

INFO

Foreningen af Interne Revisorer

Nummer 75 | September 2020 | 25. årgang

Minitema: COVID-19

- EY Virtual Risk assessment
- IT-beredskabets processer
- Indvirkning på revisors arbejde

Markedsmisbrugsområdet

En praktisk tilgang til revision af pengeinstitutters foranstaltninger mod markedsmisbrug og insiderhandel

Governing Bodies

Internal Audit's Role in Board and Executive Committees

IIA Prisen 2020



Outsourcing



Compliance

INFOs redaktion

Ansvarshavende redaktør

Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
Express Bank
☎ 36 39 52 61 ✉ bisv@expressbank.dk

Øvrig redaktion

Assistant 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

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

Intern revisor
Mai-Britt Soo
Sparekassen Kronjylland
☎ 89122400 ✉ mais@sparkron.dk

Revisor
Klaus Nordmann Østrup
Københavns Kommune
☎ 33 66 24 13 ✉ zx7z@ir.kk.dk

Næste nummer

INFO 76 udkommer i december 2020.
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@iaa.dk

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

Forsidefoto

UnknownNet

Redaktionens adresse

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

redaktionen@iaa.dk

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

Indhold

Leder	3
Nyt fra bestyrelsen - CPE point	5
Nyt fra redaktionen	6
Vindere af IIA Prisen 2020	7

Minitema: COVID-19

EY virtual risk assessment in light of COVID-19	10
Et praktisk indblik i revision af IT-beredskabets processer.....	13
COVID-19 - Indvirkning på Intern revisions arbejde	17
COVID-19 & Intern revision.....	19

Internal Audit's Role in Board and Executive Committees	21
Revision af pengeinstitutters foranstaltninger mod markedsmisbrug og insiderhandel – en praktisk tilgang	23
Nye skærpede regler om finansielle virksomheders outsourcing	28
Compliance, compliance	32
Nye medlemmer	34
Bagsmækken	35

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.iaa.dk

Leder



Birgitte Rousing Svenningsen, Revisionschef, CIA, CISA, Express Bank

En verden i forandring

”En verden i forandring” er et udtryk, som flere gange er blevet brugt til fremsættelse af politiske budskaber - såsom Nyrup regeringens oplæg til udviklingspolitik i 1994 og Anders Fogh regeringens bud på nye prioriteter i Danmarks udenrigspolitik i 2003. Udtrykket blev også anvendt efter 9/11, som udtryk for øget terrorisme i verden. I dag forbinder vi nok alle udtrykket mere med COVID-19 og de konsekvenser, pandemien har haft for vores hverdag og for verdenssamfundet i det hele taget. Verden er under forandring!

Hvad betyder det for os som interne revisorer?

Vi har i dette nummer af INFO samlet en række erfaringer og gode råd. Vigtigt af alt er måske, at COVID-19 har vist os, at store dele af vores samfund kan fortsætte upå-

virket, selv om de enkelte medarbejdere arbejder hjemmefra. Det er formodentlig ikke sidste gang, at vi ser, at virksomhederne opfordres til at anvende så meget hjemmearbejde som muligt. Under alle omstændigheder vil vi komme til at se mere hjemmearbejde, idet vi også som danskere har fundet ud af, at det giver os nogle fordele og fleksibilitet, som vi også gerne vil have i fremtiden. Man skal derfor regne med, at fremtiden bliver, at de interne revisorer såvel som de reviderede har flere hjemmearbejdsdage. Dette stiller krav til nye måder at planlægge på og krav til at anvende nye elektroniske værktøjer.

Som altid skal vi som interne revisorer være på forkant med udviklingen. Det er derfor nu, at vi skal investere i nye arbejdsmetoder.

COVID-19 har også medført, at der er revisionsområder, som er blevet mere centrale end før. Et af disse områder er virksomhedernes IT beredskabsprocesser. Du vil derfor finde en artikel i dette nummer af INFO, som giver en konkret anvisning på, hvordan en intern revision kan revidere IT beredskabsprocesserne.

IIA's nye Three Lines Model

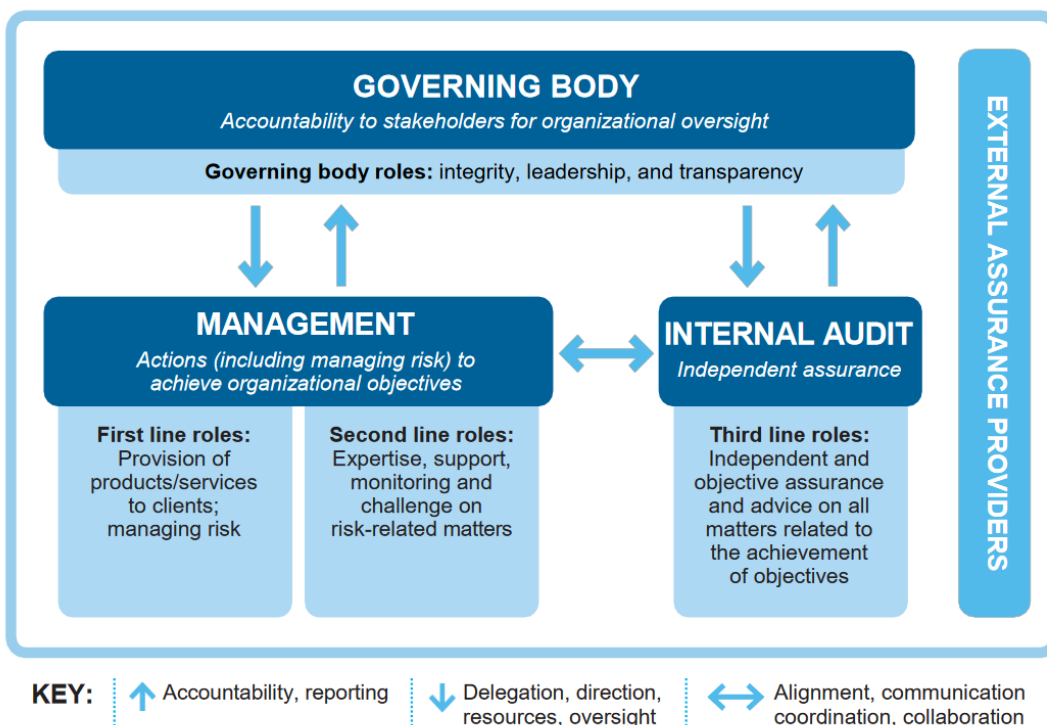
I sidste nummer af INFO bragte vi en artikel om nye tiltag vedrørende 3 Lines of Defense Modellen. Et af initiativerne var, at IIA arbejdede med en fornyelse og modernisering af modellen.

Dette arbejde er nu færdigt og IIA har udgivet dokumentet ”The IIA's New Three Lines Model” der kan downloades gratis af alle medlemmer på www.theiia.org. Det er

et MUST for alle interne revisorer at læse dette dokument, som er forholdsvist kortfattet (10 sider). <https://na.theiia.org/about-us/about-ia/Pages/Three-Lines-Model.aspx>

Kort fortalt lægger den nye model op til øget kommunikation, koordination og samarbejde mellem de 3 forsvarslinjer. Endvidere er beskrivelsen af modellen gjort lidt mere præcis ved definition af 6 principper. Modellen er angivet i figur her ved siden af. Hvis du klikker på figuren er der et link til dokumentet, som beskriver modellen.

The IIA's Three Lines Model



IIA Prisen

Foreningen stiftede for et par år siden IIA Prisen. Formålet med prisen er at skabe øget interesse for intern revision blandt de cand.merc.aud. Studerende, samt at fremme kendskabet til og forskningen inden for intern revision.

Prisoverrækkelsen finder normalt sted på vores Årsmøde, men da dette er blevet udskudt på grund af COVID-19, offentliggør vi nu dette års vindere – se side 7. Vinderne har skrevet to spændende kandidatafhandlinger og vi vil i løbet af efteråret udgive nogle korte artikler, som opsummerer de væsentligste pointer fra afhandlingerne.

Tillykke til vinderne og såfremt COVID-19 tillader det, vil vi lave en officiel overrækkelse af priserne ved morgenmødet den 6. oktober.

Intern revisions rolle

IIA Global udgiver løbende såkaldte "Position Papers". Disse beskæftiger sig typisk med nogle af de problemstillinger, vi kender fra vores hverdag som intern revisor.

En af disse problemstillinger er, hvorledes vi som intern revisor kan/bør arbejde sammen med bestyrelsen, direktionen og diverse udvalg, uden af vi samtidigt mister vores uafhængighed. Vanita Shukla Hork deler, med udgangspunkt i IIAs Position Papers herom, Nordeas erfaringer hermed.

Markedsmisbrug og insiderhandel

Markedsmisbrug og insiderhandel er et centralt revisionsområde for revisorer i banker med værdipapirhandlestilla-

delse. Med udgangspunkt i EU-kravene og Finanstilsynets temaundersøgelse giver Ulrich Rasmussen konkrete bud på, hvad den interne revisor skal forholde sig til.

Outsourcing

Ud over COVID-19 og sol har sommeren også budt på en ny bekendtgørelse om outsourcing i finansielle virksomheder. Bekendtgørelsen stiller en række nye og ændrede krav, fx. nye krav vedrørende udpegelse af en outsourcingansvarlig, et outsourcingregister, risikovurderinger og exitstrategier.

Det vil kræve en del arbejde for virksomhederne at leve op til de nye krav. Den interne revisors kan hjælpe hermed og med rådgivning herom, hvorfor det er væsentligt, at den interne revisor gør sig bekendt med de nye regler. Reglerne bygger grundlæggende på gode governance-regler og ønsket om, at de ydelser, som virksomheden modtager fra tredjepart, lever op til virksomhedens forventning og krav. Reglerne kan derfor passende anvendes som inspiration for virksomheder uden for den finansielle verden.

Compliancefunktion

Hvad er en compliancefunktions opgave? Hvordan bør opdelingen være mellem første og anden forsvarslinje? INFO bringer i dette nummer en artikel, som giver et konkret indblik heri.

God læselyst og pas på jer selv og andre derude.



Nyt fra bestyrelsen - CPE point



Birgitte Rousing Svenningsen, Revisionschef, CIA, CISA, Express Bank

Som oplyst har vi desværre fundet det nødvendigt at udskyde Årsmødet til 2021 på grund af COVID-19.

Vi er i bestyrelsen klar over, at det aflyste årsmøde og andre aflyste uddannelsesaktiviteter vil for nogle give udfordringer i forhold til at opnå det årlige mindstekrav om CPE point, som er gældende for CIA certificeringer mv.

Vi har derfor kontaktet IIA Global med henblik på at undersøge, om der for 2020 stilles lempeligere krav på grund af COVID-19. IIA Global har oplyst, at de ikke vil dispensere for det årlige krav om opnåelse af CPE point.

Kravet er derfor, at der skal opnås minimum 40 CPE point i 2020, hvoraf 2 CPE point skal vedrøre etik.

Der er jo mange måder at opnå CPE point på for eksempel:

Optjen CPE point

Mange oplever, at COVID-19 tiderne giver udfordringer med hensyn til optjeningen af de nødvendige CPE-point til vedligeholdelse af deres internationale certificeringer.

I denne forbindelse vil vi gerne gøre lidt reklame:

Vidste du, at du kan optjene CPE-point ved at skrive artikler til INFO?

Du kan optjene et point per 200 ord til CIA, CCSA, CFSA, CRMA og øvrige IIA-certificeringer. Der er dog et maksimum på, hvor mange CPE point du kan optjene hvert år.

Dette maksimum er 15 for CIA og 6 for de øvrige IIA certificeringer.

- Deltage i online undervisning (webinars mv.)
- Skrive artikler (fx til INFO)
- Deltage i klasseundervisning
- Deltage i frivilligt arbejde i IIAs udvalg
- Undervise i relevante emner.

De nærmere regler finder du her: <https://na.theiia.org/certification/Public%20Documents/CPE-Policy.pdf>

IIA Global uddannelsesaktiviteter

Ud over de uddannelsesaktiviteter, som IIA Danmark løbende vil tilbyde resten af året, har IIA Global også en lang række uddannelses tilbud. Her vil vi særligt reklamere for Webinars og OnDemand training.

I tillæg til de mange tilbud fra IIA findes der på markedet en række andre kursusudbydere, som tilbyder online undervisning. Disse kan også benyttes til opnåelse af de krævede CPE point.

Frivilligt udvalgsarbejde

Hvis du er interesseret i at deltage i noget frivilligt arbejde for foreningen, hvorved du kan optjene CPE point både i 2020 og fremtidige år, er du meget velkommen til at kontakte foreningens formand Jesper Siddique på formand@iia.dk. Vi kan altid bruge aktive hænder til at hjælpe med foreningsarbejdet. Lige nu har vi i særdeleshed brug for et par personer, som vil arbejde i vores Nyhedsbrevsudvalg og meget gerne en person fra industri-sektoren. Der er også plads i andre udvalg.

Artikler til INFO

Hvis du er interesseret i at skrive en artikel til INFO, er du velkommen til at skrive til redaktionen@iia.dk med en kort beskrivelse af artiklens emne. Vi vil herefter vende tilbage med et svar på, om vi finder artiklen relevant og ønsker at udgive den.

Quiz om Internal Auditor bladet

Indtil udgangen af 2020 kan man tage en quiz i Internal Auditor bladet. Det kan give max 6 CPE point.

Du kan også optjene CPE point til en CISA certificering. Her er reglerne, at der ikke er noget maksimum, og at der optjenes 1 CPE point per anvendt time til udarbejdelse af artiklen.

Der er altså rig mulighed for at optjene nogle CPE point ved at skrive artikler til INFO. Hvis du er interesseret i at skrive en artikel, er du velkommen til at skrive til redaktionen@iia.dk med en kort beskrivelse af artiklens emne.

Vi vil herefter vende tilbage med et svar på, om vi finder artiklen relevant og ønsker at udgive den.

Nyt fra redaktionen



Birgitte Rousing Svenningsen, Revisionschef, CIA, CISA, Express Bank

Nye tiltag

I sidste nummer af INFO bekendtgjorde jeg, at redaktionen ville barsle med nye tiltag. Det vil vi gøre i løbet af efteråret.

De sidste mange år er INFO blevet udgivet 3 gange om året. Det vil vi fortsætte med.

På den anden side vil vi gerne imødekomme de læsere, som sommetider synes, at det er overvældende at få et helt blad ind af døren. Endvidere vil vi gerne skabe øget fleksibilitet for at sikre, at vi udgiver artikler, når emnet er højaktuelt. Vi har derfor besluttet, at vi vil udgive artikler løbende.

Det betyder, at vi i løbet af oktober og november vil udgive enkelte artikler og medlemmerne vil hver gang blive informeret via mail.

I december vil vi som sædvanligt udgive et helt nummer af INFO. Dette blad vil komme til at indeholde de artikler, som vi har udgivet i oktober og november samt flere artikler, som ikke tidligere har været udgivet.

Vi håber på denne måde at kunne udgive artikler på det helt rette tidspunkt og give vores læsere øget mulighed for selv at bestemme, hvornår de læser artiklerne.

Nyt redaktionsmedlem

I dette nummer af INFO har jeg æren at kunne byde velkommen til et nyt redaktionsmedlem – Mai-Britt Soo.

Mai-Britt kommer med en bred erfaring inden for intern revision, compliance, risikostyring og regnskab. Mai-Britt arbejder i dag i den interne revisionsafdeling i Sparekassen Kronjylland. Dette er en af de interne revisionsafdelinger, som de seneste år har arbejdet med at få øget fokus på operationel revision.

Som første-generations indvandrer til Hovedstadsområdet fra Jylland, er det mig en særlig ære at byde velkommen til et redaktionsmedlem bosat i Jylland. Jeg ser meget frem til det fremtidige samarbejde med Mai-Britt.





Vinderne af IIA Prisen 2020



Intern revisions udbredelse i Danmark. En undersøgelse om til og fravalg af intern revision i danske børsnoterede virksomheder.

Forfattere: Malthe Riegels og Mads Skovgaard Larsen

Begrundelse:

Kandidatafhandlingen omhandler et område, som er yderst relevant at undersøge. Det påvises, at valg eller fravalg af intern revision hænger sammen med størrelsen af virksomheden, andelen af udlændinge i bestyrelsen og bestyrelsens kendskab til intern revision. Afhandlingen afsluttes med to konkrete anbefalinger til forbedringer, idet det anbefales, at virksomhederne skal redegøre for et eventuelt fravalg af intern revision, og at kompetencekravene til medlemmerne af revisionsudvalgene skærpes, således at der fremover skal være kompetencer inden for både regnskab og revision. Disse anbefalinger virker relevant og realistisk at indføre. På baggrund af kandidatafhandlingens undersøgelser har IIA's bestyrelse indledt et samarbejde med bestyrelsesuddannelser med henblik på at øge kendskabet til intern revision og intern revisions værdiskabelse.



Intern revisions værdiskabelse ved anvendelse af IPPF i danske banker

Forfattere: Peter Dalgaard Villumsen

Begrundelse:

Kandidatafhandlingen undersøger værdien af IIA's framework IPPF. Konklusionen er, at IPPF hjælper interne revisionsafdelinger til at strukturere afdelingens opgaver og derigennem tilfører værdi. Afhandlingen er relevant og meget velstruktureret. Selv om afhandlingen omhandler værdiskabelse i danske banker, kan dens analyse og konklusioner også anvendes uden for den finansielle sektor. Det er en afhandling, som giver anledning til eftertanke. På baggrund af afhandlingens konklusion kan man med rette overveje, om danske interne revisionsafdelinger i tilstrækkelig grad anvender IIA's IPPF framework.

IIA PRISEN

Prisopgave om intern revision

Foreningen af Interne Revisorer uddeler 2 præmier til hovedopgaver på cand. merc. aud. studiet

1. præmie: 25.000 kr.

2. præmie: 15.000 kr.

Prisens formål er at fremme kendskabet til og forskningen inden for intern revision.

Hovedopgaven skal omfatte et emne og en problemformulering, som er relevant for forståelsen af intern revisions arbejde og betydning for de virksomheder, som har eller overvejer at etablere(t) en intern revisionsfunktion. For at komme i betragtning skal hovedopgaven være afsluttet i perioden 1. januar 2020 til 31. december 2020.

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

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

Ansøgningsfristen er 15. januar 2021. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iia.dk.

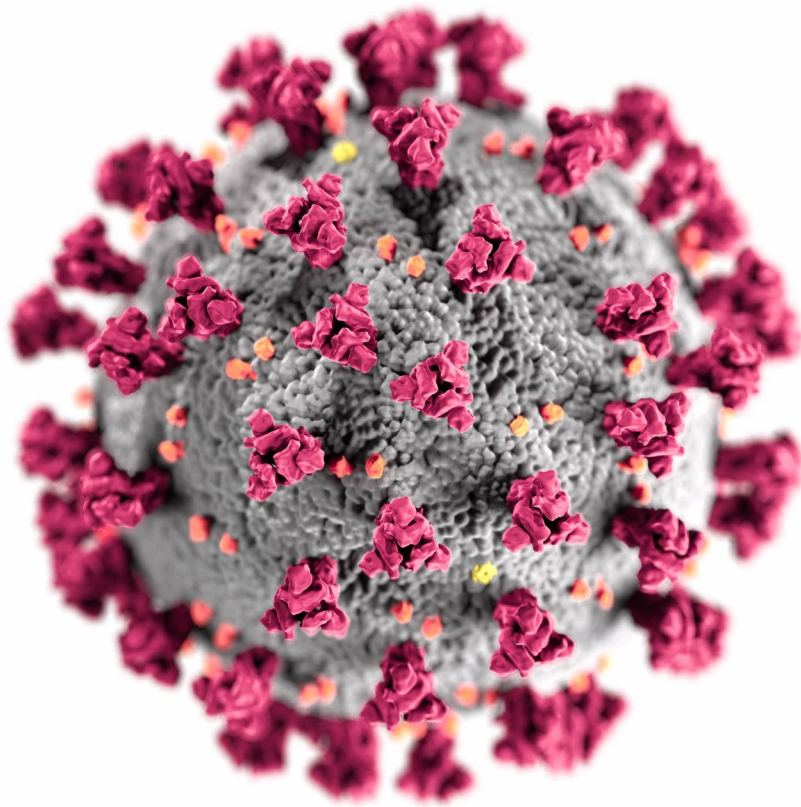
Prisoverrækkelsen vil ske på IIA's årsmøde i maj 2021. Bedømmelsesudvalget består af Dorthe Tolborg (Danske Bank), Kim Klarskov (CBS) og Birgitte Rousing Svenningsen (Express Bank).

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.



Foreningen af Interne Revisorer
The Institute of Internal Auditors - Denmark

Minitema: COVID-19



Hele verdens opmærksomhed har i foråret været rettet et helt andet sted end før. COVID-19 udbruddet satte hele verden og dermed også vores branche i et nyt lys. I dette nummer har INFO et minitema om emnet med fokus på konsekvenserne heraf for vores branche. Læs de meget direkte og ærlige udtalelser fra 17 revisionschefer om, hvordan pandemien og følgerne heraf har påvirket hverdagen, både på hårde og bløde værdier. Læseren tages også med på en spændende tur blandt de nordiske revisionschefer i krishåndtering mv. både i revisionsafdelingerne og i de reviderede virksomheder.

Sidst men ikke mindst har vi samlet et overblik til læseren om, hvor der kan findes spændende artiklerne om emnet på IIA Global.

God læselyst!

EY virtual risk assessment in light of COVID-19



Henrik Lind, EY Nordic Enterprise Risk Leader



Christine Sandnes, EY Sweden Enterprise Risk Leader

Introduction

EY teams have engaged the Nordic Chief Audit Executives (CAEs) in several discussions to conclude on the business impacts of the COVID-19 pandemic.

The overall purpose of the discussions was to provide insights and experience in how Internal Audit (IA) should respond to potential updates on the internal audit plan, how to execute internal audit projects and how to communicate with key stakeholders. This article highlights the outputs.

According to the EY Global Risk Survey 2020, 79% of board members state that their organizations are not very well prepared to deal with a crisis event. There are five essentials steps to take during crisis management:

1. Put employee well-being above all else
2. Communicate promptly, clearly and transparently
3. Keep expenses in check and have backups for budget deficits
4. Identify and repair broken links in the supply chain
5. Prepare for the unexpected.

For IA it is now essential to repurpose resources to directly support the business in identifying vulnerabilities and provide real-time risk advisory services to crisis response, such as:

- crisis management
- business continuity planning
- work from home capability
- cybersecurity
- technology effectiveness
- employee well-being
- customer safety
- supply chain effectiveness
- working capital management
- brand protection

Next step is to focus on cost recovery through remote auditing and performing analytics-based procedures. Finally, this means that IA needs to adjust a new normal and focus on the risks that matter, better enabled by technology and resources with deeper business skills.

What could IA do in order to support the organization?

On EY virtual roundtables, EY teams discussed if IA for example should support the organization in establishing business continuity or plan to use staff in audit units for tasks other than assurance engagements. However, most of the CAEs believe that the COVID-19 pandemic will last for six to twelve months. By that, EY teams ended up asking what the highest risks are. Is there a greater chance of fraud now? If yes, why? What can EY teams do about it? What are the risks and vulnerabilities when everyone is working from home?

EY teams identified 27 risks that can be clustered into nine main categories:

- supply chain and globe trade
- employee health and well-being
- talent and workforce
- customer safety and brand protection
- financial and investor
- risk
- government and public policy
- technology and information security
- insurance and financial recovery.

The CAEs concluded that cashflow, market conditions and regulatory landscape are among the top three risk areas of focus.

EY teams also identified eight relevant audit needs to meet the current challenges and provide relevant insights to key stakeholders.

1. Liquidity

With a global economic unbalance due to the COVID-19 outbreak, liquidity and cash management become essential for companies searching for near-term solutions, e.g. cash shortage, credit squeeze, contingency planning and supply chain disruptions. The main identified risk is severely deteriorated liquidity inflows; deterioration in forms of the customers' ability to meet their financial obligations impacting the company's liquidity inflows and cash management.

Audit needs to assess the company's financial resilience and highlight the necessity for appropriate treasury and cash management. Achieving visibility and control over cash flows and driving sustainable working capital improvements are the most cost-effective forms of finance for most organizations.

2. Adaptation to market conditions

All sectors are reporting a drop in demand. Customers oriented to traditional channels are opting for online

channels, requiring companies to make immediate adjustments. The risks here are the overall market health and changes in consumer demand impacting turnover. There might be decreased demand due to decline in customer sales, global recession, loss of market share or changed customer behavior.

Audit should assess how decisions are made and what information companies need in order to make decisions for business survival. IA needs to evaluate if the decisions are made according to the company's risk appetite and the information the decisions are based upon.

3. Supply chain resiliency

94% of the Fortune 1000 companies are experiencing disruption to their supply chains as a result of COVID-19. As the pandemic continues to evolve, organizations around the globe are struggling to align supply and demand and are facing numerous issues across the end-to-end supply chain. There is a risk that the interrupted supplier ecosystems will lead to halt in production, increased costs and reduced customer trust. Increased operation costs or liquidity risks might lead to replacing affected suppliers with more expensive substitutes, temporary layoffs and factory closures.

Audit needs to assess the company's supply chain resilience by auditing the area, route to market and channel strategy, integrated sales and operations planning, logis-

tics and distribution, manufacturing and plant operations, procurement and supplier management and crisis management and governance.

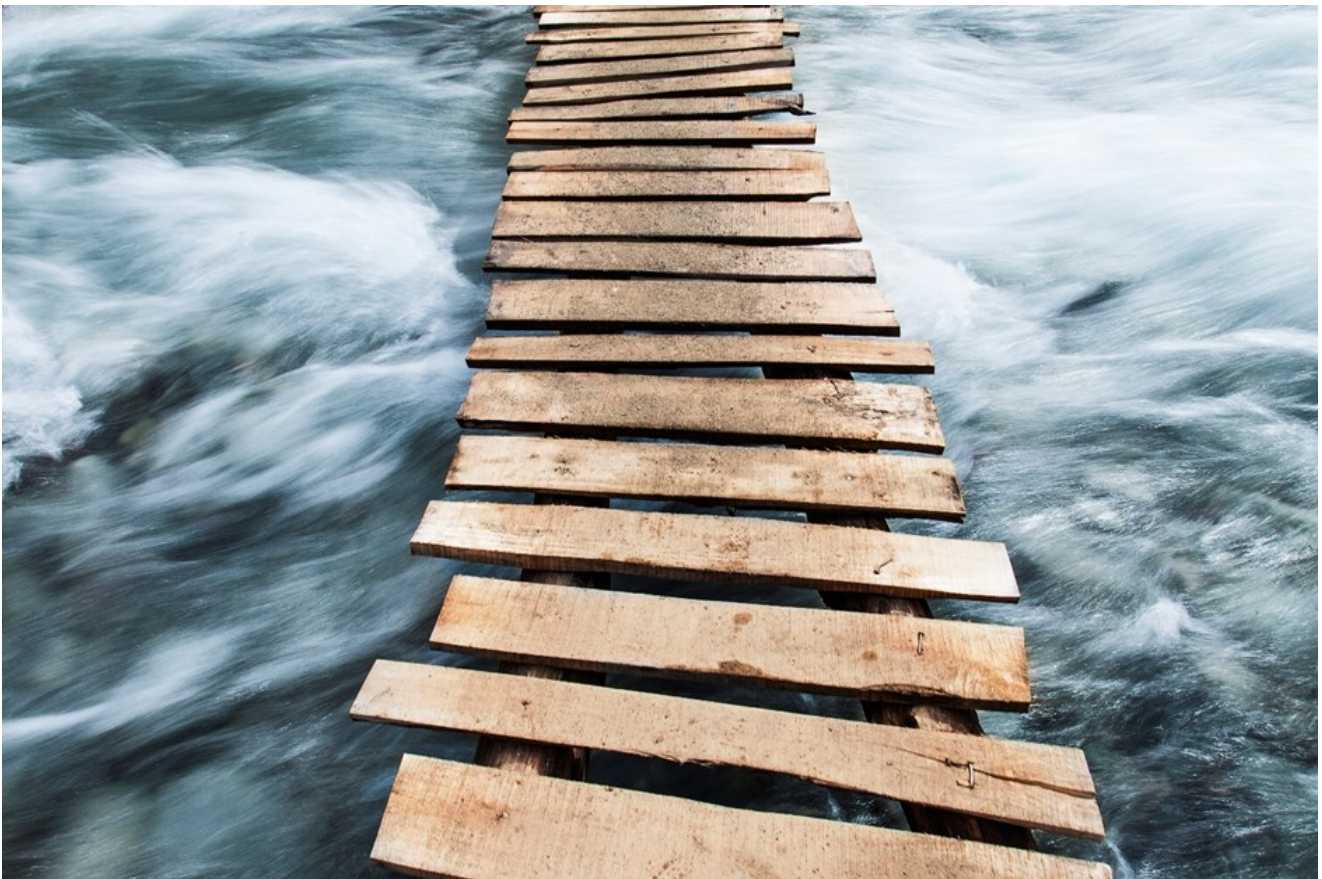
4. Compliance with regulatory changes

Disruptive and sudden regulatory changes cause severe business disruption. Governments may take quick disruptive decisions, e.g. new or updated regulations and legislations on how to protect citizens and national interests.

Audit needs to assess the compliance framework and regulatory monitoring process with focus on COVID-19. Also, there is a need to assess whether the process considers actions and guidance from regulators and the government, business strategy and the organization's crisis response.

5. Business continuity and crisis management

As companies navigate the ongoing pandemic in order to reshape their business plan for recovery, there are several key issues corporate leaders should keep in mind. There is always a risk that companies end up leading insufficient processes and procedures for business continuity and crisis management. Lack of robust, consistent, and agile processes may result in the company not being able to efficiently and adequately manage crises and disruptive changes such as COVID-19.



Audit needs to assess the company's crisis management and strategy for business continuity. Areas to audit can be short term liquidity, financial and operational risks, alternative supply chain options and the COVID-19 pandemic effect on budget and business plan.

6. Fraud

During a crisis, the risk of fraud increases because companies and individuals face more financial pressure. The opportunity for fraud also increases if key internal controls are weak and if people find it easy to rationalize their actions. These three elements – pressure, opportunity and rationalization – are always present in every case of fraud (also known as the Fraud Triangle). COVID-19 offers all three and more. Naturally, there are always increased internal and external fraud risks involved.

Audit needs to assess the implication of the business's continuous activities on controls, systems, governance, and culture as these activities might increase the fraud activities in the short term.

7. Access to funding

The current financial disorder has resulted in tensions in capital and commercial paper markets, with potentially severe implications for the global economy and financial stability. Reduced demand for commercial papers deprives the access to short and mid-term funding through the commercial paper market.

Audit needs to assess the company's funding strategy, capital market options, and contingency plan.

8. Cybersecurity

Security centers in COVID-19 affected areas have been shut down, rendering several companies exposed. Many such companies have been hit by cyberattacks compromising sensitive data. Cyberattacks and breaches cause leakage of sensitive data and fraud. Both increased exposure and degradation of cybersecurity programs lead to higher risk of breaches.

Audit needs to assess the company's preparedness and defense mechanisms against cyber threats.

Summary

Internal Audit has a real opportunity to collaborate with business and support continuity by reposting IA resources, providing real time risk advice through crisis management, helping the organization to assess exposure to emerging risks, revisiting your risk assessment and planned audit procedures, ensuring the needed technology infrastructure and tools to support remote audit activities, planning to supplement your resources to address new ways of working and evolving risks and leveraging downtime to enhance the IA function.



Et praktisk indblik i revision af IT-beredskabets processer



Lene Bach Sørensen, CISA, Intern IT-revisor, DSB

Indledning

I min mangeårige karriere som IT-revisor inden for eksternt finansiel revision og rådgivning, har revision af IT-beredskabet typisk kun fyldt en lille del af IT-revisors revisionsplan. Dette skyldes at IT-beredskabet kan klassificeres som en forretningsmæssig risiko, og derfor ikke som udgangspunkt medfører en væsentlig fejl i regnskabet. I min nuværende rolle som intern IT-revisor i DSB's Interne revision arbejder vi alene med operationel revision, og har derfor et mere forretningsorienteret fokus.

Jeg vil gerne med denne artikel henlede opmærksomheden på vigtigheden i at få revideret virksomhedens beredskab, herunder IT-beredskabet. I nærværende artikel vil jeg beskrive mine erfaringer med revision af IT-beredskabets processer, og dele "take aways" herfra.

Baggrund for revision af IT-beredskabet

Vi befinder os i skrivende stund midt i en COVID-19 krise, hvor mange arbejder hjemmefra, hvilket afstedkommer ændringer i vores interaktion med vores virksomheders systemer og processer. Det har mange hackere luret og øjnet en forretningsmulighed i. Vi ser derfor en stribe af daglige angreb mod virksomhederne i form af bl.a. ransomware og phishing mails. Men den forhøjede hackeraktivitet kan ikke alene tilskrives COVID-19 krisen. Crime as a Service eller CaaS, er hackerens seneste skud på stammen, hvor hackeraktiviteter nu bliver leveret som en service til de kriminelle. Center For Cyber Sikkerhed (CFCS) advarer derfor generelt om et højt trusselsniveau.

Hvis en virksomhed ikke allerede har været udsat for et hackerangreb, er det formentligt kun et spørgsmål om tid før det sker. For at virksomhederne er bedst muligt rustet til et angreb fra hackere, er det nødvendigt med et robust, sikkert og effektivt beredskab, herunder IT-beredskab.

Med IT-beredskab menes her de planer og processer, der skal sikre at virksomheden kan håndtere, afbøde og inddæmme en krise eller katastrofe, der omfatter virksomhedens IT-systemer. Dette indebærer en sikker og forsvarlig nedlukning af virksomhedens systemer og dernæst en kontrolleret genetablering, der er afstemt med forretningen. En fremgangsmåde, som kan sammenlignes

med Regeringens og Folketingets håndtering af COVID-19 krisen.

Mange virksomheder har outsourcet IT-driften og data til eksterne IT-driftsleverandører. Dette medfører at man som virksomhed er afhængig af tilfredsstillende processer hos leverandørerne og, at der er etableret en governance, der sikrer et tilstrækkeligt IT-beredskab hos leverandørerne.

Ved outsourcing til en IT driftsleverandør aftales typisk et SLA-niveau for manglende tilgængelighed til systemer (RTO) og tab af data (RPO). Dette SLA-niveau bør forretningen godkende og evaluere løbende vha. risiko- og konsekvens analyser (Business Impact Assessments) og Gap-analyser. Dette med henblik på at sikre et tilstrækkeligt udgangspunkt for planlægningen af IT-beredskabet og afstemning med forretningens nødprocedurer.

Det aktuelle nyhedsbillede viser også at mange virksomheder har været eller er udsat for angreb, hvor beredskaber, og samarbejder med eksterne leverandører bliver sat på en prøve. Men typisk har virksomhederne på forhånd forberedt sig via løbende gennemførte beredskabstests, der i praksis gennemføres som skrivebordsøvelser, og ofte i et samarbejde mellem IT-driftsleverandøren, forretningen og IT. Formålet med beredskabstests er derfor, at virksomheden gennemfører en simulering af et eller flere aktuelle scenarier som interessenterne kan stifte bekendtskab med, herunder teste deres kendskab til roller og ansvar i en beredskabssituation. Endvidere er formålet at efterprøve om genetableringsplanerne fungerer som tiltænkt, herunder sikre og teste, at backups af systemer mv. kan anvendes.

Men et øvelser, noget andet er når virksomheden står i en virkelig krise eller katastrofe. Her er det ikke altid at alle IT-beredskabets processer og væsentlige risici er adresseret, forberedt eller indbyrdes afstemt,

En intern revision af IT-beredskabets processer kan derfor hjælpe til at belyse virksomhedens "øømme tæer" og bidrage med at styrke virksomheden ift. et robust, sikkert og effektivt IT-beredskab.

Anvendelse af rammeværk for revisionen

Ved planlægningen af revisionen af IT-beredskabets processer er det vigtigt at målrette revisionen til de væsentlige risici. Her kan det være en hjælp at tage udgangspunkt i et anerkendt rammeværk som udgør best practice på området.

DSB er af Trafik-, Bygge- og Boligstyrelsen udpeget som operatør af væsentlige transporttjenester, der er væsentlig for opretholdelsen af kritiske samfundsmæssige eller økonomiske aktiviteter. I den forbindelse er det et krav, at DSB skal certificeres i ISO 27001. Derfor var det nærliggende for os at anvende ISO 27001 standarden for informationssikkerhed som rammeværk for revisionen.

Eftersom revisionen ikke var en compliance revision ift. ISO 27001 var vores udgangspunkt alene at give IT-

ledelsen vores vurdering af, om risici generelt var adresseret og mitigeret ud fra et best practice synspunkt. Men samtidig så vi også en mulighed for at give IT vores vurdering af behovet for evt. styrkelse af compliance i forbindelse med implementeringen af ISO 27001.

Som inspiration til indhold og omfang for revision af det forretningsmæssige beredskab og IT-beredskabet kan der ligeledes med fordel hentes viden hos ISACA eller IIA, der har udarbejdet følgende vejledninger/audit programs:

- IT Continuity Planning Audit Program (ISACA)
- Business Continuity Management Audit Program (ISACA)
- Business Continuity Management - GTAC 10 (IIA)

Revisionens omfang og tilrettelæggelse

Et godt udgangspunkt for fastlæggelse af revisionens fokus og omfang kan f.eks. være en modenhedsvurdering af virksomhedens cyber- og informationssikkerhed samt risiko- og konsekvensvurderinger ift. cyber- og informationssikkerhed på forretningsområder.

Dette bør kombineres med en tæt dialog med de ansvarlige interessenter for IT-beredskabets processer med henblik på at planlægge revisionen mere i detaljer, og tilegne sig et nærmere indblik i væsentlige risikoområder. I DSB blev vi i forbindelse med planlægningen inviteret

med til den årlige test af IT-beredskabsplanen, der foregår i et samarbejde mellem IT-beredskabets interessenter. Endvidere blev vi inviteret med til en af de stikprøvevise tests af tekniske genetableringsplaner (Technical Recovery Plans), der gennemføres for at teste planer for genetableringen af de enkelte systemer.

Fra et revisionsperspektiv er det min vurdering, at der er meget læring og indsigt at hente ved at observere virksomhedens faktiske tests af beredskabsplaner og genetableringsplaner. Jeg kan kun opfordre andre til at deltage i disse tests, som observatør.

Med udgangspunkt i det valgte rammeværk samt ovenstående modenhedsanalyse, risikovurdering, og observationer fra gennemførte tests af beredskabs- og genetableringsplaner, fastlægges revisionens omfang evt. i samarbejde med IT-ledelsen og den eksterne revision. I DSB omfattede revisionen følgende overordnede fokusområder:

- Governance – ledelse af IT-beredskabet
- Hændelse- og krisehåndtering
- Beredskab
- Genetablering (Recovery).

For at målrette indsats og ressourcer til de områder, som skal adresseres i revisionen, kan spørgsmålene i **Tabel 1** herunder, bidrage hertil.

Tabel 1. Spørgsmål der kan bidrage til at målrette indsats og ressourcer

<ul style="list-style-type: none"> • Hvilken governance er tilknyttet virksomhedens IT-beredskab og er der opstillet KPI'er, der løbende måles og rapporteres? • Hvordan sikres, at Disaster Recovery Plan (DRP) løbende bliver opdateret? • Hvordan sikres, at IT-beredskabsplanen forankres rundt til relevante interessenter i organisationen? • Er ansvarsfordelingen i virksomheden helt klar ift. hvem der gør hvad i tilfælde af IT-nedbrud? • Hvordan sikres, at der er overensstemmelse mellem Business Continuity Plan (BCP) og IT Disaster Recovery Plan (DRP)? • Tager Business Continuity planer hensyn til en reetablering, der går ud over de aftalte SLA-krav med IT? • Hvordan sikres, at DRP er i overensstemmelse med virksomhedens IT-sikkerhedspolitik? • Hvordan sikres, at evt. outsourcing til en IT-drift leverandører overholder virksomhedens krav til IT-beredskab? Hvilken assurance opnås i de modtagne revisionserklæringer fra IT-drift leverandøren? • Hvordan sikres en klar ansvarsfordeling mellem virksomheden og IT-drift leverandøren ift. hændelser og beredskab? • Hvordan fører virksomheden tilsyn med og overvåger aktiviteter, der er outsourcet? 	<ul style="list-style-type: none"> • Udfører forretningen risikovurderinger af forretningsapplikationer, herunder fastsættelse af Recovery Point Objective (RPO) og Recovery Time Objective (RTO)? • Håndteres incidents i henhold til retningslinjer? • Hvordan sikres, at opnået læring fra incidents og test af IT-beredskabet bliver håndteret, indarbejdet i processer og kommunikeret til relevante medarbejdere? • I hvilket omfang testes DRP samt er roller og ansvar klart defineret og delegeret? • Hvorledes udvælges testscenarier og tests? Og tager testscenarier hensyn til de nyeste trusseltendenser? • Hvilken træning gennemgår medarbejdere med ansvar for IT-beredskabet? Og hvorledes sikres, at medarbejdere med ansvar for IT-beredskabet er up-to-date ift. til nyeste Cyber tendenser på markedet? • Hvilke recovery muligheder har virksomheden? Hvorledes testes disse? • Hvordan sikres, at virksomheden hurtigt og ukompliceret kan reetablere sine systemer ved eventuelle nedbrud? • Hvilken og til hvilke interessenter tilgår kommunikation i tilfælde af en katastrofe? Er der udarbejdet en kommunikationsstrategi?
--	---

Figur 1 nederst på siden illustrerer et eksempel på en række fokusområder med tilhørende underkategorier, som kan være relevante at adressere i revisionen med henblik på at understøtte en systematisk og målrettet tilgang.

Revisionens gennemførelse

Revisionen kan gennemføres vha. forskellige revisionsteknikker og jeg har på basis af vores erfaringer oplistet nogle eksempler herpå.

Med henblik på at opnå forståelse for og vurdere design og implementering af IT-beredskabs processer og procedurer, herunder identificere iboende risici/kontrolmål samt udvalgte implementerede kontroller og aktiviteter, vil interviews af udvalgte interessenter fra IT, forretningen og IT-Sikkerhed samt gennemgang af relevant underliggende dokumentation være et godt udgangspunkt for revisionen.

Med udgangspunkt i de udarbejdede beredskabs- og genetableringsplaner, herunder IT-beredskabsplanen, vurderes planernes tilstrækkelighed, indre sammenhænge, rækkefølge for genetablering og afstemning i forhold til forretningens beredskabsbehov.

En stikprøvevis gennemgang af udvalgte tekniske systemspecifikke genetableringsplaner kombineret med interviews af IT og forretningen vil kunne bidrage til at afdække og vurdere tilstrækkeligheden i sammenhænge til andre systemer og den samlede genetableringsplan.

Herudover foretages en stikprøvevis gennemgang af virksomhedens gennemførte tests af tekniske systemspecifikke genetableringsplaner, herunder en vurdering af rap-

porteringen af tests, evt. fra en IT-leverandør med henblik på at vurdere tilstrækkeligheden i virksomhedens opfølgning på og håndtering af output fra disse tests.

Særlige fokusområder i revisionen

Der bør generelt være et særligt fokus på iboende risici, og mitigerende heraf, for at sikre en robust, opdateret, og operationel beredskabsplan, f.eks. i forhold til kommunikation og samarbejde mellem IT og forretningen. Her vil ansvaret for beredskabet typisk være todelt i et forretningsmæssigt og IT-mæssigt ansvar, men disse bør hænges sammen.

En potentiel konsekvens ved et utilstrækkeligt samarbejde omkring beredskabet er, at IT-beredskabet ikke i tilstrækkeligt omfang understøtter forretningens forventninger til at kunne genetablere tilgængeligheden til IT-systemer. Dette kan medføre at nødprocedurer ikke er tilstrækkelige ift. at kunne fortsætte de forretningsmæssige processer. Derfor er det essentielt, at der er udarbejdet og implementeret procedurer og kontroller for samarbejder omkring beredskabet, herunder bl.a. løbende gennemførelse af Business Impact analyser og gap-analyser.

Et andet væsentligt fokusområde omfatter den tekniske genetablering af virksomhedens systemer, herunder dokumentation og vedligeholdelse af genetableringsplaner samt udvælgelse og test heraf. Utilstrækkelige processer og kontroller kan medføre forsinkelser i genetableringen af systemer, manglende understøttelse af organisationens nødplaner samt en risiko for at væsentlige eller kritiske systemer ikke bliver testet tilstrækkeligt og hyppigt nok.

Figur 1. Eksempel på en række relevante fokusområder



Ved ISO henvisning refereres til ISO 27001 og 27002

I de tilfælde hvor virksomheden har outsourcet IT-driften af systemerne, er det vigtigt at have fokus på indholdet i de rapporteringer, som virksomheden modtager fra leverandøren i forhold til test af IT-beredskabet samt tekniske genetableringsplaner, herunder de observationer og mangler der er konstateret ved tests. Utilstrækkelig kontrol og opfølgning herpå kan medføre at identificerede svagheder ikke bliver prioriteret og udbedret i den rækkefølge, som virksomheden ønsker og dermed skaber usikkerhed omkring en tilstrækkelig og sikker genetablering.

Opsummering

Revision af beredskabet, herunder IT-beredskabet er et vigtigt område, som Interne revisioner bør have fokus på. Det bør således være i alles interesse at være så godt rustet som muligt - især i disse tider, hvor intet er som det plejer at være. Stigningen i de IT-kriminelles handlinger og angreb på virksomheder gør ligeledes dette fokus højaktuelt. En revision af beredskabet vil tillige understøtte det fokus, som bestyrelser bør anlægge og fastholde ifølge "Anbefalinger til Styrkelse af Cyberkompetencer" for bestyrelser udgivet af Center For Cybersikkerhed (CFCS) sammen med bl.a. Bestyrelsesforeningen.

Vores erfaring med revision af IT-beredskabet har vist, at det er vigtigt at være forberedt og få planlagt revisionens fokusområder i et tæt samarbejde med interessenterne, samt at observere de beredskabstests, som virksomheden måtte afholde. Tillige har vores erfaringer vist at det er vigtigt at have en løbende konstruktiv dialog og kommunikation med interessenterne forud, under og efter revisionen. Derved opnåede vi en vigtig indsigt samt buy-in til revisionen og dens resultater.



COVID-19 - Indvirkning på Intern revisions arbejde



Lars Geisler, Afdelingsdirektør,
Nykredit

Indledning

Det er nok de færreste af os, der i vores vildeste fantasi har forestillet sig et forår som dette med en global viruspandemi og økonomisk krise til følge. Vores hverdag blev med et forandret.

Men hvordan har COVID-19 egentlig påvirket vores profession? Det tænkte vi i redaktionen kunne være interessant at få belyst. Jeg har derfor kontaktet 20 revisionschefer fra finansielle virksomheder, det offentlige og industrien og stillet dem følgende spørgsmål:

1. Har I kunnet gennemføre det planlagte revisionsarbejde på trods af COVID-19 ?
2. Har COVID-19 bevirket, at I har måttet ændre jeres revisionsplaner, som følge af et ændret risikobillede (emerging risks) ?
3. Har I som følge af COVID-19 draget jer nogle erfaringer, som vil påvirke den fremtidige arbejdsform i jeres afdeling ?

Jeg har modtaget i alt 17 svar. Tak for jeres opbakning og bidrag til artiklen. De modtagne svar giver formentlig en meget god temperaturmåling på påvirkningen, selvom der selvfølgelig er forskelle mellem revisionsafdelingerne. Herunder har jeg sammenfattet tendenserne i de modtagne svar.

Påvirkning af revisionsarbejdet

Generelt set ser det ud til, at de interne revisionsafdelinger er sluppet godt igennem det første halvår i 2020. De fleste svarer, at deres revisionsplan i al væsentlighed har kunnet gennemføres.

En del har dog konstateret forsinkelser på grund af længere svartider fra auditees, som har været travlt beskæftiget med Corona-relaterede opgaver, medens forsinkelse i andre tilfælde skyldes øget ferieafholdelse og afspadsering blandt medarbejderne i Intern revision og auditees.

Nogle afdelinger har byttet rundt på planlagte revisionsopgaver som følge af, at fysisk tilstedeværelse er påkrævet på nogle opgaver eller for at skåne auditees, som i en periode var meget presset. Enkelte revisionsafdelinger har været nødt til at revurdere deres revisionsplan og udskyde eller helt fravælge revisioner i lavrisiko områder.

Andre har fastholdt deres revisionsplan, men har måtte justere i scope på den enkelte opgave – ikke nødvendigvis på grund af 'nød', men også som følge af ændrede risici.

En revisionsafdeling med normal høj rejseaktivitet har været nødsaget til at genoverveje revisionsplanen på grund af rejserestriktionerne. Det har derfor været nødvendigt at foretage tilpasninger til revisionsplanen for at imødekomme den nye virkelighed.

Ændring af revisionsplan som følge af ændret risikobillede

Af de modtagne svar fremgår det, at de fleste revisionsafdelinger har foretaget en vurdering af risikobilledet i deres organisation, men at det i varierende grad har påvirket revisionsplanen. Mange har haft fokus på, om det interne kontrolsystem fortsat har fungeret enten i form af interviews, test af nøglekontroller eller drøftelser med risikostyrings- og compliancefunktionen. Nogle organisationer har været nødt til at ændre visse processer og kontroller, hvilket har påkaldt sig Intern revisions opmærksomhed. En revisionsafdeling har fået forskellige forretningsenheder til at udarbejde memoer om deres Corona-håndtering.

En del afdelinger har fulgt det etablerede beredskab tæt, og enkelte har også foretaget test heraf. Flere har også haft fokus på cyber-sikkerheden primært som følge af, at medarbejderne har arbejdet hjemmefra. En revisionschef beskriver arbejdet hermed således:

Emerging risks forårsaget af COVID-19 pandemien, vurderes løbende med input fra relevante stakeholders. Som eksempel kan bl.a. nævnes den potentiel øgede risiko for besvigelser, herunder cyber fraud, da kriminelle forsøger at udnytte COVID-19-pandemien. Derudover afsøger vi også de nye risici, der er forbundet med data og data sikkerhed. Med den nye tendens, hvor medarbejderne arbejder hjemmefra, kræves der forhøjet fokus på data-tilgængelighed/adgang og lagring af data. Medarbejdere arbejder nu potentielt med følsomme data i mindre sikrede hjemmebaserede arbejdsmiljøer. Dette er et område, som IT-revisorerne har fokus på.

Endvidere foreligger en emerging risk, at interne kontroller ikke udføres tidsmæssigt og i samme kvalitet når medarbejdere arbejder på distancen. Dette er et forhold, som bl.a. de interne finansielle revisorer har haft fokus på i forbindelse med udførelse af deres revisioner.

Den fremtidige arbejdsform

Næsten samstemmende skriver revisionscheferne, at erfaringerne vil påvirke den fremtidige arbejdsform, selvom ikke alle har draget endelige konklusioner endnu. Erfaringerne er todelt, idet der både er forholdet til medarbejderne og til auditees.

Generelt lægges der op til en større fleksibilitet for medarbejderne, end der har været før.

En revisionschef skriver: "Mennesker er forskellige, og vi har nu mulighed for at optimere arbejdssituationen for den enkelte", og en anden, at det giver endnu bedre muligheder for 'work-life-balance' for medarbejderne. Grunden til den større fleksibilitet er, at hjemmearbejdet ikke behøver at gå ud over effektiviteten. Nogle vurderer, at hjemmearbejde faktisk kan forbedre effektiviteten bl.a. på grund af tidsbesparelse ved reduceret rejseaktivitet, og fordi medarbejderne kan arbejde mere koncentreret.

Samtidig påpeger en anden, at "vi stadig finder, at den fysiske tilstedeværelse styrker samarbejdet og sammenhængskraften i en afdeling". Endelig skriver en revisionschef, at der er "større krav til ledelse, når der skal ledes over afstand. Det er en anderledes måde at opsætte mål og forventninger samt løbende sparring. Dels for at opgaverne løses mest effektivt med den ønskede kvalitet, men også til gavn for den enkelte medarbejders arbejdsglæde og udvikling."

Selvom det har fungeret med at holde møder med auditees via Teams, Skype eller lignende, og at det formentlig fremover også vil blive benyttet i større omfang end før COVID-19, skriver nogle revisionschefer, at anvendelsen af virtuelle møder med auditees bør anvendes med omhu.

En revisionschef har draget sig følgende erfaringer:

- "Udveksling af synspunkter foregår bedre ved fysiske møder end de virtuelle. Jo større observationer/issues des større behov for fysisk møde.
- De reviderede kan håndtere at blive revideret på af-

stand. Vigtigt at der findes den rette balance mellem at revidere på afstand og være fysisk tilstede.

- Den lange periode med hjemmearbejde har vist, hvor IT-data-drevne processerne egentlig er. Det bør give revisionen nogle større muligheder i forhold til data mining osv. Mere automatiserede revisionsprocesser."

En anden revisionschef skriver:

- "Det er sværere at skabe dialog om komplekse og/eller omfattende forhold via telekonferencer.
- Møder (med spørgsmål til / interaktion med de reviderede) og revisionshandlinger skal planlægges omhyggeligt. Formål og spørgsmål skal udsendes inden mødet.
- Der skal under revisionsmøder, som ikke gennemføres som fysiske møder, være stor fokus på at sikre forståelse mellem revisionen og de reviderede, da manglende fysisk møde begrænser muligheden for at opfange misforståelser parterne imellem.
- Konklusioner fra møderne bør afstemmes umiddelbart efter, disse er gennemført.
- Det kan godt lade sig gøre at udføre revision "på distancen"."

Afrunding

COVID-19 har udfordret Intern revision som profession på flere fronter: medarbejdertrivsel, ledelse, agilitet, kvalitet, teknik, håndtering af auditees, nye forventninger fra stakeholdere mv. Hver enkelt revisionsafdeling har gjort sig sine egne erfaringer, men det er oplagt at lade sig inspirere af kollegaer i vores profession, som jeg håber, at denne artikel kan medvirke til.



COVID-19 & Intern revision



Lea Kehlet Halsø, Intern revisor,
PFA Pension

I artiklen her vil jeg give dig en introduktion til, hvor du kan søge inspiration, læse artikler og nyheder om COVID-19 i forhold til intern revisors virke samt rolle og ansvar i en verden med pandemier.

IIA Global forsøger løbende at give medlemmerne seneste nyheder, artikler og overskrifter om pandemien og dens indflydelse på medarbejder, organisationer og branchen.

Derudover har de også i april 2020 foretaget en undersøgelse af COVID-19's indflydelse på Intern revision, som er ret interessant. I undersøgelsen har man forespurgt 400 revisionschefer og direktører om COVID-19's indflydelse på Intern revision. Næsten 40% svarede at under pandemien har medarbejdere i intern revision assisteret deres forretningen med ikke-revisionsmæssigt arbejde. 40% tilføjet nye opgaver pga. COVID-19, og 75% har opdateret deres revisionsplaner for at adressere risici relateret til COVID-19. Derudover har mere end halvdelen af respondenterne afbrudt eller reduceret omfanget af planlagte revisionsopgaver, og næsten halvdelen har annulleret planlagte revisionsopgaver.

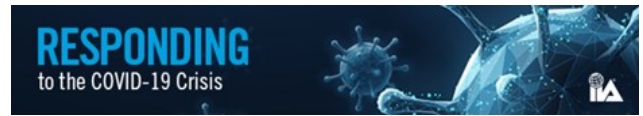
Se resultaterne af undersøgelsen her:

<https://dl.theiia.org/AECPublic/COVID-19-Quick-Poll-Results-April-17-2020.pdf>

På websiden **COVID-19 Newswire** (<https://iaonline.theiia.org/2020/Pages/COVID-19-Newswire.aspx>) opdateres løbende seneste nyt, og her finder du også links til følgende artikler:

- Assessing Risk in a Post-pandemic World
- Beware the Coronavirus Scams
- COVID-19: The Ultimate Governance Challenge
- Exploiting the Crisis
- Innovation in a Time of Crisis
- Navigating the Crisis
- Responding to the Crisis
- Six Tips for Auditing From Home
- Testing the Boundaries
- The Virtual Audit
- Update: Recovery Through Digitization
- Update: The Pressure of Pandemics.

Jeg vil kort give en introduktion til nogle af dem og hvorfor disse kan være interessante at læse.



Assessing Risk in a Post-pandemic World

Artiklens hovedformål er, at den revisionsplan, der eksisterede før pandemien, er baseret på et gammelt risikobillede. Revisionscheferne skal tænke anderledes ifht. deres organisations risici og hvordan de kan omfordele revisionsressourcer. I artiklen er der opstillet en række spørgsmål som IIA Global og artiklens forfatter mener revisionscheferne bør stille sig selv, når de revurderer deres revisionsplaner som følge af COVID-19.

Forfatteren af artiklen er klart af den holdning, at revisionsplanen som følge af COVID-19 vil og bør ændre sig, da COVID-19 grundlæggende har ændret risikobilledet for mange virksomheder og organisationer.

COVID-19: The Ultimate Governance Challenge

Virksomheder kæmper for at forstå, hvad deres nye risici er, og hvordan man ændrer forretningsprocesser for at holde disse risici på et acceptabelt niveau, og her spiller intern revision en vigtig rolle. Artiklen sætter fokus på, at Intern revisions opgave er at udføre kritiske vurderinger af nye risici, bruge dataanalyse til at opbygge overvågningsværktøjer og rådgive ledelse om mulige ændringer i forretningsprocesser. Dette er noget intern revision allerede gør, men det er nu vigtigere end nogensinde for at guide og assistere virksomheden, når COVID-19 fortsætter.

Six Tips for Auditing From Home

Hjemmearbejde er blevet en realitet for mange interne revisorer, artiklen beskriver med seks eksempler, hvordan man kan forblive produktiv:

1. Opret et hjemmekontor
2. Agér professionelt
3. Udnyt Cloud teknologier
4. Sikre fortrolighed
5. Planlæg og kommunikér
6. Anerkend klienternes udfordringer.

The Virtual Audit

En vellykket virtuel revision kræver, at revisoren anerkender og adresserer måden, hvorpå revisionsopgaven adskiller sig fra den traditionel revision, hvor de involverede parter er fysisk tilstede. Virtuel eller "fjern"-revision er ikke nødvendigvis et nyt koncept, men når alle arbejder på denne måde samtidig, er man i langt højere grad tvunget til at vurdere, hvordan man gør dette bedst. Artiklen giver læseren nogle overvejelser til vejledning af den virtuelle revision.



**IIA Årsmøde flyttes til
18.05.2021 - 19.05.2021
på Hotel Comwell, Kolding
Sæt kryds i kalenderen**

Internal Audit's Role in Board and Executive Committees



Vanita Shukla Hork, CIA, Chief Expert, L&D, Marketing and Communications, Group Internal Audit, Nordea

Introduction – IIA Position Paper

The Institute of Internal Auditors (The IIA) regularly publishes Position Papers, for informational and educational purposes. Position Papers address key issues of interest to both stakeholders and practitioners of internal auditing, with the aim of promoting sound governance and offering insights into Internal Audit's important role in improving governance at all levels of the organisation.

In this article, I will present the key points in the IIA Position Paper, 'Internal Auditing's Role in Governing Body/ Executive Committees¹', and illustrate with examples from Nordea Group Internal Audit (GIA), where relevant and appropriate.

What role can Internal Audit play?

The Position Paper starts by establishing clearly that the value that Internal Audit can bring to an organisation is greatly influenced by how broadly or narrowly the Board ('governing body') and senior management view the scope of its work.

Internal Audit adds value by providing an enterprise-wide perspective; by applying a variety of critical skills; and by providing independent assurance and advice. Inviting Internal Audit to participate in Board and executive committees in an advisory capacity enables it to provide value in these meetings.

Internal Audit can participate in, strengthen and support any number of permanent or special Board or senior management committees, for example, Risk Committee, Technical (IT) Committee and Performance Evaluation Committee, to name a few.

In Nordea, the Chief Audit Executive (CAE), Chief Internal Auditors and other senior audit managers in GIA participate in relevant Board and executive committees. For example, the CAE participates in Nordea's Board Risk Committee and Board Audit Committee at every meeting, and in other relevant committees and meetings, such as the Board Remuneration Committee and Nordea Leadership Team (executive management) meetings on an ad-hoc basis, depending on the agenda.

However, the Position Paper emphasises that it is critical that the organisation first considers *how* Internal Audit would operate within these committees, including clearly defining Internal Audit's role and setting proper precautions to protect its continued independence and objectivity.

To support the decision to invite Internal Audit to committee meetings, the Board can encourage input from both management and Internal Audit regarding which committees would benefit most from Internal Audit's participation.

Useful roles for Internal Audit could be:

- Observer or invitee
- Contributor or participant
- Consultant or advisor
- Educator
- Subject matter expert.

In Nordea, GIA has the role of observer or invitee (only), when participating in Board or management committees.

Be clear on the objectives

As mentioned above, it is important that the Board is clear about the objectives for having Internal Audit participate in such committees, and precautions must be taken to maintain Internal Audit's independence.

There are many benefits for the organisation by involving Internal Audit in committee meetings. Internal auditors are willing to ask difficult questions; they can raise the level of discussion and debate on challenging issues; and they can contribute with specific knowledge in key areas.

The benefits of participation are also significant for the Internal Audit function. For example, participation helps reinforce a proactive role for the function; Internal Audit gets exposure to the organisation's priorities, emerging risks and corporate strategies, and thereby improves its knowledge of the business; the function improves its understanding of the management decision-making process, which encourages better communications; and finally, participation in committees improves overall relationships with the Board and executive management.

However, all these benefits must be weighed against any perceived or real impairment of Internal Audit's independence and objectivity. In addition, the CAE and the Board must be mindful of any perceived or real conflicts of interest created by participation in committees.

Precautions and safeguards

The Position Paper gives several examples of precautionary measures and safeguards to protect against conflicts of interest or impairing Internal Audit's independence and objectivity. For example:

- Internal Audit should not participate in decision-making in committee meetings.

- Internal Audit must always comply with relevant IIA Standards, including IIA Standard 1112: Chief Audit Executive Roles Beyond Internal Audit.
- Internal Audit must adhere to The IIA's Code of Ethics.
- Internal Audit's role on committees should be clearly delineated in the Internal Audit charter.
- The audit committee should guide the extent of Internal Audit's participation.
- All proceedings should be reported to the audit committee.
- Internal Audit's contributions are in the form of questions and insights, not conclusions or advocacy.

In Nordea, GIA's charter (which is approved by the Group Board) states that GIA has the right to *attend and observe* Group Board committees, executive management meetings, overall committees and fora for the Nordea Group, and other key management decision-making fora when relevant and necessary.

Furthermore, GIA's charter clearly states that the work of GIA shall, amongst other things, conform to the definition of internal auditing and comply with the Code of Ethics and the Standards for the International Professional Practice of Internal Auditing issued by the IIA. GIA's Quality Assurance (QA) function self-assesses on an annual basis GIA's conformance with the IIA Standards and Code of Ethics.

Finally, the charter also stipulates that GIA should be present at appropriate governing bodies, including the Board Audit Committee, and any other Board Committees as appropriate.

GIA's involvement in such committees and fora is further delineated in GIA's operations manual, which states, amongst other things:

- Committee attendance should be subject to a yearly review by GIA's executive management, or more frequently, as deemed necessary.
- In all cases GIA's role should be clearly defined in advance of attendance, and GIA should remain in a non-voting capacity in order to ensure GIA's independence is maintained.
- GIA staff are expected to either participate in the respective committees periodically or on an ad-hoc basis when relevant, and/or obtain access to committee material as deemed necessary, to stay informed about the activity in the committee.

5 questions to be asked

The Position Paper reiterates that inviting Internal Audit to participate in Board and management committees is a major step for an organisation, to be taken carefully with proper preparations and a thorough understanding of the risks and benefits.

According to the Position Paper, the Board and management should ask the following 5 questions:

1. What is Internal Audit's current scope of work, and how does that affect its ability to provide advisory services to Board and executive committees?
2. What is the audit committee's view on Internal Audit serving on Board and executive committees?
3. What precautions are in place to protect Internal Audit's independence and objectivity?
4. What precautions are in place to keep Internal Audit out of the decision-making process?
5. Will Internal Audit's participation impair its ability to audit the committee's work in the future?

Other concerns

In addition to the above five questions, there are practical considerations influenced by whether the organisation's Internal Audit function is a fully in-house activity, is co-sourced, or is fully outsourced.

In a co-sourced or outsourced relationship, participation of Internal Audit or the CAE in Board and executive committees might result in inviting outsiders into the boardroom.

In cases where the CAE or equivalent head of audit is an outsourced position, the IIA recommends that the organisation carefully weighs the benefits of participation in Board/executive meetings because of potential confidentiality concerns.

Summary – key takeaways

Internal Audit adds value to an organisation via an enterprise-wide perspective, varied critical skills, as well as independent assurance and advice that support healthy transparency in risk management processes. Participation in Board or executive committees positions Internal Audit well in providing such value.

Internal Audit can strengthen and support any number of permanent or special committees of senior management and the Board, for example the Risk Committee or a Technology (IT) Committee.

However, the organisation and Board must first consider how Internal Audit would operate within these committees, including clearly defining Internal Audit's role and setting proper precautions to protect its continued independence and objectivity.

In cases where the CAE or the equivalent head of audit is an outsourced position, the IIA recommends that the organisation carefully weighs the benefits of Internal Audit participation in Board or executive meetings with potential confidentiality concerns.

Notes

¹Internal Auditing's Role in Governing Body/Executive Committees, The Institute of Internal Auditors, January 2019

Revision af pengeinstitutters foranstaltninger mod markedsmisbrug og insiderhandel – en praktisk tilgang



Ulrich Rasmussen, Seniorspecialist, Nykredit

Indledning

Det er tanken med artiklen, at give revisorer input til brug for revision af institutters håndtering af EU-krav vedrørende "Forebyggelse og afsløring af markedsmisbrug", der udspringer af artikel 16 stk. 2 i markedsmisbrugsforordningen (MAR, EU. 596/2014), samt krav fra Kommissionens delegerede forordning afsnit 2-5 (EU 2016/957). Artiklen er ikke en udtømmende gennemgang, men indeholder erfaringer fra udført revision og Finanstilsynets temaundersøgelse fra foråret 2019. Det er et krav, at intern revision årligt gennemfører en revision på markedsmisbrugsområdet i de pengeinstitutter, som er omfattet af krav til værdipapirhandlere.

MAR 16.2

"En person, der som led i sit erhverv organiserer eller gennemfører transaktioner, skal indføre og opretholde effektive ordninger, systemer og procedurer med henblik på at afsløre og indberette handelsordrer og transaktioner. Når den pågældende person har begrundet mistanke om, at en handelsordre eller transaktion vedrørende et finansielt instrument, hvad enten denne placeres eller afvikles på eller uden for en markedsplads, kunne udgøre insiderhandel, markedsmisbrug eller forsøg på insiderhandel eller markedsmisbrug, skal personen straks underrette den i stk. 3 omhandlede kompetente myndighed."

Ordningerne skal, jf. den delegerede forordning (se herunder), sikre "effektiv og løbende overvågning af alle modtagne ordrer og alle gennemførte transaktioner med henblik på at forebygge, afsløre og identificere insiderhandel, markedsmisbrug og forsøg på insiderhandel eller markedsmisbrug".

Delegeret forordning (EU 2016/957) artikel 2-5

- Generelle krav (artikel 2)
- Forebyggelse, overvågning og afsløring (artikel 3)
- Uddannelse (artikel 4)
- Indberetningsforpligtelser (artikel 5)

Det er vigtigt at være opmærksom på, at det ikke kun er udførte handler, der er omfattet, men også ordrer, som ikke nødvendigvis har medført en handel. Dette indebæ-

rer, at såvel ændrede og annullerede ordrer/handler er omfattet. Artiklens primære fokus er artikel 2-4 og omhandler ikke-konkrete indberetninger til Finanstilsynet (artikel 5) vedrørende mistanke om insiderhandel eller markedsmisbrug.

Finanstilsynets temaundersøgelse

Finanstilsynets temaundersøgelse omfattede institutternes:

- Ordninger og systemer (markedsovervågning og systemunderstøttelse)
- Procedurer (forretningsgange)
- Træning og uddannelse af medarbejdere
- Intern rapportering og kontrol (compliance og intern revision)
- Sagsbehandling og underretninger til Finanstilsynet.

Til brug for temaundersøgelsen i foråret 2019 udbad Finanstilsynet bl.a. institutterne om at redegøre for:

- forretningsaktiviteternes omfang
- anvendte overvågningssystemer (og alarmopsætning)
- procedurer for gennemgang af alarmer
- hvordan institutterne sikrer, at overvågningsfunktionerne er passende i forhold til instituttets aktiviteter.

Kendskab til forretningen og forretningsomfang

I forbindelse med revisors planlægning og risikovurdering bør revisor indledningsvis tage kontakt til forretningen og undersøge, om man i forbindelse med etableringen af overvågningen har skabt overblik over:

- 1) Hvilke typer af ordrer/handler (transaktioner) instituttet har, som er omfattet af MAR
- 2) Forretningsomfang (antal transaktioner og volumen) og kompleksitet
- 3) Risikovurdering af handelstransaktioner og krav til overvågning.

1. Hvilke finansielle instrumenter er omfattet

Det fremgår af MAR (artikel 2), at det er instrumenter, der er optaget på et reguleret marked, MHF (multilateral handelsfacilitet) og OHF (organiseret handelsfacilitet), som er omfattet af forordningen. Derudover er visse derivater ligeledes omfattet (artikel 2.1.d).

Kortlægningen af hvilke typer transaktioner, der er relevante for instituttet, skal sikre, at alle relevante finansielle instrumenter omfattes af overvågning. Typen af det finansielle instrument er også relevant for instituttet, når det skal vurderes hvilken overvågning, der skal etableres, idet der er forskel på, hvor stor risikoen er for, der sker insiderhandel og markedsmisbrug for de enkelte instrumenttyper. Der kan eksempelvis argumenteres for, at FX-transaktioner kan undtages for den automatiserede markedsovervågning af markedsmisbrug, såfremt en risikovurdering viser, at det ikke er sandsynligt, at disse handler kan påvirke markedet.

2. Forretningsomfang og kompleksitet

Det er ikke nødvendigvis et krav, at der sker automatiseret overvågning af alle transaktioner. Det er dog et krav i den delegerede forordning (2.5), at:

"Personer, der som led i deres erhverv planlægger eller gennemfører transaktioner, markedsoperatører og investeringselskaber, der driver en markedsplads, skal sikre, at de i stk. 1 og 3 omhandlede ordninger, systemer og procedurer:

- a) er passende og står i et rimeligt forhold til deres forretningsaktiviteters omfang, størrelse og art
- b) vurderes regelmæssigt, som minimum i forbindelse med en årlig revision og intern kontrol, og opdateres om nødvendigt
- c) er genstand for tydelig skriftlig dokumentation, herunder eventuelle ændringer eller opdateringer heraf, med henblik på at sikre overensstemmelse med denne forordning, og at de dokumenterede oplysninger opbevares i en periode på fem år."

Revisor skal derfor påse, at der er udarbejdet skriftlig dokumentation, der overholder kravene i den delegerede forordning (2.5), herunder at den revurderes årligt, samt at der udføres intern kontrol. Ved gennemgangen skal revisor vurdere, om den etablerede overvågning er tilstrækkelig set i forhold til forretningsaktiviteterne.

3. Risikovurdering af handelstransaktioner og krav til overvågning

De fleste institutter har transaktioner, hvor instituttet ikke selv foretager handel på markedspladsen, men handler udføres af brokere, eksempelvis som led i porteføljevaltningsaftaler. Institutterne har i disse tilfælde "organiseret handlen". Derudover er der handelstransaktioner, hvor instituttet selv gennemfører handel på markedspladsen, eksempelvis OMX Nasdaq, enten på vegne af sig selv eller som led i en ordre fra en kunde. Der kan derfor være forskel på hvilken risiko der er, for at instituttet medvirker til insiderhandel eller markedsmanipulation.

Når instituttet foretager en risikovurdering af, hvor stor risikoen er for at udføre eller medvirke til insiderhandel og markedsmanipulation, er der en række faktorer, der er relevante. Ved vurderingen af hvilke ordninger, systemer og procedurer, der er passende, skal instituttet bl.a. forholde sig til:

- Antallet af transaktioner
- Det marked hvor instrumenter handles (eksempelvis værdipapir- og valutamarkedet)
- Hvilken rolle instituttet har ved handlen
- Hvordan ordrer håndteres (modtages, opbevares, udføres)
- Hvor handler gennemføres (på eller uden for en markedsplads)
- Hvordan handler udføres (telefon, chat, elektronisk handelsplatform).



Den delegerede forordnings artikel 3.1 stiller krav om, at ordninger, systemer og procedurer skal:

"a) muliggøre individuelle og sammenlignende analyser af enhver transaktion, som gennemføres, og ordre, som afgives, ændres, annulleres eller afvises i markedspladens systemer, og i forbindelse med personer, der som led i deres erhverv planlægger eller gennemfører transaktioner, også uden for en markedsplads

b) udløse varslinger om aktiviteter, som kræver yderligere analyser med henblik på at afsløre eventuel insiderhandel, markedsmanipulation eller forsøg på insiderhandel eller markedsmanipulation

c) omfatte samtlige handelsaktiviteter, som de pågældende personer udfører."

Revisor skal derfor påse, at institutterne har udarbejdet dokumentation for, hvordan de anvendte ordninger, systemer og procedurer – under hensyntagen til instituttets forretningsaktiviteters omfang og art – er compliant med den delegerede forordnings artikel 3.

Etablering af passende og effektiv overvågning

Ved vurdering af, om der er etableret passende overvågning, kan revisor eksempelvis vurdere, om:

- A. Overvågningen er passende i forhold til forretningsaktiviteter
- B. Alle transaktioner er omfattet af overvågning
- C. Der er etableret tilstrækkelig funktionsadskillelse
- D. Overvågningssystemer indeholder tilstrækkelige oplysninger og alarmer er kalibreret hensigtsmæssigt
- E. Personer der udfører overvågning har tilstrækkelige kvalifikationer
- F. Der er etableret procedurer for sagsbehandling af alarmer
- G. Der er udført tilstrækkeligt arbejde i 2. line (compliance)

A. Passende overvågning

Overvågningen skal overholde den delegerede forordnings afsnit 2-5. Det vil typisk være et krav, at overvågningen er systemmæssigt understøttet og er automatiseret, idet der typisk er mange transaktioner i de fleste institutter, hvor det vil være vanskeligt at etablere passende overvågning ved manuel kontrol.

B. Fuldstændighed

Revisor bør sikre sig, at instituttet – ud over at have kortlagt hvilket typer af transaktioner der er omfattet – kan dokumentere, at transaktionerne er omfattet af overvågning.

Finanstilsynet udstedte bl.a. påbud om, at institutter skal sikre, *"at markedsovervågningen dækker alle ordrer, uanset hvordan instituttet modtager, videresender og afgiver ordrer. Det indebærer, at institutter systematisk ud fra en proportionalitets- og risikobaseret tilgang, skal overvåge*

ordrer, de modtager, videresender og afgiver telefonisk, pr. e-mail, via chatforum eller lignende". Revisor skal sikre, at disse kilder er omfattet af overvågning, når man vurderer, om alle relevante transaktioner er omfattet.

Instituttet bør endvidere have procedurer, der sikrer, at fuldstændigheden af overvågningen kontrolleres periodisk og mindst én gang årligt.

C. Funktionsadskillelse

Revisor skal sikre, at markedsovervågningen er tilrettelagt med en tilstrækkelig funktionsadskillelse. Ud over adskillelse mellem de 3 forsvarslinjer, skal der være organisatorisk funktionsadskillelse i 1. line mellem personer, der udfører eller organiserer handel, og markedsovervågningsfunktionen.

D. Effektivitet af overvågning

For at sikre en effektiv overvågning er der behov for at have en række datakilder til rådighed. Eksempelvis oplysninger om ordre- og transaktionsdata, instrumentdata, kundeoplysninger, priser, regnskabsnyheder m.v. Der er således behov for både markedsdata og kundedata til brug for etablering af en effektiv overvågning.

Overvågningssystemet Nasdaq SMARTS (efterfølgende skiftet navn til Nasdaq Trade Surveillance) fra OMX Nasdaq er meget udbredt i danske banker. Systemet indhenter automatisk handelsoplysninger direkte på OMX Nasdaq, men der er endvidere behov for at tilføje yderligere data fra pengeinstitutets egne systemer, eksempelvis regnskabsdata, kundedata og handler, som ikke er udført direkte i markedet.

På tidspunktet for temaundersøgelsen var det Finanstilsynets vurdering, at de institutter, der anvendte SMARTS overvågning, der var i drift hos datacentralen BEC, ikke



udførte tilstrækkelig overvågning af insiderhandel for handler i udenlandske værdipapirer. Institutterne modtog derfor påbud om at udbygge overvågningen for disse instrumenter. SMARTS har efterfølgende tilkøbt yderligere data, som gør brugerne i stand til at etablere effektiv overvågning.

Effektiviteten af overvågningen afhænger desuden af, at de alarmer, der er taget i anvendelse, er hensigtsmæssige i relation til instituttets produkter og de forskellige kundetyper handelsadfærd.

Finanstilsynet bad ved temaundersøgelsen institutterne om at redegøre for, hvordan alarmerne er passende til de forskellige kundetyper, og hvordan man håndterer risikoen for, at alarmerne overser mistænkelige forhold i værdipapiraktiviteten.

Revisor skal således påse, at der med udgangspunkt i udbudte produkter og institutternes kunders adfærd er etableret alarmer, der vil fange tegn på insiderhandel og markedsmanipulation, og alarmernes kalibrering bør revideres mindst én gang årligt.

E. Uddannelse og kvalifikationer

Det fremgår af MAR-fordringens artikel 4, at personale, der deltager i overvågning, afsløring og identifikation af handelsordrer og transaktioner, som kunne udgøre markedsmanipulation, insiderhandel eller forsøg på markedsmanipulation eller insiderhandel, skal have en tilstrækkelig og relevant uddannelse. Finanstilsynet bad institutterne om at redegøre for, hvem der er involveret i overvågning, hvilken træning de havde modtaget og hvilket uddannelsesmateriale, der anvendes i markedsovervågningsfunktionen.

Opfølgning på alarmer kan være kompleks og kræver indgående viden om markedet. Revisor skal derfor efterprøve, at instituttet har procedurer, der sikrer, at personalet er tilstrækkeligt kvalificeret.

F. Sagsbehandling

Finanstilsynet lagde endvidere vægt på, hvilke omstændigheder og kriterier institutterne lagde til grund ved vurderingen af, om en alarm henlægges eller undersøges nærmere.

Revisor skal påse, at der er etableret procedurer for, hvordan sagsbehandlingen af mistænkelige transaktioner og handelsordrer udføres i praksis. Proceduren skal sikre, at der udføres tilstrækkelig sagsbehandling, samt at den udføres ensartet. Der bør endvidere foretages stikprøvevis intern kontrol i 1. line med, at sagsbehandlingen er udført i henhold til vedtagne procedurer.

G. Anvendelse af 2. lines arbejde

Compliancefunktionen er ikke eksplicit nævnt i MAR, men risiko for markedsmisbrug for institutter, der foretager værdipapirhandel, vil typisk medføre, at MAR er en fast del af complianceafdelingens arbejde. Compliancefunktionen bør årligt foretage kontrol med, om kravene fra den delegerede forordnings artikel 2-5 er overholdt.

Gennemgangen bør bl.a. omfatte vurdering af, om:

- der er etableret tilstrækkelige forretningsgange og procedurer
- uddannelsesplaner er overholdt
- overvågning er udført kontinuerligt
- der er foretaget betryggende sagsbehandling
- mistanke om insiderhandel eller markedsmanipulation er indrapporteret rettidigt til Finanstilsynet.

Intern revision skal inddrage compliancefunktionens arbejde i størst muligt omfang. Efter udførelse af risikovurderingen og fastsættelse af revisionens omfang, kan revisor stikprøvevis efterprøve compliancefunktionens vurderinger og udføre supplerende revisionshandlinger, til brug for vurderingen af, om der er etableret et tilfredsstillende kontrolmiljø.

Best practice og branchebefalinger

Nykredit deltog i en konference i London i maj 2019, hvor foredragsholderne var repræsentanter fra Nasdaq Markets, samt det britiske Finanstilsyn (FCA). Her blev der lagt vægt på, at der generelt set bliver brugt for langt tid på at arbejde med at løse alarmer. Der er mange falske positive alarmer, og det er en ganske lille andel af alarmerne, der ender med at blive eskaleret.

Institutter kan med fordel bruge mere tid på at undersøge u hensigtsmæssig adfærd, fremfor at løse en stor mængde alarmer. Institutterne skal dog fortsat sikre, at kalibreringen sker ud fra en risikobaseret tilgang, som ikke må påvirkes af hvor mange ressourcer, det vil kræve at følge op på alarmerne.

FCA anbefaler, at institutter foretager QA-stikprøver på medarbejdere med jævne mellemrum. Dette skal sikre, at der til enhver tid arbejdes i overensstemmelse med vedtagne procedurer og branchebefalinger. QA bør være en del af den formaliserede uddannelsesplan og introduceres til nye medarbejdere under deres oplæring.



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.iaa.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 den udviklingen indenfor feltet intern revision.

Den digitale udgave af Ia er en fuld replikeret version af magasinet, så du kan se hele udgaver og blade mellem siderne - ligesom den trykte udgave. Du finder en række navigationsværktøjer til at gennemse artikler samt bonusvideoinhold 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.theiaa.org

 **The Institute of
Internal Auditors**

Nye skærpede regler om finansielle virksomheders outsourcing



Nina Trolle Boldt, Director, Deloitte

Introduktion og formål

Den 1. juli 2020 trådte Finanstilsynets nye bekendtgørelse nr. 877 af 12. juni 2020 om outsourcing for kreditinstitutter mv. i kraft. Den nye bekendtgørelse erstatter den eksisterende outsourcingbekendtgørelse fra 2010, og er med til at bringe de danske regler i overensstemmelse med EBA's "Retningslinjer for outsourcing" fra februar 2019 for så vidt angår kreditinstitutter, fondsmæglerselskaber, investeringsforvaltningselskaber m.fl.

Det er i overensstemmelse med anbefalingerne i Erhvervsministeriets rapport fra april 2018 om "Eftersyn af den finansielle regulering".

Outsourcing dækker over situationer, hvor en virksomhed vælger at købe varer eller ydelser hos en leverandør, fremfor at opgaverne (eksempelvis dataopbevaring eller håndtering af bogføring) varetages internt i den enkelte virksomhed. Bekendtgørelsen afgrænser således outsourcing til "enhver form for ordning mellem en virksomhed og en leverandør, i henhold til hvilken leverandøren udfører en proces, en tjenesteydelse eller en aktivitet, som outsourcing-virksomheden ellers selv ville udføre".

Outsourcingreglerne på det finansielle område har overordnet til formål at sikre, at finansielle virksomheder fortsat bærer ansvaret for de opgaver, der udføres hos leverandøren i tilfælde af outsourcing samt at sikre, at Finanstilsynet fortsat kan udøve et effektivt tilsyn. Reglerne fastsætter således, hvordan de finansielle virksomheder skal sikre, at en opgave varetages i henhold til gældende lovgivning, selv om den er henlagt til en leverandør. Ved outsourcing skal outsourcingvirksomhederne derfor sikre, at de har kontrol over opgaverne, og at outsourcingvirksomhederne har mulighed for at udøve nødvendig indflydelse på opgavernes udførelse.

Ikrafttræden

Fra 1. juli 2020 vil bekendtgørelsen finde anvendelse på alle outsourcingkontrakter, der indgås, revideres eller genforhandles efter denne dato.

Outsourcingkontrakter, der er indgået inden den 1. juli 2020, skal senest den 31. december 2022 være i over-

ensstemmelse med reglerne i den nye bekendtgørelse. For så vidt angår outsourcingkontrakter, der er indgået inden den 1. juli 2020, finder de hidtidige gældende regler anvendelse indtil den 31. december 2022.

Er outsourcingkontrakter om kritisk eller vigtig outsourcing ikke bragt i overensstemmelse med denne bekendtgørelse senest den 31. december 2022, skal outsourcingvirksomheden underrette Finanstilsynet herom, herunder om de foranstaltninger, der er planlagt for at bringe outsourcingkontrakten i overensstemmelse med bekendtgørelsen eller den mulige exit strategi.

Det må umiddelbart antages, at de generelle krav i bekendtgørelsen fx om krav til politik for outsourcing, oprettelse af et outsourcingregister, udpegning af en outsourcingansvarlig mv. allerede skal efterleves fra den 1. juli 2020, selv om en outsourcingvirksomhed alene har outsourcingkontrakter indgået før den nævnte dato.

Anvendelsesområde

Bekendtgørelsens anvendelsesområde er ændret i forhold til den nugældende outsourcingbekendtgørelse.

Blandt andet er e- pengeinstitutter, betalingsinstitutter samt fælles datacentraler omfattet af reglerne i bekendtgørelsen. Derudover er gruppe 2-forsikringselskaber udskilt fra bekendtgørelsens anvendelsesområde og i stedet reguleret i en selvstændig bekendtgørelse, hvis regler er sammenlignelige med de regler, som gruppe 1-forsikringselskaber er underlagt i medfør af Solvens II-forordningen.

Begrebsanvendelse

I modsætning til den nugældende outsourcingbekendtgørelse, hvor det alene er "væsentlig" outsourcing, der er omfattet, vil al outsourcing blive omfattet af den nye bekendtgørelse. Det nugældende begreb "væsentlig outsourcing" udgår herefter. Der sondres herefter mellem outsourcing og "kritisk eller vigtig" outsourcing i den nye bekendtgørelse, hvor der for "kritisk eller vigtig" outsourcing stilles skærpede krav.

Det er outsourcingvirksomheden selv, der skal vurdere, om den outsourcete proces, tjenesteydelse eller aktivitet er "kritisk eller vigtig" for virksomheden.

Det fremgår af forarbejderne til det lovforslag, der blev fremsat i begyndelsen af februar 2020, om ændring af bl.a. lov om finansiell virksomhed (L 109 2019-20) om en ny definition af outsourcing, at outsourcingreglerne finder anvendelse, uanset at der ikke er indgået en formel, skriftlig aftale.

Heraf fremgår desuden, at outsourcing-virksomheder til enhver tid bør opretholde tilstrækkelig substans og ikke blive "tomme skaller" eller "postboks-selskaber". Virksomheder kan eksempelvis ikke outsource ledelsesorganets effektive udøvelse af det ansvar, som påhviler dem. Som noget nyt i bekendtgørelsen er også en række eksempler på forhold, der ikke udgør outsourcing, og som



kan hjælpe virksomheden med at vurdere, hvorvidt outsourcingen vil være omfattet af bekendtgørelsen eller ej. Ud over eksemplerne clearingydelser og korrespondentbankydelse, fremhæves køb af tjenester, som ikke normalt ville høre ind under virksomhedens aktivitetsområder, som eksempler på ydelser, hvor bekendtgørelsen ikke gælder.

Outsourcingansvarlig

Som noget nyt skal direktionen i de omfattede virksomheder udpege en outsourcingansvarlig, der er ansvarlig for styring, overvågning og kontrol af virksomhedens outsourcing. Den outsourcingansvarlige skal desuden sikre fyldestgørende dokumentation og skal være direkte ansvarlig over for direktionen.

Det er et generelt krav, at outsourcingvirksomheden har tilstrækkelige kompetencer og ressourcer til at sikre en tilstrækkelig styring og overvågning af og kontrol med outsourcing.

Efter EBA's "Retningslinjer for outsourcing" kan den outsourcingansvarlige fx være en ledende medarbejder, der er direkte ansvarlig over for direktionen (fx en chef for en kontrolfunktion). Desuden fremgår det, at små og mindre komplekse virksomheder som minimum skal sikre en klar opdeling af opgaver og ansvar for styring og kontrol af virksomhedens outsourcing-arrangementer og kan tildele outsourcingfunktionen til et medlem af virksomhedens direktion.

Risikovurdering

Den nye bekendtgørelse bygger på en risikobaseret tilgang samt et proportionalitetsprincip, hvilket bl.a. kommer til udtryk ved, at outsourcingvirksomheden skal foretage en risikovurdering forud for den påtænkte outsourcing. Gennemføres outsourcing, skal outsourcingvirksomheden tillige foretage løbende risikovurderinger af outsourcingarrangementet.

Outsourcingvirksomheden skal herunder som led i sin risikostyring og interne kontrol sikre, at risici forbundet med outsourcing inden for alle forretningsområder indgår i outsourcingvirksomhedens øvrige risikostyring og interne kontrolforanstaltninger.

Bestyrelsen skal, som led i den løbende risikovurdering, overvågning og kontrol, modtage periodisk rapportering om risici og eventuelle ændringer heri, der er identificeret i forbindelse med kritisk eller vigtig outsourcing.

Underretning til Finanstilsynet

I den nugældende outsourcingbekendtgørelse skal outsourcingvirksomheden senest 8 hverdage efter indgåelse af en outsourcingkontrakt underrette Finanstilsynet herom. Dette ændres i den nye bekendtgørelse, hvorefter outsourcingvirksomheden i "god tid" skal meddele Finanstilsynet om den planlagte kritiske eller vigtige outsourcing. Dette betyder, at virksomhederne fremover i god tid skal orientere/indgå i dialog med Finanstilsynet om den

planlagte outsourcing. Det tilsvarende vil gøre sig gældende ved væsentlige ændringer i outsourcingarrangementet.

Outsourcingpolitik

I lighed med den gamle outsourcing-bekendtgørelse stiller den nye bekendtgørelse krav til virksomhederne om, at de skal have en outsourcingpolitik.

I modsætning til tidligere opstilles der i den nye bekendtgørelse specifikke krav til indholdet af outsourcingpolitikken.

Outsourcingkontrakten

På samme vis som i den nugældende outsourcingbekendtgørelse opstilles der i den nye bekendtgørelse en række krav til outsourcingkontraktens indhold. På en lang række områder adskiller kravene fra den nye bekendtgørelse sig dog fra de nuværende krav, hvor dette er særligt udtalt for "kritisk eller vigtig" outsourcing.

Outsourcingregister

Det er efter den nye bekendtgørelse et krav, at outsourcingvirksomheden fører et register med oplysninger om alle outsourcingarrangementer i overensstemmelse med kravene i bekendtgørelsens bilag 2.

For de outsourcing, der ikke er kritiske eller vigtige, er der tale om stamoplysninger såsom leverandør, omfattede ydelser, relevante datoer for ophør og genforhandling og i hvilket omfang, der er overført data og persondata til leverandøren. Derudover opstiller bekendtgørelsen yderligere registerkrav for kritiske eller vigtige outsourcingkontrakter. Bekendtgørelsen fastlægger desuden, at virksomhederne, på anmodning fra Finanstilsynet, skal kunne fremsende deres outsourcingregister elektronisk.

Outsourcingvirksomheden skal opbevare dokumentation for afsluttet outsourcing i registeret og øvrig dokumentation i minimum 5 år, medmindre andet følger af anden lovgivning.

Exitstrategier

Endelig skal virksomhederne som noget nyt have skriftlige exitstrategier for kritisk eller vigtige funktioner ved opsigelse, fejl og mangler, risikoforøgelse hos leverandøren eller ved fald i kvalitet. Exitstrategierne skal være i overensstemmelse med virksomhedens outsourcingpolitik og beredskabsplaner, og skal sikre, at virksomheden er i stand til at afslutte en outsourcing uden afbrydelse af forretningsaktiviteter, fortsat kan overholde myndighedskrav samt sikre, at kontinuiteten og kvaliteten af virksomhedens tjenester ikke lider skade.

Bekendtgørelsens bilag 4 oplister de krav, som exitstrategierne nærmere skal opfylde.

Sammenfatning

De nye krav for de finansielle virksomheder vurderes at indebære en ikke ubetydelig skærpelse af reglerne og de enkelte krav til outsourcing for de omfattede finansielle virksomheder m.fl., end tilfældet er i dag. Dog forventes præciseringen af kravene at gøre det nemmere for virksomhederne at vurdere, hvorvidt der er tale om "kritisk eller vigtig" outsourcing. Der forventes at forekomme justeringer af virksomhedernes gældende praksis for anvendelse af outsourcing, hvilket kan afføde ajourføring af outsourcingkontrakter, politikker og forretningsgange mv.





CCSA®

CFSA®

CGAP®

CRMA®



Drive Your Career Forward IIA Certifications and Qualifications

An IIA Professional Credential can move your career in the right direction, whether you're just starting down the audit path or taking your career to new heights. Drive to new opportunity, with increased earning potential, deeper knowledge, and enhanced credibility.

Invest In Your Tomorrow, Today.
www.TheIIA.org/Certification



Global

1A1731

Compliance, compliance eller compliance?



Martin Lindholst, Assistant Manager, Deloitte

Indledning

I de seneste år er fokus på compliance i finansielle virksomheder vokset betydeligt. Det er en naturlig konsekvens af skærpet regulering i kølvandet på finanskrisen. Det skyldes formentlig også de mange dårlige sager, der har præget den brede nyhedsstrøm i dagspressen. Der forekommer dog at være en vis begrebsforvirring – eller i hvert fald forskellige anvendelser af begrebet compliance – når man taler med forskellige finansielle virksomheder. Overordnet er der tre anvendelser af begrebet, man typisk møder i det finansielle landskab:

1. Compliance som en generel forståelse af det at overholde lovgivningen, herunder hvidvaskregulering, investorbeskyttelse, persondataregulering mv.
2. Compliance som en intern funktion, der overvåger, kontrollerer og rådgiver om gældende og kommende regulering
3. Compliance som udførelsen af handlinger, der er med til at sikre overholdelsen af gældende regulering.

Man kan nok svært tale om, hvad der er den rigtige forståelse af compliance, idet ordets danske oversættelse implicerer, at der ikke er noget forkert ved nogen af ovenstående tre anvendelsesformer. Punkt 1 ovenfor er formentlig med henvisning til en samlet forståelse af det apparat, der sikrer overholdelsen af gældende lovgivning. Punkt 3 ovenfor vil typisk omfatte de opgaver, der ligger i første forsvarslinje, hvis vi tager udgangspunkt i den klassiske forståelse af de tre forsvarslinjer. F.eks. kreditcontrollere, der overvåger, at kreditpolitikken i et pengeinstitut overholdes, eller AML-controllere, som overvåger, at sagsbehandlingen

i hvidvaskafdelingen sker på en ensartet måde, og at de alarmer, der bør indberettes til SØIK, også bliver det. Så når der i Børsens overskrift (se nederst på siden) henvises til, at bankernes 4.300 compliancemedarbejdere sendte 41.000 tips til Bagmandspolitiet, skal vi lige være enige om, hvad vi taler om. Det er i hvert fald ikke compliance forstået som punkt 2 ovenfor, der menes. Nok snarere punkt 3.

Når man ser på reguleringens anvendelse af begrebet, er der dog ikke nogen tvivl om, at der med compliance menes den interne funktion i en finansiell virksomhed, som overvåger, kontrollerer og rådgiver om gældende og kommende regulering.

I ledelsesbekendtgørelsen for pengeinstitutter m.fl.¹ fremgår om compliancefunktionen, at den skal fungere uafhængigt, og at den skal kontrollere og vurdere, om metoderne og procedurerne og de foranstaltninger, der træffes for at afhjælpe eventuelle mangler, er effektive. I ESMA's retningslinjer² er compliancefunktionen defineret som:

Den funktion i et investeringsselskab, der har ansvaret for at identificere, vurdere, rådgive, kontrollere og rapportere om investeringsselskabets compliancerisiko.

Sammenblanding af første og anden forsvarslinje

Når alle de ovenstående opfattelser af begrebet compliance er rigtige på hver sin måde, vil det derfor være væsentligt for interne revisorer at forholde sig til den enkelte virksomheds forståelse af compliance. For interne revisorer vil det være væsentligt at forholde sig til compliancefunktionens selvopfattelse i den enkelte virksomhed. Der vil ofte – og særligt i mindre virksomheder – være en tendens til, at compliancefunktionen delvist opfattes som en del af første forsvarslinje, og dermed ikke som en uafhængig anden linje funktion eller en blanding af begge. Nedenfor er et par typiske eksempler på sammenblandingen mellem første og anden forsvarslinje, som man bør være opmærksom på:

Et klassisk eksempel på sammenblandingen mellem første og anden forsvarslinje er, når det er compliancefunktionen, der er ansvarlig for at udarbejde politikker og forretningsgange. Det vil for mange virksomheder være nærliggende, da ansatte i compliancefunktionen, qua den typiske uddannelsesmæssige baggrund, vil være vant til at formulere sig skriftligt i et formelt sprog. Denne sam-



menblanding leder dog til en åbenlys konflikt, når compliancefunktionen skal forholde sig til, om virksomhedens politikker og forretningsgange er effektive. Her vil der i så fald ikke være den fornødne uafhængighed. Omvendt vil det ofte være formålstjenesteligt, hvis compliancefunktionen yder råd og vejledning i forbindelse med udarbejdelsen af de interne procedurer.

Grænsen for, hvor meget compliancefunktionen kan deltage i udarbejdelsen af de interne procedurer eller retningslinjer, skal formentlig drages ved, hvem der "fører pennen". Herudover forekommer det med jævne mellemrum, at vi støder på virksomheder, hvor compliancefunktionen er reduceret til en enhed, der alene er ansvarlig for at udarbejde og vedligeholde politikker og forretningsgange, og hvor man dermed åbenlyst har misforstået funktionens formål. I disse tilfælde vil compliancefunktionen alene være en formaliafunktion, som rigtigt nok sørger for, at virksomhedens interne retningslinjer er compliant med gældende regulering, men hvor retningslinjerne typisk ikke afspejler den faktiske virkelighed og de faktiske risici i virksomheden.

Et andet klassisk eksempel er, at kreditcontrollere og AML-controllere bliver opfattet som en del af compliancefunktionen, idet de er med til at sikre virksomhedens compliance, forstået som virksomhedens overholdelse af gældende regulering. Når det er tilfældet, vil det være relevant at forholde sig til, hvordan der kompenseres herfor i anden forsvarslinje. En oplagt compensation kan bestå af, at risikostyringsfunktionen foretager andenlinjekontrollen på de områder, hvor compliancefunktionens uafhængighed ikke kan opretholdes i fuldt omfang. Ellers risikerer man at udvande anden forsvarslinje, da der i så fald vil mangle en forsvarslinje på kredit og AML. Det sker ikke sjældent, at compliance er en del af første forsvars-

linje, uden at virksomheden – herunder compliancefunktionen – selv er opmærksom herpå.

Afslutning

Når der knytter sig en vis begrebsforvirring til compliance, er det vigtigt, at den rette betydning udledes. Compliance som anden forsvarslinje skal forstås som:

"Den funktion i en virksomhed, der har ansvaret for at identificere, vurdere, rådgive, kontrollere og rapportere om virksomhedens compliancerisiko".

Hvis denne forståelse ikke afspejler sig i virksomhedens compliancefunktion, vil det for virksomheder, som enten er pålagt det via lov, eller som frivilligt har oprettet en compliancefunktion, medføre, at compliancefunktionen ikke har den tiltænkte effekt. Det vil potentielt kunne føre til, at virksomhedens setup med de tre forsvarslinjer ikke fungerer, da anden forsvarslinje enten udfører førstelinjearbejde eller ikke fungerer uafhængigt. Den interne såvel som eksterne revisor bør derfor være opmærksom på, hvordan compliance forstås i virksomheden, som den pågældende reviderer.

I forhold til den tilsynsmæssige praksis ses der en stigende tendens til, at fokus rettes mod stærke forsvarslinjer, idet der i de seneste år er givet tillæg for operationelle risici til det individuelle solvensbehov som følge af svage forsvarslinjer.

Noter

¹ Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. af 30/6/2016

² Retningslinjer for visse aspekter af kravene til compliancefunktionen ifølge MiFID af 25. juni 2012



Nye medlemmer

Nye medlemmer i IIA fra 26.3.2020 – 7.9.2020

Danmarks Nationalbank

Helle Hyldegård Holm

Danske Bank

Lochini Vithana
Leon Engels
Maria Lucchi
Ragnar Lien

Deloitte

Pia Lundtoft

Falck

Didde Svendborg Østergaard

Handelsbanken

Sara Berggren Brandt
Helle Hyldegaard Holm

Jyske Bank

Sara Fard

KPMG

Kit Vinther Buchholtz

Københavns Kommune

Jørn Boy Petersen
Lourd Wael Jamil Somo

Middelfart Sparekasse

Ole Munch Christensen

Nordea

Anastasiya Shandyga

Novo Nordisk

Cecilie Brudager

Nykredit

Steffie Hede Rosenberg

Rigspolitiet

Vibeke Møgelvang

Sampension

Celina Cartilli Meric

SEB

Henrik Nygaard

Skatteministeriet

Inge Andersen
Birgitte isker
Steen Lange
Jens Amtoft Jensen

Spar Nord

Simon André Thomsen

Ørsted

Thomas Holst Nielsen

Uddannelsesaktiviteter

Er du opdateret på IIAs kursusudbud? Som altid findes datoer og emner for gå-hjem møder, kurser og konferencer på foreningens hjemmeside www.ia.dk under rubriken "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.

Kurser og gå-hjem møder

28.09.2020: Kursus for pengeinstitut og realkredit, Høje Taastrup

30.09.2020: Kursus for forsikringsrevisorer. Forsikringshøjskolen

06.10.2020: Morgenmøde: Audit planning in an operational audit perspective

12.11.2020: Temadag for den finansielle sektor

18.05.2021 - 19.05.2021: IIA Årsmøde i Kolding

”Bagsmækken”

Foreningens adresse

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

CVR nr. 73954215

Indmeldelse i foreningen

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

Chefsekretær Dorte Drejøe
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.globaliaa.org eller ved kontakt til:

Heino Hansen, Internal Audit Manager, CIA, Nordea
☎ 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

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

Næstformand

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

Kasserer

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

Sekretær

Internal Audit Manager, CIA
Anita Damgaard Laugesen
Nordea
☎ 55 47 33 18 ✉ anita.laugesen@nordea.com

Bestyrelsesmedlemmer

Koncernrevisionschef, COR
Pia Sønderlund Nielsen
Finansministeriet
☎ 25 26 27 72 ✉ pnn@fm.dk

Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
Express Bank
☎ 36 39 52 61 ✉ bisv@expressbank.dk

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

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

Revisionschef
Christoffer Max Jensen
ATP
☎ 70 11 12 13 ✉ CXJ@ATP.DK

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

Suppleant

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