentlighed og finansiel væsentlighed.

Virkningens væsentlighed: Et bæredygtighedsspørgsmål er væsentligt ud fra et påvirkningsperspektiv, når det vedrører virksomhedens væsentlige faktiske eller potentielle, positive eller negative virkninger på mennesker eller miljøet på kort, mellemlang eller lang sigt.

Finansiel væsentlighed: Et bæredygtighedsspørgsmål er væsentligt ud fra et finansielt perspektiv, hvis det udløser eller med rimelighed kan forventes at udløse væsentlige finansielle virkninger for virksomheden.

De to dimensioner er indbyrdes forbundne og en virkning kan vurderes væsentlig på en af dimensionerne eller begge. For at vurdere væsentlighed skal virksomheden sætte passende kvantitative eller kvalitative tærskler, da tærsklerne afgør hvilke virkninger, risici og muligheder er er væsentlige i forbindelse med rapporteringen.

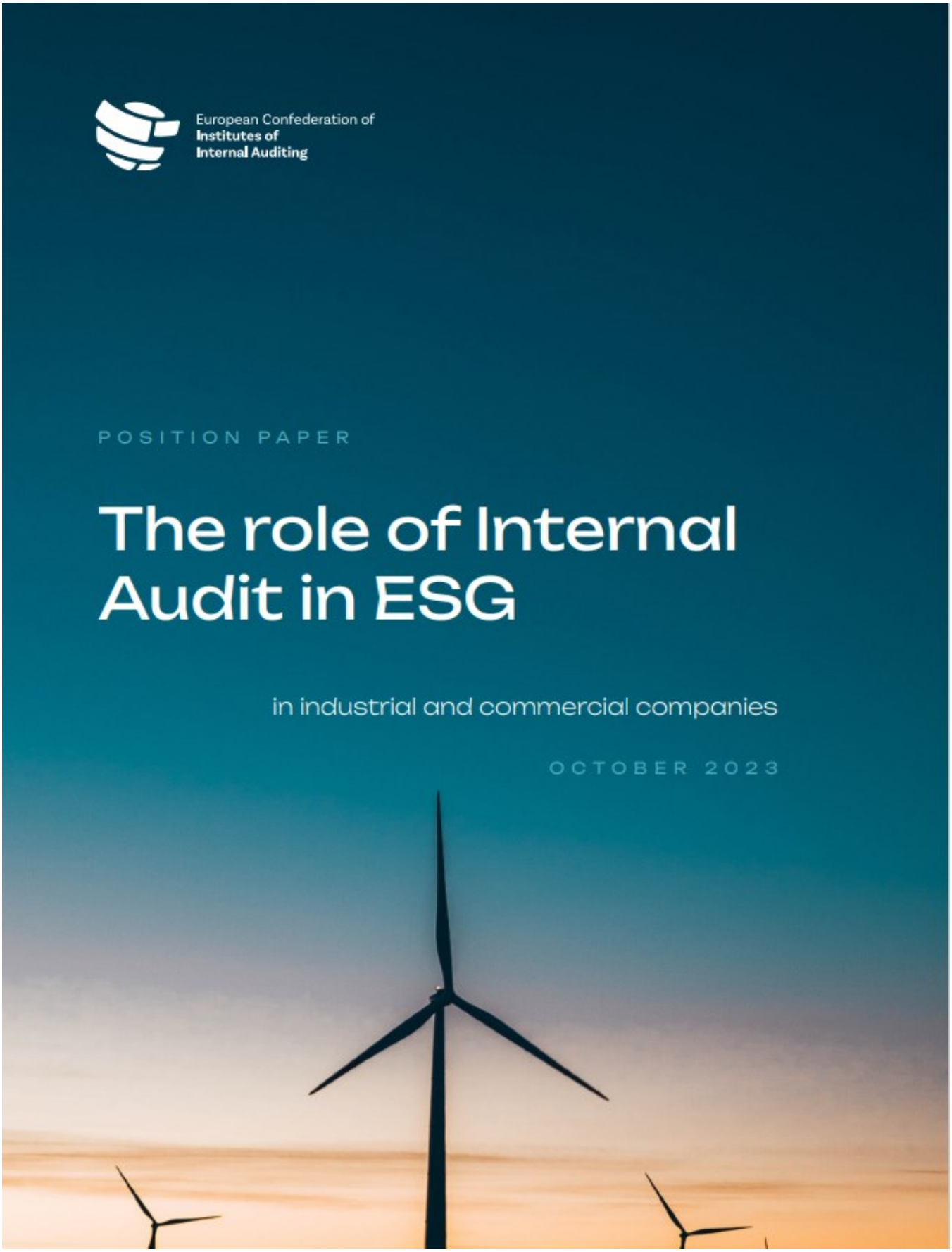
Processen bag den dobbelte væsentlighedsvurdering er underlagt revision med begrænset sikkerhed i samme omfang

som rapporteringen i øvrigt. Dette betyder at væsentlighedsvurderingen skal dokumenteres og at beslutninger truffet vedrørende væsentlighed skal træffes på et transparent grundlag. Her kan revisorer være behjælpelige med hvilken dokumentation der bør supplere processen bag væsentlighedsvurderingen.

Indfasning af ESRS'erne

Der indføres bestemmelser, hvorefter børsnoterede små og mellemstore virksomheder kan begrænse deres bæredygtighedsrapportering til at følge de særlige standarder, som EU-Kommissionen vedtager for netop denne type virksomheder. Desuden er der indfasninger for alle virksomheder, eksempelvis at virksomheden i de første tre år efter ikrafttrædelsestidspunktet kan undlade detaljeret information om værdikæden. For virksomheder med under 750 ansatte gælder yderlige lempelser, hvor rapportering på dele af ESRS'erne indfases over en periode på op til fem år.

Indfasningerne har til formål at lette den administrative byrde for omfattede virksomheder, og dertil at facilitere en lettere prioritering af indsatser i forhold til bæredygtighedsrapporteringen og det arbejde der skal lægger bag. Det vil nemlig være nødvendigt for omfattede virksomheder at prioritere for at nå i mål med CSRD. Det vil kræve ressourcer at nå i mål, men processen kan også være værdiskabende for de virksomheder, der evner at gribe de muligheder.


European Confederation of
Institutes of
Internal Auditing
POSITION PAPER
The role of Internal Audit in ESG
in industrial and commercial companies
OCTOBER 2023

INTRODUCTION

Our world faces several global challenges such as climate change, transitioning from a linear economy to a circular one, increasing inequality, and balancing economic needs with societal needs. Many stakeholders including investors, regulators, consumers and employees are now increasingly demanding that companies should not only be good stewards of (financial) capital but also of natural and social capital and have the necessary governance framework in place to support this. Furthermore, investors are incorporating ESG elements into their investment decision making process, making ESG increasingly important.

The purpose of this document is to create awareness of the role that Internal Audit could play in this journey, with specific focus on Industrial and Commercial companies. Regardless of the level of maturity of each company on ESG, the added value of Internal Audit ranges from a more advisory role such as, assisting in setting up corporate culture and behavior changes towards a sustainability embedded decision-making process and strategy in less mature environments, to a pure independent assurance role where the ESG agenda is already well embedded in organizations.

With the new upcoming Regulations deeply impacting the way the organizations operate, there is an important call now for Boards and Top Management to recognize that Internal Audit, while remaining independent, could help them in this important journey.

VARIOUS REGULATIONS AND THE DIFFERENT MATURITY IN ESG

The spotlight on ESG commitments and reporting continues to expand, as stakeholders increasingly demand organizations to drive a sustainable business, providing evidence of ESG progresses achieved. ESG reporting is quickly moving from a voluntary to a mandatory activity, with Regulators accelerating the interest on corporate responsibility, as part of the Journey for the European Green Deal.

The European Commission recently revised the **Corporate Sustainability Reporting Directive (CSRD)** to modernize and strengthen the rules with the objective of accelerating the transition towards a more sustainable economy. The new CSRD, that will take effect from FY 2024, enlarges the scope to be covered, expecting to quadruple the number of covered organizations.

A strong intent of CSRD is to standardize and simplify sustainability reporting for companies, consolidating this into a one ESG report that meets the needs of EU community (Consumers, Regulators, Investors, and other stakeholders). The CSRD standards (**European Sustainability Reporting Standards — ESRS**, with a first set issued in July 2023) are designed to make corporate sustainability and ESG reporting within the EU more accurate, common, consistent, comparable, and standardized, just like financial reporting. The ESRS has been developed taking into account the existing EU law and initiatives (e.g. double-materiality principle, Climate Law and Taxonomy Regulation). The assurance by an independent provider becomes compulsory with CSDR: limited assurance applicable from FY 2024 and the goal is to extend to reasonable assurance in the medium term, with a horizon of 3 years.

As part of a set of measures under definition by the EU to support the ESG evolution, the EU proposal for the **Corporate Sustainability Due Diligence Directive (CSDDD)** is of particular importance for industrial companies. It is designed to foster sustainable and responsible corporate behavior throughout global value chains (with focus on human rights and environmental impacts in supply chains). It should be noted that Certain EU countries — such as Germany and the Netherlands — have already moved ahead with country-specific laws.

The European regulatory landscape is complex with several initiatives that will impact organizations particularly the E & the S (e.g., green claims directive, forced labor ban, work life, and Diversity and Inclusion Directive). Multinational companies will also have to deal with the difficulties arising from the geographical operations, given

that each country will bring local emphasis or accents when transposing these EU regulations into the respective national laws.

In this articulated environment, we observe various levels of ESG maturity amongst different organizations1 ; it is time for everyone to start embedding ESG in the organizations[1] and engage the assistance of internal audit in this evolving process, adding value.

THE INTERNAL AUDIT AND THE OTHER FUNCTIONS INVOLVED IN THE ASSURANCE PROCESS IN INDUSTRIAL AND COMMERCIAL COMPANIES

Internal Audit represents a key counterpart for Governing Bodies and Management providing objective assurance and insight on the effectiveness and efficiency of risk management, internal control, and governance processes. Internal Audit is best positioned to provide assurance when its resource level, competence, and structure are **aligned with organizational strategies** and when it has the in-depth understanding of business systems and processes.

Independence does not mean isolation! Each Internal Audit needs to cooperate with other relevant players accountable for governance, risk management and internal controls. **The Three Lines Model**, published by The Institute of Internal Auditors, clarifies each player's role and the interactions.

Internal Audit, with its independence from Management has a third line role and is the only function within the company able to provide independent and objective assurance. However, it should be considered that besides Internal Audit, industrial & commercial companies generally have other distinct functions that provide a certain level of assurance (as second line), that is relevant also for ESG purpose.

In particular, Internal Audit — while maintaining its independence – due to its privileged transversal perspective, plays a **key role in guaranteeing collaboration, cooperation and communication** between the different assurance providers (internally and externally) to collectively contribute, in a more efficient and effective way, to the creation and protection of value for ESG progress.

The key purpose of this chapter is to create awareness about the assurance providers as they provide a level of assurance that needs to be taken into consideration by Internal Audit in its role of supporting the Governing Body and Management with objective assurance, insights, and advice on ESG matters.

Below is a list of the most common assurance providing functions in industrial and commercial companies, whose presence and role varies according to the maturity of the organization:

- **Compliance function** — with the calls for more transparency and openness in companies growing increasingly louder, the role of Compliance functions is becoming more and more relevant as they provide support to the organizations in enhancing structures and processes aimed at guaranteeing corporate and regulatory compliance. The topics that follow under the umbrella of Compliance can vary based on the industry and country, from data privacy (e.g. GDPR, including customer consent, relevant for the commercial processes), anti-trust and competition, crime prevention and anti-corruption, trade sanctions to environmental, labor and Code of Conduct.
- **Health, Safety & Environmental function (HSE)** — all manufacturing companies generally have an HSE function that provides governance rules and guidelines to identify, assess, prevent, and mitigate potential hazards in the workplace or environment and ensure compliance with local regulations. A well-developed and mature HSE management represents a fundamental support in the ESG journey.
- **Human Resources (HR)** ensures that the company complies with social and labor laws and regulations – both in a production and non-production environment — but also plays a key role in ESG assurance (e.g. promoting Equality, Diversity and Inclusion in the Workplace).
- **IT risk, information security and cybersecurity** department support companies in protecting data and information systems from inappropriate access, manipulation, modification and destruction. Although cybersecurity has long been viewed as an IT issue, the effects of breaches, nefarious use and social engineering extend well beyond the purview of IT, and it is now regarded as a key ESG concern, falling under the "Social" pillar. Although cybersecurity as an ESG metric is still a relatively new stance, all evidence points to increasing and continued interest across the Board. Imperative here, is that risk should be evaluated in conjunction with the sharp evolution of the Artificial Intelligence research and development across the organization.
- **Product Quality and Product Development functions** are responsible for standards, rules and operational processes to ensure that products are developed in a sustainable and ethical manner. For manufacturing companies in particular, this includes guaranteeing that products are safe, meet regulatory requirements, and are produced in a socially and environmentally responsible manner.
- **Supply Chain Compliance** plays a critical role in ensuring (through the Third Party management Process, that includes supplier due diligence in terms of economics/finance ratios, corporate and social responsibility, information security, etc.) that the company's suppliers comply with ethical and CSR standards, and with local regulations, providing a certain level of assurance which is relevant for the ESG reporting domain. For companies with international supply chains and commercial networks, they also have to ensure compliance with relevant import / export regulations

and therefore perform control & audit activities on processes and/or suppliers / customers (e.g. sanctions to black listed countries). Many industrial and commercial companies also have certifications (e.g. ISO certifications that cover a range of topics, including quality, information security management systems, environment and health and safety) that represent a tool to support the pillars of sustainable development.

- **Sustainability** is becoming more and more common in the organizations as it provides a certain level of assurance with a crucial role in the to ESG data gathering and reporting process and internal control over Non-Financial Reporting. Nevertheless, Sustainability plays an important role in governing the ESG projects, in alignment with other functions within the organization, making sure that disclosed targets are met.

It should be noted that the list of functions that drive risk mitigation strategies across business units and processes is not exhaustive. In addition, we cannot forget the other functions that are generally present in all the companies, such as Finance, Tax & Legal, ERM, etc.

Considering the increase of demands and complexity of the business and regulatory environments, and several actors involved in the assurance process, it is key that assurance objectives and activities are linked to the company's goals with a holistic and integrated view in supporting the overall company strategy.

ROLE OF IA IN ESG

Potential roles for an Internal Audit in manufacturing companies in the ESG domain

The implementation of credible strategies that support a sustainable value creation is now a business imperative. This requires strong governance over ESG with alignment among all the principal players involved in the process, in particular, a Governing Body, Management (specifically, Sustainability, ERM and Compliance functions, if they exist) and Internal Audit.

Internal Audit, having a systematic and disciplined approach and a very good understanding of the organization, in terms of governance, risks and processes, could play a crucial role supporting companies with **objective assurance, insights, and advice on ESG matters, enhancing credibility and trust**.

Internal audit can begin offering **advisory services** when companies are just getting started in ESG, — e.g. those that were not subject to the EU's Non-Financial Reporting directive (NFRD) and are now just approaching ESG topics also in light of the new law requirements — supporting Management and the Board in the establishment of the ESG governance program. As companies become more mature in the ESG journey, Internal Audit should move to its typical role of **assurance provider**, providing an independent and objective review of the effectiveness of ESG risk assessment, data governance and management, reporting, and related regulatory compliance.

Advisory

Internal Audit can help the organization in defining the **building blocks of good ESG**, with a key role in supporting the corporate culture and behavior changes towards sustainability that is embedded in the decision-making process and strategy. This means for Internal Audit needs to assist organizations to focus on the right priorities, thereby setting impactful yet realistic targets and building culture and expertise, and provide advice on governance practices and internal controls, also raising awareness and sense of urgency to Management and the Board.

Internal audit can embrace the following roles that can add value to an organization's ESG journey, always without compromising its independence or objectivity:

- **Advise on ESG Governance & Strategy**. ESG covers many topics that traditionally are widely dispersed within the organization with no single point of contact, generating difficulties in data collection, reporting and disclosures. Internal audit can facilitate consensus on organizational priorities for ESG ensuring the alignment with the overall Company strategy, convening functions that should be involved in ESG matters, reporting, disclosures, and risk management. A strong ESG governance, with consensus-building conversation between the Board, Management and Internal Audit, is fundamental for the execution of the ESG strategy.
- **Support in the definition of an ESG control environment**. Internal Audit can use its structured approach and framework (e.g., COSO's Internal Control – Integrated Framework) offering its expertise to develop a strong control system to manage and mitigate ESG risks, with the same rigor as controls over financial reporting. Internal audit can also advise on defining specific controls that are sufficiently robust to support external reporting to capital markets. Considering the new requirements – for example, "double materiality" and upcoming Supply Chain obligations, particularly relevant for manufacturing companies – Internal Audit can support in the implementation of these new concepts.
- **Recommend reporting metrics**. Internal audit can provide insights into the kind of data (quantitative and qualitative) that accurately reflect sustainability efforts within the organization, taking into account the already existing process & KPIs. For manufacturing companies, the focus is on data collected to manage the environmental impact of the operations, ensuring safe working conditions for employees, and addressing supply chain risks (e.g data available for certifications).
- **Support in the "double materiality" definition**. While materiality assessment is already an established market practice for companies reporting under NFRD, the CSRD regulation gives to materiality a broader meaning, recognizing the importance of sustainability topics in driving long term financial performance. In particular, CSRD introduces the concept of 'double

materiality" with Stakeholders that are now asked not only to identify most material topics to the organization but to evaluate company's most significant impact on people and the environment, after they have to identify sustainability risks and opportunities for the company. Internal Audit has already started to provide assurance on the materiality matrix required for companies under NFRD and now needs to broaden its scope by initially offering support in the definition of the double materiality approach, supporting stakeholders in this new challenge, leveraging its knowledge of the organization and then gradually moving towards more traditional assurance activities on the double materiality assessment methodology, incorporating a "double materiality" lens of both traditional financial data and non-financial ESG information.

Assurance

As ESG risks become more relevant in decision-making by the Governing Body and Executive Management, companies are moving quickly to disclosing ESG information. Organizations should have assurance on the effectiveness of ESG risk management, including ESG reporting. Internal audit is ideally placed to be a **major assurance provider** and the only independent one in the ESG domain, bringing a systematic, disciplined approach to evaluate and improve the effectiveness of ESG risk management, control, and governance processes.

Assurance over ESG will become increasingly important as this is one of the cornerstones of CSRD, aiming towards a more reliable and comparable Non-Financial Reporting.

While the external auditor will first conduct a review and express an opinion with *limited assurance*, CSRD will later on impose that an external audit expresses an opinion with *reasonable assurance*. In such context, the alignment between internal auditors and external auditors assumes relevance as they both play an important role not conflicting but complementing each other fostering the overall robustness of assurance provided to the Governing Body and Executive Management.

Below are some examples of the relevant assurance activities that can be performed by Internal Audit in manufacturing companies:

- **Review ESG Governance & Strategy**. When the maturity level of the company on ESG increases, Internal Audit can evaluate the effectiveness of the company's governance and oversight of ESG. This can involve reviewing the roles and responsibilities of the Board and Management, and the inclusion of sustainability performance into the overall business strategy, that is fundamental for manufacturing companies considering the unique ESG-risks they are facing.
- **Review how changing ESG Regulations and Reporting Standards are tracked**. Internal Audit can assess the organization's process of tracking upcoming ESG regulations, ensuring new requirements are followed and implemented by all the areas of the organization.
- **Review ESG projects vs communicated targets**. Internal Audit can play an important role in providing assurance over ESG priorities and related targets disclosed in Non-Financial Reporting. Organizations most probably need to establish new processes, new projects, new teams, new investment to reach such targets. The Governing Body and Executive Management need to be safeguarded that ESG ambitions can be achieved and consequently informed in a timely manner in case of delays or issues. It is therefore important to assess the consistency between strategic ESG goals and the decision-making process across the different operational activities of the company (for example, investment and divestment, maintenance, purchasing and contracting, human resources decisions, etc). Defining a combined assurance map for the ESG strategic goals, metrics and reporting processes, together with the other assurance functions (such as Sustainability), supports the achievement of this objective.
- **Review ESG Data Governance, Collection and Reporting**. Evaluate the governance of management's selection and tracking of ESG metrics, taking into account the existing process & KPIs in the organizations. Considering the different functions involved,

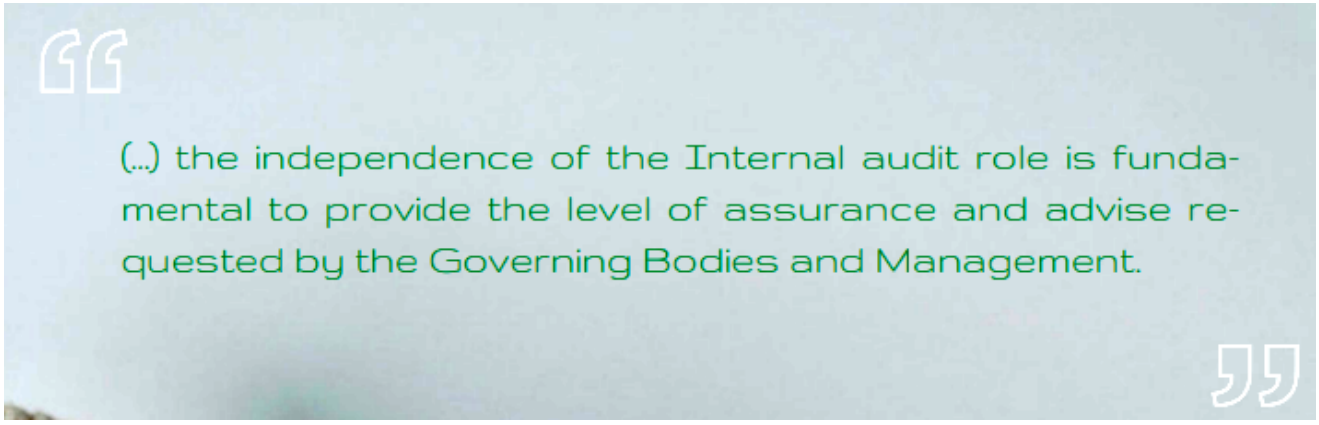


Figure 1. Corporate Sustainability Reporting Directive (CSRD)

as also represented in the paragraph B, it is important to review how information is collected and aggregated to ensure figures represented are accurate, relevant, complete, and timely. For example, in the greenhouse gas emission, Internal Audit can assess how data, coming from different sources within the organization and supply chain, is collected, consolidated, and reported; thereby evaluating the achievement of the defined targets.

Internal Audit has already started to provide assurance over the materiality matrix required for companies under NFRD and now needs to broaden its scope by initially offering support in the definition of the double materiality approach and then focusing its assurance activities on the double materiality assessment methodology, incorporating a "double materiality" lens of both traditional financial data and non-financial ESG information.

- **Review ESG Risk Management**. Assess how sustainability risks as results of the "double materiality assessment" are integrated into the existing Risk Management Framework and the effectiveness of the internal controls.
- **Review ESG Disclosures & Reporting**. Internal Audit can review the organization's ESG disclosures & reporting to ensure they are complete, accurate, and in compliance with relevant reporting frameworks or regulations. This may involve also reviewing reporting for consistency with formal financial disclosure.
- **Assess ESG Culture**. Considering the increasing requirements for companies to account for how they promote a healthy culture around environmental, social and employee-related aspects, Internal Audit can be of value assessing the effectiveness of the initiatives and how culture and values are integrated into the business processes and decision-making processes.

CONCLUSION

With the increasing importance of sustainability deeply impacting the way the organizations operate, there is a clear call for Board Members and Top Management to move towards a more sustainable business with Internal Audit as valuable partner in this journey; leveraging on the experience, the business knowledge and the role Internal Audit plays in Governance, Risk Management and Internal Controls. The support of Internal Audit can vary depending on the maturity of the organization with opportunities also for less mature companies to invest and properly set up this value-added function. To conclude, the question "if" Internal Audit could play a fundamental role over ESG" is no longer a question Boards and Top Management should ask but rather it is more of "how" they can best benefit on this privileged view.

Appendix

1. **Details of the various regulations relevant for ESG -** See **Figure 1** on previous page**.**

2. Internal Audit in industrial & commercial companies in Europe

Compared to other more regulated markets, such as Banks and Insurance, Industrial and Commercial companies in general have some more freedom to set up their governance structure. This is especially true for the audit, risk and compliance functions, which are usually set up in such a way that optimally supports the realization of the company's mission and objectives, balancing mandatory requirements by law or listing requirements. Despite being a less regulated environment, Industrial and commercial companies in reality generally operate in complex contexts with industry driven local legislations that require the setup of a multitude of Assurance providers (2nd Line) to strengthen the robustness of the risk management process and finally, the Internal Control System.

What is the **best setting for internal audit in industrial & commercial companies** to provide the expected added value? The Chief Audit Executive (CAE) must communicate and interact directly with the board and have direct and unrestricted access to senior management. However, in certain organization this can be achieved by a dual-reporting relationship. Furthermore, to guarantee the high level of professionalism and assurance every Internal Audit (IA) function, working in companies listed or not, big or small, has to perform its activities in compliance with the International Standards for the Professional Practice of Internal Auditing. To guarantee the compliance with the standards, each IA should be subject to a periodical quality review by an external independent and professional firm.

The Three Lines Model, published by The Institute of Internal Auditors in 2020, applies to all organizations, clarifies each player's role and the interactions. In such model, while the first and the second line roles might be blended or separated, the independence of the Internal audit role is fundamental to provide the level of assurance and advise requested by the Governing Bodies and Management.

Given the huge diversity of manufacturing companies and local legislations formally not requiring the setup of Audit shops, there are clearly some organizations with a relatively 'lower' maturity level of corporate governance, including risk and control functions. In such cases, Internal Audit could balance its advisory and assurance services.

This paper provides more insight on governance elements typical for manufacturing companies in Europe, and the role and positioning of the IAF in such companies. Such insight is relevant for anybody who wants to understand the potential of internal auditing in manufacturing companies in relation with ESG, but especially for all stakeholders and decision makers and external auditing bodies.

Final remarks

BIOs

- The IIA "The IIA's Three Lines Model — An update of the Three Lines of Defense" July 2020

- The IIA "Internal Audit's role in ESG Reporting" – May 2021
- ECIIA "Corporate Governance Codes on Internal Audit — Current status in the EU" 2012
- Gartner "2022 Audit Plan Hot Spots"
- Gartner "2023 Audit Plan Hot Spots"
- The IIA & World Business Council for Sustainable Development (WBCSD) — "Embedding ESG and sustainability considerations into the Three Lines Model"
- The ECIIA, ecoDa and Ferma: ESG embedding: are you ready?

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

The mission of ECIIA is to be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union, its Parliament and Commission and any other appropriate institutions of influence. The primary objective is to further the development of corporate governance and internal audit through knowledge sharing, key relationships and regulatory environment oversight. ECIIA represents around 56.000 internal auditors.

ECIIA Industrial Committee
ECIIA set up an Industrial Committee in 2022 with Chief Audit Executives of European Companies active in industrial and commercial sectors.

The mission of the ECIIA Committee is:

"To be the consolidated voice for the profession of Internal Audit in the Industrial and Commercial sector in Europe by dealing with the Regulators and any other appropriate institutions of influence at European level and to represent and develop the Internal Audit profession as part of good corporate governance across the Industrial and Commercial Sector in Europe".

Thank You
The paper describes the results of discussions amongst the ECIIA Industrial Committee members and we want to thank the Committee members for their input. A big thanks as well to the redaction team: Massimiliano Turconi, CAE of Telecom Italia and Vice President of ECIIA, Carlotta Boccadoro, Spot & Subsidiaries audit of Telecom Italia and Arjan Man, CAE at Atotech Group for their support.

Thank you!

NOTES

[1] (see paper ECIIA/ecoDa / Ferma on the topic "ESG embedding:are you ready?"

Intern Revision som et springbræt

Introduktion

Vi ser fra tid til anden kollegaer, som forlader intern revision for at prøve kræfter i første eller anden linje. Det giver anledning til at stille spørgsmålet, om de løber skrigende bort, eller om de forlader intern revision med en kuffert fuldt af gode erfaringer, som de kan anvende i andre dele af organisationen. Sagt på en anden måde, får man så meget erfaring og god ballast med fra intern revision, at intern revision faktisk kan ses som en del af ens karrierevej?

I redaktionen for IIA's medlemsblad INFO synes vi, at det kunne være interessant at undersøge dette nærmere ved at personer som har taget skridtet deler deres erfaringer. Vi har derfor fået tre personer til at skrive om deres oplevelser og erfaringer. Uden at afsløre for meget, kan vi allerede nu sige, at det er tre spændende personlige beretninger om hvordan man kan bruge intern revision som et springbræt til en videre karriere.

Compliance – forebyggende og fremadrettet arbejde, daglig vurdering af risici og kontrolmiljøer

Af Helle Ancher Munch, Head of Group Functions Advisory Compliance, Nordea

Helle Ancher Munch	
1996-2001	Arthur Andersen
1999-2004	Udlandsophold (og børn)
2004-2010	Nykredit, Intern Revision
2010-2011	Nordea, Group Internal Audit
2011-2013	Nykredit Bank
2014-2017	DONG, Internal Audit og Compliance
2017-	Nordea, Group Compliance

Jeg er cand.merc.aud fra 1997 med samlet 10 års erfaring fra intern revision og cirka 11 års erfaring fra compliance, primært inden for den finansielle sektor. I dag leder jeg et team på 5 erfarne Compliance Officers, fordelt i Finland, Sverige, Danmark og Polen. Vores rolle er at være risk managers for compliancerisici, samt at rådgive og supportere næsten alle Group Functions enhederne i Nordea, således at Nordeas interne regler og lovgivningen overholdes.

Hvis vi skruer tiden tilbage, startede jeg i ekstern revision ligesom de fleste andre cand.merc.aud'ere. Jeg blev ansat hos Arthur Andersen, men efter nogle år fik vi igennem min mands arbejde en vi mulighed for en udstationering. Dette gav os nogle gode og spændende år i udlandet, hvor jeg gik hjemme hos børnene.

Ved vores hjemkomst til Danmark i 2004 faldt mit valg på intern revision, og jeg begyndte at arbejde som intern revisor i Nykredit. Her fandt jeg spændende udfordringer, men også gode arbejdsforhold, som passede fint med vores familieliv.
I 2010 søgte jeg nye udfordringer og skiftede til Group Internal Audit i Nordea. Men allerede i 2011 blev jeg ringet op af Nykredit, der spurgte om jeg havde lyst til "at komme hjem" og starte en afdeling i Nykredit Bank med compliance og operationel risiko i første linje, med reference til den daværende bankdirektør. Dette gav mig mulighed for at arbejde med noget forebyggende og fremadrettet, i modsætning til revisionsarbejdet, der i vid udstrækning er opdagende. Et lys blev tændt – det var nogle gode år med masser af udfordringer.

Blandt andet rullede LIBOR skandalen, hvilket resulterede i undersøgelser hos alle de daværende panelbanker, der stillede CIBOR, her i blandt Nykredit Bank. Vi undersøgte hvorvidt der var urent trav, og samtidig med at vi var i løbende dialog med Finanstilsynet, designede og implementerede vi et nyt kontrolmiljø for de daværende referencerenter.

Efter Nykredit Bank skiftede jeg til Intern revision i DONG. I en intern revisionsafdeling opnår man god indsigt i virksomhedens organisation, og herigennem fik jeg muligheden for at komme over i den forretningsenhed der havde kundeansvar og Markets-funktionen for energi. Det var en spændende virksomhed, hvor jeg fik muligheden for at arbejde med complianceopgaver såsom implementering af markedsmisbrugsforordningen.

Både hos Nykredit Bank, DONG og Nordea har jeg arbejdet med lovimplementering og design af kontrolmiljøer, bl.a. med implementering af Shortselling-forordningen, Markedsmisbrugs-forordningen og Benchmark-forordningen.

Min erfaring fra revisionsårene er i daglig anvendelse i forbindelse med vurderinger af risici og kontrolmiljøer, og jeg anvender ofte spørgeteknik.

Jeg er meget glad for mit sidste jobskifte til Group Compliance i Nordea, hvor jeg har en spændende og alsidig hverdag med mange stakeholderinteraktioner. Jeg arbejder primært indenfor områderne Benchmark -forordningen, Markedsmisbrugsforordningen og med interessekonflikter. Men vigtigst af alt er, at mit team og jeg er med til at gøre en forskel både for Nordea, og for vores kollegaer på tværs af organisationen.

DPO – bruger i høj grad værktøjskassen, og at være tæt på forretningen giver et andet perspektiv

Af Jesper Jæger Granstrøm, DPO, PFA

Jesper Jæger Granstrøm	
2000-2003	KPMG, Ekstern revision
2004-2009	Codan, Intern Revision
2009-2015	PostNord, Intern Revision
2016-2017	EY, Konsulent
2018-	PFA, DPO

Som så mange andre, så startede min revisorkarriere i ekstern revision. Som nyudklækket cand.merc.aud startede jeg hos KPMG i København den 1. september 2000 med ambitionen og forventningen om, at det var i den del af revisionsbranchen, mit professionelle virke skulle udfolde sig.

Dette ændrede sig dog i slutningen af 2003, hvor jeg var udlånt til Intern Revision i Codan og herved fik indsigt i en anden side af revisionsfaget. Det tiltalte mig, og jeg søgte herefter en ledig stilling i den Interne Revision, som jeg tiltrådte 1. marts 2004.

Det blev til lidt over 5 år i Codans Interne Revision efterfulgt af 6,5 år i PostNords Interne Revision, hvorefter jeg havde 2 år som konsulent i EY indenfor bl.a. Intern Revision, inden jeg skiftede retning til mit nuværende virke, hvor jeg er DPO (databeskyttelsesrådgiver) i PFA.

Det at skifte fra et virke indenfor Intern Revision til en (på papiret) helt anden rolle indenfor databeskyttelse, krævede en del overvejelser. Efter mere end 15 år bliver det at være intern revisor en integreret del af ens professionelle identitet.

Med databeskyttelsesforordningens ikrafttræden i maj 2018 kom der et behov for, at flere virksomheder skulle udpege en DPO – en funktion man ikke tidligere havde haft, og som skulle bygges op. En rådgiverfunktion i anden linje, der både skal rådgive og vejlede om reglerne og føre tilsyn med, at de efterleves i virksomheden. Med en forordning, vejledningskompleks og praksis, der stadig var (og er) under udfoldelse, lå der en stor opgave i at fastlægge, hvordan DPO funktionen og rollen kunne udfoldes, forankres og samordnes med de øvrige funktioner i anden linje.

Et regelsæt med en potentielt meget alvorlig bødesanktion, hvis det ikke blev tilstrækkeligt implementeret og efterlevet i praksis, hvilket skulle tænkes ind i virksomhedens processer og kontroller med et fokus på risikoen for de registrerede. Dvs. en ny måde at tænke risiko på, end det man havde været vant til i den finansielle og operationelle revision. Eller sagt helt kort – en ny funktion, hvor der er behov for god risiko- og procesforståelse, godt kendskab til tekniske og organisatoriske foranstaltninger, og hvor man skal arbejde ud fra et regelsæt, der kan være komplekst.

Da den mulighed åbnede sig i Danmarks største kommercielle pensionsselskab med 1,3 mio. kunder, var overvejelserne reelt ikke så svære. Det var en fagligt spændende udfordring, hvor jeg kunne se rig mulighed for at bygge videre på den værktøjskasse, som jeg havde opbygget i mit virke i Intern Revision.

Men hvad har de seneste godt 5 år i rollen så vist i forhold til forventningen om, at min baggrund fra Intern Revision var både en fordel og en styrke i rollen som DPO?

Efter min egen oplevelse har det holdt stik. I hele mit virke gør jeg brug af de værktøjer og erfaringer, som jeg havde med i bagagen, da jeg startede hos PFA. Der skal laves aktivitetsplaner, der skal gennemføres konkrete tilsyn/analyser, der skal rapporteres, der skal følges op på anbefalinger, der skal samordnes med

andre funktioner for at undgå dobbeltarbejde, der skal være en metode og dokumentationskrav til det udførte arbejde, forretningen skal have råd og vejledning til risikoidentifikation og håndtering heraf, etc. Så i praksis rigtig meget af det samme, som lå i rollen som Intern Revisor – nu bare med et primært risikoperspektiv på personniveau frem for virksomhedsniveau (selvom de to perspektiver er nært forbundne i mange sammenhænge). Jeg har dog en del mere koordination og dialog med kolleger i Jura nu, end jeg havde i mine tidligere roller i Intern Revision.

Jeg vil helt klart anbefale Intern Revision som en del af ens karrierevej. At være tæt på forretningen giver et andet perspektiv og indsigt i både de formelle og uformelle processer, som man ikke oplever på samme måde, når man "bare" kommer ind som ekstern revisor eller konsulent. Man får selvfølgelig ikke samme mulighed for inspiration på tværs af virksomheder og brancher, men man kommer tættere på, at ens rådgivning og anbefalinger rent faktisk implementeres, og at dette reelt også styrker kontrolmiljøet, da der kan være en løbende dialog om forståelsen af anbefalingerne, når implementeringen rammer virkeligheden, og alle tvivlsspørgsmålene opstår.

Den procesforståelse man opnår, og metoden til risikoidentifikation og kendskab til tekniske og organisatoriske foranstaltninger til håndtering af risici, er almengyldige uanset hvilken jobfunktion man efterfølgende måtte få. Det at kunne sætte sig ind i en forretningsproces, analysere og forstå, hvor noget kan gå galt (og hvorfor), er fundamentet for at kunne fastlægge en effektiv governance og kontrolmiljø, der tager højde for de mange forskellige krav, der kan være til samme proces.

For den enkelte medarbejder skal det at efterleve forskellige regelværk gerne være integreret i måden at arbejde på i størst mulig udstrækning, og ledelsesmæssigt skal man have forståelsen af, hvilke kontrolforanstaltninger der er kritiske i forhold til at kunne påvise, at man har overholdt de forskellige krav – det giver en effektiv risikohåndtering på flere planer. I teorien en let opgave, men i praksis noget mere udfordrende – værktøjskassen fra Intern Revision vil dog altid komme brug.

Group Business Support – den tværgående forståelse af forretningen, risici og risikostyring er unik og værdifuld for første linje

Af Morten Vilstrup Olesen, Chief Business Risk Manager, Nordea

Morten Vilstrup Olesen	
2010-2013	Nordea, Personal Banking
2013-2015	Nordea, Group Internal Audit
2015-2017	Deloitte, Ekstern revision
2017-2022	Nordea, Group Internal Audit
2022-	Nordea, GBS Risk Reduction Plans

Min interesse i den finansielle sektor startede tidligt, og langt tidligere end jeg overhovedet havde overvejet at blive revisor. En aftale om praktik i Nordea startede rejsen og praktikpladsen og efterfølgende Trainee stilling i Personal Banking - nærmere bestemt filialen i Værløse - blev starten på det hele. Kunderne, produkter, dag-til-dag bankforretning og service var i højsædet.

Det lå ikke umiddelbart i kortene, at jeg skulle være revisor. Jeg fandt ud af, at kredit og de tungere dele af rådgivningsarbejdet var interessant, og jeg søgte derfor i retning af en HD 2. del i Regnskab og Økonomistyring. På HD'en mødte jeg en masse revisorer, og selv om man normalt siger, at revisorer er kedelige, blev jeg inspireret til at tage den retning. Det blev til 3 år i filialnetværket, og 3 røverier, som også var med til at inspirere mig til, at en hovedkontorsfunktion nok var en god ide.

Da jeg blev færdig med min HD og blev optaget på cand.merc.aud., ville Banken ikke af med mig (eller jeg ville ikke af med Banken). I hvert fald hjalp HR mig med at få en studenterstilling i Intern Revision – den første og eneste af sin slags i GIA hos Nordea. Efterfølgende har GIA taget del i et traineeprogram på tværs af Banken. Tiden i GIA var super lærerig og revisionsteorien fra cand.merc.aud. studiet blev sat i perspektiv, og sammenlagt fik jeg en god værktøjskasse at gå videre med.

Jeg kunne derfor stå på egne ben, da jeg var færdig med CMA, og besluttede mig for, at nu skulle jeg være 'rigtig revisor'. Jeg fik en trainee stilling hos Deloitte, hvor hverdagen skulle bestå af ekstern revision af finansielle virksomheder – herunder kredit/udlån hos Danske Bank og aktivsiden hos Danica Pension, m.v.

Efter to år i Deloitte var det gået op for mig, at rejsen imod statsautoriseret revisor ikke var det, jeg ville. Jeg var meget mere interesseret i processerne og operationel revision, og heldigvis var GIA hos Nordea på jagt og kom med et godt tilbud om at komme tilbage.

Det startede 5 gode år som intern revisor, i første omgang med fokus på Group Finance og lidt andre hovedkontorsfunktioner, samt Nordea Kredit. Senere tog jeg en mere faglig profil i GIA Quality Assurance hvor intern uddannelse, kvalitetssikring, rådgivning og sparring med kollegaer i GIA var de primære opgaver. Undervejs i dette forløb havde jeg drøftet med min leder muligheden for at komme på 'rotation' i en anden del af forretningen – ikke fordi jeg var træt af intern revision, men fordi jeg også gerne ville se, og prøve kræfter med andre dele af Nordea.

Det førte til, at jeg i 6 måneder blev lånt ud til Group Business Support – Management Oversight. Det var en aftale som opstod på ret senior niveau mellem revisionschefen (CAE) og Head of GBS, som ønskede en profil der kunne hjælpe førstelinjen med at 'tænke som en revisor'. Det vil sige tænke i risici, kontroller, iboende og residual risici, hvordan man mitigerer og kvantificerer ricisi, m.v. … og ikke mindst, en som kunne agere diplomat i mellem førstelinjen og GIA, da de ikke altid snakker samme sprog, hvilket nemt resulterer i misforståelser og konflikter.

Det gav mig blod på tanden og endte med en permanent stilling i GBS, som Chief Business Risk Manager. I dag består opgaverne fortsat af risikostyring samt en del ledelse, strategi og eksekvering af strategi for at reducere risici. Jeg har fortsat en del interaktioner med GIA (flere gange ugentligt), så jeg bliver fortsat holdt til ilden, og agerer også fortsat diplomaten som sikrer at vi ikke snakker forbi hinanden i løsningen af revisionsbemærkningerne.

Min baggrund og mit netværk i GIA er unikt og ganske værdifuldt for forretningen. Først og fremmest er det vigtigt, at jeg taler samme sprog som GIA og dermed kan skabe en bro mellem første linje og intern revision. Dernæst kan jeg bruge flere af de kompetencer, som jeg har fået i GIA. Fx skal man ikke undervurdere hvor godt et overblik af forretningen, og unikt indblik, man får ved at arbejde i intern revision.

Jeg nyder således godt af, at jeg i GIA fik et unikt og fantastisk overblik over banken, dens struktur og dynamikker, rapporteringer, interne regler, risiko værktøjer, nøglepersoner, osv. Det er noget, som er svært at få, hvis man sidder i andre positioner i banken og 'bare' passer sit eget område.

Jeg nyder desuden godt af, at jeg har fået en forståelse for risici og kontroller, hvordan man kvantificerer en risiko med sandsynlighed og konsekvens, hvilke kontroltyper der er; detective, preventive, osv., samt hvilke attributer (revisonsmål) som der kan fokuseres på; completeness, accuracy, timeliness, etc. og hvordan man formulerer en risiko skarpt og præcist…. Denne måde at tænke på er virkeligt noget, man lærer i intern revision, som er guld værd for resten af forretningen.

Jeg gjorde mig mange overvejelser før jeg forlod intern revision og tog springet ud i noget andet. Ens identitet knytter sig meget til, hvad man laver, og jeg var revisor. Så hvis jeg pludseligt ikke skulle være revisor mere, hvem var jeg så egentligt?! Den del var nok den største barriere for mig.

Jeg gjorde mig overvejelser ift. 'at det jo blot var en rokade internt i banken', og så gjorde jeg mig umage med ikke at 'smække nogle døre', men tværtimod at bevare de gode relationer til GIA og mine kollegaer der. Derudover overbeviste jeg mig selv om, at det nok var et godt karrieretræk.

Væk fra intern revision har jeg skulle vænne mig til at alting går hurtigere. Der er ikke 3 måneder til at levere et projekt, men måske få dage til at komme med et oplæg og nogle konklusioner. Jeg har skullet lære at 'sætte baren lavere' for at nå det hele, tage chancer og forbehold, og 'være mere agil'.

Derudover er der naturligvis også et andet fokus på omkostninger og tid. I GIA ser vi ikke ofte omkostningen af at drive GIA, eller omkostningerne ved at skrive de konklusioner og bemærkninger der kommer ud af en revision. Men i forretningen bliver alting en prioritering. Alle prioriteringer koster. Sættes forventningerne 'for højt' et sted, så er det på kompromis af noget andet – og så er der ikke en nul-fejls kultur, men en forståelse af at man må tage risici for at drive forretning. I GIA kom jeg nok med en forståelse af, at alt skulle være 100%, imens i forretningen kan man godt nogle gange være tilfreds med 95% eller 90%, så længe det er et bevidst valg.

For mig har intern revision været en genial karrierevej. Man får i intern revision nogle værktøjer og en forståelse af forretningen, som er unik. Selv om jeg nu har valgt en anden retning, så kan jeg til enhver tid anbefale intern revision som en god arbejdsplads og en karrierevej.

Omvendt gælder det også, at ønsker man at gøre karriere i intern revision, så vil jeg også anbefale, at man gør stop i andre dele af forretningen (fx Personal Banking og Group Business Support, som jeg selv) for at forstå virksomheden og

for ikke blive for teoretisk og 'støvet revisor'.
Jeg har nu et super interessant job hvor jeg fortsat lærer en masse, og gør en forskel med de værktøjer og den viden jeg har med fra tidligere, men man skal aldrig sige 'aldrig'. Så kun tiden kan vise, om jeg på et tidspunkt vender tilbage til intern revision.

Konklusion

Helle, Jesper og Morten har hver især givet deres personlige beretning om deres karrierevej. En karrierevej som i alle tre tilfælde er sket via intern revision. Fælles for alle tre beretninger er, de kan anbefale intern revision som en del af en karrierevej. De fremhæver alle den dybe forståelse, man som intern revisor får, af risiko og interne kontroller som grundstenen i deres værktøjskasse. En værktøjskasse som de flittigt bruger i jeres nuværende job uden for intern revision.

Konklusionen må derfor være, at der er mange grunde til at blive intern revisor. Arbejdet som intern revisor er i sig selv spændende, men kan også være et springbræt til mange andre spændende jobs i virksomheden. Helle, Jesper og Morten repræsenterer tre muligheder for, hvad en karriere som intern revisor kan føre til. Det er nok kun fantasien som sætter grænser for, hvilke muligheder der er.

Time to look again at Root Cause Analysis (RCA)

James C Paterson, Director Risk & Assurance Insights Ltd.
www.RiskAI.co.uk

As many readers may be aware, Root Cause Analysis (RCA) is proposed to be incorporated into the new Global Internal Audit Standards (GIAS). RCA is a vital tool for delivering insight and value, and it is also invaluable to develop a better thematic analysis of findings (another proposed new GIAS requirement).

As the former CAE of AstraZeneca, we used various RCA techniques, but in the dozen years I have been working on this topic with others, I have seen a range of good and not so good practices. As a result, I have just completed writing a book called "Beyond the Five Whys: Root Cause Analysis and Systems Thinking." I was able to share a few messages at the IIA international conference in Amsterdam. However, since the session was full, I want to share some of the headline messages with other internal audit colleagues.

The first thing to say is that while the Five Whys technique is still quite commonly used by audit teams, its major shortcoming is that it implies there will be just one root cause for a problem, which is rarely the case.

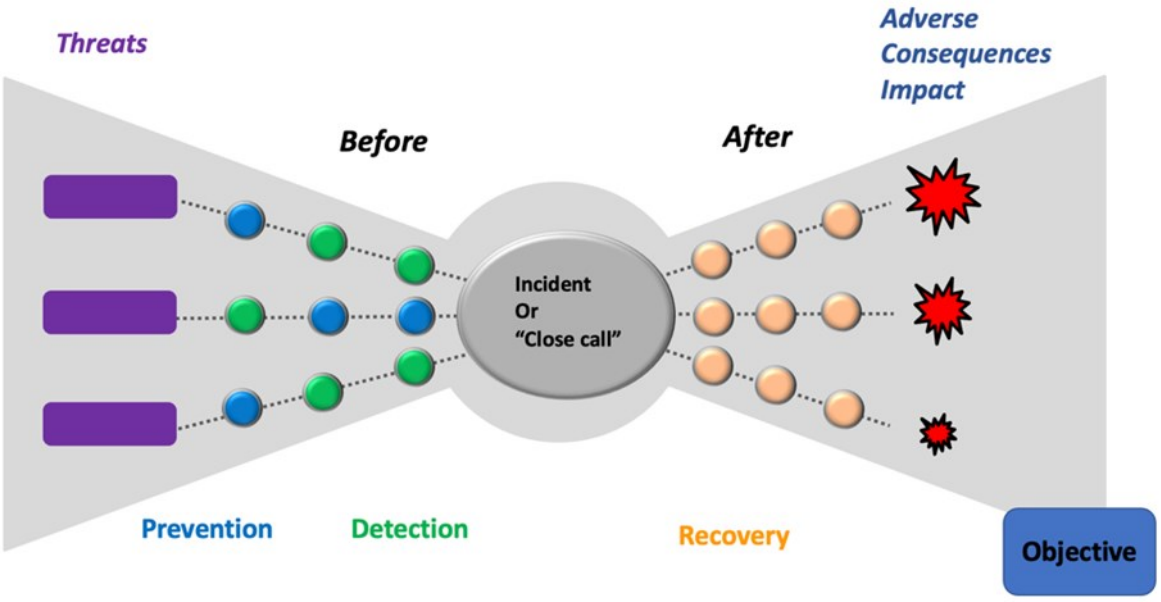
The best way of understanding why one root cause is a problem is to look at the Bowtie diagram (diagram 1). Here, we can see how threats and risks can result in incidents or near misses (risk exposures) which can, in turn, result in consequences of different sizes. As readers will appreciate, we use detective and preventative controls to stop incidents (or risk exposures) arising in the first place, and we use recovery controls to reduce the severity of any impact if the other techniques fail.

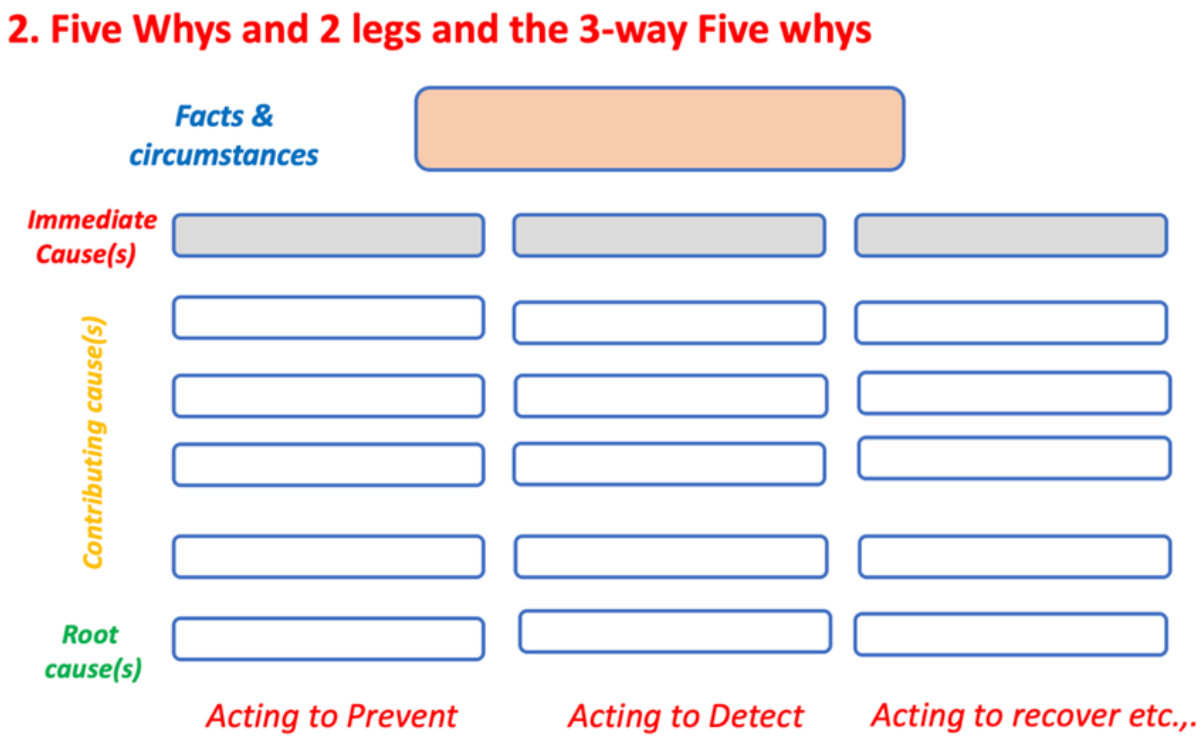
This means that if something goes wrong, or nearly goes wrong, *at least one preventative and one detective control will have let us down (and possibly recovery measures as well)*. Basic accounting training reminds us of prevent and detect controls being needed, and the COSO framework also highlights why a range of measures are necessary to keep things 'in control.' This takes us to a 'minimum viable' RCA technique to use, which is called the Five Whys Two Legs, or the Three-way Five Whys. These are encapsulated in diagram 2 on the next page.

For some audit teams it can be a challenge to 'let go' of having just one cause for an audit observation, but sometimes we need to take a step back to take two steps forward.

A further point that is often overlooked is to recognise the difference between different cause types. There are *immediate* causes, (think of a spark), then there are *con-*

1. Bowtie diagram (illustrative)





tributing causes (think of dry tinder on a forest floor). And then, there are root causes (i.e., the range of other things that might reduce or increase the chances of a forest fire). Root Causes are the underlying reasons why problems arise. Understanding root causes help us address *classes of problems rather than single problems or faults.*

So, if a person makes a mistake, or even if they deliberately cause harm, *the person will not be a root cause.* After all, if we find fraud or bribery and punish the person, we still need to ask ourselves, 'Were the anti-fraud or anti-corruption arrangements adequate?' Here, we realize, deep down, that *there may have been shortcomings in risk assessments, processes, systems, etc., that explain why the fraud or corrupt act was possible*, it's not all about one person's behavior.

As mentioned, my new book is also about systems thinking, which is about learning to step back and see the bigger picture of connections and dependencies between one thing and another. So, if we find a fraud or corrupt act we will, of course, want to punish the person who has done something inappropriate, but that should not be the end of the story. The deeper question has to be: 'What is it in our organization as a 'system', (considering its processes, policies, systems etc.), that made the fraud or corrupt act possible?'

When you think this way, you start to ask questions about whether the organization is serious about addressing certain risks properly, which extends, sometimes, to questions around the clarity of roles and accountabilities, the maturity of certain processes (and the amount invested in making them work) and the way incentives and deterrents do or don't work. In my book, I go through eight main causal factors ('eight ways to understand why') that can explain many problems we might see. Of course, which of the eight reasons why applies in a specific situation will depend on the particular facts and circumstances at the time.

Building on this, it's important to be on the lookout for repeating problems. Afterall, if you find repeating or similar issues (e.g., access rights not up to date, or projects running into difficulty), *this is invariably a sign of systemic problems that are fuelling the repetition*. The way to understand this is to recognise that *'Every system is set up to get the issues it currently gets,'* meaning we shouldn't be surprised sometimes when we get that 'Groundhog Day' feeling (i.e., 'I have seen this sort of problem before!') because the underlying issues which have not been properly resolved and - until they have been - problems will keep occurring.

A few additional points are worth noting:

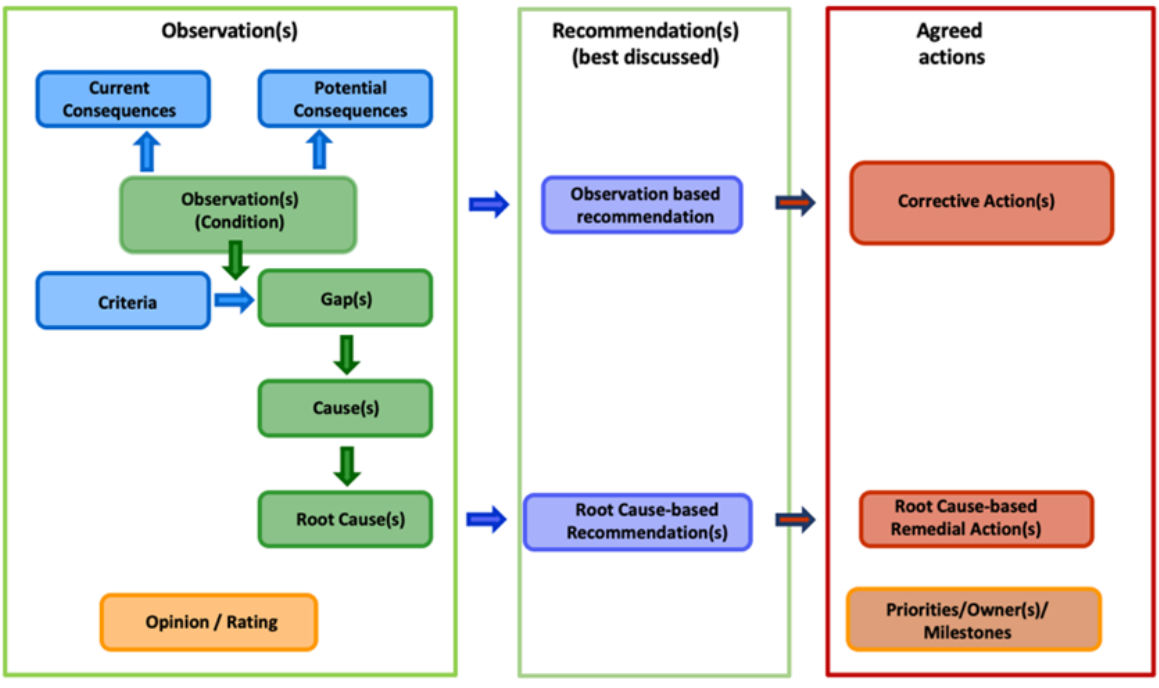
- Use of a fishbone technique for RCA can be helpful because it allows users to cluster the reasons for problems into common categories, which can then aid thematic analysis. Note, however, that *common categories of 'people, process and systems' do not explain why something happened*. Likewise, the suggestion

that 'culture' or 'tone from the top' can be the root cause of a problem does not really explain why the culture or tone at the top is not what it should be.

- Effective RCA in IA starts at the beginning of assignments, not just at the end. After all, sometimes root causes for problems lie between departments or across a process. So, if you scope an assignment without thinking about possible root causes, you may find an important cause is just out of reach of what you planned to do. This then results in seeking an extension to the assignment, which can cause delays and also frustration as business colleagues are engaged at short notice on a topic they were not expecting.
- A key myth that needs to be mentioned is the idea that RCA will inevitably extend audit assignments. Indeed, as I explained in my 2015 book "Lean Auditing," *it can be a valuable tool to help you zoom in on critical causal factors during the execution of work programs and speed up assignments*. This way, by the time you finish a work programme, you may already know most of the key causes.
- RCA is beneficial when writing audit reports since it can enable you to combine observations (which may be at the level of symptoms), writing key points and relevant actions at the level of the more significant (and interesting, insightful) underlying problems.
- Because, very often, actions to address root causes are more substantial, it is often crucial for the audit team to think carefully about the cost/benefit of what they propose should be remediated. In this regard, it becomes imperative to pay close attention to the potential impact of risk control shortcomings, not just the current impact of what has been found. With inspiration from the IIA guidance on report writing, we can see this point nicely spelled out in diagram 3.

Finally, being good at RCA goes beyond just what the audit team does in audit assignments. It can sometimes help an IA team think critically about current challenges. To give a couple of examples: If we look at issues such repeated shortcomings in getting audit actions to be fully and sustainably implemented by management, or weaknesses in second-line monitoring that have been going on for several years, *to what extent do these concerns also highlight areas for improvement in IA processes and procedures?* Often, problems with the adequate completion of follow-up actions can stem from shortcomings in how actions are agreed, how interim milestones have or have not been set, and the clarity (or otherwise) of verification requirements to demonstrate a risk is now 'in control.'

3. Seeing root causes in context when proposing actions

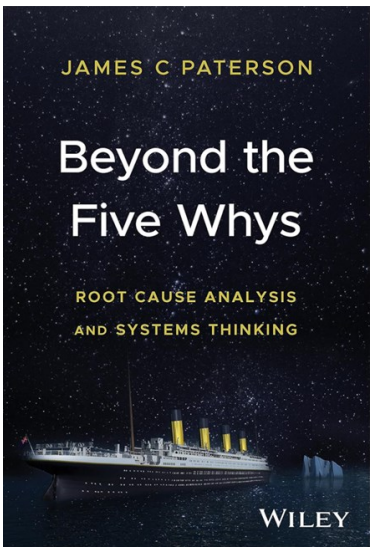


After IIA guidance

And concerns regarding the robustness of second line work (e.g., the quality of risk assessments or compliance documentation) can also stem from a need for more definition and clarity about the role and maturity goals of these functions (risk, compliance, but sometime IT, Finance, Procurement) and Internal Audit clearly calling this out (e.g., by using a maturity index for what these functions do).

Of course, raising these issues can be challenging for some IA teams, highlighting that no matter what you do on RCA, it is crucial that IA teams also work on their influencing and political savvy capabilities. This highlights another important message: RCA work gives us a better understanding of some of the cultural aspects of our organizations. So, it is worth noting that recent research by the IIA UK has identified that *nearly 50% of audit teams use RCA as a tool for understanding organizational culture*. It is outside the scope of this article to explore this point in more detail, but that's why it's timely that the IIA is giving this important technique a new prominence.

James C Paterson is the author of "Lean Auditing" and "Beyond the Five Whys. Root Cause Analysis and Systems thinking," published by Wiley.



Sæt allerede nu kryds i kalenderen!

EU ønsker at styrke den finansielle sektors modstandsdygtighed over for it-sikkerhedshændelse

Morten Hofmann, Senior Manager, PwC

Indledning

Digital Operational Resilience Act - DORA - er en del af en større lovgivningspakke rettet mod den finansielle sektor, som har til formål at udvikle en standardiseret, europæisk tilgang til it-sikkerhed, der fremmer teknologisk udvikling og sikrer finansiel stabilitet og forbrugerbeskyttelse.

Formålet med DORA er at styrke den finansielle sektors modstandsdygtighed over for forestående cyber- og informationssikkerhedshændelser. DORA indfører specifikke og standardiserede krav på tværs af EU's medlemslande. Virksomheder skal være rustet til at modstå, reagere og reetablere sig fra påvirkningen af IKT-sikkerhedshændelser (Informations– og kommunikationsteknologi) og dermed fortsætte med at være i stand til at levere kritiske og vigtige finansielle tjenester og minimere forstyrrelser for kunder og for samfundet. Dette kan eksempelvis opnås ved at underbygge en robust drift med kontroller på systemer, processer og tredjeparter og have de rigtige operationelle planer på plads, samtidig med at effektiviteten løbende testes.

DORAs centrale elementer

DORA opstiller et specifikt sæt kriterier og instruktioner, der forventes at forme, hvordan finansielle virksomheder håndterer cyber- og informationssikkerhedsrisici. EU-tilsynsmyndighederne ønsker at anvende en pragmatisk tilgang med et mere ensrettet og struktureret rammeværk, men forslaget understreger også, at EU-tilsynsmyndighederne bør tage proportionalitetshensyn i betragtning ved fastlæggelsen af standarderne for, hvordan den enkelte virksomhed bør efterleve de nye krav. Den enkelte virksomheds størrelse, type, kompleksitet og risikoprofil m.fl. er dermed afgørende for, hvordan virksomheden bedst indretter sig efter de nye regler.

Et konkret eksempel på ensretning fra dansk lov, er ledelses- og styringsbekendtgørelsen bilag 4 (Forsikring & Pension) og 5 (Pengeinstitutter), som forventeligt udgår og dermed vil alle finansielle institutter følge det samme DORA regelsæt, hvilket vil betyde en større implementeringsopgave, for virksomheder der tidligere ikke var underlagt bilag 5, som indeholdte de mest restriktive krav ift. bilag 4 for bekendtgørelsen for forsikringsselskaber.
Et centralt element i DORA-forordningen er kravet om at udføre kontinuerlige vurderinger, kommunikere og rapportere gennem standardiserede rapporteringsformater. Derudover forventer vi, at myndighederne i EU-medlemslande kommer til at ensrette deres dokumentation og testkapacitet vedrørende digital operationel modstandsdygtighed.

Harmonisering og ensretning af reglerne

DORA's udviklende effekt på finanssektoren ligger i dens kapacitet til at ensrette og harmonisere digitale sikkerhedsstandarder. Det er af stor betydning, da finansielle institutioner i stigende grad tilbyder en lang række af tjenester, der strækker sig over flere sektorer. Ved at etablere et fælles sæt af retningslinjer og standarder for operationel robusthed og cybersikkerhed, bliver det regulatoriske landskab mere forudsigeligt, hvilket er et afgørende skridt i retning af at øge sektorens modstandsdygtighed mod cyberangreb og andre digitale trusler.

Øget robusthed gennem krav og kontroller

DORA gør mere end bare at opstille minimumsstandarder for it-sikkerhed; lovgivningspakken indfører et fuldstændigt rammeværk for risikostyring og operationel robusthed. For eksempel indeholder DORA en række krav til kontinuitetsplanlægning og krisehåndtering, der sikrer, at virksomheder er forberedt på en lang række potentielle hændelser. Det inkluderer detaljerede retningslinjer for at teste, dokumentere og løbende overvåge kritiske IKT systemer. Disse krav er designet til at sikre, at alle virksomheder i den finansielle sektor har en robust og effektiv tilgang til risikostyring og kan modstå de udfordringer, som det moderne digitale landskab præsenterer.

Proportionalitet

DORA's iboende proportionalitetsprincip er et vigtigt skridt i retning af en mere nuanceret og fleksibel regulering. Forordningen tager hensyn til virksomhedernes størrelse og kompleksitet, hvilket har til hensigt at undgå, at mindre virksomheder bliver uforholdsmæssigt belastet af de nye krav. DORA giver disse virksomheder mulighed for at implementere passende sikkerhedsforanstaltninger, der er i overensstemmelse med deres operationelle kapacitet og risikoprofil.

Intern revisions rolle i DORA-Compliance
Intern revision spiller en afgørende rolle i DORA's trelinjes forsvarsmodel for risikostyring. Ud over de traditionelle opgaver stiller DORA krav om etablering af intern revision og evaluering af effektiviteten af virksomhedens it-sikkerhed og operationelle robusthed. Dette inkluderer en række opgaver fra udførelse af uafhængige risikovurderinger til løbende kontrol af de implementerede sikkerhedsforanstaltninger.

DORAs hovedtemaer

DORA opstiller retningslinjer og minimumskrav inden for fem hovedtemaer, der adresserer forskellige aspekter inden for cyber- og informationssikkerhed:

1. Risikostyring
DORA stiller krav til, at finansielle virksomheder anvender et rammeværk til risikostyring og -vurdering, og at virksomhedens governance og organisering tager sit afsæt heri. Berørte virksomheder bliver mødt med detaljerede krav til styring og kontrol af it-risici, politikker og procedurer samt tekniske og organisatoriske kontroller i bredt omfang. Virksomhederne er desuden forpligtet til at opbygge og vedligeholde uddannelse, systemer og værktøjer med henblik på at identificere og minimere cyber- og informationsikkerhedsrisici på kontinuerlig basis.

2. Hændelsesrapportering
Berørte virksomheder skal etablere og implementere en ledelsesproces for at overvåge, klassificere, kommunikere og rapportere større it-sikkerhedsrelaterede hændelser til tilsynsmyndighederne. DORA har til hensigt at harmonisere klassificering og rapportering af disse hændelser og centralisere de finansielle institutioners rapportering af større hændelser i EU.

”Berørte virksomheder skal etablere og implementere en ledelsesproces for at overvåge, klassificere, kommunikere og rapportere større it-sikkerhedsrelaterede hændelser til tilsynsmyndighederne.”

3. Test af cyberrobusthed
DORA opstiller krav om implementering af et omfattende ‘program for test af digital operationel modstandsdygtighed’. Berørte virksomheder vil være forpligtet til at teste kapaciteter og funktioner, der er inkluderet i risikostyringsrammen for cyber- og informationssikkerhed mindst én gang årligt med henblik på at identificere svagheder og træffe korrigerende foranstaltninger. Derudover skal der laves en trusselsbaseret penetrationstest (TLPT-test) minimum hvert tredje år.

Derudover er der krav om, at de respektive backupsystemer skal være fysisk og logisk adskilt fra produktionssystemer, og i tilfælde af nedbrud skal backuppen være i stand til at fortsætte driften af systemet uden datatab. Et krav, som kan være ganske omfattende for visse transaktionsbaserede systemer.

At stille krav til praktisk afprøvning, risikostyring og myndighedsrapportering har tidligere været kendt i Threat Intelligence-Based Ethical Red-teaming (TIBER), hvor pengeinstitutters og datacentralers produktionssystemer angribes for at finde svagheder i cybersikkerheden, og dette princip anvendes også i DORA.

4. Risikovurdering af tredjepartsleverandører
DORA stiller høje krav til risikovurdering, opfølgning og exitplaner, ligesom der stilles høje krav til overvågning af sikkerhed hos tredjepartsleverandører, og på sanktionssiden vil de europæiske tilsynsmyndigheder (ESA) få beføjelser til at anmode om oplysninger, udføre inspektioner, udstede anbefalinger og anmodninger og pålægge bøder.

5. Deling af viden og information om cyberhændelser
Med DORA får myndigheder og finansielle virksomheder en struktur, der giver mulighed for at lave aftaler, der tillader, at oplysninger, efterretninger og anden relevant viden udveksles indbyrdes med henblik på at minimere udbredelse af og øge viden om aktuelle cyberrisici.

Hvad får I ud af DORA?

Eftersom DORA opstiller standardiserede krav, bliver berørte virksomheder pålagt vilkår, som kan være svære at omstille sig til, hvis de ikke i forvejen har effektiv governance omkring cyber - og informationssikkerhed. Ledelsesbekendtgørelserne for finansielle virksomheder har varierende krav til digitalt beredskab, men kun ledelsesbekendtgørelsen for pengeinstitutter har krav, som er tilnærmelsesvis tæt på de krav, der opstilles efter DORA. Det betyder, at der er omfattende og skærpede krav på vej til bl.a. forsikringsselskaber, pensionsselskaber og investeringsselskaber.

Implementeringen af DORA forventes at føre til øget transparens i ledelsesrapporteringen, og ledelsen i virksomheden vil få et bedre indblik i virksomhedens modstandsdygtighed over for cyberhændelser. Det vil være en anledning til at integrere cyberrisko i den generelle risikostyring, idet alle berørte virksomheder bliver underlagt krav om at implementere et cybersikkerhedsprogram, hvilket omfatter politikker, procedurer og risikostyringsaktiviteter.

Rapportering til og fra markedet, mellem virksomheder og myndigheder, vedrørende trusselsniveauet i samfundet som helhed, vil styrke modstandsdygtigheden overfor potentielle angreb i fremtiden, hvilket bl.a. vil være suppleret af de harmoniserede krav til de tekniske opsætninger for testkapaciteterne i de enkelte virksomheder. DORA vil dermed skabe nye standarder for digital operationel modstandsdygtighed på konsolideret niveau i den finansielle sektor.

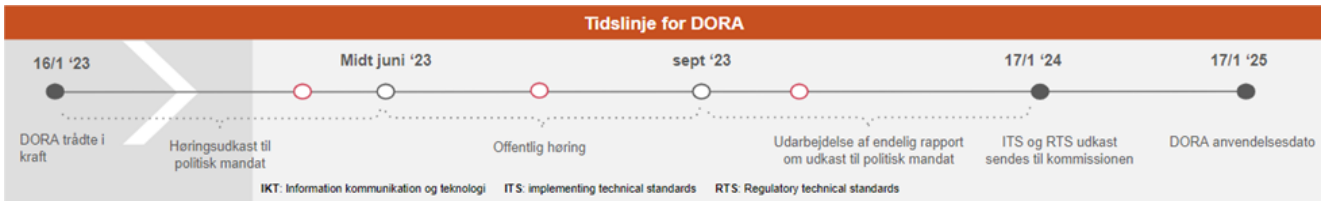
Afsluttende bemærkninger

DORA får omfattende betydning for myndigheder og berørte virksomheder, og stor indflydelse på den overordnede regulering af den finansielle sektor. Med forordningens

omfattende krav til cybersikkerhed og operationel robusthed tilbyder den en stringent, men fleksibel ramme for virksomheder at manøvrere i. Det er mere kritisk end nogensinde for virksomheder i den finansielle sektor at forstå og implementere de forskellige facetter af DORA. Dette inkluderer ikke blot tekniske og operationelle aspekter, men også den forstærkede rolle, som intern revision spiller i moderne risikostyring og compliance-processer. Den digitale æra bringer en række udfordringer, men også muligheder. Ved at forstå og omfavne DORAs principper kan virksomheder, udover blot at sikre overholdelse af forordningens regler, også trives i et stadig mere komplekst og risikofyldt digitalt landskab.

Processen for DORAs behandling, vedtagelse og ikrafttræden

- DORA blev behandlet den 9. november 2022 og er baseret på det forslag, som EU-Kommissionen og EU-Parlamentet blev enige om i maj 2022.
- DORA blev endeligt vedtaget den 28. november 2022 og trådte i kraft den 27. december 2022, hvor den blev offentliggjort i EU's Official Journal.
- DORA finder anvendelse for virksomhederne fra den 17. januar 2025 efter en toårig implementeringsperiode.



NIS2-erklæringer

Alireza Samini, Partner, PwC

Jess Kjær Mogensen, Partner, PwC

"Europe is still not well equipped when it comes to cyber-attacks. Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks."
– Jean Claude Junker, 2017 (Former President of The European Commission)

Indledning

Vedtagelsen af NIS2-direktivet er et stærkt signal fra EU samt en konsensus om, at cybersikkerhed spiller en afgørende rolle for vores evne til at kunne værne om vores samfund, der hviler på tillid, tryghed og stabilitet. De danske myndigheder står over for en vigtig opgave, der består i at få fortolket og forankret direktivet i dansk lov samt føre tilsyn med efterlevelsen af det. Samtidigt er mange virksomheder allerede i gang med at foretage en vurdering af, hvordan de bliver ramt af kravene, og hvilke tekniske, operationelle og organisatoriske foranstaltninger der skal implementeres.

I denne artikel gennemgår vi formålet med direktivet, dets fokusområder, samt hvordan vi som revisorer kan være med til at skabe tillid i forhold til efterlevelse af NIS2-kravene.

Hvad er NIS2?

Europas digitale landskab har været under konstant udvikling, og som en reaktion på de stigende trusler mod cybersikkerheden blev Network and Information Security Directive (NIS) introduceret som det første forsøg på at fastsætte fælles regler og standarder inden for EU i 2016. NIS, også kendt som NIS1, markerede begyndelsen på en koordineret tilgang til cybersikkerhed og digital infrastruktur på tværs af medlemslandene.

NIS1 var EU's første horisontale lovgivning om håndtering af cybersikkerhedsudfordringer, dvs. direktivet var gældende på tværs af forskellige sektorer i samfundet.

Direktivet fokuserede primært på at identificere og beskytte kritiske infrastrukturer og onlinetjenester. NIS1 indførte også krav til medlemslandene om at oprette nationale cybersikkerhedsstrategier og etablere samarbejdsnetværk, der kunne håndtere og reagere på cyberangreb. Selvom NIS1 var et skridt i den rigtige retning, erkendte EU, at der var brug for at sikre en mere ensartet implementering af krav og foranstaltninger samt inkludere flere sektorer for at imødegå de stadigt mere komplekse og stigende trusler.

På denne baggrund blev arbejdet med NIS2 igangsat og endeligt vedtaget i december 2022.

NIS2 træder i kraft i dansk ret den 18. oktober 2024, og en lang række virksomheder inden for 18 sektorer bliver omfattet af NIS2.

Ved at etablere ensartede standarder og regler for cybersikkerhed inden for EU, kan NIS2 bidrage til at reducere risikoen for cyberangreb og styrke beskyttelsen af digitale systemer og data på tværs af EU.

Helt overordnet er NIS2 videreudviklet på fire hovedområder:

1. Med NIS2 forsøger EU at omfatte alle private såvel som offentlige institutioner inden for kritiske infrastrukturer. Det betyder, at alle virksomheder, i visse sektorer, over en vis størrelse bliver omfattet.
2. Indførelse af krav om indberetningspligt til myndighederne inden for 24-72 timer. Formålet er at sikre, at budskabet spredes hurtigst muligt, og at andre virksomheder, der potentielt kan være udsat for samme type trussel, kan nå at reagere.
3. Indførelse af krav om sanktionsmuligheder, herunder udstedelse af bøder i størrelsesorden 1-2 % af den globale omsætning.
4. Indførelse af minimumskrav overfor ledelsen for så vidt angår ansvarsplacering samt krav til uddannelse og træning i forhold til cybersikkerhed.

NIS2 fastlægger minimumskrav til cybersikkerhed, som medlemslandene skal følge. Disse omfatter krav til beskyttelse af information og data, håndtering af cyberangreb samt implementering af sikre autentificeringsmetoder for digitale tjenester.

Direktivet støtter også forskning og udvikling af nye teknologier på cybersikkerhedsområdet og fremmer innovation og samarbejde mellem medlemslandene.

Hvilke virksomheder er omfattet?

De af NIS1 gældende definitioner, som omfattede "udbydere af essentielle tjenester" (OES) og "digitale tjenesteudbydere" (DSP'er) bliver med NIS2 erstattet af "essentielle enheder" og ""vigtige enheder". Disse virksomheder og organisationer er omfattet af NIS2-reglerne og er forpligtet til at implementere passende sikkerhedsforanstaltninger for at beskytte deres netværk og informationssystemer mod cybertrusler.

- *Essentielle enheder* er de klassisk kritiske infrastruktursektorer såsom energi, transport, bankvæsen, fi-

nansmarkedsinfrastrukturer, sundhed, drikkevand, spildevand, digital infrastruktur, IKT (Information og Kommunikationsteknologi)-tjenester (B2B), offentlig administration og rumfart.
- *Vigtige enheder* omfatter sektorer som post- og kurertjenester, affaldshåndtering, fremstilling, produktion og distribution af kemikalier, produktion, forarbejdning og distribution af fødevarer, fremstilling, digitale udbydere og forskning.

Kriterierne for, hvorvidt virksomhederne ligger i den ene eller anden kategori, kan i nogle tilfælde hvile på en konkret vurdering. Derfor skal den enkelte virksomhed eller myndighed få undersøgt, om de bliver omfattet af NIS2, hvis de opererer i én af de opstillede sektorer, jf. skemaet nederst på siden.

Herudover skal virksomheden have en årlig omsætning eller balance på 10 mio. EUR og over 50 ansatte for at blive omfattet.

Der er ingen direkte forskel mellem enheder, der er "essentielle" vs. "vigtige" i forhold til implementering af kravene. Begge udtryk refererer til det samme begreb, nemlig "operatører af væsentlige tjenester" (OES). OES er virksomheder eller organisationer, der tilbyder tjenester, der anses for at være kritiske for samfundets funktion og økonomi.

Der er krav om, at medlemsstaterne skal indrapportere alle essentielle og vigtige enheder. Der forventes derfor en obligatorisk indberetningspligt for de danske virksomheder og myndigheder, der er omfattet af direktivet. Hvorvidt tilsynsmyndighederne vil variere og tilpasse kravene til disse to type sektorer må tiden vise.

Der vil ligeledes være organisationer, der er omfattet af NIS2 uanset størrelse. Disse er ikke nærmere beskrevet i denne artikel.

Væsentlige forhold i NIS2

NIS2 medfører en række nye krav til de enheder, som er omfattet af reguleringen, og også indirekte til en række af disses leverandører. Vi har nedenfor listet nogle af de områder, som vi vurderer vil blive mest berørt.

Ledelsens ansvar: Cybersikkerhed er ikke længere noget IT eller sikkerhedsafdelingen tager sig af. Med NIS2

Sektorer	Type
Energi – elektricitet, fjernvarme og fjernkøling, olie, gas, brint	Essentielle enheder
Transport – luft, jernbane, vand, vejtransport	Essentielle enheder
Bankvirksomhed – kreditinstituttermv.	Essentielle enheder
Finansielle markedsinfrastrukturer – handelsplatforme	Essentielle enheder
Sundhed – plejeudbydere, EU-referencelaboratorier (udnævnt til beredskab), forskning og udvikling af medicinske produkter, producenter af medicinsk udstyr	Essentielle enheder
Drikkevand – leverandører og distributører	Essentielle enheder
Spildevand – indsamling, bortskaffelse, behandling	Essentielle enheder
Digital infrastruktur – udbydere af internetudvekslingspunkter, DNS, TLD, cloud computing, datacentre, indholdsleveringsnetværk, tillidstjenester, offentlig kommunikation	Essentielle enheder
Forvaltning af IKT-tjenester (B2B) – udbydere af administrerende tjenester, udbydere af administrerende sikkerhedstjenester	Essentielle enheder
Offentlig forvaltning – administration, kommuner og regioner	Essentielle enheder
Rumfart – software og services	Essentielle enheder
Post og kurertjenester – rydning, sortering, transport og levering	Vigtige enheder
Affaldshåndtering – indsamling, transport, genindvinding og bortskaffelse	Vigtige enheder
Kemikalier – produktion og distribution	Vigtige enheder
Fødevarer – produktion, tilvirkning og distribution	Vigtige enheder
Fremstilling – af medicinsk udstyr, computere, elektroniske og optiske produkter, maskiner og udstyr, motorkøretøjer, transportudstyr	Vigtige enheder
Digital providers – onlinemarkedspladser, søgemaskiner, sociale platforme	Vigtige enheder
Forskning – forskningsinstitutioner	Vigtige enheder

rykker ansvaret helt op til ledelsen, eftersom direktivet indeholder minimumskrav til ledelsens ansvar. Ledelsen skal nemlig godkende organisationens risikostyring af cyberområdet, løbende føre tilsyn med effektiviteten af kontrollerne og sikre, at virksomhedens sikkerhedsforanstaltninger og risikoappetit løbende tilpasses det aktuelle risikobillede.

Ledelsen skal modtage regelmæssig træning for at opnå grundlæggende forståelse for cybersikkerhedsrisici samt "bedst praksis" inden for cybersikkerhed og relevant lovgivning på området. Dette kan ske gennem interne eller eksterne uddannelsesprogrammer, kurser og workshops.

Risikovurdering: Traditionelt set har ledelsen i virksomhederne været vant til at vurdere de forretningsmæssige risici, altså risikoen for, at virksomheden ikke opnår sine finansielle mål.

Med NIS2 har virksomhedens, herunder ledelsens, risikovurdering fået en ny dimension, nemlig vurdering af kritikaliteten af virksomhedernes ydelser i et samfundskritisk perspektiv, som indebærer identifikation og evaluering af potentielle trusler mod informationssystemer og netværk, der er afgørende for samfundets funktion. Risikoanalysen skal udarbejdes for at kortlægge sandsynligheden for og konsekvensen af et angreb på de relevante ydelser. For eksempel, hvor sandsynligt er det, at en transportvirksomhed, som leverer medicin til borgerne, bliver ramt af et cyberangreb, og hvad er konsekvensen af sådan en hændelse?

Baseret på risikovurderingen skal organisationen træffe passende og proportionale tekniske, operationelle og organisatoriske foranstaltninger til håndtering af cybersikkerhedsrisici. Direktivet skriver følgende om vurdering af proportionalitet:

"Ved vurderingen af proportionaliteten af disse foranstaltninger tages der behørigt hensyn til graden af enhedens eksponering for risici, enhedens størrelse og sandsynligheden for hændelser og deres alvor, herunder deres samfundsmæssige og økonomiske indvirkning".

Myndighedernes tilsynsansvar: NIS2 stiller krav til, at medlemslandene udpeger nationale myndigheder, der er ansvarlige for overvågning og håndhævelse af NIS2-direktivet.

I Danmark forventes en afklaring af tilsynsansvaret samt indarbejdelse af NIS2-kravene i dansk lov at foreligge senest i sommeren 2024.

Operatører af digitale tjenester og udbydere af vigtige tjenester er forpligtede til at indberette alvorlige sikkerhedsbrud til de nationale myndigheder inden for en fastsat tidsramme. Myndighederne har beføjelse til at fastsætte standarder for, hvordan disse brud skal indberettes.

Tilsynspligten tilskriver, at de nationale myndigheder udfører audit og inspektioner for at sikre, at virksomhederne omfattet af NIS2-direktivet overholder forpligtelserne i relation til cybersikkerhed. De kan ligeledes fastsætte administrative bøder i tilfælde af overtrædelser.

Forsyningskæde: NIS2 stiller ikke alene krav til de virksomheder, der opererer i de førnævnte industrier, men også til deres underleverandører, der udgør forsyningskæden.

Her henvises til den samlede proces, hvor forskellige enheder og aktører er involveret i at levere digitale tjenester til brugerne. Dette omfatter producenter af hardware og software, udbydere af datacentre og cloud-tjenester, tredjepartsleverandører og alle andre parter, der er involveret i udvikling, vedligeholdelse og levering af digitale produkter og tjenester.

Kravene om ansvar for forsyningskæden i NIS2 har til formål at forbedre cybersikkerheden på tværs af hele forsyningskæden og sikre, at organisationerne ikke kun beskytter deres egne netværks- og informationssystemer, men også de systemer og tjenester, de er afhængige af tredjepartsleverandører. Nogle af de vigtigste elementer vedrørende ansvar for forsyningskæder i NIS2 er :

1. **Identifikation af tredjepartsleverandører**: Organisationer, der betragtes som udbydere af essentielle tjenester eller digitale tjenesteydelser, forventes at identificere de tredjepartsleverandører, der er kritiske for deres tjenesteudbud og forsyningskæde.
2. **Risikovurdering**: Organisationer skal gennemføre risikovurderinger af deres forsyningskæde for at identificere potentielle sårbarheder og risici. Dette kan omfatte at evaluere, hvor afhængige de er af bestemte leverandører og tjenester.
3. **Sikkerhedskrav til leverandører**: NIS2 giver mulighed for fastsættelse af sikkerhedskrav til leverandører i kontrakter eller serviceaftaler. Disse krav skal være baseret på resultatet af risikovurderingerne og skal tage højde for tjenestens kritikalitet.
4. **Overvågning og rapportering**: Organisationer skal overvåge deres tredjepartsleverandørers sikkerhedspraksis og reagere på eventuelle sikkerhedshændelser, der kan påvirke tjenestens kontinuitet eller datasikkerhed. De kan også kræve, at leverandørerne indberetter sikkerhedshændelser.
5. **Auditering og revision**: NIS2 giver mulighed for at udføre audit og revisioner af tredjepartsleverandørers cybersikkerhedspraksis for at verificere overholdelsen af de aftalte sikkerhedskrav.
6. **Krisehåndtering og beredskab**: Organisationer skal udvikle beredskabsplaner, der tager højde for potentielle afbrydelser forårsaget af sikkerhedshændelser i forsyningskæden. Dette inkluderer at sikre alternativ levering af tjenester i tilfælde af nedbrud hos en leverandør.

Disse krav om ansvar for forsyningskæden i NIS2 er udformet med det formål at øge robustheden af kritiske tjenester og digitale tjenesteydelser og minimere risikoen for nedbrud eller sikkerhedsbrud på grund af svagheder i forsyningskæden. Organisationer forventes at anlægge en

proaktiv tilgang til at beskytte deres forsyningskæde og at samarbejde med deres leverandører for at opfylde disse krav. Herudover skal der løbende ske overvågning og inspektion af underleverandører for at sikre, at kravene efterleves hele vejen igennem forsyningskæden.

NIS2-direktivet stiller samtidig krav til medlemsstaterne om at etablere en ramme, hvor aktørerne i forsyningskæden deler oplysninger om sikkerhedstrusler og -hændelser. Dette informationsdelingsaspekt er afgørende for at skabe et mere sikkert digitalt miljø, da det gør det muligt at reagere hurtigt på trusler og potentielle angreb på tværs af hele forsyningskæden.

Operational Technology (OT): Den samlede forsyningskæde er ikke længere begrænset til informationssikkerhed alene, men OT-sikkerhed får en lige så stor betydning i den forbindelse.

OT refererer til hardware og software, der anvendes til at styre fysiske enheder og processer i industrianlæg, kraftværker, transport og andre kritiske infrastrukturer. I NIS2-sammenhæng er OT-sikkerhed ekstremt vigtig, da angreb på disse systemer kan have alvorlige konsekvenser for samfundet og økonomien.

Traditionelt set har vi revisionsmæssigt ikke været vant til at forholde os til sikkerheden ved OT, ligesom mange sektorer mangler folk med rette kompetencer og uddannelse for at kunne understøtte denne agenda. Derfor forventes en række udfordringer med at få foretaget passende risikovurdering, få identificeret de rette leverandører, stille krav til disse samt etablere passende tekniske foranstaltninger i relation til OT. På denne baggrund tilskynder direktivet til udvikling og vedtagelse af fælles sikkerhedsstandarder og certificeringssystemer i OT-sektoren. Dette vil hjælpe med at skabe klare retningslinjer for, hvad der anses for at være tilstrækkeligt i forhold til cybersikkerhed.

Minimumskrav: Der henvises til afsnittet om kontrolmål og kontrolaktiviteter nedenfor.

Hvad er vores rolle som revisorer?

I FSR – danske revisorers strategi står "Forandring og stigende kompleksitet er blevet den nye norm i en verden, der står over for store, verdensomspændende udfordringer. I en tid, hvor disse forandringer udgør et nyt, fælles vilkår, er revisorernes opgave med at sikre tillid og troværdighed i samfundet i dag vigtigere og mere vidtspændende end nogensinde før."

Samtidig er det lovfæstet for godkendte revisorer, at de er offentlighedens tillidsrepræsentant og skal være effektive i, hvad de gør, da opgaverne skal udføres i overensstemmelse med god revisorskik, herunder skal de udvise den nøjagtighed og hurtighed, som opgavernes beskaffenhed tillader.

Kravet i NIS2 om forsyningskædesikkerhed, som blandt andet dækker sikkerhedsrelaterede aspekter ved forholdene mellem den enkelte enhed og dens direkte leverandører eller tjenesteudbydere, gør, at det er relevant for revisorer at arbejde i feltet mellem de enheder, der er underlagt reguleringen, og den forsyningskæde, de anvender.

Men for at kunne ramme balancen mellem, hvad der er need-to-know og nice-to-know i forhold til overbevisning om, hvad der sker i forsyningskæden på en effektiv måde, må der opstilles et fælles udgangspunkt, og det er netop hvad FSR – danske revisorer har gjort med opstillingen af kontrolmål og -aktiviteter.

Her ligner situationen på mange måder tiden, hvor GDPR-kravene blev indført – da var det også en del debat om, hvilket niveau af tekniske og organisatoriske sikkerhedsforanstaltninger der ville være tilstrækkeligt, og det var svært at få nogen til at lægge hånden på kogepladen – men i et godt samarbejde med Datatilsynet lykkedes det FSR at opstille en baseline på 45 kontrolaktiviteter, som mange dataansvarlige og databehandlere herefter har anvendt som udgangspunkt for databehandleraftalerne og også som scope for de ISAE 3000-erklæringer, som anvendes som helt naturlig del af opfølgningen på databehandlingen.

Håbet er, at succesen fra GDPR kan gentages med NIS2, så der rammes et niveau, som vil blive opfattet som rimeligt af de forskellige NIS2-aktører.

Arbejdet med erklæring om NIS2 i FSR – danske revisorer

I starten af 2023 blev det i FSR's cybersikkerhedsudvalg besluttet at nedsætte en arbejdsgruppe, der havde til formål at præsentere første udkast til et rammeværk/en skabelon til en NIS2 ISAE 3000-erklæring.

Erklæringen har fået navnet "Uafhængig revisors ISAE 3000-erklæring med begrænset sikkerhed om foranstaltninger til styring af risici i relation til net- og informationssystemer og rapporteringsforpligtelser i henhold til aftale med [Kunde]".

Når man læser direktivet står det hurtigt klart, at ansvaret ikke kan løftes af de enkelte aktører hver for sig, men at samarbejde og koordinering er nødvendigt, i et større omfang end vi tidligere har set. Når denne erkendelse først er nået, bliver konsekvensen også, at en erklæring aldrig vil kunne stå alene, uanset hvor bredt scope er, og hvor stærke revisionshandlinger der lægges op til. Derfor er det også relevant at se på, hvor stærk (og dermed omkostningstung) en erklæring skal være.

Revisorerklæringer med begrænset sikkerhed er i overensstemmelse med denne tankegang, idet de identificerer og adresserer væsentlige risici snarere end at forsøge at eliminere dem fuldstændigt. Dette sker i erkendelse af, at fuld sikkerhed ikke altid er mulig eller omkostningseffektiv.

I det store og hele giver en revisorerklæring med begrænset sikkerhed en balance mellem behov for overbe-

visning og omkostningseffektivitet. Det er samtidig forventningen, at denne balance med tiden vil forskyde sig. Når der er indhentet erfaring med kontrolaktiviteter og revisionshandlinger på alle de relevante områder, vil disse kunne gennemføres mere effektivt, og samtidig vil konsensus om, hvor omfattende opfølgningen på forsyningskæden skal være, også gøre, at handlingerne kan tilpasses mere præcist, hvorefter det vil være relevant at udarbejde erklæringer med høj grad af sikkerhed, såfremt disse efterspørges af virksomhederne.

Erklæringen er ikke et udtryk for minimumskrav og indeholder eksempler på kontrolaktiviteter og arbejdshandlinger. Disse er alene til inspiration og bør altid tilpasses til den konkrete risikovurdering, til de foranstaltninger, der i øvrigt måtte være aftalt parterne imellem, og under hensyn til revisors professionelle vurdering.

Erklæringen er udarbejdet til brug for de godkendte revisorer og må ikke anvendes af andre.

De konkrete kontrolmål og kontrolaktiviteter i erklæringen

Det primære fokus har i første omgang været at definere relevante kontrolmål og kontrolaktiviteter.

Vi ved, at mange virksomheder i de seneste år har arbejdet på at højne deres IT-sikkerhed med udgangspunkt i kendte og relevante standarder som ISO 27000, NIST og CIS. Derfor var udgangspunktet for erklæringen at blive inspireret af relevante kontrolaktiviteter fra forskellige standarder og samtidig gøre rammeværket letanvendeligt.

NIS2-direktivets artikel 21 pkt. 2 indeholder ti konkrete minimumskrav til etablering af tekniske og organisatoriske foranstaltninger.

Heri lægges der op til en helhedsorienteret tilgang med "all-hazards approach": "De i stk. 1 omhandlede foranstaltninger baseres på en tilgang, der omfatter alle farer og sigter på at beskytte net- og informationssystemer og disse systemers fysiske miljø mod hændelser, og mindst omfatter følgende …"

Derfor blev artikel 21 pkt. 2 ret centralt i arbejdet, og der blev skabt den nødvendige kobling mellem erklæringsskabelon og direktivet. Følgende minimumskrav blev derfor defineret som kontrolmål og understøttet med relevante kontrolaktiviteter:

A. Politikker for risikoanalyse og informationssikkerhed (17 kontrolaktiviteter)
B. Håndtering af hændelser (7 kontrolaktiviteter)
C. Driftskontinuitet og krisestyring (12 kontrolaktiviteter)
D. Forsyningskædesikkerhed, herunder leverandørstyring (10 kontrolaktiviteter)
E. Sikkerhed i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder (18 kontrolaktiviteter)
F. Politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici (8 kontrolaktiviteter)
G. Retningslinjer for basal "cyberhygiejne" og træning i cybersikkerhed (3 kontrolaktiviteter)
H. Politikker og procedurer relateret til kryptografi og kryptering (9 kontrolaktiviteter)
I. Medarbejdersikkerhed, adgangsstyring og styring af aktiver (asset management) (18 kontrolaktiviteter)
J. Anvendelse af multifaktorautentifikation eller "kontinuerlige autentifikationsløsninger" (hvor relevant) (5 kontrolaktiviteter).

I relation til ovenstående er det væsentligt at huske, at der ikke er kontrolmål, som knytter sig til alle artikler i NIS2, som direkte eller indirekte stiller krav til de virksomheder, som er essentielle eller vigtige enheder. Fokus har været på de krav, som skal stilles videre i værdikæden, og her har det været vurderingen, at disse i al væsentlighed er dækket med artikel 21.

Det vil naturligvis være relevant med yderligere krav, hvis essentielle eller vigtige enheder selv ønsker at afgive en erklæring, og denne kan da udbygges til også at omfatte disse krav. For version 1.0 har ønsket dog alene været at dække værdikæden.

Opsummering og det videre forløb

Udkast til erklæringsskabelonen blev gennemgået og kommenteret i FSR's cybersikkerhedsudvalg i april - august, hvorefter den for første gang i september 2023 blev præsenteret på konferencen Sikkerhed & Revision.

Udkastet har efterfølgende været til kommentering hos de virksomheder og personer, der har udtrykt interesse herfor, og en endelig version forventes at foreligge inden årets udgang.

Med NIS2 er net- og informationssikkerhed i samfundskritisk infrastruktur blevet institutionaliseret i meget højere grad end hvad vi hidtil har set. Dog har EU stadig givet de enkelte stater mulighed for at fortolke og tilpasse sig på nationalt plan inden for de givne rammer ved at vælge et direktiv frem for en forordning. Vi kan kun forvente øget regulering på dette område i de kommende år.

NIS2 repræsenterer en betydelig milepæl for Europas digitale fremtid, ligesom der skabes et solidt fundament for at beskytte kritisk infrastruktur og styrke cybersikkerheden i hele det digitale økosystem på tværs af medlemslandene i Europa.

Den kommende forordning om kunstig intelligens – hvad skal vi forvente?

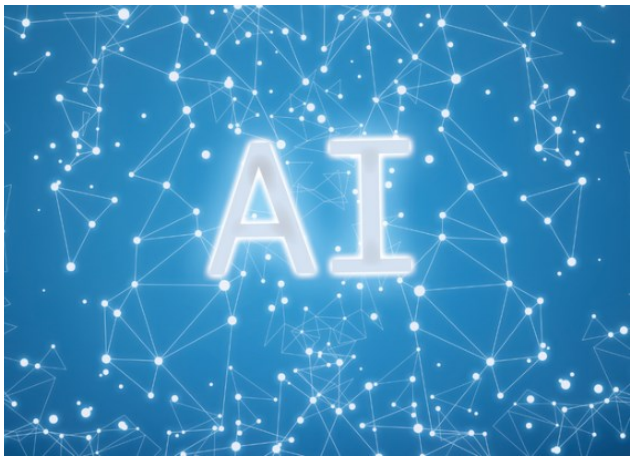
Kirsten Marie Donato, Advokat, Director, Poul Schmith Kammeradvokaten

Hvorfor en forordning om kunstig intelligens?

EU-kommissionen fremsatte i april 2021 forslag til en forordning om kunstig intelligens – i daglig tale kendt som AI-forordningen. Selvom der allerede på tidspunktet for fremsættelsen af forslaget i flere år havde været et vist fokus på kunstig intelligens samt debat om behovet for lovgivning på området, er både fokus på og udbredelse af AI-systemer i perioden efter fremsættelsen af forslaget eksploderet. Samtidig er erkendelsen af, at eksisterende lovgivning, f.eks. databeskyttelsesforordningen, ikke i tilstrækkelig grad imødegår risiciene ved kunstig intelligens, blevet fremhævet af en lang række aktører, inkl. aktører i tech-industrien.

Udviklingen har bl.a. betydet, at både Rådet for den Europæiske Union ("Rådet") og Europa-Parlamentet i forbindelse med deres behandling af EU-Kommissionens forslag, er fremkommet med en lang række ændringsforslag til forordningsteksten, f.eks. nye regler om generativ AI og foundational models. De tre kompromisforslag danner nu udgangspunktet for de såkaldte trilogforhandlinger.

Det er i skrivende stund forventningen, at AI-forordningen vedtages i slutningen af 2023 eller i starten af 2024. Under alle omstændigheder vil foråret 2024 være en vigtig ultimativ deadline pga. Europa-Parlamentsvalg og udløb af Kommissionsperioden.



Hvilke systemer er omfattet af AI-forordningen?

Udkastet til AI-forordningen (herefter blot "AI-forordningen") finder anvendelse på AI-systemer, og én af forordningens mest centrale definitioner fastlægger derfor også, hvad et AI-system er.

I det seneste udkast til AI-forordningen defineres et AI-system (kort fortalt) som *et maskinbaseret system, der er designet til at operere med varierende grader af autonomi, og som med henblik på eksplicitte eller implicitte formål generer outputs såsom forudsigelser, anbefalinger eller beslutninger, der påvirker fysiske eller virtuelle omgivelser.*

Der er tale om en bred definition af AI-systemer. Sigtet er en definition, der dels er afstemt med arbejdet i internationale organisationer, der arbejder med kunstig intelligens, for at sikre retssikkerhed, harmonisering og bred accept, dels at have en definition der giver fleksibiliteten til at imødekomme den (særdeles hastige) teknologiske udvikling.

Ved fastlæggelsen af, hvad der er et AI-system, er det værd at have for øje, at det i forordningen præciseres, at nøglekarakteristika ved kunstig intelligens er dens indlærings-, ræsonnement- eller modelleringsevner, hvilket bidrager til at adskille disse systemer fra enklere softwaresystemer eller programmeringstilgange. AI-systemer er dermed designet til at fungere med varierende niveauer af autonomi, hvilket betyder, at de i det mindste har en vis grad af uafhængighed af handlinger fra menneskelig kontrol og af evner til at fungere uden menneskelig indgriben.

En risikobaseret tilgang

AI-forordningens regulering af AI-systemer er risikobaseret. Reguleringen intensiveres afhængig af den risiko, som AI-systemet er forbundet med. Man skal dog være opmærksom på, at Europa-Parlamentet har foreslået en række generelle principper om f.eks. transparens, datagovernance, diversitet, privatlivsbeskyttelse mm., som alle AI-systemer bør leve op til. Hvorvidt dette forslag medtages i den endelige forordningstekst, vil tiden vise.

Den risikobaserede tilgang betyder først og fremmest, at AI-systemer inddeles i systemer med en 1) uacceptabel risiko, 2) høj risiko, 3) begrænset risiko, eller 4) lav eller minimal risiko, jf. **Figur 1** nederst på næste side.

AI-systemer med en uacceptabel risiko forbydes, idet de anses for at udgøre en for høj risiko for bl.a. vores grundlæggende rettigheder. Hvilke AI-systemer, der er omfattet af forbuddet, fremgår direkte af forordningens artikel 5. Dette er eksempelvis systemer, som bruges til omfattende social kontrol eller overvågning, og forudsætter naturligvis, at betingelserne for hver forbudte use case er opfyldt.

Systemer med en høj risiko er AI-systemer, som kan have alvorlige konsekvenser for bl.a. vores grundlæggende rettigheder. Det vil f.eks. være AI-systemer, der er beregnet til at blive anvendt som en sikkerhedskomponent i et produkt eller i sig selv er et produkt, der er omfattet af den EU-harmoniseringslovgivning, der er anført i bilag II til forordningen. Det vil også være AI-systemer, der fremgår af listen af "use cases" opregnet i bilag III til forordningsudkastet. Et eksempel på sidstnævnte er AI-systemer, der er beregnet til rekruttering eller udvælgelse af personer til et job, navnlig til annoncering af ledige stillinger, screening eller filtrering af ansøgninger, evaluering af ansøgere under samtaler eller prøver.

AI-systemer med en begrænset risiko er overordnet AI-systemer, der er beregnet til at interagere med fysiske personer, f.eks. chatbots. Her gælder en række minimumskrav for gennemsigtighed, som skal sikre, at personer, der interagerer med systemer, ved, at de har med et AI-system at gøre.

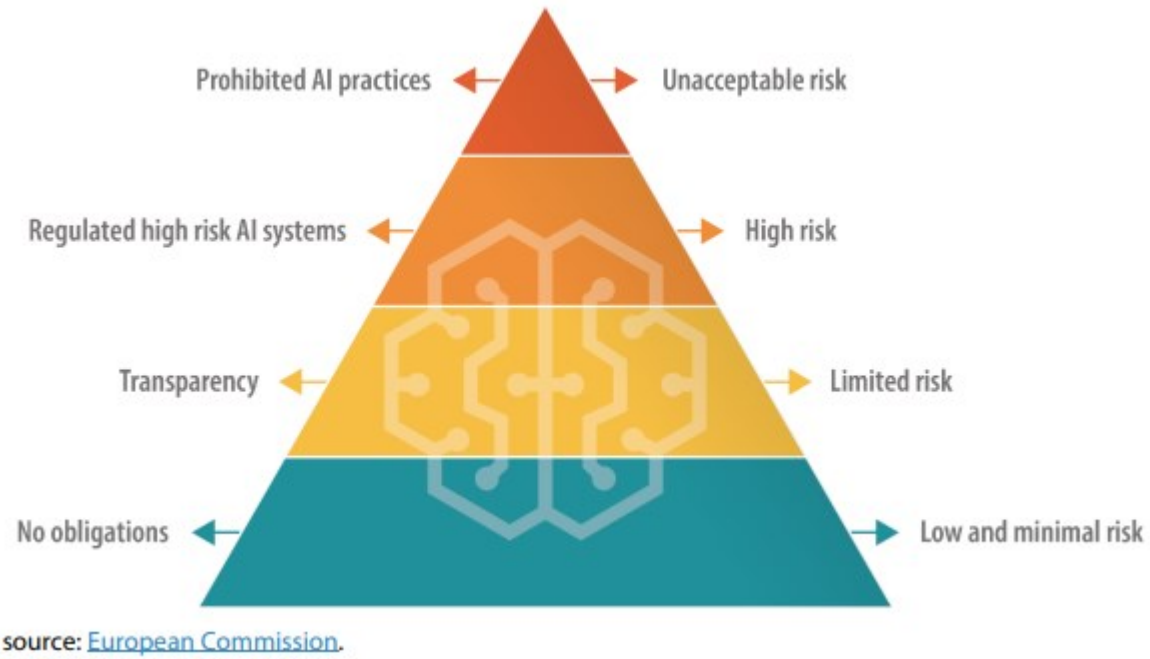
AI-systemer med lav eller minimal risiko kan frit omsættes og anvendes.

Skrappe krav for højrisiko-AI-systemer

AI-systemer, der er kategoriseret som højrisiko, pålægges en række skrappe forpligtelser i forordningens kapitel 2. Det omfatter eksempelvis følgende:

- Risikostyringssystem (artikel 9): Etablering, dokumentation og vedligehold af et risikostyringssystem, der bl.a. skal identificere risici tilknyttet systemet samt indføre passende risikostyringsforanstaltninger til at adressere de pågældende risici.
- Data og datastyring (artikel 10): Såfremt AI-systemet involverer træning af modeller med data, skal de pågældende datasæt efterleve en række kvalitetskriterier, herunder bl.a. for passende datastyring- og dataforvaltningspraksis, samt at datasæt skal være relevante, repræsentative, fejlfri og fuldstændige.
- Teknisk dokumentation (artikel 11): Der skal udarbejdes teknisk dokumentation, der påviser, at højrisiko-AI-systemet overholder de krav, der er fastsat i forordningen.
- Registrering (artikel 12): Højrisiko-AI-systemer udformes og udvikles på en sådan måde, at hændelser ("logfiler") registreres automatisk, når højrisiko-AI-systemet er i drift. Denne logning skal være i overensstemmelse med anerkendte standarder eller fælles specifikationer.
- Gennemsigtighed og formidling af oplysninger til brugere (artikel 13): Systemerne skal udformes og udvikles på en sådan måde, at deres drift er tilstrækkelig gennemsigtig til, at brugerne kan fortolke systemets output og anvende det korrekt. Systemet skal ledsages af brugsanvisninger i et passende digitalt format eller på anden vis, som indeholder kortfattede, fuldstændige, korrekte og klare oplysninger, som er relevante, tilgængelige og forståelige for brugerne.
- Menneskeligt tilsyn (artikel 14): Højrisiko-AI-systemer skal udformes og udvikles på en sådan måde, herunder med passende menneske-maskine-grænseflade

Figur 1. Inddeling af AI-systemer ud fra en risikobaseret tilgang



Data source: European Commission.

værktøjer, at mennesker kan føre effektivt tilsyn med dem i den periode, hvor AI-systemet er i brug.

- Nøjagtighed, robusthed og cybersikkerhed (artikel 15): Højrisiko-AI-systemer skal udformes og udvikles på en sådan måde, at de i lyset af deres tilsigtede formål har et passende niveau af nøjagtighed, robusthed og cybersikkerhed i hele deres livscyklus.

Forpligtelser fordelt på værdikæden

Forordningens kapitel 3 fastsætter en række forpligtelser for udbydere, brugere og øvrige aktører afhængig af deres placering i værdikæden. Det betyder, at udbydere af højrisiko-AI-systemer pålægges væsentligt flere krav end brugere af AI-systemer.

Udbydere af højrisiko-AI-systemer skal efter forordningens artikel 16 bl.a.:

- sikre overholdelse af de ovennævnte generelle krav for højrisiko-AI-systemer og foretage korrigerende foranstaltninger, hvis kravene ikke er opfyldt,
- indføre et kvalitetsstyringssystem,
- udarbejde den tekniske dokumentation for højrisiko-AI-systemet,
- opbevare de logfiler, der automatisk genereres af deres højrisiko-AI-systemer, når logfilerne er under deres kontrol,
- sørge for at gennemføre overensstemmelsesvurdering for systemet,
- sørge for at registrere højrisiko-AI-systemet i en særlig EU-database herfor,
- underrette de relevante myndigheder i de lande, hvor de har tilgængeliggjort eller ibrugtaget systemet,
- CE-mærke systemet, samt
- kunne påvise overholdelse af kravene til tilsynsmyndighederne.

AI-forordningen stiller færre krav til brugerne af højrisiko -AI-systemer. Brugerne skal efter forordningens artikel 29:

- anvende højrisiko-AI-systemet i overensstemmelse med brugsanvisningen,
- sikre relevante inputdata i lyset af formålet med systemet,
- overvåge driften af systemet på grundlag af brugsanvisningen,
- opbevare logfiler, hvis de er under brugernes kontrol, samt
- udarbejde en konsekvensanalyse vedrørende databeskyttelse (DPIA) på baggrund af oplysningerne i brugsanvisningen.

Brugere vil som nævnt blive anset for selv at være udbydere, hvis de markedsfører højrisiko-AI-systemet under eget navn eller tager det i brug, ændrer dets formål eller foretager en væsentlig ændring af systemet.

Flere gennemsigtighedsforpligtelser

AI-forordningsudkastet fastsætter forskellige gennemsigtighedsforpligtelser afhængig af, hvilken type AI-system der er tale om.
Artikel 52 indeholder en række gennemsigtighedsforpligtelser for visse AI-systemer.

Udbydere skal eksempelvis sikre, at AI-systemer, der er beregnet til at interagere med fysiske personer, udformes og udvikles på en sådan måde, at fysiske personer oplyses om, at de interagerer med et AI-system, medmindre dette er indlysende ud fra omstændighederne og anvendelsessammenhængen.

Brugere af et system til følelsesgenkendelse eller et system til biometrisk kategorisering skal oplyse de fysiske personer, der er eksponeret for systemet, om anvendelsen af systemet.

Brugere af et AI-system, der genererer eller manipulerer billed-, lyd- eller videoindhold, der i væsentlig grad ligner faktiske personer, genstande, steder eller andre enheder eller begivenheder, og som fejlagtigt vil fremstå ægte eller sandfærdigt ("deepfake"), skal oplyse, at indholdet er blevet genereret kunstigt eller manipuleret.

Der er dog undtagelser fra kravene i forbindelse med systemer, der er tilladt ved lov med henblik på retshåndhævelse. Ved sidstnævnte anvendelse af AI-systemet er oplysningspligten derudover heller ikke gældende, hvis anvendelsen er nødvendig for at udøve retten til ytringsfrihed eller retten til kunst og videnskab, der er sikret ved Den Europæiske Unions charter om grundlæggende rettigheder.

Derudover har Europa-Parlamentet i artikel 68c foreslået en ny "right to explanation of individual decision-making". Reglen betyder, at når en bruger træffer visse fuldautomatiske afgørelser ved brug af et høj-risiko AI-system over for enkeltindivider, har den pågældende person som udgangspunkt ret til at anmode brugeren om at modtage en klar og meningsfuld forklaring på AI-systemets rolle i beslutningsprocessen. Denne forklaring skal indeholde de vigtigste parametre i beslutningen og de involverede inputdata.

Denne ret til forklaring gælder ved siden af oplysningsforpligtelserne i databeskyttelsesforordningens artikel 13-14

og 22 samt indsigtsretten i artikel 15, hvor man har ret til information om forekomsten af automatiske afgørelser, herunder profilering, som omhandlet i artikel 22, stk. 1 og 4, og som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede.

Mens vi venter

Selvom AI-forordningen endnu ikke er vedtaget, er det værd allerede nu at begynde at forberede sig på at efterleve forordningen. Det kan bl.a. gøres gennem følgende aktiviteter:

1) Fokus på compliance med databeskyttelsesreglerne
   Mange AI-systemer vil være omfattet af databeskyttelsesreglerne, som allerede gælder i dag. Hvis man som virksomhed eller myndighed lever op til disse regler i forbindelse med brugen af AI-systemer, er man godt på vej, da databeskyttelsesforordningen og AI-forordningen varetager mange af de samme hensyn og regulerer flere af de samme emner, såsom data, risici og sikkerhed.

2) Kortlæg den nuværende brug af AI-systemer
   I det omfang I som virksomhed eller myndighed allerede har AI-systemer som en del af jeres systemlandskab, bør I vurdere, om systemerne vil være forbundet med uacceptabel risiko, høj risiko, begrænset risiko, eller lav eller minimal risiko. Det vil sikre, at I kan forberede jer på omfanget af krav til jeres systemer.

3) Tænk AI-forordningen ind i nye AI-systemer
   Hvis I påtænker at udvikle eller anskaffe nye AI-systemer, bør I fastlægge hvilken aktørrolle I har samt foretage samme vurdering som beskrevet ovenfor. Derudover bør AI-forordningens krav tænkes ind i udviklingsaktiviteter og i kontrakter med leverandører af AI-systemer.

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

Nye medlemmer

Nye medlemmer i IIA fra 14.9.2023 - 8.12.2023

BankNordik
Gunnvá Brockie

Deloitte
Rasmus Grynderup Kiær Steffensen

Københavns Kommune
Obi Hamdam

Novo Nordisk
Celina Meric
Tatiana Chupilina

PFA Pension
Basel Obari

PwC
Karsten Sylvest Olsen
Lars Agerstad

Sydbank
Per Asmussen

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.

08.01.2024: CIA Part 2 Virtual Training - Day 1,2,3
09.04.2024: Temadag for den finansielle sektor
11.6-12.6.24: IIA Årsmøde 2024

"Bagsmækken"

Foreningens adresse

Foreningen af Interne Revisorer (IIA Denmark)
Intern revision
Nykredit
Kalvebod Brygge 1-3
1780 København V

CVR nr. 73954215

Indmeldelse i foreningen

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

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

Jobannoncer

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

Certificeringer

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

Heino Hansen, CIA, Nordea GIA - Nordea Finance
☎ 31 18 38 01 ✉ heino.hansen@nordea.com

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

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

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

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

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

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

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

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

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

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

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