INFO

Foreningen af Interne Revisorer
Nummer 80 | April 2022 | 27. årgang

Intern revision som kulturbærer

Tanker om intern revisions fremtid

Diversity and Inclusion

Why it matters and how to audit it

Har du data kan du få …

… har du ingen må du gå

Datatilsynet i fokus ● Tips og tricks ● Explainable AI

INFOs redaktion

Ansvarshavende redaktør
Nordisk Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
BNP Paribas Personal Finance
☎ 36 39 52 61 ✉ birgitte.svenningsen@bnpparibas-pf.dk

Øvrig redaktion
Manager
Christian Barrett
Deloitte
☎ 30 93 54 24 ✉ cbarrett@deloitte.dk

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

Chief Expert, CIA
Vanita Shukla Hork
Nordea
☎ 30 12 84 34 ✉ vanita.hork@nordea.com

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

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

Koncernrevisionschef
Louise Claudi Nørregaard
PFA
☎ 61 55 84 88 ✉ lcn@pfa.dk

Næste nummer
INFO 81 udkommer i september 2022.
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

Birgitte Rousing Svenningsen, Nordisk Revisionschef, CIA, CISA, BNP Paribas Personal Finance

Vores moderorganisation "The Institute of Internal Auditors" (IIA) har siden 2008 udarbejdet en årlig undersøgelse af intern revision – den såkaldte "Pulse" undersøgelse og IIA har offentliggjort resultatet af undersøgelsen for Nordamerika for 2022. Resultatet af en lignende undersøgelse i Europa eller i Danmark vil muligvis give et lidt andet billede, men jeg tror dog, at det ikke vil være væsentligt anderledes, hvorfor man kan få relevant og brugbar information ved læsning af den amerikanske undersøgelse. Rapporten, som er på baggrund af undersøgelsen, kan man som medlem af vores forening tilgå her: https://www.theiia.org/globalassets/site/content/research/pulse/2022/2022pulse-report.pdf

Årsagen til at jeg indleder lederen på denne måde, er at Pulse rapporten angiver hvilke risici, de interne revisorer anser som mest væsentlige. De 3 væsentligste risici er:

1. Cybersecurity
2. IT
3. Third-party relationships.

For første gang siden begyndelsen af de årlige undersøgelser, viser undersøgelsen, at sustainability/ikke-finansiel rapportering anses som et øget risikoområde.

Undersøgelsen viser dog også, at de interne revisionsplaner ikke fuldt ud reflekterer dette risikobillede. Cybersecurity og IT indgår som væsentlige områder i revisionsplanerne, men i lidt mindre grad end det kunne forventes baseret på vurderingen af risicienes størrelse. Third-party relationships og sustainability/ikke finansiel rapportering er væsentligt underdimensioneret i revisionsplanerne.
Det er et billede, jeg tror, at vi er mange som kan genkende. Der er formodentlig flere årsager hertil, for eksempel:

- Vi – interne revisorer – mangler kendskab til, hvordan man reviderer disse lidt mere uhåndgribelige områder
- Der er så mange potentielle områder, som man kan revidere, så vi ved ikke, hvor vi skal starte, og hvor vi skal slutte.

Efter en forhåbentlig veloverstået påske, bringer dette nummer af INFO en række spændende artikler, som kan give inspiration til, hvordan vi kommer tættere på at reflektere ovennævnte risici i vores revisionsplaner og vores dagligdag.

Kim Guldberg skriver i artiklen "Har du data kan du få, har du ingen må du gå" om vigtigheden i, at virksomhederne logger de rigtige data, hvilket både har relation til revision af Cybersecurity og IT.

På IT og Third-party området skriver Jacob Krabbe om udfordringerne ved anvendelse af services, hvor dataene overføres til USA.

Kamil Polak skriver om risici ved brug af Artificial Intelligence (AI) i forbindelse med Model Risk Management, og hvad man som revisor skal være opmærksom på, hvis virksomheden anvender AI i denne proces.

Hvorom disse 3 artikler behandler vidt forskellige problemstillinger, er de alle relevante for de 3 risici, som de interne revisorer i Nordamerika har udpeget, som de 3 væsentligste risici.

På det mere bløde område bringer dette nummer af INFO to inspirerende artikler. Først Kristian Bollerups artikel om intern revision som kulturbærer. Kristian skriver om, hvordan den interne revision i Lego medvirker til at drive kulturen i Lego. Han understreger i den forbindelse vigtigheden af, at kulturen sættes og understøttes af topledelsen.

I forlængelse heraf giver Nina Belcaid et fyldestgørende og inspirerende indblik i, hvordan man kan skabe værdi ved at revidere området "diversity and inclusion".

Der er således nok revisionsområder at tage fat i inden for de mere bløde områder. Jeg tror, at det i denne forbindelse er vigtigt at undersøge, hvad der passer til den virksomhed, som man arbejder for, hvilket også er et af de budskaber, som Kristian Bollerup fremfører.

Tendensen med, at intern revision i større grad skal fokusere på bløde områder som for eksempel ESG, er ikke kun noget som fremgår af Pulse rapporten. Professor Kim Klarskov Jeppesen har i samarbejde med Dr. Rainer Lenz skrevet en interessant artikel om, at interne revision påvirkes af megatrends. De påpeger, at de vigtigste er digitalisering, bæredygtighed, nye arbejdsformer, individualisme og sikkerhed. Kim giver et kort resume af artiklen i dette nummer af INFO, men det er bestemt også værd at læse den fulde artikel.

Pulse undersøgelsen har også undersøgt, hvilken påvirkning CoViD19 har haft på intern revision og på de interne revisionsarbejdsmetoder. Konklusionen er, at CoVID19 ikke har haft en væsentlig negativ indvirkning på intern revision. Konklusionen er også, at intern revisions arbejdsmetoder er blevet påvirket og forventningen er, at der i højere grad vil blive arbejdet fra hjemmearbejdspladser i fremtiden.

Fortsættes næste side

Christian Barrett og Qasim Rashid skriver i artiklen "Tips og Tricks: Optagelse af walk through over Teams" om hvordan CoVID19 og øget brug af videomøder også har medført, at nogle revisorer er begyndt at optage møderne som erstatning for at skrive referater, specielt ved walk throughs. Dette er en tidsbesparende metode, men også en metode som giver visse udfordringer.

Til slut vil jeg ønske jer alle god læselyst både med artiklerne i dette nummer af INFO og med Pulse rapporten fra IIA. Jeg er overbevist om, at begge vil give jer et godt afsæt på vejen til i større grad at dække de mest væsentligste risici og på denne måde være værdiskabende.

God læselyst!

Nyt fra redaktionen

Birgitte Rousing Svenningsen, Nordisk Revisionschef, CIA, CISA, BNP Paribas Personal Finance

På redaktionens vegne er jeg glad og stolt over at kunne byde velkommen til Stine Juhl-Hansen i redaktionen. Stine har til dagligt sin gang i Danfoss, hvor hun arbejder som IT revisor. Stine supplerer ekstremt godt de andre redaktionsmedlemmer, idet hun kommer fra en industrivirksomhed i Jylland og samtidig med IT baggrund. Det vil betyde, at vi som redaktion endnu mere kan fokusere på artikelemner vedrørende Cybersecurity, hvilket alle undersøgelser viser er et høj-risiko område for de fleste virksomheder. Jeg ser meget frem til at arbejde sammen med Stine.

Har du lyst til at følge Stines gode eksempel og også stille dig til rådighed for redaktionsarbejdet, er du meget velkommen til at kontakte mig på birgitte.svenningsen@bnpparibas-pf.dk

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.

FINANSTILSYNET

Revisor til samfundsvigtigt forsikringstilsyn

Vil du være med til at sikre en robust, ansvarlig og ordentlig finansiel sektor i Danmark?
Vi søger en revisor, der vil arbejde for at sikre samfundets tillid til skadesforsikringsselskaberne.

Finanstilsynet mangler dig som kollega i vores kontor for Reassurance og Skadesforsikring.

Jobbet
Du skal først og fremmest arbejde med at vurdere selskabernes forretningsmodel ud fra selskabernes indberetninger, herunder års- og halvårsrapporten. Du vil også komme med på virksomhedsbesøg hos selskaberne, hvor vi i dialog med de ledende medarbejdere undersøger, om selskabernes forretningsmodel fortsat lever op til lovens krav. Som revisor vil du få en særlig rolle i forhold til arbejdet med regnskabs- og revisionsreglerne, herunder certificeringsordningen. Du kommer også til at lave tværgående analyser af aktuelle emner, hvor vi benchmarker på tværs af selskaberne. Endelig får du mulighed for at deltage i internationale arbejdsgrupper, ligesom der er mulighed for at undervise og holde oplæg eksternt og internt.

Om dig
Du skal være cand.merc.aud og have lyst til at lære om selskabernes forskellige forretningsmodeller og de risici, der er forbundet med dem. Du bliver motiveret af at kunne få indflydelse på en vigtig samfundsopgave og har en åben og positiv tilgang til forskelligartede opgaver indenfor dit felt. Det er afgørende, at du har gode samarbejdsevner, da vi sjældent løser opgaverne alene

Det er en fordel, hvis du har 3-5 års erfaring med revisionsarbejde og er vant til at arbejde med de internationale regnskabsstandarder. Når vi er på virksomhedsbesøg i selskaberne, har hele holdet ansvar for inspektionen. Det gør ikke noget, hvis du har lyst til at påtage dig rollen som inspektionsleder et par år efter din ansættelse.

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

Finanstilsynet
Hvis du bliver vores nye kollega, så bliver du en del af Finanstilsynets kontor for Reassurance og Skadesforsikring. Vi er 20 kolleger/ medarbejdere, som primært er økonomer, jurister, aktuarer og revisorer, der er vant til at sparre med hinanden i et fagligt stærkt miljø.

Kontoret for Reassurance og Skadesforsikring er ansvarligt for at sikre, at skadesforsikringsselskabernes forretningsmodeller er holdbare og lever op til lovens krav. Vi har også ansvaret for revisionsområdet for bank og forsikring, for regnskabsreglerne for forsikring og for certificeringsordningen. Vores ambitionsniveau er, at vi opdager eventuelle faresignaler så tidligt som muligt, så vi i samarbejde med selskabet kan finde den rigtige løsning for at sikre kunderne.

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

Som medarbejder i Finanstilsynet tilbyder vi dig også et internt karriere- og kompetenceprogram, flekstidsordning, betalt frokostpause, kantineordning, massageordning, renseriordning og en række medarbejderforeninger med fokus på bl.a. vin, fodbold, skak, løb og badminton.

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

Oplysninger om løn- og ansættelsesvilkår kan du få ved at henvende dig til vores HR Rekrutteringspartner Simone Munkholm på tlf. 91 33 70 24

Sådan ansøger du
Send din ansøgning via vores elektroniske ansøgningssystem på finanstilsynet.dk **senest den 8**. maj 2022. Husk at uploade dit CV, eksamensbeviser og andre relevante bilag sammen med din ansøgning. Vi tager ikke ansøgninger i betragtning, der er blevet indsendt på anden vis.

Vi opfordrer alle interesserede uanset alder, køn, religion eller etnisk tilhørsforhold til at søge stillingen.

Du kan læse mere om Finanstilsynet på **www.finanstilsynet.dk** – særligt under rubrikken "Karriere". Du kan også finde os på LinkedIn ved at søge på Finanstilsynet Danmark.

Tanker om intern revisions fremtid

Kim Klarskov Jeppesen,
Professor, CBS

Den 8 oktober 2021 fejrede IIA i de nordiske lande deres 70 års jubilæum med et online arrangement, hvor Dr. Rainer Lenz på min foranledning var inviteret til at tale om intern revisions fremtid. Rainer Lenz er revisionschef for SAF Holland, der er noteret på den tyske fondsbørs. Han har tillige en PhD grad i intern revision, som jeg havde fornøjelsen af at være bivejleder på.

Talen gav efterfølgende anledning til en del debat på de sociale medier, hvilket en tale med den titel også bør give, medmindre den er helt tandløs. Debatten medførte en invitation fra redaktøren af EDPACS (The EDP Audit, Control, and Security Newspaper) til at skrive en artikel baseret på talen, og Rainer og jeg påtog os i fællesskab denne opgave. Artiklen med titlen "The Future of Internal Auditing: Gardener of Governance" blev publiceret i februar 2022 og kan hentes gratis på linket nederst i artiklen.

Formålet med denne artikel i INFO er at give et kort resume og dermed lave lidt reklame for vores artikel. Synspunkterne i artiklen er alene forfatternes og repræsenterer ikke IIA Danmarks eller IIA Globals holdning. Tværtimod er vi noget kritiske over for det officielle IIAs manglende stillingtagen til nogen af de udfordringer, som vi mener, at intern revision står over for.

Hverken Rainer eller jeg har en privilegeret indsigt i fremtiden. Her støtter vi os til det tyske institut for fremtidsforskning og de megatrends, som de tror, vil præge fremtidens samfund. Vores artikel handler om hvordan vi mener, at disse megatrends påvirker intern revision. De vigtigste af disse er i vores øjne digitalisering, bæredygtighed, nye arbejdsformer, individualisme, og sikkerhed.

Digitaliseringen af samfundet er allerede vidt fremskreden og både intern og ekstern revision har de senere år haft fokus på at integrere dataanalyse i revisionsprocessen. Der er lavet mange rapporter om potentialet, men praksis halter generelt noget efter disse, for nu at sige det på den høflige måde. Hvis ikke interne revisorer bliver bedre til at skabe værdi ved at give ledelsen forretningsmæssig relevant indsigt i virksomhedens data, vil controllere eller eksterne revisor uden tvivl gøre det.

Nødvendigheden af bæredygtighed er heller ikke nyt, men mangler for alvor at sætte aftryk i virksomheders strategi og forretningsprocesser. Dette vil dog ske, som EUs nye krav om ESG rapportering for at kanalisere investeringer til bæredygtige virksomheder viser. ESG bliver en hjørnesten i virksomheders strategi, og når dette sker, vil interne revisioner kunne skabe værdi for bestyrelserne ved at give sikkerhed for, at virksomheden efterlever denne strategi.

Nye arbejdsformer og individualisme handler om, at traditionelle ansættelsesformer er på vej til at blive afløst af en mere fleksibel og løs tilknytning til virksomheder. Hvor der tidligere var ansatte, hyrer virksomheder nu i stigende grad selvstændige konsulenter for kortere eller længere perioder. Dette giver udfordringer for virksomheders interne kontrolsystem, som interne revisorer skal revidere. Men det giver også muligheder for at gentænke den interne revisionsfunktion ved at inddrage selvstændige specialister midlertidigt på ad hoc opgaver i intern revision.

Den sidste væsentlige megatrend er at de risici samfundet står over for, vokser i antal og kompleksitet. Dermed vokset behovet for sikkerhed også. Dette medfører, at virksomheders risikostyring bliver af større betydning og dermed øges interne revisorers mulighed for at bidrage til netop denne. Der er imidlertid også en risiko forbundet med udviklingen. Jo mere de risici der styres fjerner sig fra interne revisorers normale kompetenceområde, jo større er risikoen for at komme i konkurrence med andre professioner.

For at tilpasse sig disse (og andre) megatrends og forblive relevante og legitime foreslår vi en model, hvor interne revisorer overvejer fem hovedområder - Se **Figur 1** på næste side.

"Planet" handler om at give intern revision en rolle i ESG. Intern revisions potentielle rolle i relation til Environment er omtalt ovenfor, men Social og Governance er lige så vigtige. Megatrenden om nye arbejdsformer antyder, at virksomheders legitimitet fremover vil handle om mere end blot profit. Virksomheder vil også skulle vise hvordan de bidrager med værdi til samfundet for at kunne tiltrække investeringer og talent. Denne branding er både en strategisk og operationel opgave, hvor ledelser får brug for sikkerhed for at mål opnås og ekstern rapportering er korrekt. Helt centralt for intern revisions værdiskabelse er dog Governance, altså at intern revision bidrager til at skabe en bedre selskabsledelse.

"Public" handler om at give alle relevante stakeholders indsigt i den værdi intern revision kan tilbyde. Det gælder bestyrelsesmedlemmer, hvis viden om intern revisions mulige værdiskabelse generelt er på et lavt niveau. Men det gælder også de lovgivere og regulatorer, der har magten til at kræve intern revision i visse typer selskaber og stille krav til kvaliteten af den interne revision, der udføres. Også her bør kendskabet til intern revision øges.

”Profession” handler om hvad intern revision er og vil være. Enhver profession skal have et samfundsmæssigt legitimt vidensgrundlag, som professionen baserer sin praksis på, og dette vidensgrundlag skal samtidig adskille professionen fra konkurrerende professioner. Vidensgrundlaget udmøntes i de standarder og den øvrige regulering, som interne revisorer arbejder efter. Intern revisions største konkurrent er ekstern revision, så intern revision må skabe et legitimt og mere homogent vidensgrundlag, der adskiller sig fra ekstern revision. Alternativet er at bliver underlagt ekstern revision, på samme måde som sygeplejersker er underlagt læger.

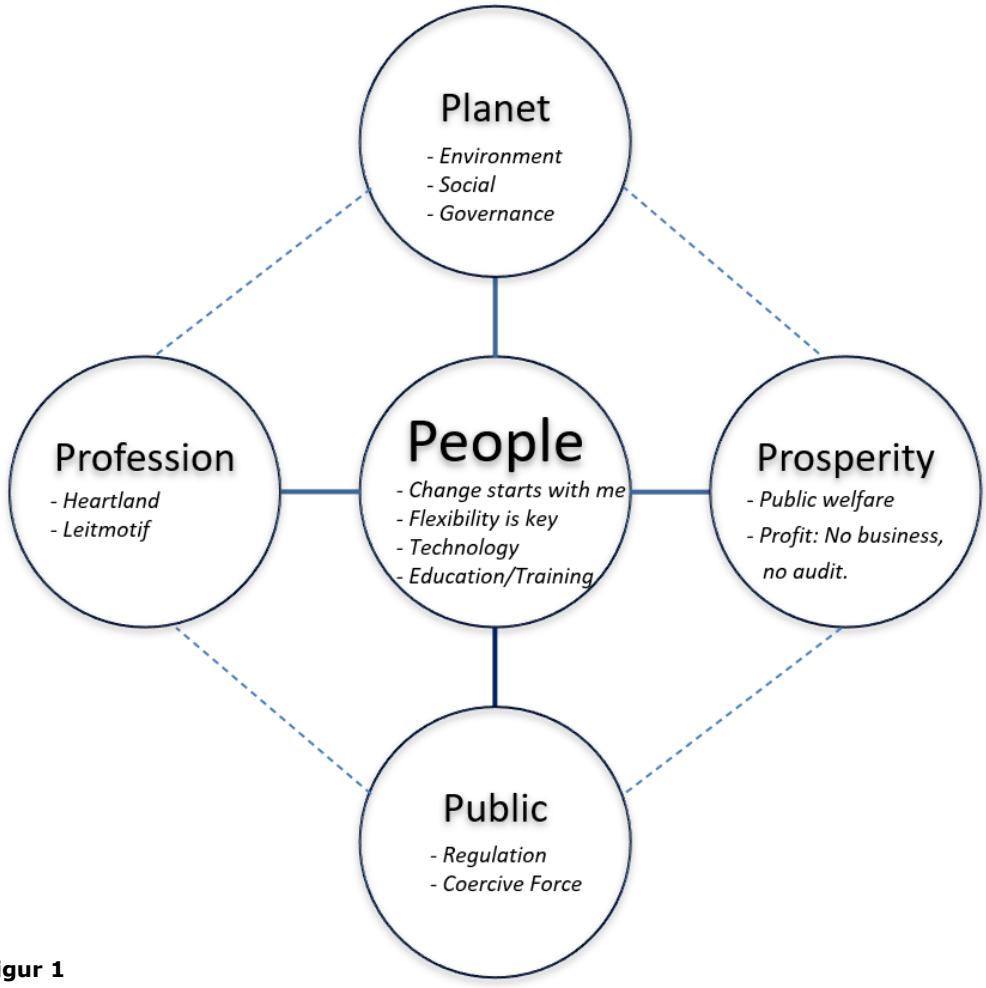
”Prosperity” handler om at virksomheder, udover at have en god selskabsledelse, også skal være profitable for at overleve. En sådan profitabilitet er ikke mulig uden at virksomheden påtager sig risici, men disse skal overvåges og styres for ikke at komme ud af kontrol. Intern revision skal bidrage til at skabe den nødvendige balance mellem risikovillighed og intern kontrol således at virksomheden når sine mål.

”People” handler om at udvikle interne revisorer i overensstemmelse med det vidensgrundlag, der er defineret under Profession, Planet og Public.

For at forklare stakeholders hvordan intern revision skaber værdi foreslår vi at bruge en metafor. Interne revisorer er ”**Gardeners of Governance**”. Vi forstår governance bredt som inkluderende alle tre elementer i ESG. Som gartnere har interne revisorer respekt for ’naturen’, forstået som det økosystem virksomheden indgår i. Interne revisorer sår frøene til god selskabsledelse i relation til ESG, og de vander og gøder de fremspirende ESG planter under hensyn til vejrudsigten og jordens beskaffenhed. Nu og da må interne revisorer også fjerne det ukrudt, der truer de fremspirende planter. Men med tålmodighed og den rette pleje vil god ESG vokse frem og sikre virksomhedens samfundsmæssige legitimitet og profitabilitet.

Den originale artikel kan hentes ved at klikke på DOI linket nedenfor:

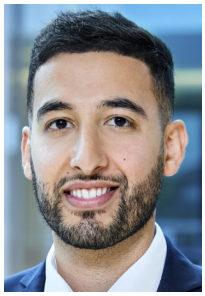
Rainer Lenz & Kim K. Jeppesen (2022) THE FUTURE OF INTERNAL AUDITING: GARDENER OF GOVERNANCE, EDPACS, https://doi.org/10.1080/07366981.2022.2036314



Figur 1

Tips og Tricks: Optagelse af walk through over Teams

Christian Barrett, Manager, Deloitte



Qasim Rashid, Assistant manager, Deloitte

Denne artikel er forhåbentligt startskuddet på en tilbagevendende type af artikler, hvor der deles tip og tricks fra den virkelige verden, og disse kan forhåbentligt bidrage til, at vi arbejder smartere. Har du tips og tricks som bør deles, er du mere end velkommen til at skrive til redaktionen.

Corona har haft stor påvirkning på vores hverdag og måden at arbejde på. Det har været på godt og ondt, og vi er heldigvis ved at være vendt tilbage til en eller anden form for normalitet. Der er dog en unik mulighed for at reflektere over nogen af de alternative måder at arbejde på og hvordan de kan hjælpe os fremadrettet. Måske har du og din organisation fundet nye veje at gå, som betyder, at I fremover ikke vender tilbage til fuld og hel fysisk tilstedeværelse.

En af de positive oplevelser som vi har haft, er i forbindelse med walk throughs. Det har som udgangspunkt altid været en handling der er udført ved, at vi fysisk har placeret os ved auditee og har påset processen fra vugge til grav. Det har bestemt sine fordele med den fysiske tilstedeværelse og for de processer som i et eller andet omfang stadig har manuelt præg giver det god mening. Vi må dog også erkende, at processer i større og større omfang finder sted i et virtuelt univers, og for de mere komplekse processer foregår processen gerne i flere forskellige IT-systemer.

Det er vores oplevelse at de komplekse processer med fordel kan køres over Teams og optages. Dette er baseret på følgende observationer:

+ Processen er mere fuldstændigt beskrevet og ikke baseret på ad hoc screenshots.
Når en walk through dokumenteres på den traditionelle måde med screenshots og dokumenter, så afspejler det færdige produkt det som preparer vælger at inkludere. Der kan derfor i større eller mindre grad være huller. Det vil ofte være uvæsentlige facetter af processen, men der er dog en risiko for at væsentlige elementer ikke er medtaget.

+ Funktionaliteter fremvises real time
Hvorvidt en video siger mere end 1.000 ord som det er tilfældet med et billede, kan vi hverken be- eller afkræfte. Det er dog en klar fordel, at en video leverer den visuelle del af processen, mens der også er mulighed for at auditee fortæller om processen. Preparer af walk through dokumentet skal derfor ikke bruge unødvendigt lang tid på at beskrive en kompleks og detaljeret proces og kan i højere grad læne sig op ad det dokumenterede, arbejde i videoen.

En af styrkerne ved video er muligheden for at påvise præventive kontroller i IT-systemer uden der nødvendigvis skal kigges dybt i kildekode. Videoen vil her kunne vise, at der f.eks. ikke kan rettes i stamdata for en debitor.

+ Reduktion af tid der bruges på reviewnotes
Dette kan også i vid udstrækning reducere tid der bruges på at cleare review notes, da processen vil stå mere klar for reviewer. Der sker ganske enkelt en minimering af forskellen mellem hvad preparer har set og hørt og hvad reviewer ser og hører.

På den anden side vil der dog også være ulemper, som skal tages med i overvejelserne inden det vælges at optage walkthroughs over Teams.

÷ Auditee kan føle det er ubehageligt at blive optaget
Det vil ikke være alle som synes det er behageligt at blive optaget, og der kan være en frygt for at komme til at sige noget forkert som så senere kan blive brugt imod en. Det er utrolig vigtigt, at der indledningsvist bliver spurgt om lov til at optage, herunder at formålet med optagelsen bliver gjort helt klart for auditee, således at denne føler sig tryg ved processen.

÷ Der skal stadig dokumenteres
Der skal stadig i et eller andet omfang nedfældes ord om processen og laves henvisninger med timestamp. Dette kan f.eks. være ved at skrive "10:00 – Brugeren skifter over i system X for at gøre Y", det kan også være timestamp med henvisning til en kontrol som er betydelig for processen. Det vil være en noget utaknemlig opgave for reviewer, og værdien som dokumentation forsvinder, såfremt der bare ligger en videofil med 1½ times optagelse.

÷ Det kan blive en rodet affære
En videofil kan, i modsætning til et word dokument, ikke løbende ændres. Der kan naturligvis altid i mindre udstrækning suppleres med dokumenter, men hvis videoen i for høj grad suppleres med screenshots, excel filer og andre former for bilag, så vil det fremstå rodet og reelt forhindre det indledende formål med en videooptagelse, som er at skabe en sammenhængende fremstilling af processen. Preparer skal derfor inden interview have læst forretningsgange og have dannet sig en overordnet forståelse af processer og tilhørende kontroller, således at denne kan styre samtalen når der optages og sikre den røde tråd.

Før mødet
Hvis du vælger at gå videre, og vil gøre brug af videooptagelse som dokumentation, vil vi foreslå at følgende bliver gjort før mødet:

- Få aftalt før mødet med auditee, at der optages og til hvilke formål.
- Læs op på processen og de tilhørende kontroller, altså være forberedt.
- Vær sikker på at organisationen har aktiveret muligheden for brug af optagefunktionen i Teams.
- For at være sikker på at have muligheden for at optage, skal det være dig, der fremsender invitation så du er mødearrangør.

Under mødet
Det er under mødet revisors opgave at sikre struktur og sørge for at formålet med mødet opnås, nemlig at processen bliver dokumenteret. Revisor bør derfor være opmærksom på følgende ting under mødet:

- Styr processen – og slip rattet, når du oplever, at I rammer noget, der må have tid og plads lige nu.
- Tag noter og notér tidspunkter som kunne være relevante for at dokumentere processen.
- Der må gerne være en god stemning, men forsøg at holde smalltalk til start eller slut på mødet.
- Opsummér og konkludér ved mødets afslutning.

Efter mødet
Det er nu revisors opgave at skabe den overordnet sammenhæng. Denne opgave afhænger af videoens længde, dvs. der behøves ikke nødvendigvis et følgedokument med timestamp, hvis det er en video med kort varighed. Det vil dog være nødvendigt, hvis det er en video af en times varighed.

En mulighed for revisor med teknisk snilde, vil være at dele den optaget video op i flere filer af mindre varighed.

Hvordan
Selve optageprocessen er forholdsvis simpel og er som følger:

- Start mødet
- Vælg knappen ”Flere handlinger”
- Tryk ”Start optagelse”.

Mødet bliver nu optaget og det vil fremgå i Teams vinduet til alle deltagere, at mødet bliver optaget.

Når optagelsen skal afsluttes, er fremgangsmåden den samme, som den er for at starte. Her trykkes bare ”Stop optagelse” frem for start.

Revisor kan efterfølgende finde filen frem og overføre den til det system, hvor revisionsdokumentation opbevares.

God fornøjelse!

Se om der er ledige pladser på
www.iia.dk

Intern Revision som kulturbærer

Kristian Bollerup, Vice President, Corporate Risk & Internal Audit i LEGO Group

Intern Revision kan spille en væsentlig rolle som kulturbærer i en organisation. Hvordan kan det imidlertid harmonere med den uafhængige rolle, vi har? Den interne revisionsfunktion tager netop ikke ansvar for nogen processer eller kontroller eller ejer daglige beslutninger på nogen måde. I artiklen gives en række eksempler på hvordan LEGO Group tilgår denne udfordring, og samtidig høster de væsentlige fordele der er ved at have en intern revisionsfunktion.

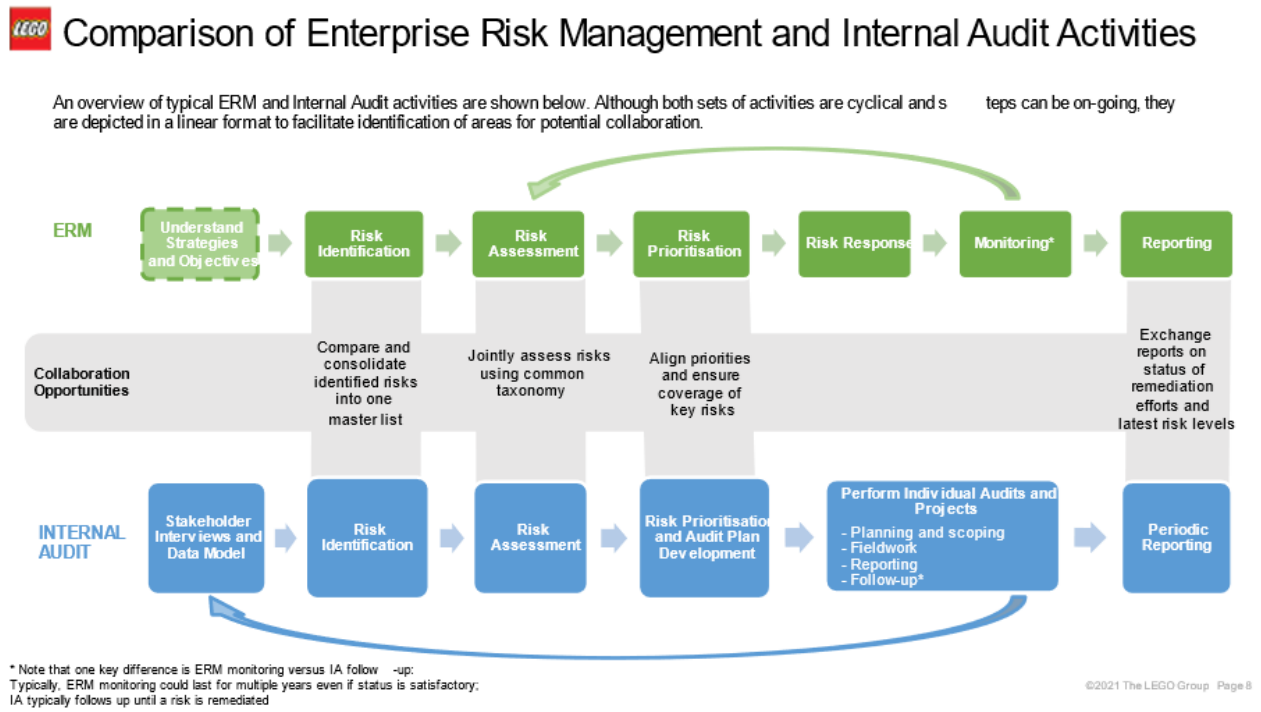
Intern Revision i LEGO Group

De fleste danskere kender vist LEGO Group – eller i hvert fald vores kerneprodukt: LEGO®-klodsen. Vi fejrer vores 90 års fødselsdag, men spiller stadigvæk en væsentlig rolle for mange mennesker, store som små, som har mødt vores produkter livet igennem. Vi er en familieejet virksomhed, og har et stærkt sæt af værdier som gennemsyrer virksomheden. Takket være høj integritet i efterlevelsen af disse værdier scorer virksomheden ofte højt i forskellige målinger af popularitet, integritet, bæredygtighed, 'sustainability', etc. – faktisk så højt at det er vanskeligt at se en yderligere up-side i mange af disse målinger.

Så hvis alle i virksomheden har en høj integritet, hvilken rolle spiller så Intern Revision? Faktisk er Intern Revision i LEGO Group en relativt ung funktion; vi er etableret i 2019, og siden 2021 har vi heddet Corporate Risk & Internal Audit – dvs. både med risk og audit som elementer i vores funktion. Blandt andet dette forhold er en væsentlig del af dét at være kulturbærer i virksomheden og er noget, jeg vil tale yderligere om i artiklen.

Den rolle, Intern Revision er udset til at spille, hænger ganske tæt sammen med den nylige etablering af funktionen. Vi er etableret på et tidspunkt, hvor LEGO Groups forretning har påbegyndt en hastig vækstrejse og selvom vi som virksomhed har høj tiltro til medarbejdere, forretningspartnere og andre interessenter, er der også en erkendelse af, at Intern Revision kan hjælpe virksomheden qua den særlige rolle, vi har. Når virksomheden skal vokse betragteligt, kan Intern Revision være et element i at sikre at alle dele af virksomheden bringes med på rejsen – både de enkelte medarbejdere isoleret set, men også de systemer, processer og kontroller, som skal skaleres op undervejs. Når LEGO Group etablerer sig i Indien, så er det ikke den finansielle eksponering i landet, der er bekymringen, men snarere at vi får startet godt op i et land, der kan være vanskeligt at drive forretning i. Når LEGO Group åbner et stort antal butikker i Kina, så er det

Figur 1.



ikke den finansielle eksponering i den enkelte butik, man er bekymret for, men snarere om vores systemer, processer og kontroller er skalérbare til at rumme et endnu større antal butikker.

Dét, at LEGO Group fortsat er familieejet spiller også en væsentlig rolle i det udtryk, man har ønsket sig omkring Intern Revision. Vi skal netop være kulturbærere. Vi er ikke en finansiel virksomhed (vi er heller ikke en PIE-virksomhed), hvor Intern Revision har en rolle der også har et eksternt bestemt element af regulering med sig; i princippet kan LEGO Group bestemme sig for ethvert ønsket indhold i intern revisionsfunktionen.

Risk og Audit i samme funktion

At have risk- og audit i samme funktion er sædvanligvis ikke et setup, der harmoner med 'three lines'. I det traditionelle setup hører risk management til i anden linje, mens den interne revisionsfunktion hører til i tredje linje. Når LEGO Group har valgt et integreret setup, skyldes det imidlertid også ønsket om at understøtte en stærk kultur i virksomheden: dét, at der arbejdes på tværs af forsvarslinjerne, understøtter efter vores opfattelse en ensartet, afstemt tilgang til risikoidentifikation, risikovurdering, mitigering og rapportering af risici.

Det er således et langt stykke hen ad vejen de samme risici, de samme nøglepersoner og de samme interessenter, som både risk management- og intern revisionsfunktionen engagerer sig i og med.

Den integrerede tilgang indebærer ikke, at det er uklart om vi kigger på et forhold som led i risk management eller som led i den interne revision: det er altid klart udmeldt til revisionsudvalget i LEGO Group, til ledelsen og til de direkte involverede i det konkrete projekt. Dette er illustreret i **Figur 1** på forrige side.

Til gengæld giver den integrerede tilgang os en unik mulighed for at være i kontakt med alle væsentlige interessenter i virksomheden. Særligt risk management-benets 'forpligtelse' til at være i kontakt med hele virksomheden på kontinuerlig basis, med henblik på at identificere og vurdere risici, er værdifuld for den integrerede funktion. Vi har kortlagt alle nøglepersoner i LEGO Group – typisk alle ledere i ledelseslag 1, 2 og 3 - og kontakter disse på minimum årlig basis.

Blot for god ordens skyld vil jeg nævne, at vi naturligvis er meget opmærksomme på, at vi hverken i risk- eller audit-benet af den integrerede funktion kan påtage os ejerskab af processer og kontroller, eller kan påtage os at tage operationelle beslutninger - se **Figur 2** herunder.

Vi er ikke et quick fix!

Når vi i Intern Revision i LEGO Group påberåber os at være kulturbærere, så er det en meget præcis definition. Vi er til tider nok kulturdrivere, men kun indenfor rammerne af den kultur, som allerede gennemsyrer virksomheden. Vi bærer en kultur, men det er ikke os, der bestemmer den: det vil være en uoverkommelig opgave selv at skulle definere en kultur, som en intern revisionsfunktion synes den skulle være, hvis ikke virksomheden i forvejen – eller i det mindste sideløbende – har en kultur, der drives fremad af ledelsen og organisationen som helhed.

Figur 2.

Highlights of Corporate Risk and Internal Audit Activities

Below is a summary of the primary activities within the mandates of the Corporate Risk ("CR") and Internal Audit ("IA") functions as well as the activities outside their related mandates.

Corporate Risk Primary Activities	Internal Audit Primary Activities	Activities Outside the Corporate Risk & Internal Audit Mandates
• Promote and facilitate a standardised approach to effective risk management • Collaborate with Strategic Office and begin to embed risk dialogue in strategic decision making • Support Internal Audit to identify and assess risks • Respond to risks (monitoring) by applying baseline criteria to evaluate (pressure test) the design and effectiveness of the risk mitigation plans from Risk Owners/Drivers • Report on risks by communicating the status of risk levels and related mitigation response statuses to relevant stakeholders, including ELT and Audit Committee • Enhance risk management culture and mindset through communication and training	• Provide independent, objective assurance and advisory services • Identify and assess risks through an annual risk assessment with support from Corporate Risk • Create and execute a risk -based audit plan • Perform internal audits, projects and investigations • Follow up on observations • Periodic reporting to Audit Committee and Executive Leadership Team • Provide advice to the business using subject matter expertise, regarding internal controls, stewardship and governance related topics • Collaborate with external auditors	• Own or manage risks • Assume management responsibilities including decision making • Own, execute or operate any internal controls • Remediate control issues or execute process improvement recommendations • Determine the risk appetite and tolerance • Direct the activities of any employee not employed by Corporate Risk & Internal Audit, except when such employees are assigned to the related Department

Således også i LEGO Group: den kultur, som vi understøtter drives meget markant af den daglige ledelse, af bestyrelsen og ejerne. Det er samme kulturbærere, som besluttede sig for at implementere en intern revisionsfunktion i 2019.

Det er således også i LEGO Group sandt, at alting starter med 'tone from the top'. Hvis ikke virksomheden har en kultur, hvor compliance, integritet, ordentlighed og styr-på-tingene vægtes højt, så vil en intern revisionsfunktion aldrig selv kunne blive succesfuld.

Èn af måder, hvorpå Intern Revision og resten af LEGO Group gensidigt arbejder med at bære en kultur, er den fokus, der er på observationer fra Intern Revision. Vi har fra etableringen af funktionen haft et nært samarbejde med virksomhedens øverste ledelse – som jo er dem, der i det daglige driver den kultur, vi ønsker – og ét af de værktøjer, vi arbejder sammen om er allokeringen af observationer: alle observationer, uanset prioritet (her arbejder vi med prioriteringerne Immediate, High, Medium og Low) allokeres til et medlem af direktionen, og hvor måned modtager disse en opfølgning på, hvor mange observationer, de hver især ejer. Denne form for ejerskab har været medvirkende til, at observationer – og dermed også de enkelte revisionsopgaver, hvorfra observationerne stammer – tages uhyre seriøst af hele organisationen. Ingen ønsker at have observationer, der ikke løses indenfor de besluttede tidsrammer: risikoen for at få et telefonopkald fra et direktionsmedlem af den årsag holder alle til ilden, så at sige.

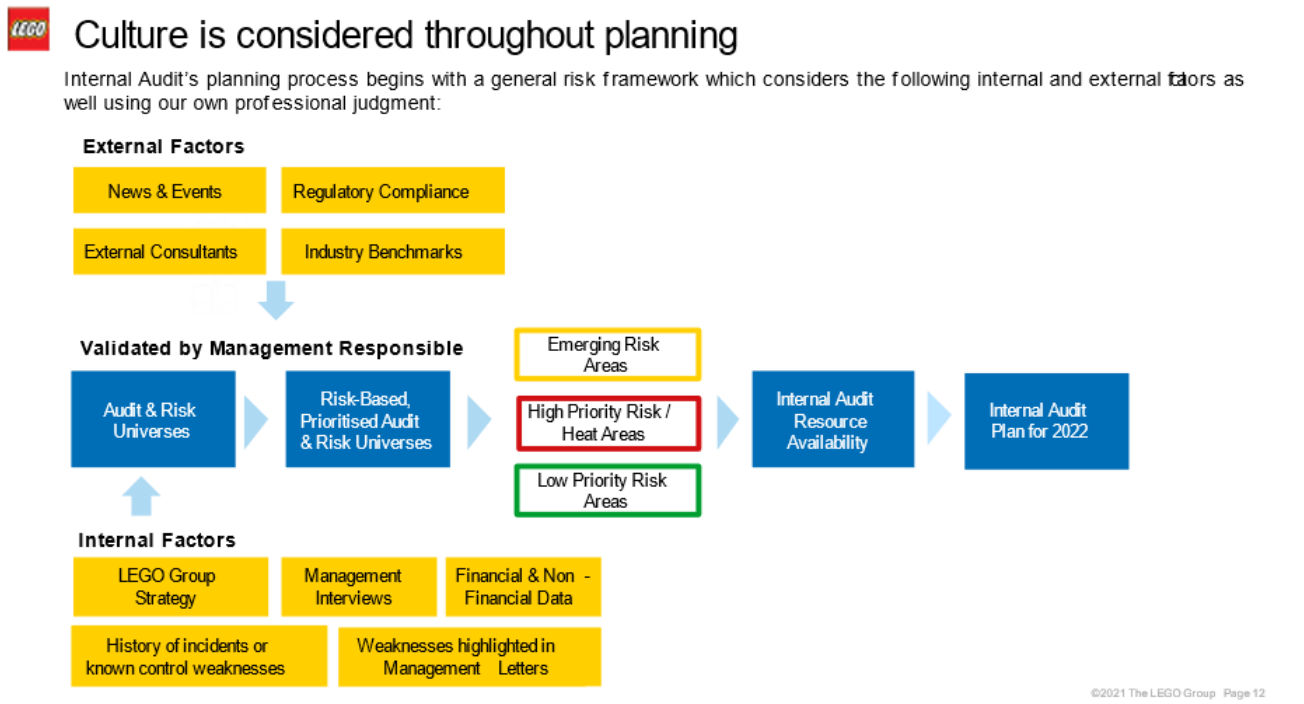
Kultur som konkret element i planlægning

Som nævnt tidligere er det ikke regnskabstallene i fx Indien, der giver bekymring ud fra en revisionsmæssig betragtning: det er snarere dét at drive forretning i et lidt vanskeligt land. Det er heller ikke regnskabstallene i fx Kina, der bekymrer; langt mere er den markant større mængde af butikker, som betinger at systemer, processer og kontroller er skalérbare, fyldestgørende og afbalancerede ud fra en risiko- og kontrolbetragtning.

Kulturelle elementer spiller ind i den måde, vi planlægger vores revisioner. Vi bruger konkrete talmæssige indikatorer i risikovurderingerne, primært et såkaldt korruptionsindeks, der rangerer forskellige lande på en talmæssig indikator for oplevet korruption. Det indebærer ikke – og det er ganske væsentligt – at vi har konkrete oplevelser af svig el.lign. i vores selskaber i disse lande. Det er imidlertid en indikator for, hvor man befinder sig i mere vanskelige forretningsmæssige klimaer, og hvor den interne revisionsfunktion derfor bør fokusere en større grad af vores opmærksomhed.

Naturligvis er et korruptionsindeks ikke det eneste parameter i vores risikovurdering. Samlet set udgør kulturelle faktorer – i forskellige former – en betydelig del af grundlaget for de planlagte revisioner (omkring 2/3 af det samlede input, mens finansielle data 'kun' vægtes med omkring 1/3) - se **Figur 3** herunder.

Figur 3.



Hvad reviderer vi så?

Så når rammerne er de rigtige, opbakningen fra ledelsen er tilstede, 'ansigtet' på Intern Revision er som ønsket, hvad er det så, vi specifikt reviderer, som understøtter en god kultur i virksomheden. Som tidligere nævnt er det ikke de finansielle risici i LEGO Group, som fylder mest i vores overordnede risikokort, så det er ikke primært dér, vi lægger vores fokus..

I stedet er vores fokus operationelt i den bredest tænkelige forstand, som det fremgår af **Figur 4** herunder.

Revisionerne kan herudover opdeles i et par hovedkategorier:

- Market Visits, som er revisioner i vores selskaber rundt om i verden. Her reviderer vi typisk de forhold som relaterer sig til vores salgsaktiviteter, dvs. kontrakter med kunder, salgs-/rabat-/tilskudsbetingelser, due diligence af tredjeparter, kendskab til og efterlevelse af forretningsetiske politikker mv.
- Corporate Audits, som er revisioner af de dele af vores forretning som foregår ud af en corporate function: IT, fabriksdrift og -etablering, ESG-rapportering, skatter/afgifter/eksportkontroller, GDPR, mv.

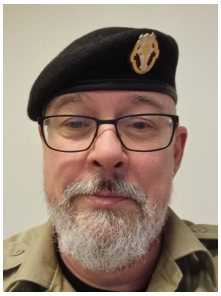
Kendetegnende for alle revisioner er en høj grad af fokus på efterlevelse af LEGO Groups egne politikker, mens vi – indtil videre – har været tilbageholdende med at revidere op imod 'best practice' som begreb: ikke fordi vi ikke har en holdning til best practice, men fordi vi ønsker at drive en kultur der indebærer, at vi som virksomhed naturligvis følger de retningslinjer, vi er enedes om (eller som er vedtaget af virksomhedens ledelse, i det mindste). Best practice prøver vi så at påvirke ved at arbejde med de corporate functions, som ejer forskellige områder: de globale ejere af forskellige politikker er de rigtige til at drive forandringer og forbedringer, så ser vi lokalt set behov for at justere på politikkerne, så skal det komme fra globalt hold.

Et andet kendetegn i vores revisioner er at der både i planlægnings- og i rapporteringsfaser er afsat langt mere tid, end der isoleret set er behov for. Det kan synes ulogisk, at vi ikke skynder os at komme i gang, eller skynder os at blive færdige, så alle kan komme videre, men netop denne tidsallokering medgår til at understøtte en høj grad af forståelse for revisionens formål, omfang, tidsforløb osv. (i planlægningsfasen), og til at forstå – og om nødvendigt diskutere – revisionens resultater, observationer og anbefalinger (i rapporteringsfasen).

Vi er således, målt på antallet af revisioner, ikke den mest produktive interne revisionsfunktion. Til gengæld har vi aldrig – eller, i hvert fald kun med særdeles veloovervejede bevæggrunde - observationer der ikke anerkendes og udbedres, og vi er i stand til at drive permanente lokale forandringer og globale forbedringer! LEGO Group blev i sin tid etableret med mottoet 'Det bedste er ikke for godt', og dette motto bruger vi fortsat både internt og eksternt. Det kan tage tid at bygge en virksomhed med den rigtige kultur, men til gengæld er det en fantastisk god virksomhed, der kommer ud af det.

Figur 4.

Har du data kan du få, har du ingen må du gå



Kim Guldberg, Major, Forsvarsministeriet

Indledning

Når man læser rapporterne fra de mange forskellige kompromitteringer vi har set i de seneste år, er det meget tydeligt, at der mellem linjerne for alle kompromitteringer står "Vi havde ikke de nødvendige informationer til at kunne give de efterspurgte svar, og det har vi stadig ikke her, måneder efter sagen er afsluttet".

De informationer der tales om, er det man i relativt bred forstand kan samle under begrebet Logs. Problemet her er, at dette begreb ikke er helt præcist defineret og i vid udstrækning giver mulighed for tolkning og forskellige valg, afhængig af hvordan kravene til logning formuleres, hvis der overhoved formuleres krav i første omgang.

Fordi begrebet logning giver mulighed for tolkning, er der en række ting man er nødt til at forstå, før man kan tale om at formulerer specifikke og detaljerede krav til denne.

1. Logning er i dag en meget konfigurerbar størrelse og INGEN systemer eller produkter logger det nødvendige out-of-the-box. Logning kræver ressourcer, og har man ikke specificeret, hvad man ønsker logget, så får man kun det absolut nødvendige for drift, ikke det nødvendige for sikkerhed.

2. Logs er i dag ikke bare en log. Hvis vi f.eks. bruger en Windows server som eksempel, så vil vi kunne tale om mange forskellige logs, Security Log, System Log og Application Log blot til en start, derudover har mange applikationer og services deres egne logs, PowerShell Log, DNS Log, IIS Log, Exchange Log, SQL Log alt efter serverens specifikke rolle.

3. Logning i dag SKAL være centraliseret, og er den ikke, har man i udgangspunktet en række udfordringer. Alt logning foretages lokalt på de forskellige bokse og opbevares der, hvis der ikke findes en central løsning. Problemet er at logs her er relativt ubeskyttede mod redigering og sletning og at den tid de opbevares før overskrivning, er ofte meget kort.

4. Logning i dag er andet og mere end det systemerne betragter som logs. Logs er også Prefetch files, som er tekstfiler med informationer om applikations eksekvering, ShimCache og AmCache (en del at Windows Registry) der bl.a. anvendes til at lave tidslinjer i forbindelse med kompromitteringer. Disse, og en lang række andre informationer, bør indsamles og håndteres centralt.

5. Commandline auditing (især PowerShell logning) er absolut essentielt. Selvom det kan siges at være indeholdt i ovenstående, vælger jeg alligevel at behandler det særskilt her. Hvis man ikke ved med sikkerhed om Commandline auditing er slået til i egen organisation, så er det med sikkerhed ikke slået til, og uden har man ikke data til at levere de efterspurgte svar. Især PowerShell versionen er vigtig, idet logning udvikles kraftigt i takt med nyere versioner udgives. Version 2 af PowerShell logger stort set ikke, version 5 logger godt.

Ovenstående er blot noget af billedet, og man kan være sikker på, at hvis man ikke har specificeret, hvad der skal logges, så har man kun det absolutte minimum der er nødvendigt for driften af systemerne. Bliver man kompromitteret vil man også være nødt til mellem linjerne at sige "Vi havde ikke de nødvendige informationer til at kunne give de efterspurgte svar".

Artiklen kunne sagtens slutte her, men der er en række yderligere pointer, som med fordel kan medtages, idet det ikke er nok at forstå hvor man skal hen, men også at have, i det mindste, nogen indsigt i hvordan man kommer derhen.

Centraliseret logning

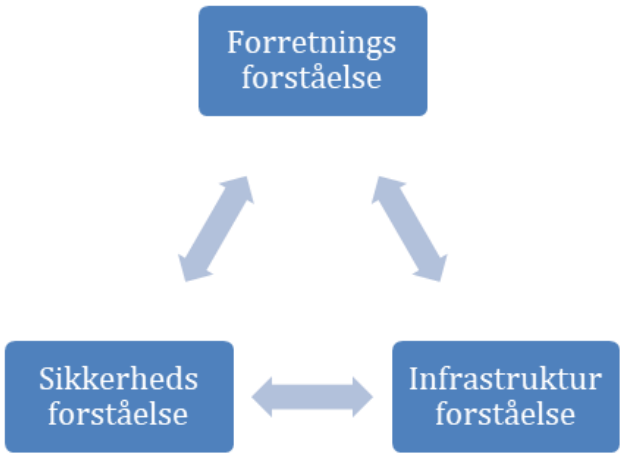
Centraliseret logning kræver et system til dette. Et sådant system kaldes oftest et SIEM (Security Information and Event Management) og et sådant system er meget udfordrende at vælge og at implementerer. Dels findes der en række forskellige leverandører, der ofte gør tingene lidt forskelligt og dels har disse deres stærke og svage sider, og det er ikke helt ligegyldigt, hvordan man implementerer et sådant system.

Et af problemerne er at der kræves en trekant af kompetencer, som næsten ingen besidder internt og aldrig findes i en person:

Forretningsforståelse er essentielt. Uden stor viden om den specifikke organisation og den specifikke branche bliver det svært at lave relevant logning og at identificerer hvad der falder uden for normalbilledet. Hvis man ikke ved hvordan virksomheden opererer eller hvilke procedurer og metoder der anvendes, så kan man ikke identificere, når en angriber opererer i infrastrukturen og laver ting der ikke normalt udføres.

Infrastruktur forståelse er essentielt. Helt grundlæggende kræver et SIEM projekt at man har styr på sit hardware, sin software, sine konfigurationer og sin opsætning. Jeg bliver ofte overrasket over, hvordan systemer kan stå hengemt i et hjørne af serverrummet i årevis og udføre deres funktioner, mens alle i virksomheden har glemt at de er der. Eller hvordan man pludselig bliver opmærksom på, at der faktisk sidder en server i den printer eller at dette specialsystem i produktionen, og faktisk indeholder en computer med et operativsystem der i øvrigt er forbundet til internettet.

Sikkerhedsforståelse er essentielt. Man er nødt til at vide hvordan angriberne arbejder, hvilke metoder de anvender, hvilke værktøjer der anvendes og hvordan disse opdages. Hvad der findes af sårbarheder der er relevante for virksomheden, hvordan disse udnyttes, og hvordan man opdager når disse bliver udnyttet.



Ovennævnte trekant giver udfordringer i forbindelse med outsourcing af projektet og kræver som minimum et tæt samarbejde med virksomhedens egne folk og dem man hyrer ind udefra

Metodisk og struktureret arbejde betaler sig

Når man har fået indkøbt og opsat sin SIEM løsning og skal i gang med at logge, er det en stor fordel at arbejde struktureret og metodisk med dette. Når man skal kunne finde en nål i en høstak, er det lettest, hvis høstakken er så lille som muligt, uden at man har frasorteret nåle. Der er også en økonomisk betragtning i, at der logges det der er brug for, men ikke en masse unødvendigt støj som fylder, kræver ressourcer og gør høstakken meget stor.

Den metode der beskrives herunder må nok betegnes som idealmetoden og måske ikke 100% realistisk for langt de fleste virksomheder. Metoden giver dog nogle svar på hvad man skal igennem og hvordan der kan prioriteres.

Start med at tilslutte securityloggen fra en domænecontroller og lad den logge til dit SIEM i et par dage. Husk det skal være et par almindelige arbejdsdage idet især brugeraktivitet medfører logs.

Når man har logs at kigge i, påbegyndes en analyse som i virkeligheden er relativt simpel og som bør gennemføres i samarbejde med driften. Man beder sit SIEM om at generere en top-10 over anvendte events. Herefter gennemgår man disse sammen med driften for at finde ud af hvorfor der er så stort et antal af disse events i loggen. Nogle af disse events vil være støj - ting der genereres fordi man ikke tidligere har været opmærksom på dem. Service konti der er låst, scripts med forkerte passwords og som ofte ikke bruges mere selvom de stadig kører. Man vil opdage, at når man kigger på logs med en sikkerhedsvinkel, så ser man ting som driften overser og dette er helt naturligt. Det er vigtigt, at man ikke undlader at logge disse events, men i stedet fjerner grunden til at der kommer mange af dem.

Når man et antal gange har trukket ovennævnte top-10 vil man se log-mængden falde ganske betydeligt og man kan nu tilslutte security logs fra resten af domænecontrollerne. Herefter gør man det samme med de andre serverroller, en ad gangen. Når man har alle security logs fortsætter man på samme måde med system logs, herefter applikations logs og så videre, indtil man har det hele.

Commandline og PowerShell logning kan behandles sideløbende med ovenstående. Her bør man slå det til generelt i hele infrastrukturen (på servere og arbejdsstationer og alle de andre steder hvor det er muligt). Det man skal være opmærksom på er, at logs kun genereres, når det der logges anvendes. Det er sjældent at commandline og PowerShell anvendes massivt hver dag af et stort antal mennesker. Man skal have data for at kunne analysere og afhængig af virksomheden kan det tage fra dage til måneder. Analysen skal, i lighed med de ovennævnte analyser gennemføres løbende, dog ikke så ofte som i starten.

Når man har commandline log data, kigger man på dette sammen med driften og danner et overblik over commandline / PowerShell brug i organisationen. Dette overblik bruges så til at lave procedurer der gør det let at genkende legitim brug af disse værktøjer. Scripts kan f.eks. placeres og køres fra en godkendt placering, og de kan dokumenteres og sikres med certifikater. Man kan også dokumentere hvem i organisationen der faktisk anvender disse værktøjer, så det fremstår tydeligt hvis en bruger (der er blevet kompromitteret) pludseligt begynder at bruge commandline og PowerShell. Hvilke procedurer man tager i anvendelse, afhænger helt af virksomheden, men formålet er at gøre det let at opdage ondsindet brug.

Som det blev beskrevet i starten, logger ingen systemer det nødvendige out-of-the-box. Dette betyder, at man nu skal til at konfigurere de enkelte systemer, så de logger det man har brug for. Hvad dette præcist er, afhænger af virksomheden, branchen, systemerne og den specifikke brug af disse systemer. Der er hjælp at hente hos leverandører af sikkerhed og sikkerhedsprodukter og der er kurser som medarbejdere kan sendes på. Disse er dog ikke billige. Et eksempel på et sådant kursus er SANS FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics. Det kan tages både af beslutningstagere og folk der skal arbejde med emnet i praksis. Beslutningstagere kan undlade at udføre alle øvelserne men blot se gennemgangene af disse. Det udførende led bør gennemføre alle øvelser inklusiv de ekstra hjemme øvelser. Se de to links herunder

https://www.sans.org/cyber-security-courses/advanced-incident-response-threat-hunting-training/

https://www.sans.org/posters/hunt-evil/

Nu har du data, så nu kan du få

Hvis organisationen har gennemført størstedelen af det ovenstående, har man nu det data der muliggør at svarene på alle de gode spørgsmål kan findes efter kompromittering. Der er dog mere at få end blot dette.

SIEM værktøjet kan potentielt give svar på alle de spørgsmål der stilles, når det har de nødvendige data. Dette betyder, at SIEM værktøjet faktisk kan opdage når man bliver kompromitteret eller forsøgt kompromitteret. Er det ordentligt sat op, kan det give disse svar så hurtigt, at man potentielt kan forhindre kompromitteringen. Dette er dog ikke noget man bare lige gør. Det kræver special-kompetencer, stor forretningsindsigt og stor infrastruktur viden. Man bør se logning og brug at SIEM som en kontinuerlig proces der udvikles i takt med at virksomheden gør det samme. Man bliver først færdig med denne proces, når virksomheden ophører med at eksistere.

Den sidste pointe der kan fremhæves, ligger egentlig uden for scopet af denne artikel, men med lidt overblik og indsigt vil der helt sikkert være læsere der kan se ideen. De ting systemerne logger og som nu befinder sig centralt kan give svar på ting der ikke har med sikkerhed at gøre. Der er her tale om Business Intelligence og fremtiden vil med sikkerhed vise at denne adgang til Business Intelligence for nogle virksomheder bliver mindst lige så væsentlig og værdifuld som den sikkerhed logningen giver. Det er ikke et område som mange har behandlet men ……

Forfatteren

Kim Guldberg hackede sin første computer i 1980 og har siden 1997 arbejdet professionelt med Cyber sikkerhed. Kim er Major i Hæren, og Subject Matter Ekspert Cyber i forsvaret. Han var i 10 år IT chef på Hærens Officersskole og efterfølgende infrastruktur og Cybersikkerhed ved KAKI (der før hed FKIT).

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

Diversity and Inclusion – why it matters and how to audit it

Nina Belcaid, M.Sc (Econ), CIA, CCSA, Internal Audit Manager, Nordea

Introduction

It has in recent years been demonstrated by research that companies having diversity and inclusion as integrated elements in their corporate culture outperform companies that have not devoted similar attention to these matters.

In this article I will take a closer look at the various ways in which diversity and inclusion can lead to organisational success, including the barriers that may hinder this, and the ways in which internal auditors can position themselves to play a central role in supporting organisations in achieving their diversity and inclusion goals.

But firstly, it is important to gain a common understanding of the definitions of diversity and inclusion. The concept of inclusion is so often included in conversation regarding diversity, that many publications bundle diversity and inclusion together using the acronym D&I. Although the two terms are interlinked, it is important not to confuse the two.[1]

What is diversity and what is inclusion?

Diversity in the workplace refers to a workforce that is made up of people from, amongst other things, different age groups, cultural backgrounds, geographies, physical abilities and disabilities, religions, genders, and sexual orientation.

Inclusion can be defined as the achievement of a work environment in which all individuals are treated fairly and respectfully, have equal access to opportunities and resources, and contribute fully to the organisation's success.[2]

Research[3] states that four elements need to be in place to cover a holistic definition of inclusion:

- Fairness and respect
- Valued and belonging
- Safe and open
- Empowered and growing

So, to put it simply, diversity is about the 'what' – it focuses on the makeup of your workforce. Inclusion, on the other hand, is about the 'how' – the creation of a work environment and culture that enables all employees to participate and thrive[4].

The culture of an organisation drives how it conducts business and executes its strategies. All organisations have a culture, whether intentionally created or not[5]. So, inclusion is an element of the corporate culture and how that is carried out. In order to make an organisational success out of having a diverse workforce, inclusion - and thereby the culture - must be supportive.

So, even though diversity and inclusion are often used in tandem rather than as diversity versus inclusion, they are in fact two different concepts. I would go even further and say that inclusion is a prerequisite for nurturing a diverse organisation. So, diversity in itself does not necessarily lead to inclusion.

Let's take a closer look at the various ways in which inclusion and diversity lead to organisational success.

Why diversity and inclusion are important

In its 2018 report, 'The Diversity and Inclusion Revolution', Deloitte found that organisations with inclusive cultures were much more innovative and agile: They see more angles on potential problems, imagine smarter and multi-faceted solutions, and spot the biases in what they are creating.

Also, research by PricewaterhouseCoopers (PwC) indicates that more than 80% of the CEOs whose organisations have a diversity and inclusion strategy believe it has enhanced business performance[6].

McKinsey has also tracked diversity and inclusion for years, investigating the business case for diversity through their reports[7]. Their 2020 report 'Diversity wins – How inclusion matters' shows not only that the business case remains robust, but also that the relationship between diversity on executive teams and the likelihood of financial outperformance has strengthened over time.

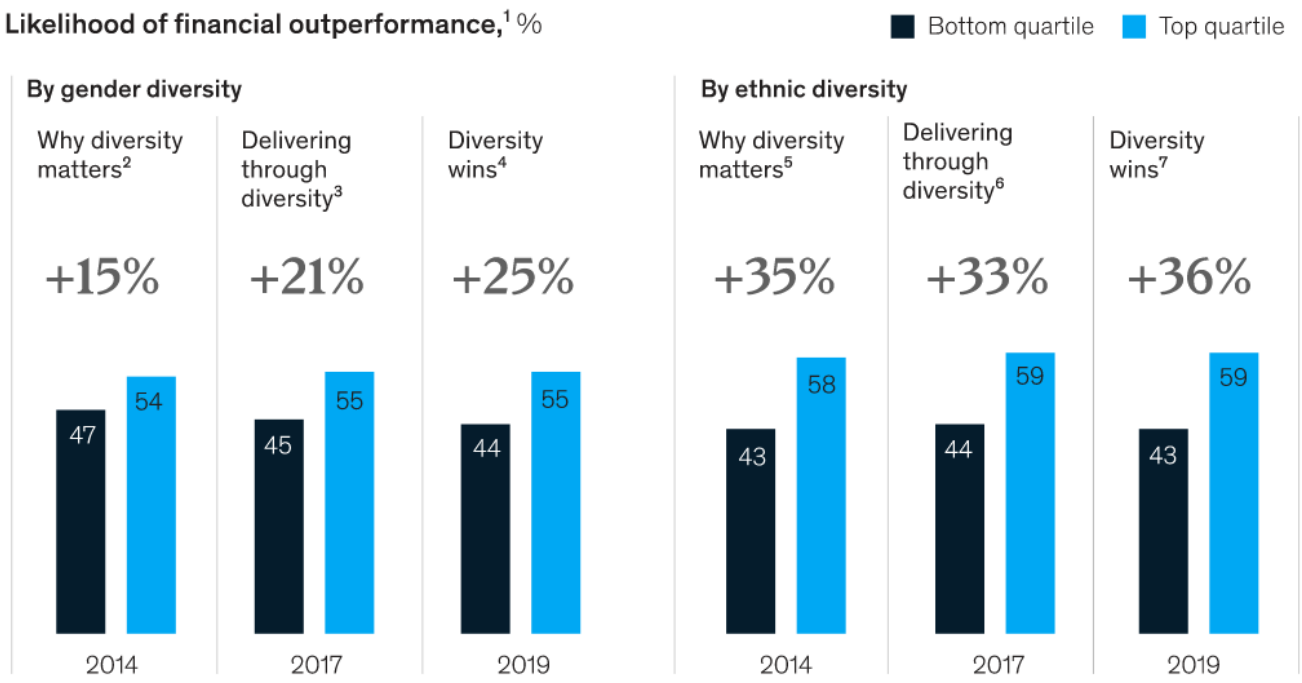
These findings emerge from a data set encompassing 15 countries and more than 1,000 large companies. The likelihood of outperformance continues to be higher for diversity in ethnicity than for gender - see **Figure 1** on next page

Why is it difficult?

Unfortunately, it seems as if the progress is quite slow for gender and ethnic diversity in leadership teams in the same period according to the McKinsey 2020 report, and there seems to be a growing divergence between high and low performers.

To further understand how inclusion matters - and which aspects employees regard as significant - McKinsey con-

Figure 1: The business case for diversity in executive teams remains strong



[1]Likelihood of financial outperformance vs the national industry median; p-value <0.05, except 2014 data where p-value <0.1. [2]n = 383; Latin America, UK, and US; earnings before interest and taxes (EBIT) margin 2010–13. [3]n = 991; Australia, Brazil, France, Germany, India, Japan, Mexico, Nigeria, Singapore, South Africa, UK, and US ; EBIT margin 2011–15. [4]n = 1,039; 2017 companies for which gender data available in 2019, plus Denmark, Norway, and Sweden; EBIT margin 2014–18. [5]n = 364; Latin America, UK, and US; EBIT margin 2010–13. [6]n = 589; Brazil, Mexico, Singapore, South Africa, UK, and US; EBIT margin 2011–15. [7]n = 533; Brazil, Mexico, Nigeria, Singapore, South Africa, UK, and US, where ethnicity data available in 2019; EBIT margin 2014–18.
Source: Diversity Wins data set

Source: 'Diversity wins – How inclusion matters', McKinsey 2020

ducted an analysis of inclusion-related indicators and the following 'pain points' in the experience of employees were identified:

- Overall sentiment on diversity was 52 percent positive and 31 percent negative, but sentiment on inclusion was markedly worse, at only 29 percent positive and 61 percent negative. So even diverse companies face challenges in tackling inclusion: Hiring diverse talent isn't sufficient—it's the workplace experience that shapes whether people remain and succeed.
- Opinions about leadership and accountability in inclusion and diversity accounted for the highest number of remarks and were strongly negative. On average, across industries, 51 percent of the total comments were related to leadership, and 56 percent of those were negative. This finding underscores the increasingly acknowledged need for companies to improve their inclusion and diversity engagement with core-business managers.
- For three indicators measuring the degree of inclusion - equality, openness, and belonging - there was a particularly high level of negative sentiment about equality and fairness of opportunity. Negative sentiment about equality ranged from 63 to 80 percent across the industries analysed. The work environment's openness, which encompasses bias and discrimination, was also a significant concern - negative sentiment across industries ranged from 38 to 56 percent. 'Belonging' obtained overall positive sentiment.

In other words, the dynamics around inclusion is a critical differentiator for companies. The McKinsey 2020 report emphasises two critical barriers for organisations to have a successful inclusion culture:

- The first barrier is a lack of purposeful follow-through on diversity promises. Many companies have yet to adopt the systematic, business-led approach to diversity and inclusion that is needed to translate these promises into actual change. Such companies have tended not to give managers true accountability for strengthening diversity.
- The second barrier relates to inclusion, where unaddressed misconceptions about fairness is a critical issue. There is often a prevailing belief that 'everything should be the same for everyone', and this fails to factor in the reduced extent to which women and ethnic minorities are extended support and sponsorship — and the greater extent to which they face bias, bullying and harassment, compared to the dominant majority.

Therefore, organisations must challenge their unconscious thought processes to ensure inclusion. It is only possible to fully embrace diversity (and ensure a diverse workforce) if inclusion is on the agenda.

All the above make it seem as if diversity is easier to boil down by being a more concrete concept. Diversity seems easier to grasp - we are all different; without trying that's just how it is. But factors of diversity also vary, so some of them are easier to be aware about (e.g., gender, nationality, age, physical ability), while others are more intangible from an outside perspective (such as belief, values, perception of justice, habits, experiences, sexual identity etc.).

You can't manage what you can't measure

Governance structures around diversity and inclusion seem generally to be in place and have been for quite some time. A 10-year-old survey from Forbes Insight indicated that approximately 70% of the respondents had some kind of internal board or committee to oversee the diversity and inclusion strategy. These were typically represented by managers and executives from across the organisation, where members of the human resources department were the most common[8].

For an organisation to establish a proper diversity and inclusion strategy and follow track of their goals, careful consideration must be undertaken as to the intended outcome of the strategy. Once this decision has been taken, tangible outcomes should be described, and a metric should be attached to each desired outcome.

For outcomes around feelings, perspectives, or other non-numerical items, it is suggested to use the ranking method for the metrics i.e., where one offers a statement that speaks of the outcome, such as 'I believe this company is inclusive' and asks respondents to rank their feelings about the statement on a scale from one to five[9].

The method gives numbers for outcomes that are important but difficult to quantify. For more concrete or completion-based outcomes, metrics chosen can be tied to clear milestones. Correlational metrics can also be used (e.g., promotion rates, turnover rates), and can be real storytellers when including ranking method metrics, demographic metrics, and company-wide metrics.

The survey from Forbes Insight indicated that organisations were aware of the need to have metrics in place, as 88% had them in place or were then in the process of developing them. However, this does not necessarily say anything about the outcomes or the quality of the metrics i.e., if they support the diversity and inclusion strategy defined for the respective organisations.

It stands to reason that teams made up of people from different cultural backgrounds, ages, genders, and experiences will be more likely to have a broader view of the world. Recruitments are also focusing on diversity and inclusion matters. As Eileen Taylor, Global Head of Diversity in Deutsche Bank states, 'If you want to have the best talent you need to be reflective of the talent in that market' [10].

Today HR departments in successful organisations are aware that there is a pool of talent out there which has not been tapped into earlier, because they come from a different cultural background. But when a business is known to be pro-diversity and pro-inclusion, it will attract these talented people, giving the organisation access to high-performing individuals.

This mindset is supported by research: In a survey of more than 10,000 millennials (people born between 1980 and 1995), over 80% said that an employer's policy on diversity and workforce inclusion is an important factor when deciding whether to work for them[11]. Also, staff will be more inclined to stay in a business where they are heard and valued (i.e., the dimension of inclusion), so retention is also higher in such organisations. Consequently, pro-diversity and pro-inclusion organisations have access to a broader range of top talent and find it easier to keep them.

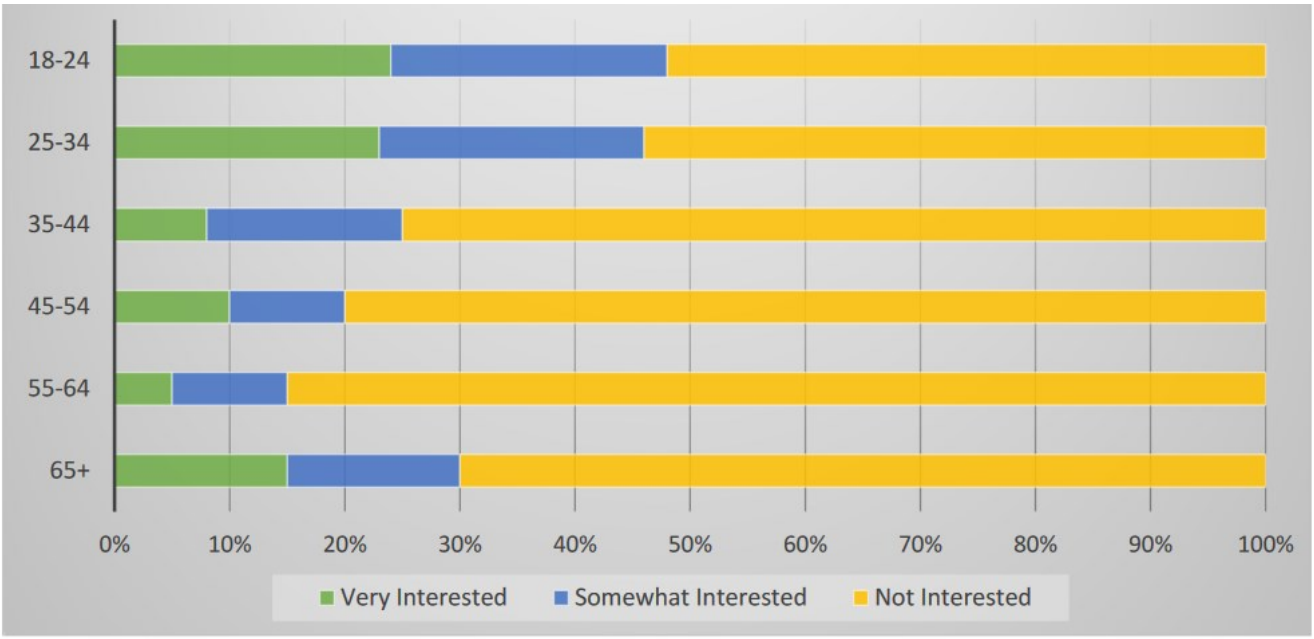
For these reasons metrics on diversity and inclusion is a hot-button issue. But they are also crucial for a successful journey on the diversity and inclusion road. It is very difficult for an organisation to improve its diversity and inclusion strategy if they do not know what they are starting with or what they are working toward. It is important to remember that metrics do not exist to tell the whole story but should be used as a tool for support. Organisations should on a continuous basis evaluate their metrics and try to develop them even further to cultivate a culture which has diversity and inclusion as part of their DNA.

How are we doing in the Nordics?

Organisations can create a diversity and inclusion strategy and ensure a proper governance structure. This would be perceived as a top-down approach. But there are also possibilities to set up bottom-up processes to nurture a good environment for diversity and inclusion.

One possibility is to create employee resource groups (ERGs) to cater for a more inclusive environment and address diversity and inclusion in a more holistic, community-based way. Normally, ERGs are voluntary, employee-led groups, and they could be on gender, age, culture, abilities etc. Particularly in the US ERGs are widespread -

Figure 2: Interest in joining an ERG by age, Osterhaus



Source: Taking Employee Resource Groups to the Next Level, Bentley University 2016

nearly 90% of all Fortune 500 companies have ERGs. Also, interest in joining an ERG depends significantly on age[12] - see **Figure 2** above.

Research[13] has revealed that the Nordics still do not embrace diversity and inclusion. For example, recent rankings show the Nordics being outpaced on women's participation in leadership. Development of women's share in leadership positions has stagnated: All countries except Sweden have declined in ranking over the last 10 to 15 years. In 2006, Norway and Sweden shared rank 36th, Finland ranked 46th, and Denmark was 53rd. Today, Sweden ranks 35th, the only Nordic country in the top 50, while Finland, Norway, and Denmark stand at 51, 68, and 101 respectively - see **Figure 3** on next page.

This might come as a bit of a surprise since Nordic countries are well-known for being egalitarian and have historically been highly regarded on overall gender equality.

Also, the gap between women and men on the tendency to seek career advancement is much larger in the Nordics (24 percentage points) than on a global level among younger generations (6 percentage points). However, the gender gap decreases with age in the Nordics - see **Figure 4** on next page.

In addition, different nationalities are not well represented in the Nordics. Assessing the executive teams of the 30 largest listed companies in each of the Nordic countries, 80% were born in the Nordics, while, for example, only 2% of the executive teams were from Asia, Africa and Australia.

Finally, for LGBT+ (lesbian, gay, bisexual, transgender, and additional groups) approximately 20% are still not comfortable being open about how they identify while at work in the Nordics.

How to audit diversity and inclusion

No specific guidance on how to audit diversity and inclusion has yet been issued by the IIA. However, as the Internal Audit department is the provider of independent assurance within an organisation's governance framework, it is well positioned to assess culture[14], and diversity and inclusion are elements of the corporate culture[15].

The audit can be performed as a stand-alone audit on diversity and inclusion, but it could also be integrated into a culture audit, where diversity and inclusion could be a specific focus area.

It will require skilled and experienced auditors. The auditor's ability to ask the right questions and focus on key aspects of the diversity and inclusion strategy within the organisation will require core competencies such as critical thinking, problem solving, and root cause analysis.

The question '*why was that/why is it so?*' should be asked to keep drilling down and revealing potential shortcomings to the strategy and to assess the true nature of the diversity and inclusion effort carried out.

The audit of diversity and inclusion can be tackled by dedicating focus on the governance aspects, for example:

Figure 3: Looking at women's share in leadership, Nordics' progress has stagnated, while being outpaced by other countries

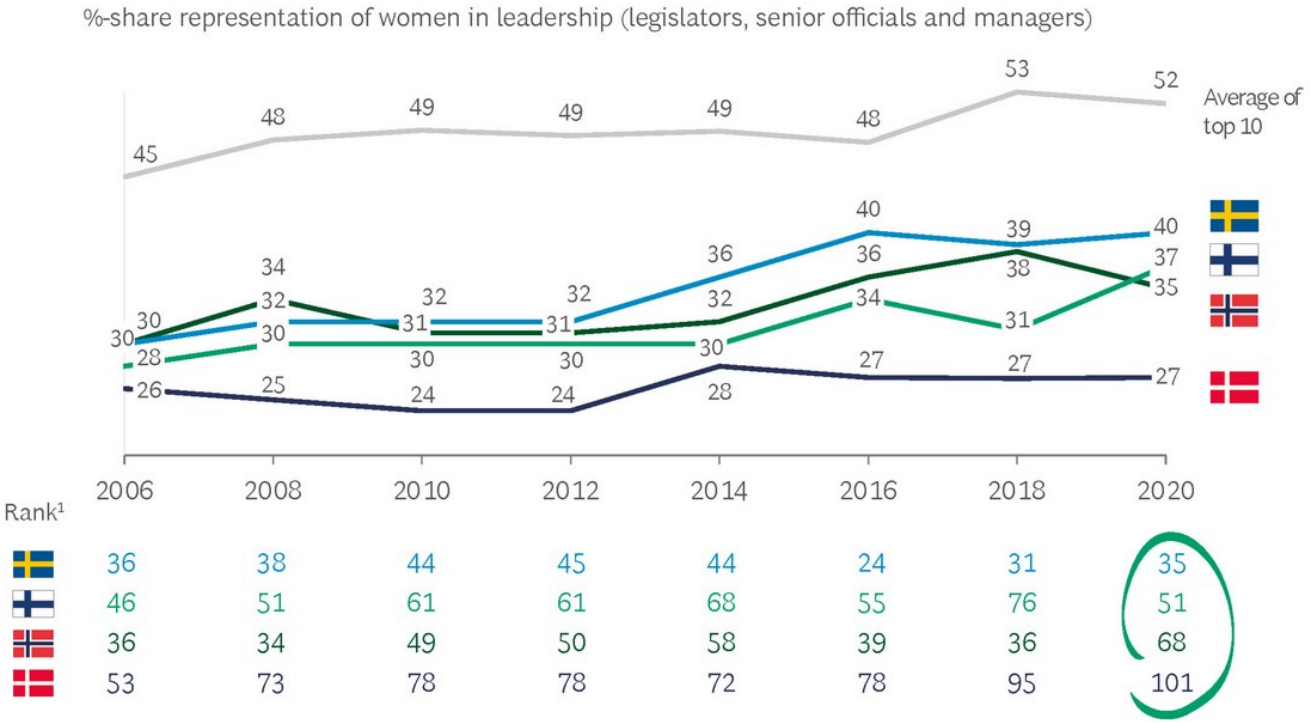
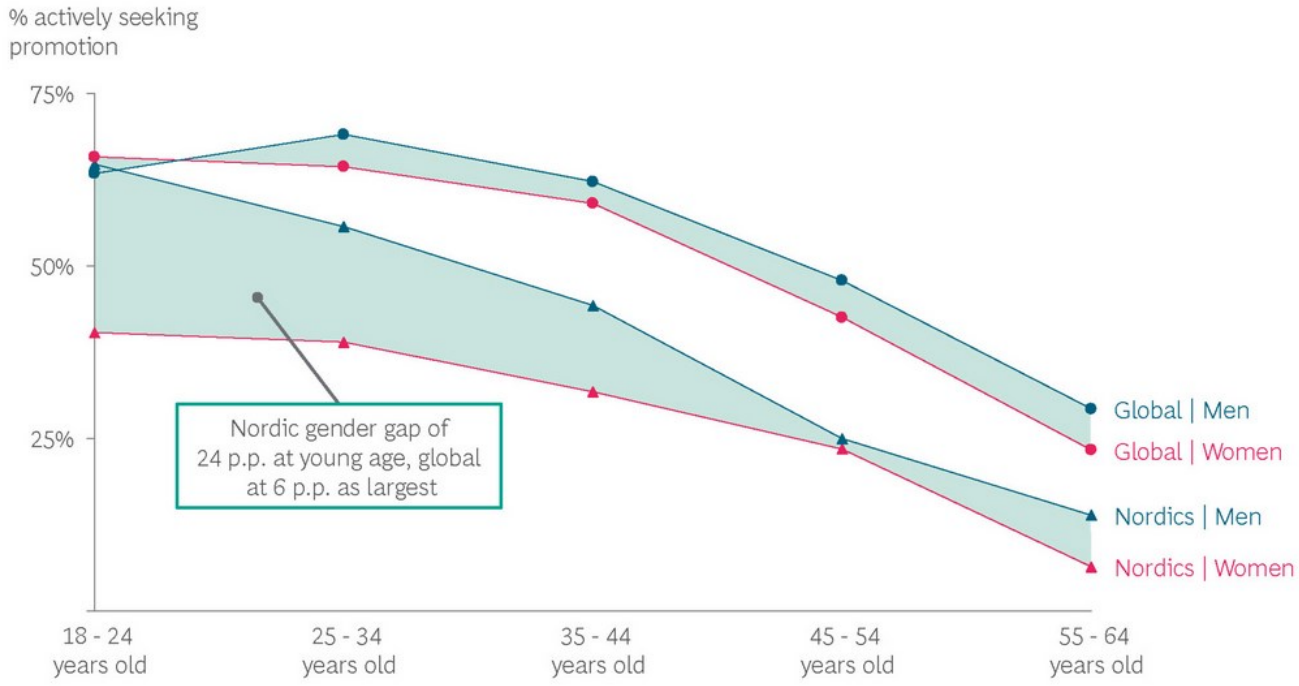


Figure 4: Young Nordic women actively seek promotions less than men and gender gaps is significantly higher in Nordics than globally



Source: *Finding the Value in Diversity: Diversity and Inclusion Isn't Just a Fix, Boston Consulting Group 2021*

- Is the design and effectiveness of the diversity and inclusion strategy sufficient, and is it linked to the business strategy?
- Is there a clear link from the principles in the organisation's Code of Conduct towards diversity and inclusion?

Furthermore, it should be investigated if the organisation is structured to handle diversity and inclusion matters, for example:

- Has a committee been established?
- Do the members represent the different business areas and group functions, and are they on a senior managerial level so they have sufficient power and influence?
- Has managerial oversight been established?
- Has management ensured issuance of guidelines and Standard Operating Procedures (SOP), where applicable?
- Does top management receive regular reporting on diversity and inclusion, and what is reported upon (i.e. are relevant metrics in place)?

As stated earlier in the article, special attention should be given to the quality of the metrics and to the responsibility for this area, since it can be tricky to measure meaningfully on inclusion aspects, as well as some of the diversity parameters where registration on individual level is not allowed. Here the ranking method metrics are a solution for obtaining information.

The McKinsey review highlighted bias, bullying and harassment to which minorities, in particular, were exposed. In an audit it would therefore be relevant to include a review of the harassment policies in the organisation (have they been established, are they instructional and transparent, and have they been communicated to all the staff), and if there is a zero-tolerance towards harassment i.e., what is the consequence management policy addressing these.

Lastly, establishment of ERGs and assessment of their operating effectiveness could be in scope of the audit, as well as looking through the entire diversity and inclusion set-up with a country dimension in mind.

Summary

Diversity and inclusion are two different concepts where inclusion is a prerequisite for nurturing a diverse organisation. There is substantial evidence that organisations with a prioritised diversity and inclusion agenda outperform other organisations less mature in this area.

But diversity and inclusion are not that easy to implement properly. Pain points in the experience of employees were identified as lack of accountability for managers, and inclusion items specifically directed towards minorities. A sound governance structure and proper metrics are valuable in steering organisations on the diversity and inclusion journey.

A starting point for an audit is to take a close look at the quality of the established governance structure and whether it is sufficiently supported by guidelines, reporting structures, and metrics.

Auditing diversity and inclusion can be challenging because of the intangible nature of some of the underlying components. Extensive root cause analysis may be needed to drill down to understand and disclose underlying mechanisms and behaviors. Consequently, it will require a skilled audit team to be able to ask the right questions and to assess the true nature of the diversity and inclusion effort carried out by the organisation and within the scope of the audit.

Notes

[1] IIA Global: 'Global Perspectives and Insights Understanding the effects of Diversity and Inclusion on organizations', IIA Global 2020
[2] Verlinden Neelie: 'Diversity vs Inclusion: What's the difference?' https://www.aihr.com/blog/diversity-vs-inclusion/
[3] Burke, Juliet and Dillon, Bernadette: 'The Diversity and Inclusion Revolution' Deloitte Review January 2018
[4] Verlinden Neelie: 'Diversity vs Inclusion: What's the difference?' https://www.aihr.com/blog/diversity-vs-inclusion/
[5] Belcaid, Nina: 'Auditing Culture', INFO April 2020
[6] 'No holding back: Breaking down the barriers to diversity', PwC 2017
[7] McKinsey: 'Why diversity matters' (2015), 'Delivering through diversity' (2018) and 'Diversity wins – Inclusion Matters' (2020)
[8] Forbes Insight 2011: 'Global Diversity and Inclusion Fostering Innovation Through a Diverse Workforce'
[9] Crescendo 28 February 2019: 'What DEI Metrics You Should Use'
[10] Forbes Insight 2011: 'Global Diversity and Inclusion Fostering Innovation Through a Diverse Workforce'
[11] 'No holding back: Breaking down the barriers to diversity', PwC 2017
[12] Foster, Trish: 'Taking Employee Resource Groups to the Next Level', Bentley University, Fall 2016
[13] Pollmann-Larsen Matias, Poulsen Mai-Britt and Jensen Thomas etc: 'Finding the Value in Diversity: Diversity and Inclusion Isn't Just a Fix', Boston Consulting Group May 2021
[14] IIA Global: 'Beyond diversity and inclusion - Social equity and corporate social responsibility', IIA Global September 2020
[15] The IIA has in 2019 issued a practice guide on culture, but it does not touch upon diversity and inclusion: IPPF: Supplemental Guidance Practice Guide: 'Auditing Culture', IIA, November 2019

Explainable AI: New challenge for Model Risk Management

Kamil Polak, Ph.D., Internal Audit Manager, Nordea

Introduction

The financial services industry, leveraging its experience in quantitative modelling, has been one of the early adopters of artificial intelligence (AI). While capable of bringing massive improvements and efficiency, AI creates an exposure to a number of risks that need to be managed via effective model risk management frameworks.

The aim of this article is to increase the awareness of specific problems related to AI models that may impact the model risk management framework, and discuss the nascent regulatory landscape aimed at addressing this risk.

Adoption of AI models

The business uses, regulatory interest and research regarding artificial intelligence and machine learning (AI/ML)[1] have seen an exponential increase over the last few years.

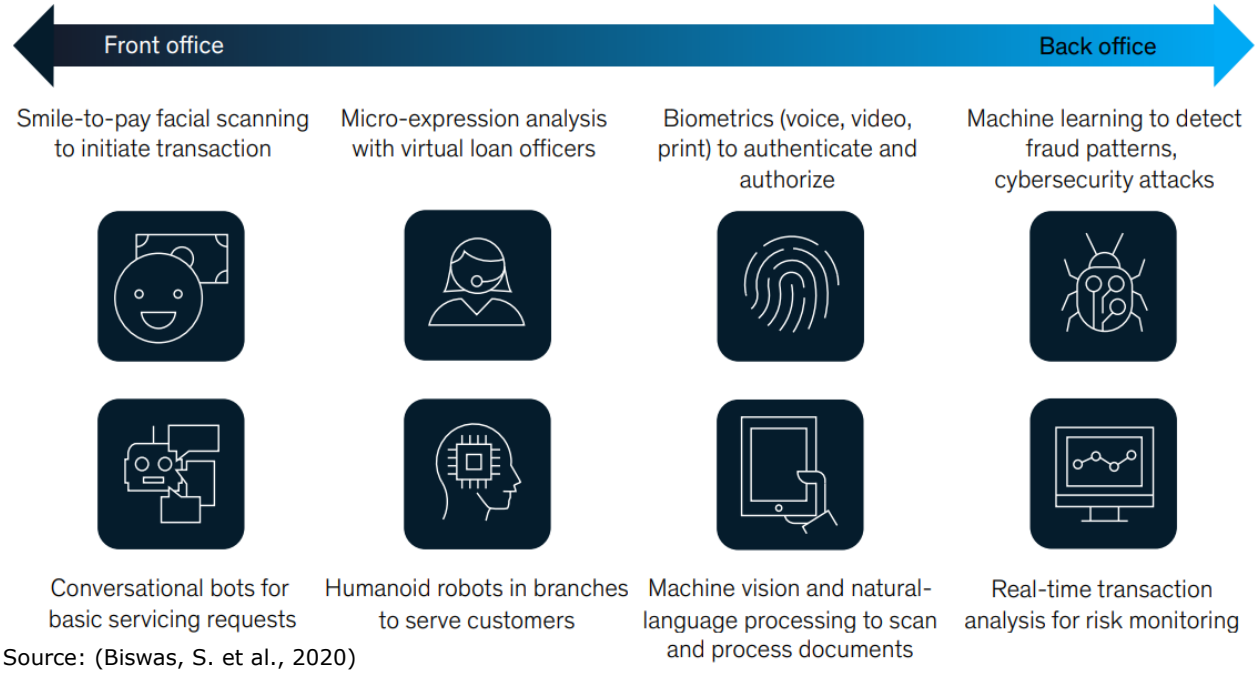
AI may be defined as *the ability of computer systems to perform tasks commonly associated with intelligent beings*. AI is a broad field, of which machine learning is a sub-category. Machine learning may be defined as *a method of designing a sequence of actions to solve a problem, known as algorithms, which optimise automatically through experience and with limited or no human intervention*.

According to *"Modeling the impact of AI on the world economy"* (Bughin, J. et al., 2018), while 70 per cent of companies may have adopted at least one type of AI/ML technology (e.g. computer vision, natural language, virtual assistants, robotic process automation, and advanced machine learning), by 2030 less than half will have fully absorbed all five categories.

What is more interesting, they estimated that AI has the potential to deliver additional global economic activity of around USD 13 trillion by 2030, or about 16 per cent higher cumulative Gross Domestic Product (GDP) compared to today. This amounts to 1.2% additional GDP growth per year.

ML-based predictive techniques are also seeing increased adoption within finance. As set out in *"AI-bank of the future: Can banks meet the AI challenge?"* (Biswas, S. et al., 2020), almost 60 per cent of financial services companies have embedded at least one AI capability. The most commonly used AI technologies are robotic process automation (36%) for structured operational tasks; virtual assistants or conversational interfaces (32%) for customer service divisions; and machine learning techniques (25%) to detect fraud and support underwriting and risk management.

Figure 1.



Source: (Biswas, S. et al., 2020)

More importantly, it can be seen that an increasing number of banking leaders are taking a comprehensive approach to deploying advanced AI and embedding it across the full lifecycle, from the front to the back office - see **Figure 1** on previous page.

However, it should be borne in mind that advanced AI algorithms, like any type of technology, are a double-edged sword that can be used in both useful and harmful ways. Simple models, such as linear and logistic regression, provide high interpretability but with limited predictive accuracy. Complex machine learning models, like deep neural networks, on the other hand, provide high predictive accuracy at the expense of limited explainability (Bussmann et al., 2021).

The reason for this is that in complex ML models, e.g. neural networks, how outputs correspond to inputs may be unclear without adequate transparency. This means that it is difficult to understand how inputs get transformed into outputs, or explainable on a stand-alone basis.

As described in the EY report *"Supervisory expectations and sound model risk management practices for artificial intelligence and machine learning"* (EY, 2020), lack of transparency can undermine an assessment of conceptual soundness, especially as related to sampling bias and fairness, because it makes it difficult to understand whether models are successfully meeting testing objectives and are fit for purpose.

For example, an ML model used to predict mortgage defaults may consist of hundreds of large decision trees deployed in parallel, making it difficult to summarise how the model works. This is often referred to as machine learning's 'black box'.

Lack of explainability[2] started a wide debate relating to techniques for making machine learning models more explainable (XAI). According to a working paper published by the Bank of England (Datta, A. Bracke, P. Jung, C., & Sen, S., 2019), explanations can answer different kinds of questions about a model's operation depending on the stakeholder they are addressed to.

In the financial context, we can differentiate the following types of stakeholders (Datta, A. Bracke, P. Jung, C., & Sen, S., 2019):

1. Developers
2. Model Users directly responsible for making sure model development is of sufficient quality
3. Model Validators who independently check the quality of model development and deployment
4. Management responsible for the model application
5. Regulators.

This article focuses on the last category of stakeholders, i.e. regulators.

Regulatory perspective

Governments and policymakers are increasingly recognising the problems posed by the widespread adoption of AI. Realising this, while preparing plans to use AI systems to reap their benefits, they also evaluate potential threats. This is visible not only at national, but also at the European, level.

European law (Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR), 2016) states that *"the existence of automated decision-making should carry meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."*

Furthermore, in April 2019 the European Commission High-Level Expert Group on AI (AI HLEG) presented the Ethics Guidelines for Trustworthy Artificial Intelligence[3], presenting seven key requirements that AI systems should meet in order to be deemed trustworthy.

Among them, three relate to the concept of explainable artificial intelligence:

- Human agency and oversight: Decisions must be informed, and there must be a human-in-the-loop oversight.
- Transparency: AI systems and their decisions should be explained in a manner adapted to the concerned stakeholder. Humans need to be aware that they are interacting with an AI system.
- Accountability: AI systems should develop mechanisms for responsibility and accountability, auditability, assessment of algorithms, data and design processes.

The Commission's AI HLEG was not the first to work on an ethical framework for AI. On a national level, a few countries already started similar exercises within the context of their own national strategies, e.g. Denmark[4], Finland[5], the UK[6] and Germany[7]. Also outside the EU, countries such as Singapore, Japan, Canada and Dubai started the development of their own ethical principles for AI (Smuha, 2019).

Additionally, in November 2021 the European Banking Authority (EBA) published a discussion paper on machine learning used in the context of internal ratings-based (IRB) models to calculate regulatory capital for credit risk[8]. The paper provides a set of principle-based recommendations that aim to ensure that machine learning models adhere to the regulatory requirements set out in the Capital Requirements Regulation (CRR), should they be used in the context of the IRB framework.

To ensure that the model is correctly interpreted and understood, EBA recommends to:

- Analyse, in a statistical manner, the relationship of each single risk driver with the output variable and the overall weight of each risk driver in determining the output variable.

- Assess the economic relationship of each risk driver with the output variable to ensure that the model estimates are plausible and intuitive.
- Provide a summary document in which the model is explained in an easy manner based on the outcomes of the analysis.
- Ensure that potential biases in the model (for example, overfitting to the training sample) are detected.

Explainable AI methods

Explainable artificial intelligence (XAI) is the title of an active research field focused on resolving the black box characteristic of machine learning.

According to Artificial Intelligence Risk & Governance (AIRS 2020)[9], examples of newer and perhaps relatively more accurate and sophisticated types of interpretable AI/ML systems include scalable Bayesian rule lists, Explainable Boosting Machines (EBMs), monotonic Gradient Boosting Machines (GBMs), various Bayesian or constrained variants of traditional AI/ML systems and other novel interpretable-by-design systems[10].

As described in the EY report *"Supervisory expectations and sound model risk management practices for artificial intelligence and machine learning"* (EY 2020), there are two common approaches to handle ML model explainability.

The first is to assess the importance of input features for the model predictions. This can be done on global and local levels.

Evaluation is performed globally when the importance of the overall impact of an input feature on model predictions is assessed. Examples include tree-based importance, permutation test-based importance and global sensitivity analysis.

Local evaluation is done where the effect of an individual observation's attributes on the model's prediction can be evaluated. Two popular approaches are LIME (Local Interpretable Model-agnostic Explanations) and SHAP (Shapley additive exPlanations). The latter is a game-theoretic approach to explain the output of any machine learning model. It connects optimal credit allocation with local explanations using the classic Shapley values from game theory and their related extensions[11].

The second approach of using surrogate models can also be employed, which entails using a simpler and more transparent model (e.g., tree, linear regression) as a proxy for a less transparent model (e.g., neural network).

However, it should be noted that such solutions are not free from limitations. As described by Deutsche Bundesbank (Deutsche Bundesbank, 2020) *"There is a fundamental conflict between the implementation of ML, with its potentially highly non-linear behaviour, and the demand for comprehensible linear explanations. Explanations put forward by XAI seem to be appealing and convenient, but they only show a limited picture of model behaviour, from which it is hard to draw general conclusions. Thus, ML combined with an XAI approach cannot make the black box fully transparent, merely less opaque. Nonetheless, it seems to be helpful to use XAI to provide more reliable risk metrics for control processes. We propose a balanced approach with XAI methods to be tailored to the use case and the stakeholders' demands"*.

Further limitations of XAI methods should not be overlooked. In particular, some methods require high computational power or only deliver minor insights into algorithms' behaviours. XAI methods should support established and used risk control processes, and be able to demonstrate effectiveness. If not applying XAI methods, control processes should be in place to compensate for limited transparency.

How can the Audit function support an organisation?

Internal Audit should be able to help an organisation to evaluate, understand, and communicate the degree to which artificial intelligence will have an effect (both negative and positive) on the organisation's ability to create value. This implies the need to have the necessary expert knowledge in the field of AI.

According to the IIA report *"Artificial Intelligence – Considerations for the Profession of Internal Auditing"*[12], the internal audit activity collectively must have a sufficient understanding of AI, how the organisation is using it, and the risks that AI represents for the organisation. This condition should be clearly communicated by the CAE to senior management, the board, and the audit committee.

Furthermore, it is recommended that Internal Audit consider the following activities:

- Include AI in its risk assessment and consider whether to include AI in its risk-based audit plan
- Be engaged in AI projects (without impairment of independence and objectivity)
- For partial implementation of AI provide assurance related to the reliability of underlying algorithms and data on which the algorithms are based
- Assess whether the moral and ethical issues that may surround the organisation's use of AI are being addressed
- Provide assurance on IT controls.

Specifically for the XAI area, Internal Audit should review AI development and implementation policies, processes and procedures, to assess whether there are controls in place to identify, understand and explain "black-box" data.

Concluding remarks

Since the subprime crisis, banks have focused on strengthening their model risk management framework, supported by new regulations and financial supervision. However, with the advent of machine learning, model risk has transformed.

Despite the apparent increase in interest in new sources of risk from both regulators and institutions, it is still unclear whether the financial services sector has reached the appropriate level of maturity to properly assess and control machine learning risk.

This applies to, amongst other things, the proper interpretability of model results. For this reason, I believe that further work is needed both on model assessment techniques, and also on a new approach to auditing the control environment focused on AI risk. This requires not only gaining expert knowledge,but also understanding the goals which the institution seeks to achieve through the implementation of AI models.

Notes

[1] I use the terms AI and ML interchangeably for ease of exposition, but in practice, ML is a subset of AI. For more details see https://www.fsb.org/wp-content/uploads/P011117.pdf.

[2] A term used interchangeably with explainability is interpretability, but some authors cite differences. A model is interpretable when it can be understood by human beings. A model is explainable when it provides a rationale for its results. See "Explaining Explanations: An Overview of Interpretability in Machine Learning," Leilani H. Gilpen, David Bau, Ben Z. Yuan, Ayesha Bajwa, Michael Specter and Lalana Kagal, 2019.

[3] See: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1

[4] In March 2018, the Danish Ministry of Industry, Business and Financial Affairs established an expert group on data ethics, tasked to draw up a set of data ethical recommendations.

[5] The Finnish Ministry of Economic Affairs and Employment launched an AI Ethics Challenge, encouraging companies to publicly subscribe to ethical principles for AI, as part of its AI strategy.

[6] In November 2018, the UK's Department for Digital, Culture, Media and Sport launched a new Centre for Data Ethics and Innovation, tasked to look into ethical issues relating to data and AI. It is but one of the various governmental initiatives around the subject.

[7] Both the German Parliament and the German Federal Government set up an AI Ethics Commission in late 2018, each of which are expected to deliver ethical guidance.

[8] See: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Discussions/2022/Discussion%20on%20machine%20learning%20for%20IRB%20models/1023883/Discussion%20paper%20on%20machine%20learning%20for%20IRB%20models.pdf

[9] AIRS is an informal group of practitioners and academics from varied backgrounds, including technology risk, information security, legal, privacy, architects, model risk management and others, working for financial and technology organisations and academic institutions. See: https://ai.wharton.upenn.edu/artificial-intelligence-risk-governance/

[10] See, for example, XGBoost, h2o's GBM or Microsoft's InterpretML toolkit, available at https://xgboost.readthedocs.io/en/latest/tutorials/monotonic.html, https://github.com/h2oai/h2o-3/blob/master/h2o-py/demos/H2O_tutorial_gbm_monotonicity.ipynb and https://interpret.ml/, respectively.

[11] For more details see technical documentation: https://shap.readthedocs.io/en/latest/

[12] See: https://iia.no/product/artificial-intelligence-considerations-for-the-profession-of-internal-auditing/

References

Artificial Intelligence – Considerations for the Profession of Internal Auditing. (2017). The Institute of Internal Auditor.

Biswas, S., Carson, B., Chung, V., Singh, S., & Thomas, S. (2020). *AI-bank of the future: Can banks meet the AI challenge?* McKinsey & Company.

Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). *Modeling the impact of AI on the world economy.* McKinsey Global Institute.

Bussmann, N., Giudici, P., Marinelli, D., & Papenbrock, J. (2021). Explainable machine learning in credit risk management. *Computational Economics*, 57(1), 203–216.

Datta, A. Bracke, P. Jung, C., & Sen, S. (2019). Machine learning explainability in finance: An application to default risk analysis. *Bank of England Staff Working Paper*, 816.

Deutsche Bundesbank. (2020). Policy Discussion Paper *The Use of Artificial Intelligence and Machine Learning in the Financial Sector*.

Discussion paper on machine learning for IRB models. (2021). The European Banking Authority.

Gilpin, L. H., Bau, D., Yuan, B. Z., Bajwa, A., Specter, M., & Kagal, L. (2018). Explaining explanations: An overview of interpretability of machine learning. *2018 IEEE 5th International Conference on Data Science and Advanced Analytics (DSAA)*, 80–89.

Regulation (EU) 2016/679—General data protection regulation (GDPR). (2016). Official Journal of the European Union.

Smuha, N. A. (2019). The EU approach to ethics guidelines for trustworthy artificial intelligence. *Computer Law Review International, 20*(4), 97–106.

Supervisory expectations and sound model risk management practices for artificial intelligence and machine learning. (2020). Ernst & Young LLP.

INTERNATIONAL CONFERENCE CHICAGO 2022
CHICAGO, ILLINOIS, USA / 17–20 JULY

https://ic.globaliia.org/Pages/about.aspx

50+ Sessions

16 Language Translations

100+ Speakers From Around the Globe

17-20 July 2022

The IIA's International Conference is the premier training and networking event for internal audit professionals worldwide. The IIA is preparing a world-class program focused on delivering topical and forward-thinking presentations to our in-person and virtual audience.

Why should I attend?

1. Experience a comprehensive program focused on timely, global issues impacting the profession.
2. Network with like-minded colleagues from public and private sector organizations.
3. Earn up to 18 CPE in support of your IIA certifications.
4. Share and discuss innovative ideas and concepts with recognized thought leaders, speakers, and practitioners from around the world.
5. Participate in interactive sessions on pressing topics such as emerging technology trends, culture, ethics and governance, fraud prevention, financial services, risk, and CAE insights.
6. Engage with leading-edge product, service, and technology providers with innovative offerings to help you succeed.

De gode grunde til at have Datatilsynet i fokus

Jacob Krabbe, advokatfuldmægtig, ComplyCloud

Indledning

Datatilsynet er en uafhængig statslig myndighed, hvis opgave er at føre tilsyn med overholdelse af Persondataforordningen og Databeskyttelsesloven.

Datatilsynet behandler klager og tager også af egen drift initiativ til at føre tilsyn med, at databeskyttelsesreglerne overholdes. Hvert år offentliggør Datatilsynet en strategi for at styrke sin data- og risikobaserede tilsynsindsats.

Det betyder, at der er områder, som Datatilsynet vil have særligt fokus på i koordineringen af deres tilsynsarbejde. Ud fra en pragmatisk, forretningsmæssigt risikobaseret tilgang til compliance-arbejdet, er det derfor en god ide også i jeres organisation at have særligt fokus på at få styr på de dele af organisationen, der omfattes af fokusområderne.

På den måde kan I nemlig reducere risikoen markant for at modtage kritik eller blive indstillet til bøder.

Fokusområder

Herunder ses en række udvalgte fokusområder for 2022:

Iagttagelse af oplysningspligt ved uanmodet henvendelse
Behandling af personoplysninger skal ifølge databeskyttelsesforordningen foregå på en rimelig og gennemsigtig måde. Det sikres først og fremmest gennem den dataansvarliges oplysningspligt.

Denne pligt kan som regel overholdes ved at gøre den registrerede bekendt med en persondatapolitik. Men når en dataansvarlig uanmodet henvender sig til registrerede, f.eks. ved telefonsalg, kan denne pligt være vanskelig at opfylde. Derfor er det formentligt også noget, der ofte glipper i praksis.

Behandling af personoplysninger om hjemmesidebesøgende
Dette er en opfølgning på Datatilsynets vejledning fra 2020 om behandling af personoplysninger fra hjemmesidebesøgende, jf. https://www.datatilsynet.dk/media/7784/vejledning-om-behandling-af-personoplysninger-om-hjemmesidebesoegende.pdf

Persondatasikkerhed, inkl. brud på persondatasikkerheden
Datatilsynet vil have fokus på myndigheders og virksomheders ansvar for at etablere et passende sikkerhedsniveau når der behandles personoplysninger.

I forbindelse med persondatasikkerheden skal brud som udgangspunkt anmeldes til Datatilsynet, og i nogle tilfælde skal den dataansvarlige også anmelde bruddet til de berørte.

Der vil også være fokus på, om de fornødne konsekvensanalyser er blevet foretaget, sådan at det sikres at IT-systemer til behandling af personoplysninger sikres at have det nødvendige sikkerhedsniveau.

Datatilsynet har derfor i 2022 besluttet at føre tilsyn med persondatasikkerheden mv. inden for følgende områder:

- Fællesoffentlige it-løsninger og fællesstatslige it-løsninger.
- Om brud på persondatasikkerheden håndteres og anmeldes i overensstemmelse med reglerne herom.
- Om der i de tilfælde, hvor der foreligger en høj risiko for de registrerede som følge af et brud på persondatasikkerheden, sker den fornødne underretning af de berørte registrerede, og
- Om de dataansvarlige i forbindelse med, at it-løsninger designes, udvikles, indkøbes eller tilpasses, overholder reglerne om databeskyttelse gennem design og udarbejdelse af konsekvensanalyser.

Her vil Datatilsynet graduere indsatsen efter typen af de virksomheder, der føres tilsyn med, sådan at tilsynet i visse tilfælde kan have en mere generel karakter.

Kontrol med databehandlere
Som dataansvarlig er man forpligtet til at føre kontrol med ens databehandlere, og sikre, at disse generelt efterlever databeskyttelsesforordningens regler, og konkret behandler personoplysningerne i overensstemmelse med den dataansvarliges instruks.

Forpligtelsen udspringer af samme bestemmelse, som opstiller kravet om, at der indgås en databehandleraftale mellem den dataansvarlige og tilknyttede databehandlere. Det er i sagens natur nødvendigt regelmæssigt at kontrollere, at behandlingen lever op til de aftalte krav. Datatilsynet har siden 2016 haft fokus på kontrol med databehandlere. I 2022 vil Datatilsynet føre tilsyn med, om private virksomheder har en passende kontrol med sine databehandlere. Det kan man læse mere om i Datatilsynets vejledning herom: https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning_om_tilsyn_med_databehandlere_oktober-2021.pdf

Tv-overvågning
Datatilsynet vil i 2022 udføre flere tilsyn med private og offentlige myndigheders behandling af personoplysninger i forbindelse med tv-overvågning. Dette initiativ skal ses i lyset af tv-overvågningsloven, der trådte i kraft i 2020, som lempede kravene for, hvornår der må foretages videoovervågning.

At holde sig opdateret er nøglen til succes

Datatilsynets fokusområder spænder vidt, så alle der arbejder med compliance vil drage fordel af at holde sig orienteret om lige netop disse områder. Der er også truffet nogle afgørelser, der har særlig relevans for revisorer - se **Tabel 1** nederst på siden.

I ComplyClouds casebooks kan I læse resumeer af sager der udspringer fra afgørelser fra Datatilsynet og vores bemærkninger til disse sager. ComplyClouds casebooks udgives flere gange om året, ligesom der udgives en årsbog, der samler op på sagerne.

Nedenfor kommer vi ind på, hvad der er det seneste nye på databeskyttelsesområdet.

Et complianceområde i heftig udvikling

Databeskyttelsesområdet er ret turbulent, og der træffes i øjeblikket afgørelser, som påvirker virksomhedernes omkostninger til compliance. Derfor bør man være omstillingsparat. Særligt på området for overførsel af personoplysninger til uden for EU går det stærkt. I juli 2020 tog EU-Domstolen stilling til spørgsmålet om tredjelandsoverførsler til USA i den banebrydende "Schrems II"-afgørelse.

Ifølge Schrems II er dataoverførsler til USA omfattet af den amerikanske lovgivning i FISA 702. FISA 702 giver amerikanske efterretningstjenester mulighed for at tilegne sig oplysninger om ikke-amerikanske statsborgere, som er i amerikanske virksomheders varetægt.

Sagen ved EU-Domstolen udsprang af i alt 101 klagesager, der er anlagt ved en række europæiske datatilsynsmyndigheder af organisationen None of Your Business ("NOYB") med Max Schrems i spidsen. Sagerne omhandler dataoverførsler fra EØS-baserede websteder til Google LLC og Facebook Inc. i USA.

Som konsekvens af Schrems II-dommen har der for nyligt været en række sager ved europæiske datatilsyn, som har undersøgt organisationers brug af hjemmeside-analyseværktøjet Google Analytics. Sagerne er eksempler på, hvordan det nye regime om tredjelandsoverførsler kan gøre livet surt for europæiske virksomheder, der for eksempel bruger amerikanske tjenester, som Google Analytics, men også tjenester fra andre amerikanske udbydere som Microsoft, Facebook, Amazon og andre tjenester, hvor tjenesteudbyderen ikke kan garantere, at persondata forbliver inden for EU's grænser.

Som det første datatilsyn traf man i Østrig en afgørelse og erklærede brugen af Google Analytics i den konkrete sag ulovlig, og senere fulgte Frankrig efter med en afgørelse der er beskrevet herunder.

Det franske datatilsyns afgørelse
Personoplysninger blev overført til Google i USA på baggrund EU-Kommissionens standardkontraktsbestemmelser ("SCC"). I tillæg til SCC havde Google implementeret en række supplerende sikkerhedsforanstaltninger.

Ifølge det franske datatilsyn var de supplerende sikkerhedsforanstaltninger, implementeret af Google, ikke tilstrækkelige.

Det franske datatilsyn konkluderede i sin afgørelse, at personoplysninger om hjemmesidens brugere blev overført til USA via Google Analytics. Datatilsynet anførte, at de supplerende foranstaltninger ikke var effektive, idet foranstaltningerne ikke udelukkede amerikanske efterretningstjenesters adgang til personoplysningerne, og at der dermed ikke var tilstrækkelige sikkerhedsgarantier ved

Tabel 1.

Sag	Afgørelse
Kolding Kommune havde ikke truffet passende tekniske og organisatoriske foranstaltninger	https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/apr/kolding-kommune-havde-ikke-truffet-passende-tekniske-og-organisatoriske-foranstaltninger
Tilsyn med behandlingssikkerhed hos revisionsfirma	https://www.datatilsynet.dk/afgoerelser/afgoerelser/2019/nov/tilsyn-med-behandlingssikkerhed-hos-revisionsfirma
Afslutning af planlagt tilsyn hos Viborg Kommune	https://www.datatilsynet.dk/afgoerelser/afgoerelser/2019/aug/afslutning-af-planlagt-tilsyn-hos-viborg-kommune
Afslutning af planlagt tilsyn hos Randers Kommune	https://www.datatilsynet.dk/afgoerelser/afgoerelser/2019/aug/afslutning-af-planlagt-tilsyn-hos-randers-kommune

dataoverførslen. På baggrund heraf fandt det franske datatilsyn, ligesom det østrigske datatilsyn, at dataoverførslen til USA ved brug af Google Analytics var i strid med GDPR.

Hvad betyder det for danske virksomheder?
Afgørelserne i Østrig og Frankrig er truffet i samråd med andre datatilsynsmyndigheder i EU. Det betyder, at der som udgangspunkt er enighed om beslutningerne.

Det danske datatilsyn har endnu ikke udtalt sig konkret om emnet. Dette på trods af, at Datatilsynet har ført tilsyn i en sag vedrørende Den Blå Avis og dennes samtykkeløsning til Google Analytics. Datatilsynet udtalte i sagen alvorlig kritik af løsningen, men kritikken gik ikke på en eventuel overtrædelse af reglerne om tredjelandsoverførsler.

Det, man skal være opmærksom på i forhold til sagerne om Google Analytics er, at der i ingen af sagerne var foretaget den fornødne vurdering af overførslen, nemlig en Transfer Impact Assessment (TIA), som ifølge Schrems II skal foretages, før den er lovlig. Derfor virker polemikken i medierne, om at brugen af Google Analytics uden videre er ulovlig, og Googles trusler om at stoppe med at udbyde tjenesten i EU, stærkt overdrevne og baseret på manglende forståelse for reglerne.

Konkrete løsningsforslag

- Alternative leverandører
  Den første løsning på problematikken er simpel: stop brugen af Google Analytics og benyt i stedet en EU-baseret leverandør. Google Analytics er ikke det eneste analyse- og rapporteringsapparat på markedet. Der findes en række EU-baserede leverandører, som er compliant med GDPR, og som kan bruges som alternativ til Google Analytics. Alternative leverandører til Google Analytics er for eksempel Simple Analytics, der er baseret i Holland, Matomo, der er baseret i Tyskland og Piwic Pro, der er baseret i Polen.

- Supplerende foranstaltninger
  Google Analytics giver mulighed for en konfiguration, hvor man kan anonymisere de sidste fire cifre i den registreredes IP-adresse, inden eller idet oplysningerne rammer serveren i USA. I så fald kan det ikke ses, hvem IP-adressen refererer til, men kun i hvilket geografiske område vedkommende befinder sig i. Det er meget tvivlsomt, om der i så fald overhovedet vil være tale om en tredjelandsoverførsel.

- "No reason to believe"
  En anden løsning er at foretage en "no reason to believe"-vurdering i sin TIA. I den forbindelse skal virksomheden vurdere, om oplysningerne konkret kan tænkes at have interesse for de amerikanske efterretningstjenester, og om der derfor er grund til at tro, at problematisk amerikansk lovgivning, herunder FISA 702, vil blive anvendt i praksis. Kan det dokumenteres, at der *ikke er grund til at tro*, at FISA 702 mv. vil blive anvendt i praksis, kan overførslen fortsætte.

  Dertil kan ressource- og sandsynlighedsbetragtninger understøtte vurderingen. Ifølge det amerikanske efterretningstilsyns (ODNI) årlige statistiske rapport for anvendelsen af FISA 702, anvendes lovgivningen på omkring 200.000 ikke-amerikanske mål om året. Hvert enkelt mål kræver en individuel rimelighedsvurdering, og dokumentation herfor skal godkendes i flere lag.

  De enorme mængder af mulige mål for FISA 702, f.eks. alle IP-adresser i Googles varetægt, sammenholdt med den ressourcetunge proces, det kræver at få adgang til oplysningerne, kan formentligt inddrages, når det vurderes, om der er grund til at tro, at den problematiske amerikanske lovgivning vil blive anvendt i praksis på almindelige oplysninger af kommerciel karakter.

Link til ComplyCloud vidensdeling:
https://www.complycloud.com/viden/

Link til ComplyCloud legaltech løsning:
https://www.complycloud.com/produkt/

Nye medlemmer

Nye medlemmer i IIA fra 7.12.2021 - 8.4.2022

A.P. Møller Mærsk
Morten Kjær
Pramod Mundanat
Danny Ravn Pedersen
Sujeet Sonawane

Coloplast
Niklas Mengel

Danmarks Nationalbank
Gülhan Duvarci Rasmussen

Danske Bank
Helle Madsen
Carsten Dyrfeldt
Maria Concetta Barbano
Søren Garbøl
Mie K. Bolt Therkelsen
Heidi Lange
Iben Nøhr

Deloitte
Lars Dalgaard Agersted
Lica Lyngsø Nielsen

Falck
Petur Pauli Mikkelsen

Finansministeriet
Tanja Vibeke Moldrup

Forsvarsministeriets Interne Revision
Bo Herbst

Himmerland Forsikring
Tanja Hedegaard Kristensen

Københavns Kommune
Abdur Rahman Ahmed

Nordea
Eleni Liapi
Steve Steyn

PensionDanmark
Cemile Özdemir

PwC
Annelise Møller

Solar
René Budde Gade

Sydbank
Anne Cathrine Schoop Pallesen

Sønderjysk Forsikring
Tue Brink

vestjyskBANK
Karsten Gatten Vestergaard

Ørsted Services
Muhammad Altamash

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.

Kursuskataloget

04.05.2022 Kursus for forsikringsrevisorer
10.05.2022 IIA Årsmøde 2022
02.06.2022 IIA Generalforsamling

"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, Chefkonsulent - Intern Revisor, CIA, Forsvarsministeriets Interne Revision
☎ 31 18 38 01 ✉ fir-hnh@mil.dk

Peer Højlund, Chefspecialist, Nykredit
☎ 44 55 93 14 ✉ phc@nykredit.dk

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

Formand
Audit Director
Jesper Siddique Olsen
Danske Bank
☎ 45 12 76 58 ✉ jol@danskebank.dk

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

Kasserer
Koncernrevisionschef , CIA
Morten Bendtsen
Alm. Brand
☎ 35 47 47 47 ✉ abmobn@almbrand.dk

Sekretær
Internal Audit Manager
Vibeke Arnholst
Nordea
☎ 55 47 81 81 ✉ vibeke.arnholst@nordea.com

Bestyrelsesmedlemmer
Nordisk Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
BNP Paribas Personal Finance
☎ 36 39 52 61 ✉ birgitte.svenningsen@bnpparibas-pf.dk

Partner, CIA, CISA, CGEIT
Johan Bogentoft
PwC
☎ 29 27 62 96 ✉ joa@pwc.dk

Professor
Kim Klarskov Jeppesen
CBS - Copenhagen Business School
☎ 38 15 23 06 ✉ kkj.acc@cbs.dk

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

Afdelingsdirektør, CIA
Tobias Zorde
Nykredit
☎ 44 55 93 35 ✉ tzo@nykredit.dk

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