INFO

Foreningen af Interne Revisorer
Nummer 82 | December 2022 | 27. årgang

Mangler vi interne revisorer i Danmark?

Chromebooks-sagen i Helsingør kommune

Nordic Financial CERT

En eksperts vurdering af Cyber-truslen mod finanssektoren

NIS2 - Nyt EU-direktiv

Skærpede krav til cyber- og informationssikkerheden.

Staffing for Success ● Scrum Security ● Tips og tricks

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 83 udkommer i april 2023.
ISSN: 1903-7341 (Elektronisk version).

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

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

Forsidefoto
UnknownNet

Redaktionens adresse

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

redaktionen@iia.dk

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

Indhold

Nyt fra bestyrelsen

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

www.iia.dk

Leder

Tobias Zorde, Afdelingsdirektør, Nykredit

Da jeg modtog udkastet til dette nummer af INFO, lod en sandsynligvis ikke-forsætlig rød tråd sig tegne tværs igennem en række af artiklerne. Det var en rød tråd, der snoede sig rundt om nogle af tidens store opgaver og udfordringer for interne revisionsfunktioner. Vi taler om produktion, tilførsel og vedligeholdelse af talentmassen på denne ene side og så cybertruslen på den anden. Det der naturligvis binder disse områder sammen er, at cyber er et af de områder, hvor spørgsmålet om kompetencer og ressourcer er særligt udtalt grundet kombinationen af teknisk kompleksitet, kreativitet iblandt interessenter med ilde intentioner og ikke mindst allestedsnærværet som følge af stigende automatisering og digitalisering.

Udfordringer omkring ressourcer og kompetencer er ikke mindst en rekrutteringsudfordring, og gør sig efter undertegnedes bedste vidende gældende for de fleste interne revisionsfunktioner i landet, men fremtræder selvfølgelig på forskellige måder. Er rekrutteringen global eller lokal? Er revisionsfunktionen lille, mellem eller stor? Geografisk placering? Skal/kan vi outsource?

Spørgsmålet omkring talentmassen stilles først og fremmest af revisionschefen i Danske Bank, Dorthe Tolborg, i artiklen "Mangler vi interne revisorer i Danmark?" En række yderligere spørgsmål følger i kølvandet – *hvilke kompetencer har vi brug for, findes kompetencerne i Danmark, hvorfor er det attraktivt at arbejde i intern revision, hvor rekrutterer vi fra?* Tolborg konkluderer slutteligt, at der ikke er tale om mangel i talentmassen. Varen, der er i fare for at komme i restordre, er professionens mod på at turde at gå nye veje i sine rekrutteringsstrategier.

Tråden snor sig videre i artikel "Staffing for Succes" af Geoffrey Nordhoff. Nordhoffs fokus er på digitale trusler og det deraf affødte behov for at justere ekspertisesammensætningen på revisionsteamet. Nordhoffs artikel er meget hands-on og udgør et godt katalog for hvilke kompetencer, kvalifikationer og soft skills, man skal lede efter i rekrutteringen samt hvilke strategier, man kan gøre brug af i opbygningen af talent.

Endelig bindes sløjfen på den røde tråd af Morten Tandle, Leder af Nordic Financial CERT, via artiklen "Cybertruslen mod finanssektoren – en ekspertvurdering".

Denne artikel går et spadestik dybere ned i cybertruslen, som karakteriseres som *overhængende* men *diffus*. Dette er en rammende karakteristik. Vi er jo alle enige om, at det er useriøst at levere en koncernrevisionsplan, hvor ordet "cyber" ikke fremgår et to-cifret antal gange, men når det kommer til fastlæggelse af revisionstrategi og ressourcer – altså når vi skal have cyber-jord under neglene – bliver situationen straks mere diffus. Bevæbnet med Tandles perspektiver står vi dog en anelse bedre og begaves med en bedre forståelse af det såvel nuværende som fremtidige trusselbillede.

At styrke professionens talent-pipeline er ikke blot en udfordring for de fleste interne revisioner, og noget man kan læse om i dette nummer af INFO. Det er også et strategisk anliggende for IIA, hvorfor der er igangsat en række initiativer, herunder yderligere styrkelse af partnerskaberne med Danmarks uddannelsesinstitutioner. Dette kommer særligt i form af tilstedeværelse på CMA-uddannelserne; introforløb, valgfag, moduler på obligatoriske fag etc. Inspireret af ovennævnte artikler kunne man dog overveje at udvide fokus til også at omfatte andre talentkilder? Vi må i hvert fald forstå, at verden forandrer sig, og hvis vi skal med på toget, ligger løsningerne sjældent i den konventionelle vanetænkning.

Jeg håber, I vil lade jer inspirere af ovenstående- og de øvrige artikler i dette nummer af INFO. Og når I er færdige med læsningen og er sultne efter dessert, anbefaler jeg, at I orienterer jer i nyeste notat fra Fagligt udvalg for SIFI-institutter, som udgør et forsøg på at levere anbefalet praksis for interne revisorer i krydsfeltet mellem IPPF-standarderne og Revisionsbekendtgørelsen. Notatet er udarbejdet i samarbejde mellem Danmarks SIFI-institutter og kan findes på IIAs hjemmeside under menupunktet "Standarder" og "Øvrige" under titlen "Praksis for afgivelse af § 27-konklusion iblandt Danmarks SIFI-institutter".

God læsning, god jul og godt nytår!

Tips and Tricks – Teams Viva Insight app

Stine Juhl-Hansen, IT-auditor, Danfoss

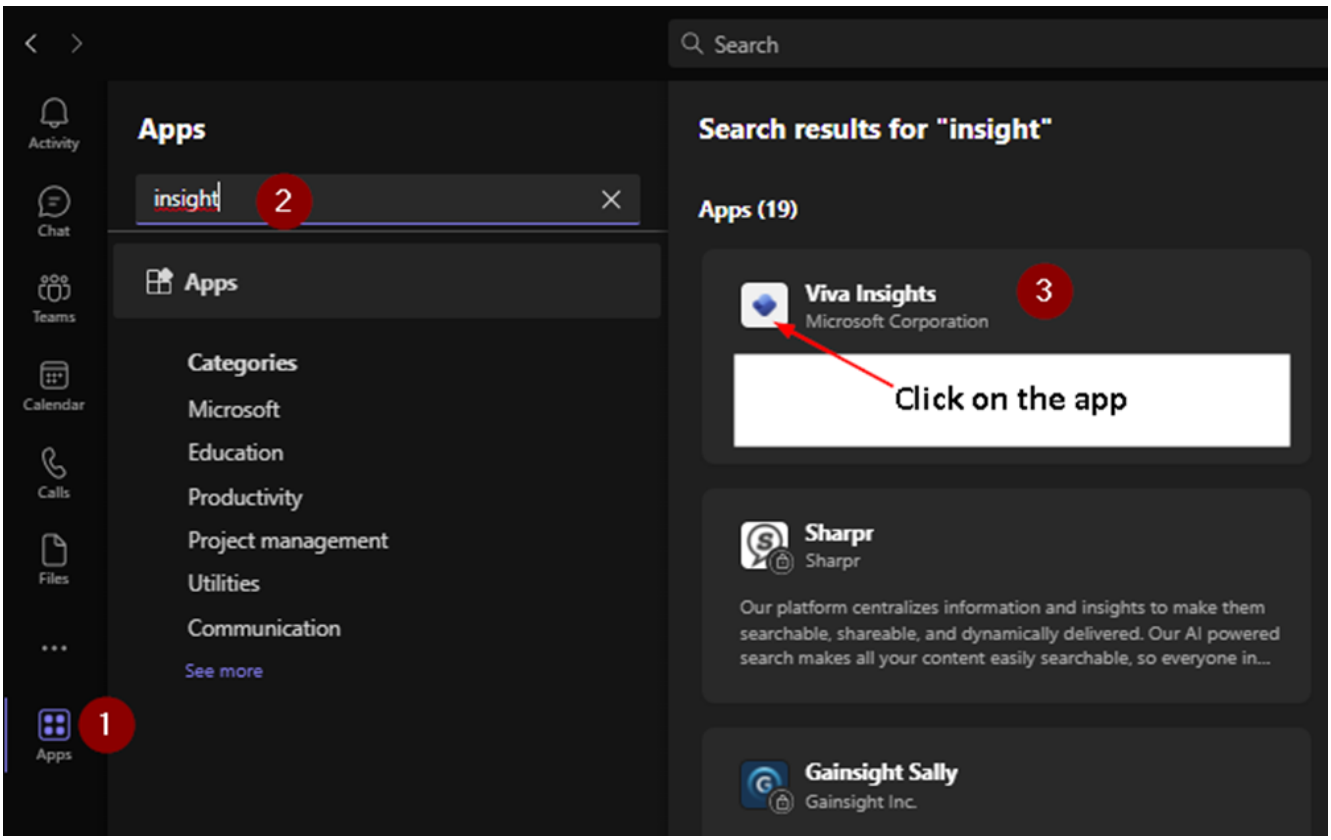
Improve your productivity and well-being with Teams and Microsoft Viva Insights

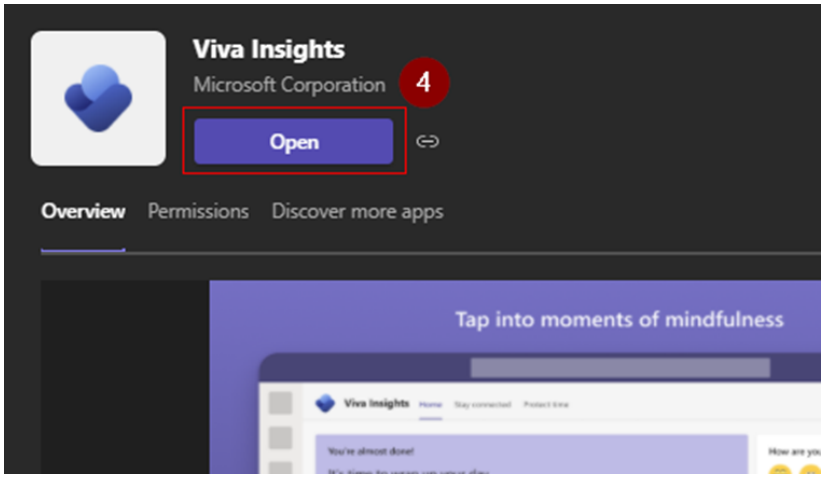
Microsoft Viva Insights provides personalised recommendations to help you do your best work. Get insights to build better work habits, such as taking regular breaks, following through on commitments made to collaborators and protecting focus time during the day for uninterrupted, individual work.

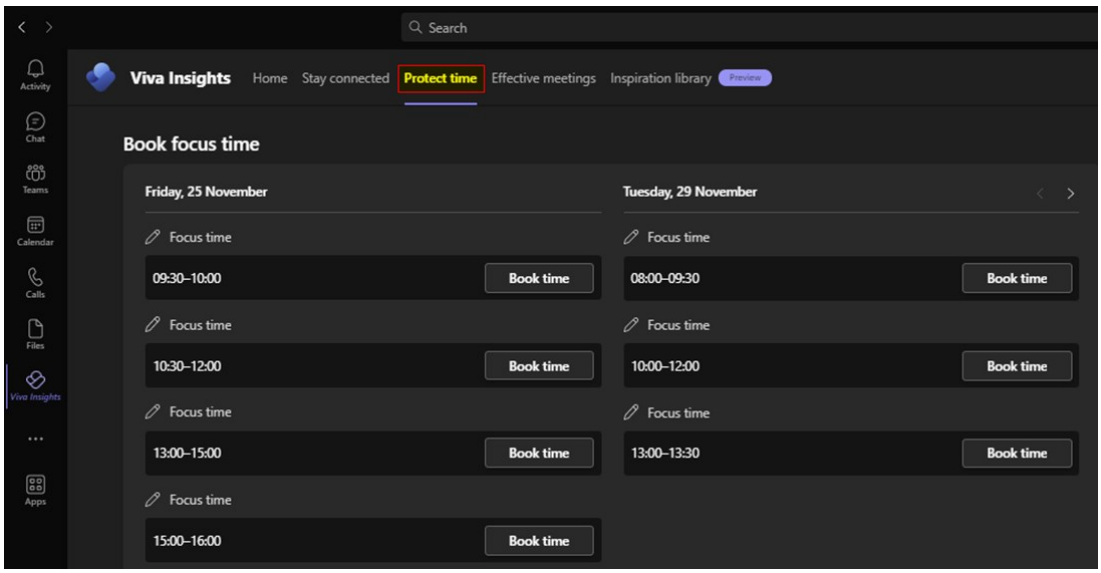
Step 1: Open the Viva Insight app in Microsoft Teams
Check if you already have the app in the menu bar.
If not; you can access it via

1. Apps
2. Search Insights
3. Click on app
4. Click open in the pop-up

Step 2: Go to "Protect Time"
Here Teams will help you find timeslots during you day where you can focus.







Bliv en aktiv del af IIA!!!!

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

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

IIA PRISEN

Prisopgave om intern revision

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

25.000 kr.

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

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

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

Ansøgningsfristen er 31. januar 2023. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iia.dk.

Prisoverrækkelsen vil ske på IIA's årsmøde i maj 2023. Bedømmelsesudvalget består af Dorthe Tolborg (Danske Bank), Kim Klarskov Jeppesen (CBS) og Birgitte Rousing Svenningsen (Express Bank).

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

IIA Denmark

Mangler vi interne revisorer i Danmark?

Dorthe Tolborg, CAE, Danske Bank

Introduktion

En række forudsætninger skal være til stede for, at en intern revisionsfunktion kan fungere optimalt. En af de altafgørende forudsætninger er, at de nødvendige og tilstrækkelige ressourcer er tilstede til at kunne levere på den revisionsplan, som er godkendt af bestyrelsen.

Her spiller kompetenceniveauet naturligvis ind. Den Interne Revision skal være i stand til at demonstrere, at den besidder de rette kompetencer til at kunne gennemføre revisionsarbejdet og til at kunne kommunikere resultatet af revisionerne internt i organisationen og opad i systemet til både direktion, revisionsudvalg og bestyrelse. Hvis det ikke er tilfældet, bliver det unægtelig vanskeligt at være en succesfuld revisionsfunktion.

En succesfuld revisionsfunktion er i min optik en funktion, som på den ene side lever op til alle de krav om integritet, objektivitet, ekspertise og uafhængighed, som kendetegner intern revision, og som på den anden side udfordrer forretningen til hele tiden at udvikle sig indenfor governance, risk management og kontrolområdet.

Spørgsmålet er derfor, om der i Danmark mangler interne revisorer med de nødvendige kompetencer, som sikrer, at de interne revisionsfunktioner fortsætter med at være i en position, hvor funktionen er anset for at være værdiskabende for organisationen og for at hjælpe med at fokusere på de områder hvor kultur og mindset ikke er som forventet.

I denne artikel vil jeg beskrive mit perspektiv på emnet med udgangspunkt i den virkelighed, som jeg befinder mig i.

Men først et par fakta om Intern Revision i Danske Bank:

- 103 medarbejdere
- Kønsfordeling: 49% mænd; 51% kvinder
- Gns. alder: 42 år
- Gns. anciennitet: 10 år
- Personaleomsætning: 9%
- Uddannelsesmæssig baggrund: Ingeniør, Cand.scient.pol, Masters i Mathemetics-Economics, International Security, Business Controlling, og Science in Economics, Bankuddannet, Cand.merc.aud og meget andet……
- Krav til løbende videreuddannelse hos Intern Revision = 40 timer pr. år i gns. over en 3-årig periode
- Intern Revisions mandat: Operationel revision

Hvilke kompetencer har vi brug for?

Vi måler og følger op på vores færdigheder og kompetencer for at sikre og dokumentere, at vi til stadighed har en tilstrækkelig indsigt og viden. Vi stræber efter at have kompetencer, der kan opfylde de forventninger, som vores revisionskunde har til os, og således at vi er i en position, hvor vi kan udfordre vores revisionskunde i passende omfang på alle væsentlige og risikofyldte områder.

Vi måler vores niveau for kompetencer på syv områder:

- Audit, Risk and Control Knowledge
- Business/Industry Knowledge
- Core Auditing skills
- Technical skills
- Financial Service Industry and product Knowledge
- Stakeholder partnering skills
- Development and Personal Commitment skills

Ofte oplever vi, når vi opdaterer vores kompetence GAP-analyse, at vi har en nøglepersonafhængighed på flere områder. På trods af vores funktions størrelse, er det næsten umuligt på alle områder at have flere medarbejdere, som overlapper indenfor samme tekniske område. I andre tilfælde identificerer vi, at vi mangler kompetencer på specifikke områder.

Vi reducerer vores primære personafhængighed og kompetence GAP ved at uddanne medarbejdere internt og eksternt, ved 'on the job training' samt ved at ansætte medarbejdere med de færdigheder og den erfaring, der er påkrævet for, at vi kan gennemføre vores revisioner med den nødvendige kvalitet.

Hvad angår kompetencer på stakeholder-management området samt personlig udvikling, så betragter vi disse som en væsentlig del af den kultur, som vi ønsker at fremme sammen med den øvrige organisation, som vi er en del af. Vi evaluerer løbende disse 'bløde færdigheder' for at vurdere behov for generel uddannelse eller specifikke personlige udviklingsinitiativer.

På baggrund af ovenstående rapporterer vi årligt til Revisionsudvalget og til Bestyrelsen om, hvorvidt vi er trygge ved den aktuelle situation, eller om der er behov for at gennemføre initiativer for at nå det niveau af kompetencer, som vi mener er både nødvendigt og tilstrækkeligt. Alt sammen med det formål at kunne bekræfte over for vores primære interessenter, at vi har tilstrækkelige kompetencer på tværs af vores revisionsteam – eller har en plan for, hvordan vi får dem – således at vi er i stand til at levere som lovet i revisionsplanen.

Findes de kompetencer, som vi har brug for i Intern Revision i Danmark?

Det korte svar er 'ja'.

Men hvad karakteriserer egentlig en 'intern revisor'? Hvilke kompetencer skal vi sikre os, at vi har i teamet, eller alternativt har adgang til via en co-sourcing aftale, for at kunne revidere alle relevante risici, f.eks. de risici som er relateret til IT-infrastruktur, cyber-sikkerhed, finansiel kriminalitet, modeller, kredit, likviditet, kapital, regnskabsaflæggelse – for blot at nævne nogle områder.

En intern revisor besidder en eller flere spidskompetencer. Samtidig er den interne revisor kontinuerligt interesseret i at erhverve sig ny viden på andre områder, som er nødvendig for at kunne gennemføre en revision, eller at samarbejde med andre i teamet, som har den nødvendige indsigt. Og så vi hjælper med en plan for, hvorledes en evt. manglende teknisk eller 'blød' disciplin kan tilegnes.

Når det så er sagt, så er der ingen tvivl om, at mens medarbejdere, som allerede arbejder i en Intern Revisionsfunktion i Danmark naturligt ved hvad jobbet som intern revisor indebærer, så er det langt fra lige så lysende klart for medarbejdere eller potentielle medarbejdere, som ikke arbejder direkte eller indirekte med intern revision.

Bevæger vi os ind på universiteterne og ser vi bort fra de cand.merc.aud. studerende, så vil der formentlig være relativt få studerende, som har en idé om, hvad det vil sige at arbejde som intern revisor. Det på trods af, at der er en lang række uddannelser, som er et oplagt grundlag for et efterfølgende arbejde i en Intern Revisionsfunktion.

For at få adgang til disse kompetencer, kræver det, at vi aktivt også opsøger mulige kandidater på sådanne uddannelsesretninger. Brug af diverse netværk kan være en hjælp til at komme i kontakt med relevante kandidater – enten direkte efter endt uddannelse eller efter erfaring fra andet job.

Så ja, de kompetencer, som vi har brug for, findes – også i Danmark.

Udfordringen er, at vi i foreningsregi (IIA) og selvfølgelig også i regi af hver enkelt Intern Revisionsfunktion har behov for at kommunikere mere og bedre om de muligheder, der er for at arbejde i Intern Revision, også på nye og måske hidtil uvante 'markeder' for os. Og vi må ikke glemme, at vi er i konkurrence med både første og anden linje, som efterspørger nogle af de samme kompetencer.

Her skal vi gøre det bedre kommunikationsmæssigt, for vi har meget at byde på i Intern Revision.

Hvorfor er det attraktivt at arbejde i Intern Revision?

Intern revisors indsigt er værdifuld for ledelsen

Som intern revisor reviderer man end-to-end processer. Det giver en unik mulighed for, at den enkelte interne revisor kan få indsigt i og forstå det samlede proceslandskab på organisationens væsentlige områder.

Dette giver mulighed for at drøfte problemstillinger på højeste niveau i organisationen med henblik på at der findes løsninger, som bringer organisationen i en bedre situation set fra et risikoperspektiv.

Dette bidrager også til indsigt hos den enkelte revisor og til revisionsteamet – en indsigt, som efterspørges af organisationen og af ledelsen, og som Intern Revision dermed kontinuerligt kan bidrage med.

Intern Revision = 'en hjælper'

I vores funktionsbeskrivelse, som er godkendt af bestyrelsen, fremgår det, at vores primære rolle er at hjælpe bestyrelsen og direktionen med at beskytte koncernens aktiver, omdømme og levedygtighed. Dette er dermed kort fortalt vores formål.

Det er ligeledes beskrevet, at Intern Revision er en uafhængig og objektiv 'assurance aktivitet', som implicit indebærer, at der skabes værdi for koncernen. Samtidig fremgår det, at vores scope er ubegrænset indenfor koncernens forretningsområder.

Ved den metode, som Intern Revision hos os og andre steder anvender til at tilrettelægge og gennemføre arbejdet, hjælper vi med at sætte lys på netop de områder, hvor organisationens risikostyring, kontroller og governance-processer kan styrkes.

Og netop på den måde hjælper vi både bestyrelsen og direktionen.

Karrierevej

Med den størrelse som den Intern Revisionsfunktion har i Danske Bank, giver det os mulighed for at tilrettelægge en egentlig karrierevej internt.

Men en karrierevej kan også meget vel omfatte den øvrige del af organisationen, hvor de kompetencer, som intern revisor har tilegnet sig, kan tages i anvendelse i enten første eller anden linje samtidig med, at den enkelte tilegner sig nye færdigheder 'på den anden side af bordet'.

Work-life balance

Vi har i stort omfang muligheden for at tilrettelægge vores revisionsarbejde, således at vi får en så jævn belastning som muligt hen over året.

Det betyder ikke, at der ikke er teams eller medlemmer af teams, som oplever spidsbelastninger, men vi har gode muligheder for at imødegå de største udfordringer ved at have en god planlægning.

Dermed får vi også de bedste forudsætninger for at have en god 'work-life balance', hvilket er nogen af de værdier vi har bygget vores organisation op omkring.

Hvor rekrutterer vi fra?

Vi rekrutterer primært fra (i ikke prioriteret rækkefølge) første eller anden linje i koncernen, universiteterne, ekstern revision, andre interne revisionsfunktioner og fra andre finansielle institutters risk og compliance funktioner.

Vores rekrutteringsstrategi er med andre ord 'bred'.

Som nævnt tidligere i denne artikel, så kan interne revisorer have meget forskellig baggrund. Med det udgangspunkt, hjælper vi efter omstændighederne med en plan for, hvorledes en evt. manglende teknisk eller 'blød' disciplin kan tilegnes.

Nogle gange kan der være behov for træning i at kunne revidere. I andre tilfælde vil der være behov for træning i forståelse af de risici, som kendetegner finansiel sektor – altså forretningsmæssig forståelse – samt forståelse af de produkter, som udbydes.

Konklusion

Tilbage til spørgsmålet:

Mangler der i Danmark interne revisorer med de nødvendige kompetencer, som sikrer, at de Interne Revisionsfunktioner fortsætter med at være i en position, hvor funktionen bliver anset for at være dels værdiskabende for organisationen og dels hjælper med at sikre at vi sætter forkus på de områder, hvor kultur og mindset ikke er som forventet?

Min vurdering er, at der ikke mangler interne revisorer i Danmark.
Men – og der er et men – en intern revisor er ikke altid en 'plug and play' person. Ofte vil der være behov for træning, før vi kan konkludere, at de samlede nødvendige og tilstrækkelige kompetencer er til stede i revisionsteamet.

Samtidig mener jeg, at vi har alle muligheder for fortsat at kunne rekruttere nye medarbejdere, hvis vi tænker bredt i kompetencer og tænker bredt i måden at rekruttere på, samt på fra hvilke kanaler vi rekrutterer. Vi skal dog sikre, at vi har et setup, som er konkurrencedygtigt i forhold til alternative jobs i første og anden linje.

Vi kan rekruttere bredt. Og det skal vi turde at gøre.

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

Cybertruslen mod Finanssektoren – En ekspertvurdering

Morten Tandle, Leder af Nordic Financial CERT

Interviewet af Kim Nehls, Intern revisor, DSB
Ifølge Center for Cybersikerhed (CFCS) har Ruslands invasion af Ukraine d. 24. februar 2022 forandret det sikkerhedspolitiske landskab, og øget usikkerheden på en lang række områder. Truslen mod kritisk infrastruktur, herunder energiforsyning og transport, er blandt andet stærkt forøget, hvilket senest blev tydeliggjort med den formodede sabotage mod gasledningen Nord Stream 2 og tyske jernbanekabler, som lammede den nordtyske togdrift i flere timer i oktober.

Usikkerheden har også hurtigt spredt sig til cyberområdet, hvor det frygtes at Rusland, som modsvar på Vestens sanktioner, vil iværksætte mere avancerede og omfattende cyberangreb. For den danske finanssektor betyder det, at cybersikkerheden om muligt skal tillægges endnu højere bevågenhed. Konkret anfører Center for Cybersikkerhed i deres seneste trusselsvurdering, at truslen fra cyberkriminalitet mod den danske finanssektor er meget høj.

Dette trusselbillede stiller høje krav til den danske finanssektor. For hvordan navigerer og prioriterer man bedst muligt i et risikounivers, hvor cybertruslen er overhængende, men samtidig er diffus? Hvilke konkrete typer cyberangreb udgør den største trussel? Og hvordan kan vi forvente at cybertruslen udvikler sig fremadrettet?

Som leder af Nordic Financial CERT har Morten Tandle en bedre udkigspost end de fleste til at levere kvalificerede svar på disse spørgsmål. Nordic Financial CERT overvåger cybertruslen for en række nordiske finansielle institutioner. Virksomheden er funderet i en mission om, at samarbejde og vidensdeling på tværs af den finansielle sektor, er essentielt for den fælles styrkelse af IT-sikkerheden og bekæmpelse af cyberangreb. Vi har derfor sat Morten stævne for at indhente hans bud på det aktuelle og fremadrettede trusselsbillede på cyberområdet.

Nordic Financial CERT

Indledningsvist bad vi Morten uddybe hvilke opgaver, som varetages i regi af dette nordiske samarbejde i finanssektoren.

"Nordic Financial CERT er et 'pan-Nordic cyber defense information sharing hub and community'. Herigennem får vores medlemmer tilgang til de andre medlemmer igennem samarbejdsgrupper samt til eksterne partnere og myndigheder såsom CFCS og politiet. Medlemmerne er primært virksomheder, som har licens fra Finanstilsynet i et af de nordiske landene. Det omfatter særligt de virksomheder, som udgør kritisk finansiel infrastruktur, f.eks. FSOR-medlemmerne i Danmark (Finansiel Sektorforum for Operationel Robusthed). De fleste af vores medlemmer er banker, forsikringsselskaber, pensionsselskaber, værdipapircentraler eller centralbanker."

Medlemmer af NFCERT fremgår af **Figur 1** på næste side.

Morten Tandle fortællere endvidere, at Nordic Financial CERT's leverer en lang række ydelser, men at hovedaktiviteten varetages af 4 faggrupper/Erfagrupper indenfor:

- Cyber Threat Intelligence
- Incident Response (Cyber Defense) Teams
- Anti-Fraud Teams
- Strategic Cyber Group

Med afsæt i disse operative gruppers arbejde dannes der et løbende situationsbillede af den aktuelle cybertrussel. Relevant viden deles og udveksles bl.a. med CFCS og DCIS'erne (decentral enhed for cyber- og informationssikkerhed for finanssektoren), og disse informationer tilgår tillige Nordic Financial CERT's medlemmer.

Derudover råder virksomheden over et team, som leverer support og rådgivning til medlemmerne 24/7 i forbindelse med eksempelvis hændelseshåndtering. Endelig udarbejder Nordic Financial CERT en årlig trusselsvurdering, som supplerer CFCS's trusselsrapport med en større detaljeringsgrad.

Det aktuelle trusselsbillede

Hvad er egentlig den største cybertrussel, som virksomhederne aktuelt står overfor? Og hvad kan der gøres for at modstå disse trusler?

Lederen af Nordic Financial CERT indleder med at fortælle, at hans virksomheds trusselsvurdering på et overordnet niveau følger CFCS's trusselsvurdering.
Mere konkret fremhæver han cyberkriminalitet, i form af ransomeware angreb, som en af de største aktuelle cybertrusler. Denne type angreb kan således få betydelige konsekvenser for en virksomhed, hvis den ikke afværges. Ransomware er en malware, som IT-kriminelle anvender til at krypterer filer og derved forhindre brugeren i at få adgang til indholdet. Adgang kan ofte først genoprettes ved at betale en løsesum til de IT-kriminelle (kilde: Det Kriminalpræventive Råd). Store virksomheder som Mærsk, ISS og Demant har bl.a. været udsat for denne type angreb med betydelige økonomiske tab til følge.

Han tilføjer dog, at han ikke er bekymret for finanssektoren, hvor cybertruslen generelt tages yderst alvorligt. Dette afspejles bl.a. i de økonomiske og ressourcemæssi-

ge prioriteringer og investeringer, som foretages i branchen.
"Sektoren er godt forberedt på cyberangreb. Men det betyder ikke at man kan hvile på laurbærrene. Truslen ændrer sig konstant og vores medlemmer investerer derfor kontinuerligt i forbedringer af IT-sikkerheden".

Nordic Financial CERT overvåger desuden udviklingen i omfanget og karakteren af cyberangreb på den finansielle sektor. Morten Tandle påpeger i den forbindelse, at angrebene på sektoren typisk kommer i bølger og varierer over tid, men angrebene har vist en nedadgående tendens de sidste måneder. Konsekvenserne af cyberangrebene har desuden været minimal, idet sektoren som tidligere omtalt er godt sikret.
"Mange af angrebene stoppes tidligt og opdages hurtigt, og berørte systemer kan derfor fortsætte eller hurtigt bringes tilbage til normal drift".

På spørgsmålet om der efter hans vurdering bør prioriteres anderledes eller mere for at imødekomme de aktuelle cybertrusler mod den danske finanssektor svarer han:
"I finanssektoren mener jeg at der foretages gode prioriteringer og at indsatsen er på det rigtige niveau. Det gøres en stor indsats, og de fleste virksomheder investerer tungt i cybersikkerhedstiltag, også i 2022 og 2023.".

Han understreger igen, at selvom finanssektoren efter hans vurdering er godt forberedt på cyberangreb, og kontinuerligt investerer i forbedret cybersikkerhed, så er det essentielt at dette fokus fastholdes. Trusselsbilledet forandrer sig hele tiden og fordrer konstant bevågenhed fra finanssektorens side. En indsats som Nordic Financial CERT bidrager til ved deling af erfaring og læring mellem organisationens medlemmer fra konkrete cyberangreb samt håndteringen heraf.

Krigen i Ukraine

Morten Tandle er enig i Center For Cybersikkerheds trusselsvurdering om at krigen i Ukraine har ændret trusselsbilledet for den finansielle sektor, og at branchen derfor fortsat bør prioritere foranstaltninger, som kan modstå de aktuelle cybertrusler.
"Jeg tænker at sandsynligheden eller risikoen for at en fremmed stat vil udføre cyberangreb mod den finansielle infrastruktur er ændret. Selvom den aktuelle trussel fortsat er lav, så kan det hurtigt ændre sig. Det er noget som den finansielle sektor også har taget højde for i sine risikovurderinger", siger han.

Krigen har således ikke afstedkommet væsentlige ændringer i finanssektorens cyberberedskab, men Morten Tandle oplever dog at noget har forandret sig.
"Jeg oplever at sektoren agerer lidt anderledes. Mange har opprioriteret deres sikkerhedsarbejde og måske gennemført systemforbedringer eller udfaset gamle systemer hurtigere end planlagt for at være bedst muligt forberedt, da truslen hurtigt kan ændre sig".

Det fremtidige trusselsbillede

Til trods for at finanssektoren ifølge Morten Tandle står godt rustet til at modstå cybertruslerne er det ikke uden

Figur 1. Medlemmer af NFCERT

bekymring, at han ser ind i fremtiden i et bredere perspektiv.

Det overordnede trusselsbillede for cyber kriminaliteten vurderer han dog ikke står over for en forbedring i den nærmeste fremtid. Det til trods for de mange penge og ressourcer, som virksomhederne investerer i cybersikkerhed.
"Jeg er lidt nervøs. Jeg bryder mig ikke om at cyber crime sektoren er blevet så stor og ressourcestærk. De tjener for mange penge, som de kan reinvestere i kapacitet til at gennemføre endnu flere cyberangreb".

Ifølge Morten tyder alt på at cyber kriminalitet et vilkår, som vi er nødt at acceptere i fremtiden.
"Ja, den trussel og risiko tror jeg vi skal leve med nu og i fremtiden. På samme måde som vi skal leve med kriminalitet i den fysiske verden.

Morten Tandle understreger dog, at det er muligt at påvirke denne trussel og reducerer risikoen, men at det forudsætter tiltag på flere områder.
"De forskellige brancher kan producere og sælge mere sikre produkter by default. Myndighederne kan regulere disse områder bedre og derved bidrage til den udvikling. Politiet kan bidrage mere til at gøre det mere risikabelt og mindre lønsomt at begå cyberkriminalitet. I dag tager det internationale samarbejde i internationale cyber crime sager meget lang tid. Endelig kan virksomhederne generelt tage bedre ansvar for sine egne systemer og data og dermed for egen cybersikkerhed, så risikoen bliver nedsat til et acceptabelt niveau".

Han peger konkret på en række tiltag, som alle virksomheder generelt bør prioritere for at styrke cyber sikkerheden:
"Arbejd struktureret med digitale systemer og risikovurderinger. Tag en risikobaseret approach baseret på anerkendte metoder og standarder, f.eks. ISO eller NIST Cyber Security Framework. Denne tilgang giver en god kobling mellem forretningens konkrete anvendelse af digitale tjenester og den cyber-risiko, som følger med. Det bidrager også til at skabe et risikoejerskab i forretningen.

Lederen for Nordic Financial CERT anerkender, at det er kompliceret at navigere i et landskab med cybertrusler under konstant forandring, hvorfor han også afslutter interviewet med en opfordring.
"For at komme i gang og videre – søg professionel hjælp hos nogen, som har erfaring med cybersikkerhed, og har prøvet at arbejde med det før. Så lærer man hurtigere hvordan man skal prioritere og håndtere cybertrusler, og har dermed større chance for at komme ind på et godt spor."

Chromebooks-sagen i Helsingør kommune - ændringer i revision af GDPR compliance ved brug af cloud

Birgitte Toxværd, advokat og partner, Horten Advokatpartnerselskab

Det var et gevaldigt wake-up call for alle, da Datatilsynet i juli måned nedlagde et forbud mod brug af Chromebooks i Helsingør Kommune. Sagen berører en del juridiske elementer inden for databeskyttelsesret og sætter barren højt for, hvornår revisorer må give grønt lys til brug af cloud. Der opfordres til et større samarbejde mellem revisorer og juridiske rådgivere på dette område.

I denne artikel tager jeg udgangspunkt i intern revisions metode til at gå til en opgave og giver nogle forslag til, hvornår revisorer bør være særligt opmærksomme på at få de juridiske kompetencer i spil for at vurdere, om en revision skal gå igennem med eller uden anmærkninger.

Compliance med GDPR er jo bredt, og det kommer an på hvilken standard, revisoren skal arbejde op imod, og hvilke kriterier der skal opfyldes. I denne artikel holdes det generisk, og gennemgangen angår forhold, der er specifikke efter GDPR ved brug af cloud-systemer et eller andet sted i kæden af behandlinger for en given behandlingsaktivitet. De specifikke krav vil også afhænge af, om organisationen har rollen som dataansvarlig eller databehandler.

1. Kriteriet

Der er en lang række regler i GDPR, der skal efterleves ved brug af cloud.

Datatilsynet har udgivet flere vejledninger om emnet, herunder vejledningen om cloud, vejledningen om tilsyn med databehandlere og vejledningen om risikovurderinger.

I Datatilsynets sag om Chromebooks var der særligt fokus på nedenstående punkter, som vi uddyber nogle af efterfølgende:

- Artikel 5 om grundlæggende principper og dokumentation
- Artikel 6 om hjemmel til behandling og til videregivelse til cloudleverandøren
- Artikel 24 om ansvarlighed
- Artikel 28 om databehandleraftaler
- Artikel 32 om risikovurderinger
- Artikel 33 om sikkerhedsbrud og anmeldelse heraf til Datatilsynet
- Artikel 34 om information om sikkerhedsbrud til de registrerede
- Artikel 35 om konsekvensanalyser
- Artikel 36 om høring af Datatilsynet
- Kapitel 5 om overførsler til tredjelande, herunder brug af standardkontrakter og udarbejdelse af Transfer Impact Assessments.

I Chromebooks-sagen fra Helsingør (og 20 andre kommuner) var det helt grundlæggende problem, at kommunen ikke havde dokumenteret og forholdt sig til den teknologistak, som indgår i de computere, der var blevet udleveret til skolebørnene. Teknologistakken bestod blandt andet af hardware (udstyret), Chrome OS (styresystemet), browser samt cloudapplikationer som den i sagen omhandlede Workspace for Education. Det er i sig selv fire forskellige lag, og mens kommunen er dataansvarlig for nogle lag, og Google er databehandler, var der andre behandlinger, som kun Google var dataansvarlig for. Datatilsynet er p.t. i gang med at gennemgå den indleverede dokumentation med overblik over datastrømme mellem de forskellige stacks og ud til Googles backend, så de kan vurdere rollerne som dataansvarlig, databehandler og evt. fælles dataansvarlig. Det forventes, at Datatilsynet kommer med en afgørelse inden nytår.

Det er nødvendigt at få klarhed over datastrømme og dataansvaret, fordi anvendelsen af de ovenfor citerede bestemmelser i GDPR afhænger af rollerne. Det er en juridisk øvelse at starte med at finde ud af det, ligesom det er en juridisk øvelse at finde ud af, om der er hjemmel efter fx artikel 6 og 9 i GDPR til at videregive oplysninger fra en dataansvarlig til en anden dataansvarlig efter GDPR.

I cloud er der ofte en databehandler og mange underdatabehandlere, da det jo er en del af forretningsmodellen i cloud, at der er kapacitet og service, hvor det er billigst. Det skal sikres, at kravene i den første databehandleraftale følger i "flow-down" til de næste databehandlere i kæden. Det er også en juridisk opgave.

Vurderingen af risiko i relation til sandsynlighed og konsekvenser for de registrerede er en opgave, der kan varetages i fællesskab mellem it-sikkerhedskyndige og dem, der kender forretningen i relation til risikovurderinger. Det er vigtigt, at risikovurderingsprocessen er forankret i organisationen, herunder at ledelsen har forholdt sig til, hvilken

risiko der er acceptabel. Risikovurderingerne skal mitigeres ned til lav.

Et af de helt store omdrejningspunkter har været, om der skulle udarbejdes en konsekvensanalyse eller ej i Chromebooks-sagen. Kommunen har holdt på, at risikoen for børnene var lav, og Datatilsynet har holdt fast i, at den iboende risiko for de registrerede var høj, fordi der var tale om både ny teknologi og sårbare personer, herunder børn. Ansatte er også sårbare personer efter de kriterier, som Det Europæiske Databeskyttelsesråd har opsat i retningslinjerne i WP248. Kommunen havde forsøgt at lave en konsekvensanalyse, men Datatilsynet fandt den utilstrækkelig, herunder at risikovurderingen ikke tog stilling til hele teknologistakken. Det er en juridisk vurdering, hvornår der skal laves en konsekvensanalyse, og hvilke elementer der skal med i den, men den skal laves i samarbejde med dem, der kender systemerne og har indsigt i it-sikkerhedskrav.

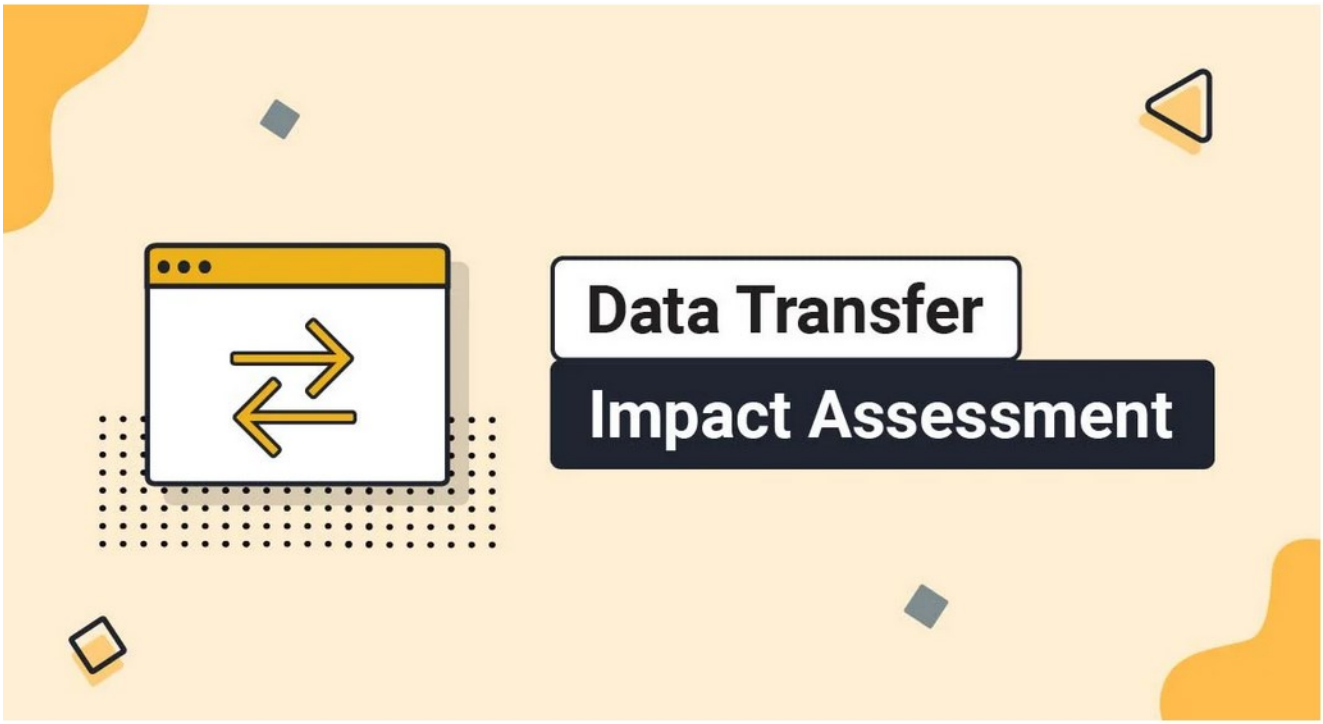
Endelig vil jeg fra Chromebooks-sagen fremhæve overførsler til tredjelande efter kapitel 5 i GDPR. Efter Schrems II-dommen i juli 2020 har det været svært at få overført personoplysninger i "klar tekst" (dvs. almindelig læsbar tekst i modsætning til krypterede eller hashede oplysninger) til USA og andre - i GDPR-henseende - usikre tredjelande. Systematikken er ofte den, at en overførsel til tredjelande skal baseres på EU's standardoverførselskontrakter fra 2021. Det er dog ikke tilstrækkeligt, idet det også skal vurderes, om de modtagende tredjelande i databehandlingskæden opfylder EU's grundlæggende principper for databeskyttelse i relation til myndigheders adgang til personoplysninger og en række andre grundlæggende krav, fx retten til at håndhæve rettigheder ved domstolene. Hvis ikke, skal der implementeres "supplerende foranstaltninger" af teknisk, organisatorisk eller fysisk karakter, der kan imødekomme de identificerede risici. Det Europæiske Databeskyttelsesråd har i Vejledning 01/2020 uddybet mulighederne for supplerende foranstaltninger. Vejledningen har - ligesom Schrems II-dommen - en binær tilgang til problemet. Det identificerede problem skal løses fuldstændigt med foranstaltninger, og kan det ikke løses, skal overførslen ophøre eller suspenderes, indtil en løsning er fundet. Analysen laves i en såkaldt "Transfer Impact Assessment" (TIA).

Nogle har dog – i stedet for en binær tilgang – antaget en risikobaseret tilgang til vurderingen i TIA'en med en beregning af, hvor mange år der ville gå, før en given organisation ville få en henvendelse om udlevering fra udenlandske myndigheder. På baggrund af det, har man så vurderet, at sandsynligheden var så lille, at overførslen kunne tillades. Den metode har Datatilsynet – ikke helt overraskende - vurderet ikke opfylder kapitel 5 i GDPR. Det betyder, at de organisationer, der har brugt sandsynlighedsmetoden, nu skal genbesøge deres TIA'er og på ny tage stilling til tredjelandsoverførslerne.

Der er mange flere nuancer i de juridiske forhold, men ovenfor er medtaget dem, der står klarest i Chromebooks -afgørelsen. Det er dog også særligt relevant at få vurderet, om databehandleraftalen tillader cloudleverandøren at overføre personoplysninger til tredjelande, fx hvis der kommer en henvendelse fra myndighederne i tredjelandet.

2. Tilstand

Når revisorerne skal finde ud af, hvad organisationen har gjort, vil det være nødvendigt at forstå faktum i sagen.



Det vil være relevant at bede om at få udleveret dokumentation for datastrømsanalyser, hjemmelsbetragtninger, dokumentation for overholdelse af artikel 5 og 24, databehandleraftaler, risikovurderinger og konsekvensanalyser samt dokumentation for, hvorfor der eventuelt ikke er udarbejdet konsekvensanalyser.

Det vil også være relevant at bede organisationen udfylde det spørgeskema, som Datatilsynet for nylig har udarbejdet til tilsyn med cloud, indeholdende 47 spørgsmål inden for generelle emner, risikovurdering af servicen, screening og aftalegrundlag med leverandøren, tilsyn med leverandøren og underleverandører, og overførsel til tredjelande.

3. Årsag

Når der skal peges på årsagerne til, hvorfor der er et gap i kriterierne over for de faktiske tilstande, vil det være relevant for revisorerne at forholde sig til, om der er tilstrækkelige menneskelige ressourcer, om de rigtige juridiske kompetencer er ansat, eller om der er afsat ressourcer til rådgivning fra fx eksterne advokater, om det ikke er muligt at finde lovlige alternativer, fx hvis en tjeneste på et vist sikkerhedsniveau alene ydes af leverandører i USA osv. Ofte er compliance med databeskyttelse et område, der ikke afsættes tilstrækkelige ressourcer til, og væsentlig non-compliance inden for databeskyttelse findes i alle størrelser af organisationer.

4. Effekter og konsekvenser

Hvis en organisation ikke overholder databeskyttelsesreglerne, og forholdet ender ved domstolene, evt. på baggrund af en tilsynssag eller en klagesag ved Datatilsynet, vil der være risiko for, at Datatilsynet nedlægger forbud mod fortsat brug af en ulovlig cloud-løsning. Det var måske til at overskue for skolebørnene i Helsingør, men hvis et sådant forbud rammer en organisation med kritisk infrastruktur eller en privat virksomhed, der er afhængig af cloudløsningen for sin indtjening, vil det være meget kritisk for virksomheden.

Manglende overholdelse af databeskyttelsesreglerne skal derfor ses i det lys, at det ultimativt kan være en risiko for den fortsatte virksomhedsdrift, hvis der kommer et forbud eller en bøde, der kan tage livet af en virksomhed. Foreløbig er de danske domstole dog meget lempelige i deres tilgang til bødernes størrelser.

5. Anbefaling

Når revisorer laver anbefalinger til organisationen, vil en væsentlig anbefaling være, at der skal afsættes tilstrækkelige ressourcer til databeskyttelse, og at databeskyttelsesrådgiveren skal involveres i højere grad.

Databeskyttelsesrådgiveren er også nedsat efter GDPR, og det skal ud fra samme systematik som anført ovenfor vurderes, om databeskyttelsesrådgiveren har tilstrækkelige kompetencer, erfaring og ressourcer til at varetage sin rolle forsvarligt samt at databeskyttelsesrådgiveren er tilstrækkelig uafhængig.

Afslutning

Som det fremgår ovenfor, er mange af de krav, som revisorerne skal efterse, rent juridiske krav. Idet revisorer ikke er jurister, kunne det være hensigtsmæssigt, hvis intern revision tager GDPR-juristerne/advokaterne med på sidelinjen i relation til, om en organisation i tilstrækkelig grad overholder databeskyttelsesrettens krav.


IIA årsmøde 2023
31.5.2023-1.6.2023
Sæt allerede nu kryds i kalenderen
HOTEL NYBORG STRAND

Internal audit's key role in addressing digital threats has spurred the need for cybersecurity expertise on the audit team.

Staffing for Success

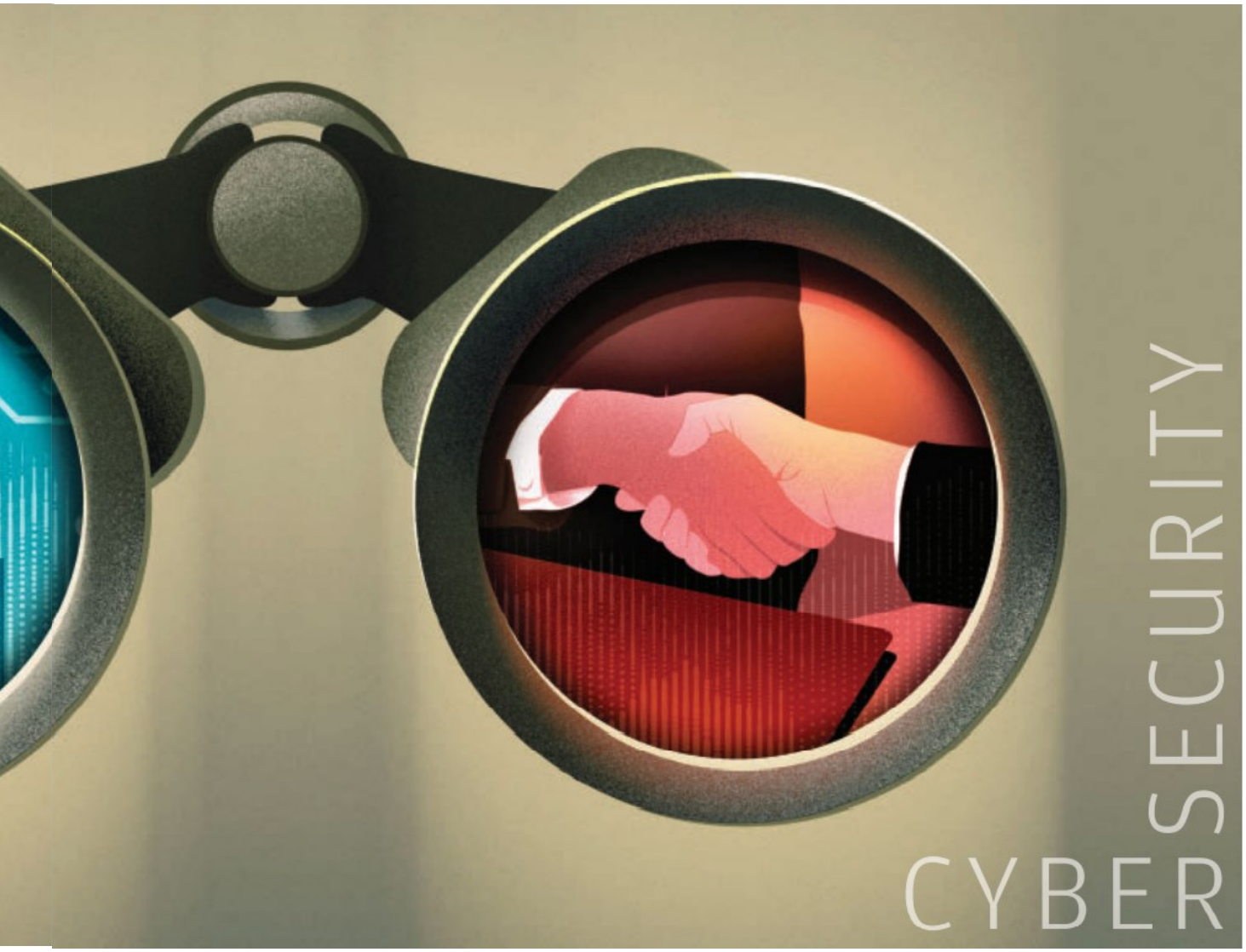
Geoffrey Nordhoff

Illustration by Sean Yates

Organizations are moving gingerly into the post-pandemic world with a heightened focus on cybersecurity, with overall cybersecurity spending projected to grow as much as 10% this year, according to IT research firm Canalys. Regulators—already concerned about cybersecurity—have ratcheted up their oversight, vividly illustrated by the U.S. Office of the Comptroller of the Currency's $80 million fine against Capital One last year (see "Capital One Data Breach" on page 21). In fact, cybersecurity was one of the top-ranked risks identified by board members, management, and chief audit executives (CAEs) in The IIA's OnRisk 2021 report.

In this environment, internal audit, as part of its oversight function, has a critical role of helping organizations manage cyber threats by evaluating risks and providing an independent assessment of controls. In turn, this role has spurred the need for cybersecurity skills in internal audit functions.

The heightened concern around cybersecurity has inevitably increased the demand for suitably experienced auditors, says Jamie Burbidge, founder of Bickham Montgomery, a London-based internal audit recruiting



firm. "Due to cybersecurity being a relatively recent concern for business leaders, the number of internal auditors at the senior level with relevant experience is quite small," he noted. At present, potential internal audit hires who have the experience and a good grasp of cybersecurity likely are coming from the Big Four accounting firms at slightly more junior levels.

Regardless of the talent source, experts point to several skills and qualifications to look for when hiring. They also cite the importance of soft competencies, the need to plan ahead for resource needs, and the advantages of developing skills internally.

THE RIGHT EXPERTISE

Shawna Flanders, director, IT Curriculum Development, at The IIA, says two general skills are important for internal auditors who will be involved in cybersecurity audits: data analysis capabilities and critical thinking. "Deploying critical thinking skills gives auditors the ability to determine how a cyber threat in the wild could impact their organization," Flanders says. Plus, they need to be able to use data to discover unusual activity, inappropriate access, and fraud, and possess a broad understanding of IT general controls as well as application, network, and information security controls, she adds.

In addition, practitioners need to have a deep understanding of relevant threats, such as malware, ransomware or spyware, denials of service, phishing, and password attacks. Given the demands, internal audit functions should consider building dedicated expertise on their team, says Jim Enstrom, senior vice president and CAE at Cboe Global Markets of Chicago. The type of person who can fill this role probably has come up through a technology, cybersecurity, or consulting background, rather than internal audit, he adds.

Ongoing training and an emphasis on more technical cybersecurity-related certifications should also be a

STAFFING FOR SUCCESS

> "You need to be able to communicate, need to be able to persuade, need to be able to partner with the business."
>
> Jamie Burbridge

focus area, Enstrom says. Certifications demonstrate a basic level of aptitude and indicate that a person is motivated for self-improvement and self-learning. The IIA offers several seminars on IT topics, including cybersecurity, as well as more than a dozen IT courses on-demand. In mid-July, The Institute launched its IT General Controls Certificate, demonstrating the certificate holder's ability to assess IT risks and controls.

In addition, more universities are offering advanced degrees in cybersecurity, in which students also are learning the principles of assurance, as well as how to evaluate controls and risk. For example, the University of Central Florida in Orlando, which offers a certificate in cybersecurity, will begin offering a master's degree in cybersecurity and privacy this fall that will include a technical track covering topics such as hardware, software, and security, and an interdisciplinary track that addresses the human aspects of cyberattacks. These types of programs are an opportunity for recruiting, Enstrom says.

Robert Berry, former executive director of internal audit at the University of South Alabama and now president of consulting firm That Audit Guy, says hands-on experience in cybersecurity is important in considering a hire. Berry says he would look for someone experienced in technology, especially with experience in how networks operate and are secured. "You want to look for somebody who is actively engaged and involved in the craft," he adds — the kind of person who builds his or her own network and tinkers with it, and who is active in chat rooms and forums.

TRAINING, SOURCING, AND COLLABORATION

Rather than hiring from outside, developing skills internally is sometimes a better option, especially in small- to moderate-size departments, Berry says. That way, the auditor is already familiar with the organization and with the procedures involved in conducting engagements, he explains. This approach also might be advantageous for a small department in an industry that does not pay well, which likely will have a hard time recruiting cybersecurity expertise, Berry adds.

In a midsize department or a midsize organization with a small audit SECURITY department, audit staff might not have the necessary IT knowledge. Keeping in mind *The IIA's International Standards for the Professional Practice of Internal Auditing*, the organization might consider a cosource provider, Enstrom says, adding that training, skill building, and certifications also are important for these departments. In addition, where the *Standards* allow, internal audit should consider collaboration with the organization's information security department, he says. Standard 1210: Proficiency, and Standard 2050: Coordination and Reliance, provide guidance in these areas.

SEEK OUT SOFT SKILLS

"Curiosity is the cornerstone of internal audit," Berry says. "If you can't be curious and ask really good questions, you will fail in your career in audit." Soft skills are probably the most important skills, he says, because a person who possesses them can be taught audit skills. Critical thinking and other soft skills give internal auditors, especially those dealing in a technical area such as cybersecurity, the ability to communicate outside their area and to under-

In a recent report, recruiting firm Hays US reveals that three in five U.S. cybersecurity professionals and executives polled say they found it difficult to recruit skilled cybersecurity personnel.

CAPITAL ONE DATA BREACH

The U.S. federal government's enforcement actions against Capital One in August 2020, which included an $80 million fine from the Office of the Comptroller of the Currency (OCC), illustrates its increased oversight of cybersecurity issues. The actions stemmed from a 2019 cyberattack that stole the personal information of about 100 million individuals. The OCC fine was the first significant penalty against a bank in connection with a data breach or alleged failure to comply with OCC guidelines. The OCC specifically called out Capitol One's internal audit function, saying it failed to identify numerous control weaknesses and gaps and did not effectively report them to the audit committee.

stand how a cyber threat could affect the organization.

When he started Bickham Montgomery about 10 years ago, Burbidge found that technical proficiency was by far the most sought-after trait for companies when hiring internal auditors. Now, he sees more emphasis on communication skills as part of an internal auditor's role. "You need to be able to communicate, need to be able to persuade, need to be able to partner with the business," he says.

Jeannie Alday, director of Internal Audit for Chatham County, Ga., says in hiring someone with an IT background, she wants to determine whether the candidate will be able to communicate with IT staff, and IT management, but also with county management and others who may have limited background in IT. "Those soft skills are huge, and they're not always easy to spot in the limited interview process," Alday says.

LOOKING AHEAD ON HIRING

Given the rapidly changing environment, cyber awareness is fundamental to the execution of an organization's strategy. "In any organization today, cybersecurity is one of the top risks," Enstrom says. In the present environment, boards, management, and other stakeholders need to focus continually on cyber risk and whether their organization has the right skills and resource strategy, he says. Importantly, organizations need to make necessary investments in skills and resources.

Post-pandemic, hiring likely will become more challenging because of pent-up demand, Enstrom says, and demand already exceeds the number of candidates. As a result, audit hiring managers should think more creatively about compensation and other job benefits. He also notes that many cybersecurity professional have had limited exposure to internal auditing and assurance, may see auditing as having limited opportunity for advancement, and might not consider going into the field.

This perception underscores the necessity of selling the opportunities and value proposition of the profession to prospective job candidates. Compared with going directly into information security, internal audit offers the potential for greater diversity of experience and breadth of opportunity — working with senior executives and board members — and exposure to different projects, Enstrom says. Moreover, because of the importance of good communication skills, time spent in internal audit can be a great learning opportunity for someone who is less comfortable in this area.

"Early in a person's career, working in internal audit really represents a great learning opportunity because you have so many different projects you can work on," Enstrom

"You want to look for somebody who is actively engaged and involved in the craft [of cybersecurity.]"

Robert Berry

"Soft skills are huge, and they're not always easy to spot in the limited interview process."

Jeannie Alday

STAFFING FOR SUCCESS

TO COMMENT on this article, EMAIL the author at geoffreynordhoff@theiia.org

> "In my experience, many students in computer science or other IT disciplines are unaware of job opportunities in the internal audit profession"
>
> Jim Enstrom

says. "I think we don't sell that enough as a profession."

As another area of focus for hiring, Enstrom emphasized the importance of partnering with outside firms, or organizations that can help with the candidate sourcing process. He highlights one example — the Greenwood Project. "The Greenwood Project is a nonprofit organization dedicated to introducing Black and Latinx students to careers within the financial industry," he says. "We've had success working with Greenwood Project and we continue to look for ways to strengthen our relationship and promote the profession of internal auditing to Greenwood students and diversity candidates. In addition to accounting and business students interested in financial services, we have been working with Greenwood to promote an interest in IT audit, data analytics, and cybersecurity roles in the internal audit profession."

Meanwhile, when recruiting through universities, internal audit functions need to look beyond the accounting and finance departments and build relationships with computer science and cybersecurity programs. "In my experience, many students in computer science or other IT disciplines are unaware of job opportunities in the internal audit profession," Enstrom says. "Given this, it's really important for the company and recruiter to understand and have relationships with faculty and staff in these colleges, not just the business schools."

The bottom line? "You have to offer competitive salaries, and you have to be very clear and crisp in your value proposition — how internal audit will benefit them in their career," Enstrom says. Moreover, companies recruiting in the post-COVID-19 marketplace will need to think more broadly and consider hiring candidates from outside their geographic area.

GEOFFREY NORDHOFF *is a content developer and writer, Standards and Professional Knowledge, at The IIA.*

This article was reprinted with permission from the August 2021 issue of Internal Auditor, published by The Institute of Internal Auditors, Inc., www.theiia.org.

Nyt EU-direktiv stiller skærpede krav til cyber- og informationssikkerheden – hvilken betydning har det for din organisation?

Peter Lind Nielsen , Advokat, Bech-Bruun

Nikolaj Strunk, Advokatfuldmægtig, Bech-Bruun

NIS2 (Network and Information Security) -direktivet øger kravene til cybersikkerheden i EU og indeholder bl.a. skærpede krav til ledelsesorganer, krav om effektiv risikostyring og håndtering af sikkerhedshændelser. Overtrædelser er bødebelagt på op til 10 mio. euro eller 2 % af omsætningen

I takt med at flere produkter og tjenester kobles på internettet, bliver organisationer mere sårbare for cyberangreb. Angreb skader både driften og økonomien i virksomheder og myndigheder, ligesom de også grundlæggende truer samfundsordenen, hvis de rammer virksomheder og myndigheder, der udbyder produkter eller ydelser, som er vigtige for at opretholde vores samfund. EU har derfor vedtaget et nyt direktiv om cyber- og informationssikkerhed, som en del af EU's digital strategi.

NIS2-direktivet vil – som navnet antyder – ændre og udvide det nuværende NIS-direktiv, som er det første direktiv om net- og informationssikkerhed. NIS2 har et bredt sigte og skal sikre et højt fælles cybersikkerhedsniveau. Det nuværende NIS-direktivs anvendelsesområde er relativt begrænset, og NIS2 vil omfatte langt flere virksomheder og organisationer, ligesom også offentlige myndigheder omfattes. Samtidig vil NIS2 skærpe kravene væsentlig til de enheder, der er omfattet af anvendelsesområdet.

NIS2 har en ledelsesmæssig forankring, og det medfører bl.a. at organisationers ledelse (i Danmark typisk bestyrelse og direktion) skal godkende risikostyringen og føre løbende tilsyn med implementeringen og sikkerhedsniveauet, ligesom ledelsen er ansvarlig for at sikre, at sikkerhedsniveauet matcher risikovurderingen. Ledelsen skal også løbende modtage træning indenfor cybersikkerhed.

Det er ikke alle organisationer, som er omfattet af NIS2. Det er derfor i første omgang relevant at fastlægge hvilke organisationer, som er omfattet af NIS2, hvorefter kravene til de omfattede organisationer gennemgås. NIS2 er en del af en bredere digital strategi fra EU, hvorfor også anden kommende regulering præsenteres, inden NIS2's implementeringsfase og forberedelsen på NIS2 slutteligt gennemgås.

Er din organisationen omfattet af reglerne?

"Væsentlige" og "vigtige" enheder

Anvendelsesområdet for NIS2 udvides betydeligt ift. det nuværende NIS-direktiv. Flere sektorer vil blive omfattet af reguleringen, hvorfor væsentlig flere organisationer vil blive omfattet. Udgangspunktet for, hvorvidt en organisation er omfattet af NIS2 er, om organisationens forretningsaktivitet hører under oplistningen af "væsentlige" eller "vigtige" enheder i NIS2s bilag 1 og 2. Denne vurdering kan være dybdegående og afhænger af en konkret vurdering, idet et eller flere kriterier skal være opfyldt. Den nærmere fastlæggelse af, hvorvidt en organisation er omfattet af NIS2, kan derfor i visse tilfælde vise sig at være vanskelig. Der vil forventeligt gå en del måneder før den danske lovtekst er kendt, ligesom der forventelig vil gå endnu længere tid før der foreligger egentlige vejledninger.

De omfattede sektorer er oplistet i **Figur 1** på næste side.

Det følger af direktivet, at *"væsentlige og vigtige enheder bør garantere sikkerheden i de net- og informationssystemer, som de anvender i forbindelse med deres aktiviteter"*. Net- og informationssystemer er ikke afgrænset til aktiviteter, som isoleret set bringer en organisationen inden for direktivets anvendelsesområde, men derimod aktiviteter i en bredere forstand, som hører under en omfattet virksomhed, og som har betydning for udøvelse af den aktivitet der er omfattet af direktivet. Direktivet er ligesom GDPR formuleret teknologineutralt, og der er lagt op til en bred fortolkning af net- og informationssystemer. Det betyder, at såvel digitale netværk, digital infrastruktur, it-systemer (applikationer) og hardware, men også såkaldt OT (Operational Technology) i form af enheder, hvor der er embedded/integreret software (som vil kunne hackes eller "angribes"), fx maskiner, robotter, controllere, PLC'ere og styringsenheder, er omfattet.

Meget taler for, at det kun er net- og informationssystemer af betydning for den drift, der gør en organisation til en "væsentlig" eller "vigtig" enhed under direktivet. I

Figur 1 - Sektorer omfattet af NIS2

Væsentlige enheder	Vigtige enheder
Energi – elektricitet, fjernvarme og fjernkøling, olie, gas og brint.	**Post- og kurertjenester**
Transport – Luft, jernbane, vand og vejtransport	**Affaldshåndtering**
Bankvirksomhed – kreditinstitutter mv.	**Kemikalier** - Fremstilling, produktion og distribution
Finansielle markedsinfrastrukturer - Operatører af markedspladser og centrale modparter (CCP)	**Fødevarer** - Fremstilling, bearbejdning og distribution til og med engrosledet
Sundhed – Tjenesteudbydere, laborationer og producenter	**Anden fremstilling** – Bl.a. fremstilling af medicinsk udstyr, computere, elektrisk udstyr, maskiner, motorkøretøjer og andre transportmidler
Drikkevand - Leverandører og distributører	**Digitale udbydere** - Udbydere af onlinemarkedspladser, online søgemaskiner og sociale netværkstjenester
Spildevand - Indsamling, bortskaffelse eller behandling	
Digital infrastruktur – Bl.a. udbydere af internetudvekslingspunkter, DNS-tjenesteudbyder, topdomænenavnregistraturer, udbydere af datacentertjenester, og udbydere af offentlige elektroniske kommunikationsnet	
Forvaltning af IKT-tjenester (B2B) - Udbydere af managed services og af managed sikkerheds-services	
Offentlige forvaltningsenheder – Defineres i henhold til national ret	
Rummet – Infrastruktur og levering af tjenester	

forhold til aktiviteter omfattet af direktivet, vil net- og informationssystemer omfatte alle it-systemer og digitale enheder, herunder anordninger og enheder og deres fysiske omgivelser, der opretholder/understøtter driften af den pågældende aktivitet, eller som er koblet sammen med disse fx på samme netværk, og som kan udgøre en sårbarhed fx i form af en "vej" ind til de centrale systemer.

Som udgangspunkt er det uden betydning, hvorvidt en organisation også udøver anden aktivitet, og hvorvidt den omfattede aktivitet kun udgør en del eller måske endda en mindre del af organisationens samlede aktivitet. For nogle af aktiviteterne gælder dog et krav om, at aktiviteten skal udgøre en vis andel af organisationens samlede aktivitet.

Undtagelser
Selvom en enheds forretningsaktivitet er indenfor én eller flere af de oplistede sektorer i **Figur 1**, vil enheden ikke være omfattet af NIS2, hvis (i) det er en "mikro-" eller "små" virksomhed, eller (ii) der er tale om visse offentlige enheder.

(i) Mikro- og små virksomheder
Undtaget fra NIS2s anvendelsesområde er virksomheder med færre end 50 ansatte og en årlig omsætning eller en årlig balance på under 10 mio. euro. Opgørelsen sker som udgangspunkt på koncernniveau.

Det er dog ikke en absolut grænse, idet visse organisation uanset deres størrelse alligevel altid være omfattet. Det er a) udbydere af offentlige elektroniske kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, af tillidstjenester eller af topdomæne-

navneregistre og domænenavnesystemer (DNS), (b) offentlige forvaltningsenheder, der i øvrigt ikke er undtaget jf. nærmere nedenfor, (c) enheder, der er eneste tjenesteleverandør i en medlemsstat, (d) enheder, hvis levering kan have indvirkning på den offentlige sikkerhed eller folkesundheden ved en potentiel forstyrrelse, herunder grænseoverskridende effekt, (e) enheder, som er kritisk på grund af dens specifikke betydning på regionalt eller nationalt plan, og (f) kritiske enheder i henhold til CER-direktivet.

(ii) Visse offentlige enheder
Nogle offentlige enheder vil ligeledes være undtaget anvendelsesområdet for NIS2. Det omfatter offentlige enheder, der udfører aktiviteter indenfor forsvar, national sikkerhed, offentlig sikkerhed, retshåndhævelse og retsvæsen, idet de typisk vil være underlagt andre lignende regler.

Hvilke krav pålægger NIS2 din organisation?

Effektiv risikostyring
Organisationer skal træffe foranstaltninger til at håndtere cybersikkerhedrisici og udarbejde politikker for risikoanalyse og informationssystemsikkerhed. Det skal ske på baggrund af en konkret, helhedsorienteret risikoanalyse, hvor bl.a. risikoeksponering og sandsynligheden samt konsekvenserne ved et angreb analyseres. Risikostyringen skal være effektiv i forbindelse med erhvervelse, udvikling og vedligeholdelse af net- og informationssystemer, herunder håndtering og offentliggørelse af sårbarheder.

Risikostyringen skal sikre driftskontinuitet og en effektiv krisestyring. Derudover skal risikostyringen løbende overvåges, og konstateres det, at kravene til risikostyring ikke er efterlevet, skal alle nødvendige korrigerende foranstaltninger træffes uden unødig forsinkelse. Informationssikkerhed skal således forblive på dagsordenen.

Håndtering af sikkerhedshændelser
Organisationer skal kunne håndtere en hændelse og dens følger, herunder driftsforstyrrelser, økonomisk tab, skade på/tab af data, skadevirkning over for tredjemand mv.

Samtidig skal organisationen indrapportere enhver hændelse til myndigheder, der har væsentlig indvirkning på leveringen af enhedens tjeneste og "Nær-ved-hændelser", dvs. enhver væsentlig cybertrussel, som kunne have resulteret i en væsentlig hændelse, fx DDOS (Distributed Denial of Service). Det skal understreges, at bevidst uvidenhed er ikke en option.

Indrapporteringen skal ske i flere etaper med (i) en indledende underretning inden 24 timer efter kendskab til hændelsen, (ii) en notifikation om hændelsen inden 72 timer, (iii) løbende statusopdateringer (efter anmodning), og (iv) en endelig, omfattende afrapportering inden for 1 måned. Man skal være opmærksom på, at ukendskab til hændelser i sig selv kan være yderst problematisk.

Organisationen har derudover en underretningspligt over for modtagere af organisationens tjeneste, ligesom myndighederne kan offentliggøre hændelsen, hvis det er i offentlighedens interesse. Man risikerer altså at skulle underrette kunder og andre samarbejdspartnere om sikkerhedsbrud.

Krav om ledelsesmæssig forankring
Ledelsesorganet skal godkende foranstaltningerne til risikostyring, føre tilsyn med foranstaltningernes gennemførelse, og stå til ansvar for manglende overholdelse af kravene. Ledelsesorganet skal regelmæssigt følge kurser for at opnå og vedligeholde sin viden omkring cybersikkerhedsrisici og styringspraksisser samt deres indvirkning på driften.

Hvis ledelsesorganet ikke opfylder kravene, kan ledelsen ifaldes et ansvar, hvis medlemmerne har handlet uagtsomt. Det følger af Selskabslovens § 115, at ledelsen skal *"sikre en forsvarlig organisation"* og etablere *"de fornødne procedurer for risikostyring og interne kontroller"*.

Øvrige krav
NIS2 omfatter også krav til en organisations leverandører og tjenesteydelser. De net- og informationssystemer, som organisationen anvender, skal indebære passende og forholdsmæssige tekniske og organisatoriske foranstaltninger, der (under hensyntagen til det aktuelle stade) sikrer et sikkerhedsniveau, der står i forhold til risikoen.

Manglende overholdelse af kravene til risikostyring og rapportering sanktioneres med maksimumbøder på:

- for "væsentlige" enheder: mindst 10 mio. euro eller op til 2 % af den samlede globale årsomsætning i det foregående regnskabsår, alt efter hvad der er højest
- for "vigtige" enheder: mindst 7 mio. euro eller op til 1,4 % af den samlede globale årsomsætning i det foregående regnskabsår, alt efter hvad der er højest.

Endelig kan virksomheden i sidste ende miste eventuelle tilladelser/autorisationer til at udøve den omfattede aktivitet, ligesom ledelsen kan frakendes retten til at udøve ledelsesbeføjelser i selskabet.

Anden regulering af cybersikkerhed

Cyber- og informationssikkerhed har været sparsomt reguleret i EU og i Danmark. NIS2 er en del af en bred digital strategi, hvor EU indfører et væsentlig antal nye direktiver og forordninger:

Critical Entities Resilience ("CER") skal mindske kritiske enheders sårbarhed og styrke deres fysiske modstandsdygtighed. De omfattede enheder er de samme enheder, der er omfattet som "væsentlige" i NIS2 jf. **Figur 1**.

Digital Operational Resilience Act ("DORA") indfører en modernisering og harmonisering af sikkerhedskravene og IT-tilsynet i den finansielle sektor.

Cyber Resilience Act ("CRA") implementerer obligatoriske cybersikkerhedskrav for produkter med digitale elementer (navnlig IoT produkter). Forslaget er fremsat af Kommissionen den 15. september 2022.

Derudover stiller EU Cybersecurity Act, Cybersecurity forordningen og Information Security forordningen visse krav til EU-institutioner.

Slutteligt vil bl.a. markedsføringsloven, lov om forretningshemmeligheder, databeskyttelseslovgivningen og sektorspecifik lovgivning være et led i den digitale compliance sammen med NIS2.

Implementering og forberedelse

NIS2 er endelig vedtaget og den formelle vedtagelse sker ved underskrift af formændene for EU-Parlamentet og Rådet den 14. december 2022. Direktivet træder i kraft 20 dage herefter, og implementeringsfristen for medlemsstaterne er 21 måneder efter ikrafttræden. Direktivet skal således senest være implementeret i dansk ret primo oktober 2024. Det vides endnu ikke hvordan implementeringen vil finde sted, herunder om den spredes som sektorlovgivning. Der er endvidere tale om et minimumsdirektiv, og ved implementeringen kan Danmark vælge at gå videre, og det kan være at inkludere flere sektorer og organisationer som fx kommunerne.

Organisationer bør dog allerede nu forberede sig på de nye lovkrav. De færreste organisationer vil på nuværende tidspunkt kunne opfylde kravene i NIS2, hvorfor mange virksomheder skal bruge væsentlige ressourcer for at sikre overholdelse af NIS2-kravene. Efter EU's udmelding skal de fleste påregne en forøgelse af IT-budgettet på mellem 15-20%. Er man allerede certificeret efter en af de anerkendte standarder som fx ISO 27001, er man imidlertid allerede godt klædt på, og NIS2 kravene kan måske være anledningen til gennemføre en egentlig certificeringsproces.

Styringen af cyber- og informationssikkerhed, der tidligere i mange organisationer har været ustruktureret og placeret langt fra ledelsesgangene, ændres nu, og ledelsesorganerne skal nu aktiv på banen for at undgå et ledelsesansvar.

NIS 2 - og hvad så nu?

Michael Tønnesen, Security Architect, ATEA

Der stilles krav til organisationer vedrørende effektiviteten af risikostyringen, ledelsens ansvar og (for de fleste) et samlet løft af virksomhedens informationssikkerhed. Men hvordan ved organisationen så, om og i hvor høj grad et løft er påkrævet? Hvad og hvem skal vi sammenligne os med, når vi vurderer, hvor vi bør være, og ved alle overhovedet, hvad begrebet informationssikkerhed dækker over?

Med disse spørgsmål i baghovedet vil jeg starte bagfra med henblik på at danne en kontekst for behovet for en metode vedrørende praktisk anvendelse af rammeværk for informationssikkerhed.

Facitliste

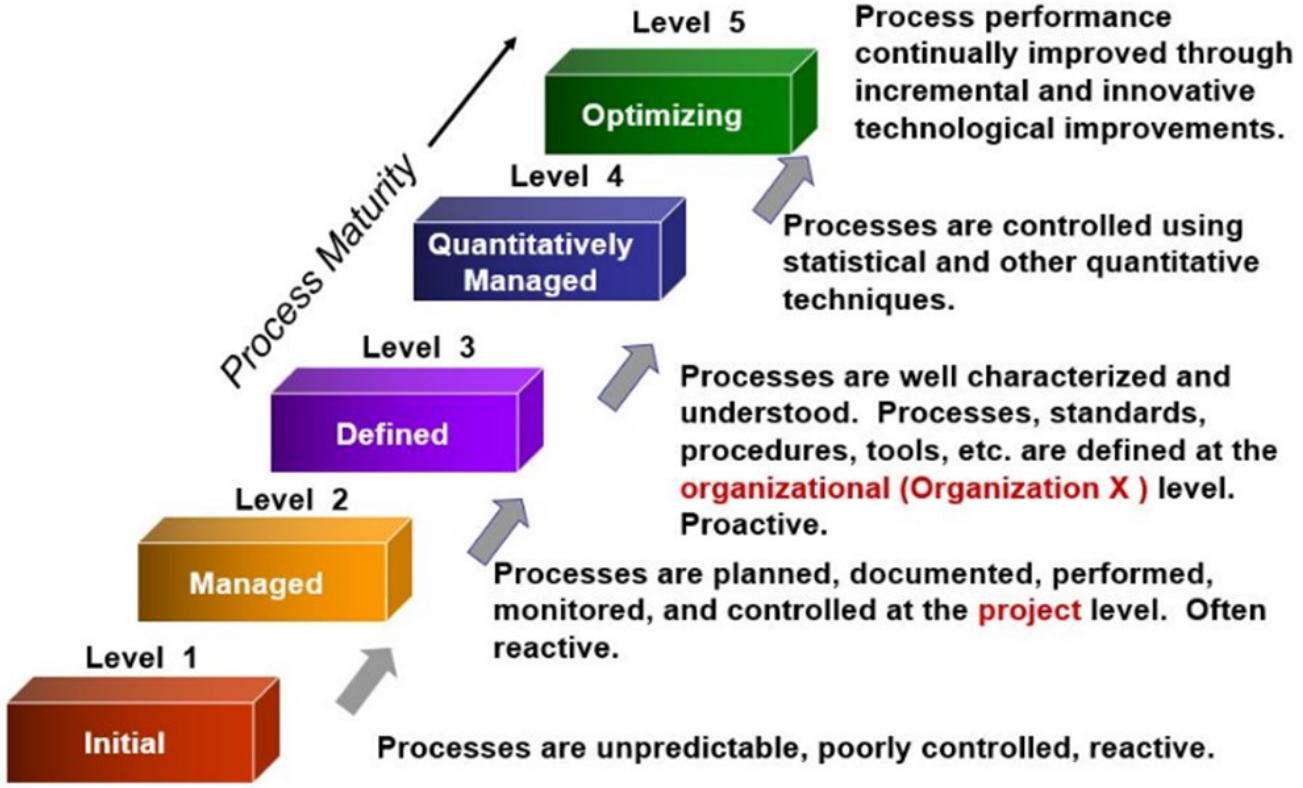
Forståelsen for informationssikkerhed bør udspringe af en fælles facitliste. Begreberne for kommunikation, inddeling af kapabilitet og organisatoriske interesser bør kunne forstås af alle parter med udgangspunkt i deres egen virksomhed. En anbefaling hertil og en personlig favorit er *Capability Maturity Model* (CMM), som er udviklet af Carnegie Mellon University.

Som figuren nederst på siden viser, definerer denne model nogle klare modenhedsniveauer for informationssikkerhed og dermed progressionsmuligheder – medmindre man har en score på 5, hvilket meget få virksomheder på verdensplan har.

Nu kommer vi så til næste spørgsmål, som er, hvad begrebet *Informationssikkerhed* præcist dækker over.

De fleste rammeværk er enige i, at en gylden standard for informationssikkerhed tager udgangspunkt i triaden CIA - og her menes ikke det amerikanske agentur men derimod begreberne Confidentiality, Integrity og Availablity.

Det er en almindelig opfattelse, at informationssikkerhed er identisk med IT-sikkerhed og primært handler om beskyttelse af teknologi – det vil sige hardware og software. Teknologi er naturligvis en stor del af IT-sikkerheden, men fokus på teknologien alene er ikke nok at beskytte virksomheden mod sikkerhedstrusler. Center for Cybersikkerhed (CFCS) har i juli og august 2018 udgivet trus-



selsvurderinger for hhv. sundhedssektoren og finanssektoren, og i begge udgivelser er det tydeligt, at den menneskelige faktor er af væsentlig betydning for at sikre virksomhedens aktiver.

Implementering af sikkerhedsforanstaltninger omfatter således både fokus på mennesker, teknologi og processer. Disse foranstaltninger skal designes til at reducere risikoen for virksomheden, dens ansatte og kunder mod sikkerhedshændelser. Effektiv IT-sikkerhed reducerer risikoen for en sikkerhedshændelse gennem bevidst eller ubevidst udnyttelse af systemer, netværk og teknologier.
Effektive og robuste sikkerhedsværn kræver et informationssikkerhedsstyringssystem (ISMS), og bygger således på tre førnævnte elementer: mennesker, teknologi og processer. For selv hvis teknologien er på plads, kan der skabes sårbarhed, såfremt der ikke er defineret fuldstændige og samstemmende processer, og medarbejderne dertil ikke er uddannede i, hvordan man beskytter virksomhedens informationer, og hvilke teknologier der skal anvendes.

Teknologi
Teknologien er naturligvis afgørende for IT-sikkerheden. Ved at identificere de risici, som virksomheden står over for, kan man begynde at se på, hvilke kontroller og værn der skal etableres – og med hvilke teknologier dette skal gøres med. Teknologier implementeres for at forhindre eller reducere virkningerne af sikkerhedstrusler med udgangspunkt i virksomhedens risikobillede og risikoappetit.

Processer
Processer er nøglen til implementeringen af en effektiv sikkerhedsstrategi. De er med til at definere, hvordan virksomhedens organisatoriske roller, aktiviteter og dokumentationen heraf bruges til at reagere på risici. Processer skal desuden løbende revurderes. Risikobilledet ændrer sig hurtigt, og processer skal tilpasses, så snart risikobilledes forandres. Men processer er ligegyldige, hvis de ikke følges. Derfor ligger der et løbende arbejde i at evaluere på, om processerne hindres, fordi de ikke er intuitive eller på anden måde ikke passer ind i de daglige arbejdsgange.

Understøttelse af processer omfatter både organisatoriske tiltag, beskrivende governance (sikkerhedsstrategier og politikker, retningslinjer mv.) samt implementering af kontroller til evaluering og justering af sikkerhedsniveauer. Dette inkluderer overvejelser om, hvordan forhold for livscyklus er (leverandørstyring, service level agreements osv.), og hvem der har ansvaret for risici og de økonomiske konsekvenser forbundet hermed. Det er vigtigt, at data både kontrolleres i dette parameter samt i teknologiparameteret.

Mennesker
Alle medarbejdere og samarbejdspartnere i virksomheden spiller en rolle i at forebygge og reducere sikkerhedstrusler. Det omfatter alle aspekter af det daglige arbejde, men kan eksempelvis være i forbindelse med behandlingen af følsomme informationer, forståelse for hvordan man identificerer og undgår phishing e-mails, eller hvordan man skaber en sikker adfærd ved brug af mobile enheder. Trusler mod virksomhedens informationer er et forretningsanliggende, og alle – fra direktionen og medarbejdere til eksterne samarbejdspartnere – har et ansvar for at beskytte dem bedst muligt. Et effektivt og velovervejet bevidsthedsprogram, der er målrettet risikobilledet for både organisationen og de individuelle medarbejdere, vil bidrage til at reducere risikoen for sikkerhedstrusler. Ressourcestyring og vidensniveau er her to vigtige elementer, der ofte overses – og det samme gælder kulturen i virksomheden. Sidst men ikke mindst er der mange psykologiske og menneskelige adfærdsmønstre, der bør omfattes i overvejelserne, men især sikring af klar og tydelig kommunikation mellem *afsender* og *modtager* er vigtigt at forholde sig til.

Desuden skal de medarbejdere, som håndterer IT-sikkerheden være fuldt opdaterede med de nyeste færdigheder og kvalifikationer for at sikre, at passende kontroller, teknologier og praksis gennemføres og evalueres løbende for at bekæmpe de nyeste sikkerhedstrusler. Medarbejdere, som ikke holder sig opdaterede, kan påvirke virksomhedens evne til at opdage, mitigere og reagere på sikkerhedstrusler.

De tre ovenfornævnte parametre er grundlæggende dem, som organisationer består af set ud fra informationsbehandlingsperspektivet.

Uden at dykke meget granulært ned i de fem modenhedsniveauer, har vi nu etableret både en målestok for vores nuværende og ønskede niveau, hvilke vigtige elementer der er i cybersikkerhed, samt at det er vigtigt, vi kan afsende et budskab i korrekt kontekst til den, der skal modtage det. Eksempelvis er en af forskellene mellem niveau 2 og niveau 3, at man har forankret sine processer tværorganisatorisk, og at der er ensartet udbytte af en given opgave. Dette kunne eksempelvis være, at to servere, som er installeret af to forskellige personer i to forskellige kundeprojekter, har ensartet minimumssikring.

Modenhedsniveau

Reelt set kan vi danne en c*ompany score 1-5* qua *CMM*, som ofte vil lægge op til en anbefaling på at øge indsatsen på et givent område. Det er her vigtigt, at man ofte vil have en bidragende negativ effekt på de andre områder, hvis ens arbejdsmetode er uden procesunderstøttelse, målbarhed eller er personafhængig.

Når man har en lavere score end ønsket, skal man udrede, hvilke trin der skal til for at løfte sikkerheden. Typisk anbefaler jeg, at man støtter sig til at rammeværk, der enten er branche- eller organisationsspecifik.
Eksempler på sådanne rammeværk kan være:

- Payment Card Industry Data Security Standard (PCI-DSS)
  En informationssikkerhedsstandard for organisationer, der håndterer kreditkort.
- ISO62443
  For produktionsvirksomheder, da denne standard er

målrettet organisationer, der bør anvende cybersikkerhed for operationel teknologi i automations- og kontrolsystemer (SCADA).

- National Institute of Standards and Technology (NIST) / CIS Critical Security Controls (CIS Controls)
  Rammeværk for mere generelle organisationer.
- ISO/IEC 27001
  International standard for hvordan man administrerer informationssikkerhed.

Ovenstående rammeværk giver enten generelle eller meget specifikke anbefalinger til kontroller, der kan implementeres med henblik på at sænke risici. Dette kan eksempelvis vær foranstaltninger såsom firewall, acceptable use policy, fysiske døre, leverandørkrav mv.

Flere af disse kontroller kan man desuden blive certificeret i, og der er forskellige metoder til at teste effektiviteten af dem, herunder ved interview, test af risikoscenarier, penetrationstest mv.

Fælles for dem alle er, at man ud fra anbefalet kontrol og ens score på kontrollen kan italesætte og vurdere om risikovilligheden og det nuværende niveau af modenhed i organisationen matcher. Hvis de ikke matcher, så bør man opruste og understøtte forretningen, som det ønskes.

Dette sidste udsagn er meget vigtig at forstå. Man har som individuel afdeling typisk ikke ansvaret for at sætte rammerne for ens egen risikostyring. Det bør være et mandat, der er givet fra en højere instans i virksomheden; typisk ejere, bestyrelse, CEO e.l. Det er dog ens pligt som afdeling at implementere, efterleve og rapportere opnåelsen af de mål, der er blevet sat i opgaven – eller at påpege, at det ikke er muligt under de nuværende forudsætninger. De særegne egenskaber og ansvar for risiko-ejer, kontrol-ejer og diverse andre roller vil blive for uddybende at dykke ned i i nærværende artikel, men sikring af ejerskab på en risiko er en primær egenskab i risikostyring.

Hvad så med NIS2

NIS2 er krav uden en facitliste. Det vil sige, at der ikke følger kontroller med til direktivet, men at dette blot er krav til efterlevelse af visse bundne opgaver. Dog matcher disse krav kontroller og intentioner fra de tidligere nævnte rammeværk og branchestandarder. Hvis vi kigger på de omfattede virksomheder, er der en stor del, der i lang tid har arbejdet med disse, og der vil også være en væsentlig mængde, der ikke vil være tilfredsstillende beskyttet. Så det er min klare anbefaling, at man undersøger, hvilke krav der stilles af NIS2, samt hvor godt man er dækket ud fra ens nuværende niveau. Herudfra defineres gaps, og opgaver til lukning af disse gaps kan opstilles i prioriteret rækkefælge med det formål at bliver bedre beskyttet.

I NIS2 er det estimeret fra The European Union Agency for Cyber Security (ENISA), at virksomheder bør regne med at afsætte ca. 22% mere i deres cybersikkerhedsbudget. Dette er *desværre* kun for virksomheder, der i forvejen har en relativ moden tilgang, og som nævnt tidligere i artiklen, vil der være nogle organisationer, der absolut kommer til at skulle investere både meget og langsigtet, for at komme så meget i kontrol, at de kan bevise, at de er godt nok på vej.

NIS2, hvorfor?

Alt dette er jo meget godt, men hvorfor skal "vi" overhovedet gøre noget? Intentionen bag NIS2 er reelt set at sikre EU som samfund mod negative konsekvenser på grund af cyberangreb. Cyber rækker langt længere ind i vores "fysiske" verden, end de fleste mennesker er bevidste om. Eksempelvis er muligheden for toiletskyl, strøm, vand og varme ofte meget påvirkelige af cyberangreb. Dette eksemplificerer, hvor meget vores daglige gøren og laden er udsat. DSB´s udfordringer ved hackerangreb på en underleverandør, der fandt sted ultimo oktober 2022 er en mærkbar konsekvens af, hvordan en mindre komponent kan påvirke vores samfund i et væsentligt omfang. Hertil kan man selv indsætte og forestille sig lignende udfordringer med MitID, sygehuse etc.

Ovenstående er vinklen fra det samfundsmæssige perspektiv, men med direktivet følger også minimumsbøder og personlige konsekvenser for ledelsesgangene. Dertil er det nok de færreste brands, der ønsker at være blandt de uheldige, der kommer på forsiderne med en historie om konsekvenserne af deres utilstrækkelige informationssikkerhed.

Min klare anbefaling for at imødegå dette er at alliere sig med en ekstern partner eller rådgiver, som spænder bredere end blot et enkelt af de felter, der er nævnt. Med dette mener jeg, at det ikke er nok at lave udgaver med særskilt juridisk- eller revisionsperspektiv, og det er omvendt heller ikke nok, kun at installere teknologien. Det kræver en holistisk tilgang at sikre virksomhederne mod nutidens og fremtidens udfordringer på informationssikkerhedsområdet, herunder compliance med de krav der stilles af direktiver som NIS2.

Scrum Security

Shantanu Desai, CISSP, CISA , VP Risk and Control Lead, Citibank

What is Scrum?

A decade ago, for some even earlier, most of us working in IT and related industries were introduced slowly to this brand new methodology. The answer to all the technical bottlenecks, delays, quality issues, team collaboration hiccups and of course, to present management with a sense of control and visibility on what goes about in their expensive and complex IT divisions.

For many, it did live up to what it claimed to do. For others it was a pain in the neck. For people like me, working in securing the digital deliveries, it did grow to present a formal way to step up, creep into the otherwise business focused product development efforts, and eventually improve the security posture. It took a while and a lot of patience. I do believe that as far as security related efforts are concerned, we are still far from what should be a great way of exploiting this framework. In this article, I present a way for enabling security focused efforts in the world of Scrum/Agile. It was drafted some time ago but still relevant. Let's start with the basics.

So, what is Scrum?

One definition is:

"Scrum methodology is used in the Agile process for software development. But rather than a full process or methodology, it is a framework. So instead of providing complete, detailed descriptions of how everything is to be done on the project, much is left up to the software development team. This is done because the team will know best how to solve the problem they are presented." [1]

I don't think anyone reading this is any wiser after this definition, but what we can take away from it is, development is in *the team* when Scrum is being practised. They gather the requirements, they plan, and they design, develop, test, verify, retest, re-develop, deploy - and then go out for a beer, together!

I was so intrigued by this word Scrum that I sought out the meaning of this word in plain old English.

SCRUM[2]

What I found was really interesting:

1. In Sports
   A play in Rugby in which the two sets of forwards mass together around the ball and, with their heads down, struggle to gain possession of the ball.

2. In general terms
   A disordered or confused situation involving a number of people.

The second definition caught my attention, so I decided to study it in detail. To make sure that the second definition does not describe Scrum correctly.

Scrum relies on a self-organizing, cross-functional team. The Scrum team is self-organizing, in that there is no overall team leader who decides which person will do which task or how a problem will be solved. Those are issues that are decided by the team as a whole. The Scrum team is cross-functional; everyone is necessary to take a feature from idea to implementation.

These Agile development teams are supported by two specific individuals: A Scrum Master and a Product Owner. The Scrum Master can be thought of as a coach for the team, helping team members use the Scrum framework to perform at their highest level. The Product Owner represents the business, customers or users, and guides the team toward building the right product and not drift far away from management's vision.

Scrum projects make progress in a series of 'sprints', which are time-boxed iterations no more than a month long. At the start of a Scrum sprint, team members commit to delivering some number of features that were listed on the project's Scrum product backlog. At the end of the Scrum sprint, these features are done - they are coded, tested and integrated into the evolving product or system. At the end of the sprint, a sprint review is conducted during which the team demonstrates the new functionality to the Product Owner and other interested stakeholders, who provide feedback that could influence the next sprint.[3]

Following four lines from the Agile manifesto are something that define the Agile mentality or DNA!

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan.[4]

What about Security?

I have been in application and information security for more than a decade now, and I know the loopholes and how 'Security' was treated as an overhead by everyone even in the traditional Waterfall model. Project managers look at it as more effort and cost for the project with no functional value, developers look at it as more and more coding with nothing much to showcase, testers look at it as something that is invisible and has no functional testing or business value... So in a nutshell, security tends to be overlooked in traditional, time consuming and well [over?] planned software development.

What got me thinking was what would happen to security in this fast and amazingly open model of Scrum, which doesn't much recognise the role structure?

Who would be responsible for security, and how can that be effectively integrated in this blazing platform, where every week, and in some cases every weekday, we add new releases, which add awesome features to the products?

Does anyone look at the security implication of ever-increasing business demands, or is it just overlooked as we add more and more functionalities at a breakneck speed?

So now, without much delay let's talk about *what* can be done to make sure that your Scrum is more secure. I would like to clarify that the approach given below is something that I have picked up from some sources on the internet, cut through some, added something of my own, and so on and so forth. It's not tested in an actual Scrum implementation. I don't have and never had that kind of authority to influence the Scrum gods!

I am going to discuss one approach which I found, and I am comfortable enough to state, would work in a Scrum setup. In one line this approach does the following:

In Scrum you sprint. So, do a Security sprint, every once in a while!

As simple as that.

Security Sprint

Following are the six steps that can be used for doing a Security sprint:

1) Know your threats
2) What's your Security Story?
3) Test strategy
4) Security sprint - Implement controls
5) Testing
6) Verification

Know your threats

The key is to identify and understand the following:

- Key Risks to the business
- Threat Agents - the groups of attackers and their likelihood factor
- Attacks - the different attacks that the threat agents might use
- Vulnerabilities - the different vulnerabilities targeted by the attacks
- Security Controls - the countermeasures to the vulnerabilities
- Technical Impacts - the impacts of successful attacks on the application and infrastructure
- Business Impacts - the impacts of successful attacks on the operation of the business
- Security Stakeholders - the stakeholders in the security of the application

Once the Scrum team has brainstormed on the above mentioned points, one thing that can be guaranteed is that a mind-set is achieved, which relates to the security of their product. This will definitely help them in the phases which follow in the Security sprint.

What's your Security Story?

As is the case with all other sprints, we would need User generated stories for anything to start. Now, we need to understand that the User here is not your normal user:

- S/He is someone who gets paid for NOT using your application as it is supposed to be used!
- S/He is an Abuser not a User

So, instead of User Generated Stories, think more on the terms of Abuser Generated Stories!

Example #1:
"As an Abuser, I can send bad data in URLs, so I can access data and functions for which I'm not authorized."

Example #2:
"As an Abuser, I can send bad data in the content of requests, so I can access data and functions for which I'm not authorized."

Example #3:
"As an Abuser, I can send bad data in HTTP headers, so I can access data and functions for which I'm not authorized."

Example #4:
"As an Abuser, I can read and even modify all data that is input and output by your application."

Test strategy
A test strategy catering to the Agile needs that a Scrum methodology demands would have to be put in place, and just like with every Agile project, it would be customized to suit the needs, timelines and requirements of that particular project.

Another approach can be inclusion of security related test cases in the normal testing flow of your Scrum implementation. This would definitely need some expertise in chalking out the SOP type of functioning, which would be all-inclusive.

This can be a totally manual testing exercise, or a completely automated one. Both have their own advantages and disadvantages, but that I would leave for a different article altogether. A recommended approach is using both approaches - manual as well as automated, in coming up with a test strategy which gives you a wide coverage within your project's timelines.

Final deliverable of this step would be a test report, listing reported vulnerabilities, their risk factor, implications if exploited, remediation techniques etc. Since the USP of Scrum is collaboration, a collaborative effort between the security personnel and development team would be the best way for remediation of issues found.

Security Sprint - Implement Controls
Once you have the 'Evil Stories' these can be converted into positive user stories i.e. a user, who is somewhat concerned, and aware of security related implications. These stories can be given a risk level along with controls that would be implemented to assist in closing the risks.

Example #1 – As a User:
"I want to be the only one who can access my account, so that I can keep my information private."
Risk level: HIGH
Controls: Authentication and Data Layer Access Control

Example #2 – As a User:
"I want my personal information encrypted in storage and transit so that it doesn't get stolen by attackers."
Risk Level: HIGH
Controls: SSL and Encryption

Example #3 - As a Manager:
"I want to be the only one who can edit employee salaries, so that I can prevent fraud."
Risk Level: HIGH
Controls: Function Layer Access Control

Example #4 - As a Business Manager:
"I want all security critical actions logged, so that attacks can be noticed and diagnosed".
Risk Level: MEDIUM
Controls: Logging and Intrusion Detection

Testing
This is the phase where you will follow the test strategy and perform testing of the implemented security controls. A final report detailing the findings would be released and distributed to the team. Facilitating the remediation efforts by providing best practices, remediation techniques, as well as guidelines, should also be included in the report.

Verification
The final step! Verify all the fixes here, and if everything looks fine, go ahead and bask in the glory of a secure deployment!

That's one of the strategies based upon some limited reading, digging up and analysis that I have performed. I have mentioned the sources for the various information used in the article (see Notes section). Some more links which were useful were as follows:

1 - "Breaking the Waterfall Mindset of the Security Industry" - Dave Wichers

2 - www.google.com

If you are reading this and if you think that there might be some input from you that would help develop better and secure Agile products, please do comment or get in touch with me at shantanudesai1@proton.me.

After all, Scrum does mean team work!

Notes

[1] http://www.mountaingoatsoftware.com/topics/scrum
[2] http://www.thefreedictionary.com/scrum
[3] http://www.mountaingoatsoftware.com/topics/scrum
[4] http://agilemanifesto.org/

Nye medlemmer

Nye medlemmer i IIA fra 8.9.2022 - 5.12.2022

A.P Møller-Mærsk
LJ Stevenson

ATP
Bo Langhoff
Marc Woodall
Louise Cubbin

Danske Bank
Nyasha Moyana
Natasha Schiøler

Deloitte
Martin Tripax
Betina Doktor

E-nettet
Michael Kvist Nissen

Handelsbanken
Helle Hyldegård Holm

Jyske Bank
Anders Wiwe Petersen

Lidl Danmark
Alberto Di Nardi

Nokia Danmark
Julia Popova Nielsen

Oxfam IBIS
Jacob Ikkala

PFA Pension
Youssef Amziane

Saxo Bank
Sune Andreas Yung Nielsen
Maria Concetta Barbano

SDC – Skandinavisk Data Center
Søren Ryberg

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

31.05.2023 IIA Årsmøde 2023

"Bagsmækken"

Foreningens adresse

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

CVR nr. 73954215

Indmeldelse i foreningen

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

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

Jobannoncer

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

Certificeringer

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

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

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

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

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

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

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

Sekretær
Head of Audit
Steve Steyn
Nordea
☎ 52 63 53 98
✉ petrus.stephanus.steyn@nordea.com

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

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

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

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

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

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