INFO

Foreningen af Interne Revisorer
Nummer 78 | September 2021 | 26. årgang

Minitema

- Anden og tredje forsvarslinje med fokus på samarbejde

IIA DK i dialog med Finanstilsynet omkring fornyelse af Revisionsbekendtgørelsen

Vinder af IIA prisen 2021

Skaber intern revision merværdi for virksomheder?

Richard F. Chambers

Internal Auditors Should Follow the Risk by Looking Ahead

Styredokumenter • Transparency • Outsourcing

INFOs redaktion

Ansvarshavende redaktør
Nordisk Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
BNP Paribas Personal Finance
☎ 36 39 52 61 ✉ bisv@bnpparibas-pf.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
☎ 89 12 25 18 ✉ mais@sparkron.dk

Næste nummer
INFO 79 udkommer i december 2021.
ISSN: 1903-7341 (Elektronisk version).

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

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

Forsidefoto
UnknownNet

Redaktionens adresse

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

redaktionen@iia.dk

Indhold

Nyt fra bestyrelsen

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

www.iia.dk

Leder

Michael Ravbjerg Lundgaard, Revisionschef, DSB

"Sommeren er forbi nu
& den nærmest fløj afsted
tomhændet står du tilbage & ka' slet ikke følge med
det sortner for dine øjne
mens du stirrende står her & ser
endnu et dødt løb bli' kørt med dig som blind passager
endnu en gang til men så heller aldrig mer'"

Så er vi alle tilbage på arbejdspladserne efter sommerferie og en lang nedlukningsperiode grundet COVID-19. Er der noget, der har ændret sig, siden du sidst så dine kollegaer i det fysiske univers?

Jeg tænker ikke lige på os, der har fået flere grå hår og flere kilo på sidebenene, men den virksomhed vi befinder os i og den opgave vi skal løse, er den forandret eller under påvirkning af nye risici?

Træd ikke bare ind i hamsterhjulet og gør som "vi plejer". Benyt chancen til at genoverveje såvel virksomhedens risici, som den måde vi planlægger, udfører, dokumenterer og rapporterer vores revision. I dette nummer af INFO, er redaktionsudvalget lykkedes med, at få tidligere IIA President, Richard F. Chambers, til at levere en artikel. Læs den! Artiklen giver os en tur ned ad memory lane, og beskriver meget rammende udviklingen i vores arbejde med risikovurderinger. Risikovurderinger er nødvendige for at sikre, at vi anvender vores tid, hvor det giver mest værdi for virksomheden, og de er obligatoriske iht IPPF standard 2010.A1. Men går vi efter de rigtige risici, hvordan scorer vi risiciene, bruger vi for meget tid på dokumentationen, og kommunikerer vi vores opnåede viden og resultat af risikovurderingerne godt nok til ledelsen?

Chambers giver os et bud på, hvilke fælder vi skal være opmærksomme på ikke at falde i, og hvilken læring der er fra en COVID-19 pandemi. Jeg bringer en spoiler – der er behov for, at vores risikovurderinger udføres hyppigere (ikke kun årligt), vi ser fremad og vores revisioner udføres hurtigere.

I min optik bør vi tillige overveje, hvordan vi arbejder med risikovurderinger. IIA standarderne kræver, at vi fokuserer på processer og forretningsenheder, men vi bør løfte det op på et højere niveau og starte med at identificere, hvad der er virksomhedsrisici. Det er disse risici vi med fordel kan kommunikere til den øverste ledelse. Formår vi at se, hvad der nu og fremadrettet kan udgøre væsentlige risici for virksomheden, og bruge dette til at gå i dialog med ledelsen, viser vi også ledelsen, at intern revision er en vigtig sparringspartner, der forstår og understøtter ledelsens strategiske mål.

Men det skal også omsættes til handling, og i min optik er det derfor vigtigt, at interne revisioner fokuserer på at begrænse deres scope til det, der virkelig betyder noget for virksomheden, at vi formår at revidere "at the speed of risk" og, at vi kommunikerer effektivt og hurtigt.

Jeg opfordrer praktikere i interne revisioner, hvad enten du kommer fra en lille eller stor revisionsenhed, til at bidrage til, at give guidance og praktiske eksempler på, hvordan I lykkes med dette. Del denne viden med os andre, gerne gennem artikler her i bladet eller deltagelse i IIA netværksgrupper. På den måde kan du hjælpe til, at IIA udvikler sig som forening, skaber værdi for sine medlemmer og være med til at advokere for værdien af intern revision.

I dette nummers minitema om anden og tredje forsvarslinje, er der netop gode eksempler på praktikere, der med deres artikler giver os ikke kun et indblik, men gode beskrivelser af metodikker og erfaringer, der er praktisk anvendelige for andre, læs f.eks. om PFA´s compliancefunktion fra 2016 til i dag.

Dette nummer af INFO indeholder også mange andre gode artikler og praktiske eksempler på revisionsrelevante forhold. Læs f.eks. "Making Internal Audit more dynamic, trusted and well-respected" som sætter fokus på revisors adfærd og selvforståelse. "Vær transparent, lyt og forstå, kommuniker", det er gode input til værktøjskassen, der kan gøre livet som revisor lettere og medvirke til, at ledelsen oplever intern revision som værdiskabende.

I bestyrelsen i IIA DK arbejder vi pt. aktivt med vores strategi, som inkluderer, hvordan vi kan advokere for værdien af intern revision, understøtte vores medlemmer med adgang til uddannelse, standarder, praktiske guidelines og facilitere netværk. Vi får brug for hjælp, når vi skal til at effektuere på strategiens indsatsområder. Vi er en forening, og vi lykkes kun, hvis vores medlemmer ikke er "blinde passagerer", men aktivt hjælper hinanden, og mange flere aktivt yder et bidrag gennem deltagelse i vores netværk og underudvalg. Du er meget velkommen!

Der er mange gode årsager til at læse resten af bladet, og du vil helt sikkert ikke "stå tomhændet tilbage".

God læselyst!

Vinderne af IIA Prisen 2021

Værdiskabende intern revision – En dansk undersøgelse af intern revisions værdiskabelse

Forfattere: Andrias Berglíð Sólsker og Petur Pauli Mikkelsen

Begrundelse:

Værdiskabende intern revision er et emne, som altid er yderst vigtigt for interne revisorer. Kandidatafhandlingen undersøger, om intern revision skaber værdi for danske industrielle virksomhed samt påpeger, hvilke forudsætninger der ligger til grund for denne værdiskabelse. Afhandlingen har via spørgeskemaer og interviews påvist, at intern revision for at skabe værdi har rykket sig fra kun at give assurance omkring virksomhedernes governance, risikostyring og interne kontroller til også at yde rådgivning. Forudsætningen for dette er, at den intern revision som en samlet funktion besidder de nødvendige kompetencer. Endvidere er konklusionen, at den moderniseret "Three Lines model" giver øget mulighed for, at den intern revision kan have en optimal fordeling af assurance og rådgivningsopgaver. Opgaven giver et super godt indblik i, hvad det kræver for at sikre, at en intern revision til stadighed er værdiskabende.

2. Præmien blev ikke uddelt

IIA PRISEN

Prisopgave om intern revision

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

1. præmie: 25.000 kr.
2. præmie: 15.000 kr.

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

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

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

Ansøgningsfristen er 15. januar 2022. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iia.dk.

Prisoverrækkelsen vil ske på IIA's årsmøde i maj 2022. Bedømmelsesudvalget består af Dorthe Tolborg (Danske Bank), Kim Klarskov Jeppesen (CBS) og Birgitte Rousing Svenningsen (Express Bank).

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

Foreningen af Interne Revisorer
The Institute of Internal Auditors - Denmark

Internal Auditors Should Follow the Risks by Looking Ahead

Richard F. Chambers, CIA, CRMA, Global Internal Audit Advocate and Former Global President and CEO, The Institute of Internal Auditors

As the world emerges from the historic Coronavirus pandemic, it is natural for people to reflect on the lessons they learned and how their lives may be changed forever. It is also important for us to reflect on the lessons from the pandemic that reinforced what we knew or believed before the deadly virus turned our lives upside down. This is true for our personal lives as well as our professional endeavors.

I have been part of the internal audit profession for more than four decades. For over 12 years of my career, I served as the Global President and CEO of the Institute of Internal Auditors (IIA). As I have traveled around the world, I have been asked one question many times: "What advice do you have for internal auditors?" My answer for many years was almost always the same – "Follow the risks." In recent years, I have refined that advice, and respond – "Audit at the speed of risk." As I reflect on the lessons the internal audit profession has learned during the Covid-19 pandemic, I believe that internal auditors learned that those two important pieces of advice are as important as ever!

My Journey on Risk-centric Auditing

Early in my career, the word risk rarely came up during my internal audit activities. In deciding what to do, we typically developed an "audit universe," consisting of all of the operating units, business entities, organizational processes, and controls that were our responsibility, then we used that universe as our "audit register" to ensure that each area was assessed on a predetermined schedule. For example, the petty cash fund had to be audited every year, whether it was needed or not. By the time I became a Chief Audit Executive (CAE), those cyclical requirements were gone, though they were still very much a force of habit.

By the late 1990s, however, internal auditors had begun to focus on risk as an important determining factor when developing their audit plans and allocating resources. We began experimenting with risk assessments as part of the audit-planning process when I was the assistant inspector general for audit at the United States Postal Service (USPS). We informally documented our view of the USPS' risks on the back of a napkin in route to an international postal conference in China in 1999. Preparing risk assessments and using the results to develop a comprehensive audit plan was still generally viewed as a leading practice at the time, so we were proud of our preliminary efforts.

By the time I moved to United States Tennessee Valley Authority (TVA) as inspector general in the summer of 2000, the USPS Office of Inspector General had completed its second risk assessment, and I thought of myself as a fast-developing expert on risk-based audit planning. So when I showed up at TVA headquarters in Knoxville, Tennessee, I was confident I already knew the key risks facing the giant power authority - and was certain the first audit plan under my direction would focus extensively on the risks posed by TVA's nuclear power plants.

Imagine my surprise when, after several days of meetings with my audit team, the risk assessment identified the authority's contracting processes for acquiring coal as the biggest risk. Buying coal riskier than operating nuclear power plants? What I hadn't realized was that TVA's IG staff had been using risk-based planning for its audits prior to my arrival - and had a much better understanding of TVA's risks than I did.

I began to appreciate that risk has at least two dimensions—likelihood and impact. While even a single accident at a nuclear power plant could be catastrophic in terms of its effect on the organization, the environment, and the surrounding community, the likelihood of such an accident was relatively remote given the oversight track record of the U.S. Nuclear Regulatory Commission and other regulatory bodies, coupled with the extraordinary safety, security, and operating controls that were in place.

Meanwhile, TVA spent billions of dollars annually buying coal, the fuel responsible for generating most of the electrical power used by its customers. Not only did wasteful, ineffective, or even fraudulent coal-acquisition practices have the potential to cost TVA and its ratepayers lots of money - but the likelihood of those things occurring in the coal-contracting processes was high as well.

So high impact combined with high likelihood trumped high impact with low likelihood. I also learned that this

risk-based approach can add real value to an organization. During my tenure at TVA, we identified more deficiencies, cost recoveries, and cost savings from our coal-contract audits and investigations than from all of the other audits - combined!

The Importance of Risk Assessment

Not long ago, annual risk assessments were considered a leading practice but were not required under The IIA's *International Professional Practices Framework* (IPPF). Today, Implementation Guide 2010: Planning, provides the following guidance when undertaking a risk assessment:

> "To ensure that the audit universe covers all of the organization's key risks (to the extent possible), the internal audit activity typically independently reviews and corroborates the key risks that were identified by senior management. According to Standard 2010.A1, the internal audit plan must be based on a documented risk assessment, undertaken at least annually, that considers the input of senior management and the board…risks are measured in terms of impact and likelihood."

The Covid pandemic taught us once again that with the speed of risk that organizations face in today's world, performing an annual risk assessment won't likely serve organizations well. Covid reinforced the importance of deploying a continuous risk-assessment component to our risk assessment methodology in order to provide assurance.

In working with different internal audit departments over the years, I have observed that, even if internal auditors vary their approach, certain features are common to the development of their risk-based plans. These include:

- The establishment and maintenance of a risk register or inventory for the organization, linked to key business objectives
- The assignment of an inherent rating for risks in the inventory
- A process for scoring or rating risks on an annual basis
- A process for gathering and analyzing data, management perspectives, and other evidence on the current level of risk for each element in the inventory
- A scoring or rating methodology that is assigned based on the data, perspective, and evidence gathered
- A ranking or prioritization of risks based on the scoring methodology
- A determination of the most highly rated risks to be included in the proposed internal audit plan
- A review of the proposed annual internal audit plan with key management officials

- Submission of the proposed annual internal audit plan to the audit committee for approval

Over the years, I have seen elaborate, time-consuming methodologies, including formulas used to score individual risks. Sometimes these formulas seemed better suited for a rocket launch than calculating a single risk in an audit plan. As I often coach internal auditors, simplified formulas can be just as effective as complicated ones. After all, risk assessment is as much art as science; no matter how complex the process, professional judgment will invariably be a factor.

Our Stakeholders Value Us More When We are Risk-Centric

While the primary purpose of most internal audit departments' risk assessment process is to generate a basis for the annual audit plan, its value to internal audit's stakeholders cannot be overstated. In the early years of risk-based planning by internal audit, managements tended to find the assessment process and outcome useful, but audit committees typically received little exposure to it. However, in recent years, audit committees have taken more direct oversight of internal audit in many organizations. Before approving internal audit's annual plan, audit committee members naturally want to know the basis for prioritization of key internal audits for the year ahead. The more they see, the more they often want to be involved. Today, many internal audit departments will include interviews with audit committee members as an integral part of the risk assessment process.

“There will always be a need for hindsight and insight, but foresight is the ultimate source of value

Internal auditors spend a great deal of time and resources to undertake an annual risk assessment. For large internal audit departments of sizable organizations, the effort can represent hundreds of staff hours. Often, the risk assessment itself is then filed away as an evidence of the planning process for possible review during a subsequent external quality assessment of the department. However, I believe internal auditors miss a significant opportunity to deliver value by not sharing the risk assessment with management. In fact, I have received favorable response from management and audit committee members by packaging the risk assessment results as an engagement deliverable - similar to an internal audit report. When internal audit is seen as the enterprise expert in risk management, its annual risk assessment can serve as an important reference document for the entire organization.

Internal audit pioneered enterprise risk assessments at many companies. As managements and boards placed greater importance on enterprise risk management (ERM) during the past 20 years, many turned to internal audit to leverage its expertise. In some companies, internal audit departments were asked to champion or implement ERM, and the CAE was asked to wear a second hat—that of chief risk officer (CRO). While such moves reflect stakeholders' growing confidence in internal audit, the long-term consequences of internal audit retaining responsibility for ERM are not without risk, because its ability to serve as an objective source of assurance on the effectiveness of risk management for the organization could be compromised. After all, internal auditors should never audit their own work.

Risk Based Audit Lessons from COVID-19

The Covid-19 pandemic emerged virtually overnight to present one of the greatest global risks ever seen. Its rapid emergence and continuous source of new and evolving risks has impacted our lives and the organizations we served for more than a year. Even looking ahead to 2022, it is likely that pandemic-related risks will continue to emerge. I believe it is more critical than ever that internal auditors embrace a continuous approach to risk assessment and audit planning.

As a profession, internal auditors have cultivated a long and respected legacy as purveyors of hindsight. Almost all of us are adept at looking at last year's data and telling management where past mistakes were made. While hindsight is a necessary part of internal auditing, 20/20 hindsight is one of our least valuable skills. Often, our clients are already aware of past mistakes.

With the advent of operational auditing and, ultimately, the introduction of consulting/advice into our portfolio of services, we also became purveyors of insight. Insight is generally seen as more valuable than hindsight to our beleaguered stakeholders, but it too suffers from limitations in an era when risks emerge at warp speed. Today's insight may well be tomorrow's hindsight.

There will always be a need for hindsight and insight, but foresight is the ultimate source of value. Stakeholders seek to navigate the future more than revisit the past or dwell in the present. As internal auditors, we must focus our telescopes ahead. We need to concentrate on the risks of tomorrow if we are to not only protect but enhance value for our organizations.

Surveys of internal auditors' stakeholders over the years reveal they are generally unimpressed with our acumen at detecting emerging risks. In a survey a few years ago, KPMG found that only 10 percent of chief financial officers and audit committee chairs agreed that internal audit adequately identified and responded to emerging risks that threatened their companies.

In 2018 I began to use weather analogies when addressing challenges and opportunities for the internal audit profession. In many ways, identifying future risks is like predicting the weather. When our parents and grandparents were young, there was no such thing as weather radar. If they were curious or concerned about potential changes in weather, they simply peered out their windows or stood on a hill and scanned the horizon for potential storms. Of course, their weather predictions were often wrong. Climbing to the hilltop may have expanded their view, but weather patterns are far too complex to know if the clouds you see contain damaging winds, or if they are even coming your way.

That's why modern meteorologists have turned to more advanced methods. They monitor approaching storms with Doppler radar. They use digital satellite images to record cloud patterns around the world, and they plug the data into supercomputers, applying advanced statistical equations and algorithms to create more accurate forecast models. Of course, we all know that even meteorologists sometimes get it wrong, but their degree of reliability has increased dramatically with the advent of new tools and technology.

From hilltops to desktops, Covid has taught us that we all need to get smarter about risks, and there's a lot we can learn from meteorologists. They don't just observe the weather and make guesses about what the future might hold. They use every resource at their disposal to identify potential trouble spots and patterns before the storm materializes or inflicts significant damage.

As we have seen during the Covid pandemic, risks can arise at frightening speed in many forms - health, safety, business continuity, supply chain, and even talent disruption. So, there is a lot for us to watch for when it comes to emerging risks. The horizon is so vast that the job will simply be too great for a CAE alone. It will take the proverbial internal audit "village" to monitor emerging risks for a typical company. Just as the department's resources are assembled when annual internal audit plans are formulated, so too should the various experts be deployed to identify and monitor emerging risks. For example, the staff with the greatest IT expertise should monitor the horizon for emerging technology risks.

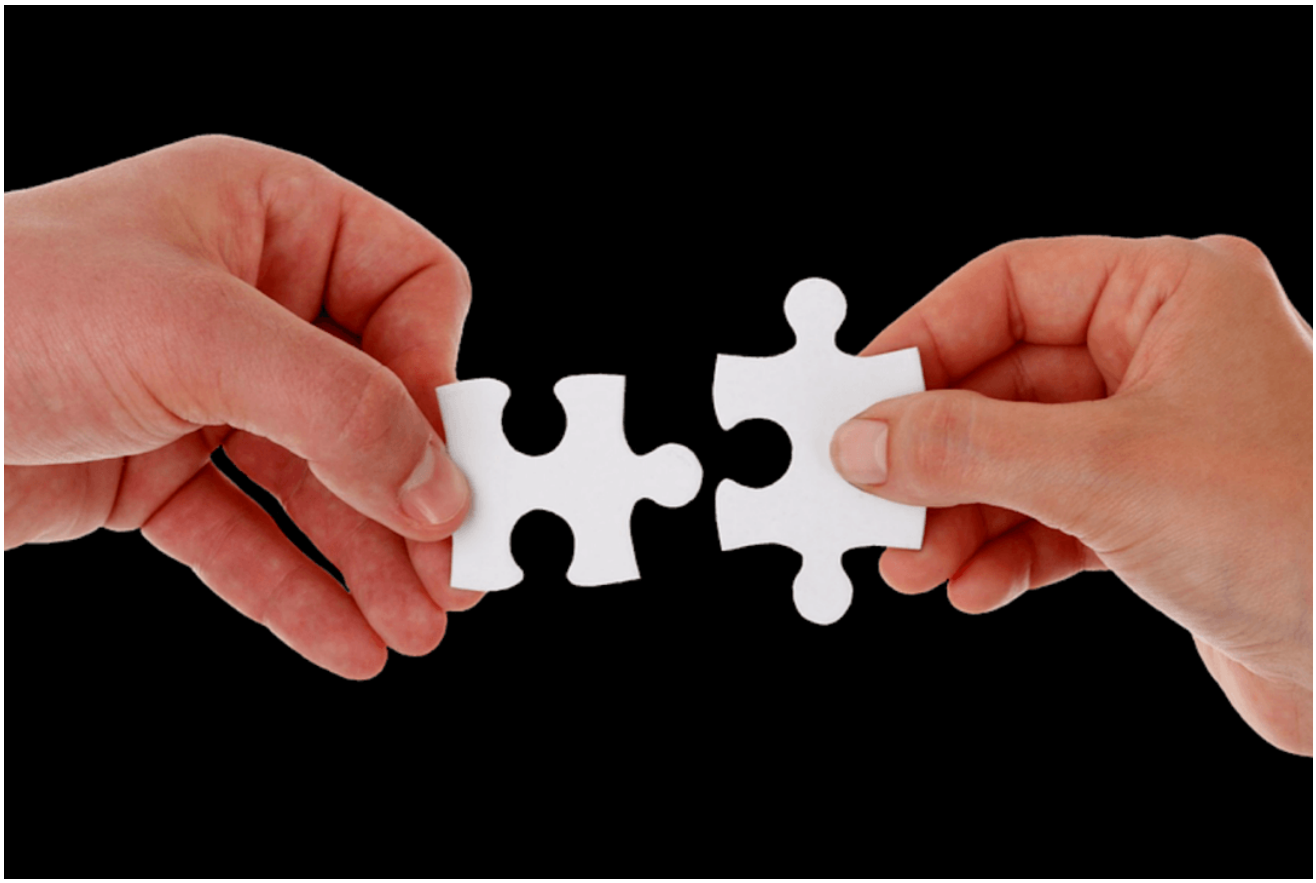
There is no silver bullet for identifying emerging risks. As I noted earlier, there is a degree of art in addition to science. However, if internal audit isn't looking in the right direction, there is a greater likelihood of missing emerging risks. But just as storms in the Northern Hemisphere often emerge from the West, there are directions from which potential risks facing your company are likely to emerge. These include:

- Economic forecasts (macroeconomic as well as those facing your industry).
- Known strategic business risks facing your company.
- New corporate initiatives being planned.
- Legislative and regulatory outlook facing your industry.
- Geopolitical developments and political risks in regions where your company operates.
- Disruptive threats or opportunities facing your industry.
- Performance of your primary competitors.
- Risks emerging as headlines via traditional or social media.

Identifying emerging risks should be a collaborative process with management. After all, management is likely to have already identified many emerging risks that threaten the organization. We should position ourselves as a partner, not a competitor trying to one-up management, when it comes to emerging risk acumen. After fully vetting our inventory of emerging risks, we should be prepared to share our perspectives with the audit committee. Our conversation must include our own plans for monitoring and responding to these risks as the organization's internal auditors.

Some internal audit functions demonstrate proficiency in identifying emerging risks, but many more need to embrace the lessons from the past year in transforming their approach. As the famous Danish philosopher Soren Kierkegaard observed: "Life can only be understood backwards; but it must be lived forwards." Let's embrace the lessons of the past year, and make sure we follow the risks by looking ahead in the future.

Minitema:
Anden og tredje forsvarslinje med fokus på samarbejde



Grænseflader mellem Compliance, Risikostyring, og Intern revision synes at være relevant og interessant i går, i dag og i morgen.

Læs om:

- **Nordeas bud på et på alle måder effektivt samarbejde mellem anden og tredje forsvarslinje.**
- **Den spændende rejse Compliancefunktionen i PFA har haft de sidste 5 år**
- **Sparekassen Kronjylland altgørende anbefalinger om dialog og afstemning af grænsefladerne mellem anden og tredje forsvarslinje.**

Tag med disse artikler inspiration med hjem til drøftelse og dialog internt i din virksomhed.

God læselyst!

Cooperation Between the Second and Third Line functions

Niklas Dahl Pind, Chief Internal Auditor, Nordea Kredit

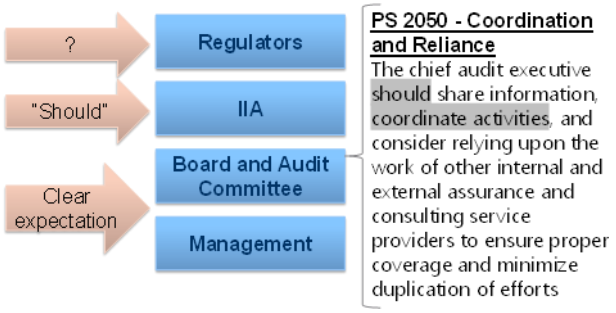
Introduction

Following previous articles and discussions on regulators' and stakeholders' view on the internal audit function, and updates to guidelines on the Three Lines model[1] (previously referred to as the Three Lines of Defence model), the question of how internal audit as a third line function (3LF) co-exists and works with other key parties in an organisation's control setup is relevant to touch upon. This article will try to provide some thoughts on the expectations and prerequisites for internal audit to cooperate with an organisation's second line compliance and risk management functions (2LF).

Expectations for cooperation

As shown in **Figure 1** below, Internal Audit's cooperation and coordination with the organisation's 2LF is in most cases required directly by the board, audit committee and other key stakeholders. In effect, this sets an expectation, which internal audit functions are required to understand, manage and execute on, in order to be perceived as a value-adding function.

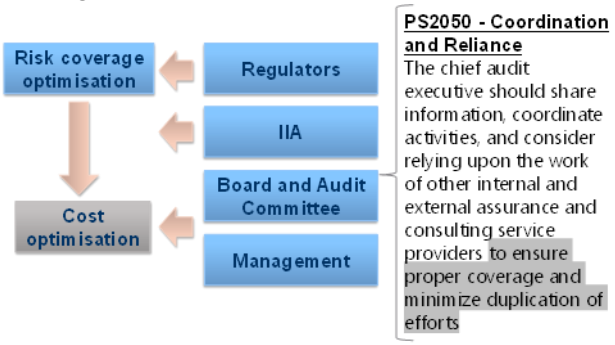
FIGURE 1 - STAKEHOLDER EXPECTATIONS



As expectations most often can be met only if the involved parties have an aligned view on what is to be delivered, the true question is, what exactly are these expectations?

In most organisations the value of both the 2LF and Internal Audit is recognised and accepted as a key part of the internal control framework, but these functions carry a cost that, as any other costs incurred, must be optimised and minimised. So, the expectations for cooperation lie somewhere between pure cost optimisation and a focus on risk coverage optimisation, as shown in **Figure 2**. It is important for the Internal Audit function to understand the focus of key stakeholders, and to assess whether to flag if cost optimisation is achieved at the expense of key risk coverage.

FIGURE 2 – STAKEHOLDERS RATIONALE FOR COOPERATION



One could argue that because Internal Audit is the "last" line of function to be added to an already extensive setup of control and oversight, there exists an even higher expectation for Internal Audit to demonstrate its relevance, which in reality is often safeguarded by direct regulatory requirements. Therefore, Internal Audit should not overlook or trivialise key stakeholder expectations towards Internal Audit's ability to cooperate with other control functions in order to provide efficient risk coverage.

Prerequisites for cooperation

Irrespective of stakeholder expectations, the extent and nature of Internal Audit's cooperation with the 2LF is primarily determined by three factors:

1) How well the organisation's stakeholders understand the differences in the roles of the 2LF and Internal Audit
2) How mature and formalised the organisation's 2LF are, and
3) How the relationship between the 2LF and Internal audit is managed.

Stakeholder perception of Internal Audit as a third line function

In the case of stakeholders viewing Internal Audit as merely being "more 2LF", it might become difficult for Internal Audit's role to be perceived as anything other than filling the gaps in a control setup.

In such cases it is pertinent for Internal Audit to communicate clearly, that due to the special nature of the Internal Audit function, whose role is to provide independent oversight also of the 2LF, there are inherent limitations to the level of cooperation between the functions, so as to not compromise the independence of Internal Audit.

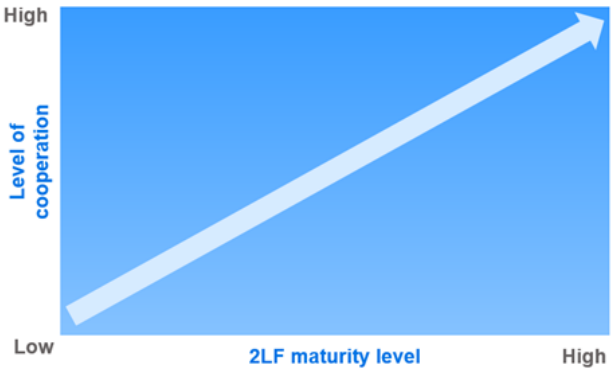
Being independent and unbiased is a key element in the role of Internal Audit, while at the same time remaining

relevant and being able to provide advice to the organisation. This represents a key topic in itself and will not be further discussed here, but it remains one of the significant underlying premises of the cooperation between the control functions in the second and third lines.

Maturity level and formalisation of second line functions

The maturity level of the second line functions (2LF) is probably the key deciding factor in how well the cooperation between the functions can be established and sustained, as shown in **Figure 3** below.

FIGURE 3 – CORRELATION BETWEEN MATURITY AND COOPERATION



In the case of very immature 2LF, there may not be sufficient basis for cooperation, and Internal Audit's task here is to assess and report on an ineffective 2LF and rely on own work exclusively, with no benefits gained.

Some basic elements should be in place in the 2LF regarding risk taxonomies and risk assessments. The optimal situation would be if the 2LF and Internal Audit use a common risk taxonomy, so that risk reporting to stakeholders are uniform and can complement each other. In addition to the use of a common risk taxonomy, the functions should also be in sync regarding the risk assessment of the organisation. If risks are perceived differently, it becomes difficult for Internal Audit to co-report on risks and re-use the work of the 2LF.

IIA Implementation Guide (IG) 2050 provides guidance on elements to assess when using and working with external providers, which is equally relevant for the assessment of the maturity level of the 2LF:

- Evaluate *objectivity* by considering whether the provider has, or may appear to have, any conflicts of interest and whether they have been disclosed.
- Consider *independence* by examining the provider's reporting relationships and the impact of this arrangement.
- Confirm *competency* by verifying whether the provider's professional experience, qualifications, certifications, and affiliations are appropriate and current.
- Assess due professional care by examining *elements of the practice* the provider applies to complete the work (i.e., the provider's *methodology* and whether the work was appropriately planned, supervised, documented, and reviewed). The CAE may also seek to gain an understanding of the scope, objectives, and results of the actual work performed to determine the extent of reliance that may be placed on the provider's work.

In addition, the cooperation requires a sufficient level of formalisation to be in place in the 2LF, in the form of charters, a defined methodology, risk assessments and coverage plans. This is illustrated in **Figure 4** below.

FIGURE 4 - ELEMENTS OF FORMALISATION

These elements are not only important for the cooperation between the functions, but also for Internal Audit's assessment of the 2LF in general. Adequate and aligned formalisation ensures that the functions speak "the same language".

If the 2LF are not defined properly and are not working according to a defined methodology that on an overall level matches that of Internal Audit, their level of coverage can be questioned. In such cases, Internal Audit would be required to perform additional work to reach a satisfactory level of assurance, and the basis for cooperation and utilisation is diminished. This in turn causes Internal Audit to not meet the stakeholder expectations of cooperation between the functions.

In such cases, it becomes important for Internal Audit to communicate to stakeholders why cooperation is not possible or not possible to the extent expected. Examples of lacking or inadequate maturity and formalisation can help Internal Audit to communicate this more clearly and in a more constructive way, including recommendations on what is advised to be in place in order to reach the expected level of cooperation.

It is important to highlight that some or many of the maturity and formalisation elements mentioned in this article are not direct regulatory requirements, although risk assessments and coverage plans are considered to be a

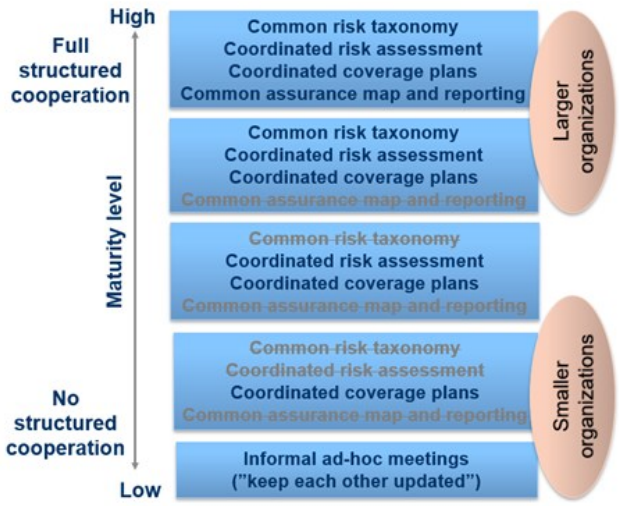
requirement from the Danish FSA for financial institutions. Nonetheless, it is logical that if a more formalised and efficient cooperation between the various control functions is to be implemented, it requires that at least some of these elements are in place.

In an optimal situation both the 2LF and Internal Audit are sufficiently and equally mature, formalised and aligned in the perception of risks in the organisation. In reality the experience is that Internal Audit functions often are more mature and formalised than the 2LF. If this is the case, Internal Audit has presumably already reported this in some form to the stakeholders as part of the ordinary coverage of the 2LF.

However, as these elements are not always a direct regulatory requirement, and hence cannot be reported as direct deficiencies, Internal Audit can make an assessment of whether to provide more direct advice on how the organisation's 2LF can improve its maturity and formalisation level to achieve better risk coverage as a function, and to engage in a cooperation with Internal Audit.

Therefore, if not in place, the first advice would be to ensure the use of a common risk taxonomy and an aligned view on key risks in the organisation, leading to usable and comparable coverage plans in 2LF and Internal Audit. Following this, a more defined 2LF methodology should be implemented to reach a higher level of maturity and formalisation, constituting the optimal situation for meeting stakeholders' expectations for the cooperation between the control functions. This is illustrated in **Figure 5**.

FIGURE 5 - LEVEL OF COOPERATION



The relevance and the extent of elements described in this article are not considered to be a function of the size and complexity of organisations, only the complexity and level of detail of the various elements. Any 2LF would benefit from e.g. implementing the outlined elements of formalisation.

Relationship between the functions

There exists a built-in challenge in a close cooperation with the 2LF, as Internal Audit has to, on the one hand, prioritise cooperation, and on the other hand, provide an unbiased, independent assessment of the 2LF.

To build a relationship between the 2LF and Internal Audit that on the one hand requires respect and trust, but on the other hand requires that one part (Internal Audit) reports on deficiencies in the other part (2LF) is inevitably a matter of balance, that is in danger of favoring either the relationship with or the assessment of the 2LF.

In this respect it is important that the relationship is managed carefully, not placing overly emphasis on securing the relationship and cooperation at the cost of providing the independent assessment of the 2LF as required. It can be a difficult challenge, especially if Internal Audit is facing stakeholders with a strong focus on costs rather than risk coverage, and who do not fully understand the proper roles of the functions.

Summary

This article argues that a sufficient level of maturity and formalisation is required to be present in the 2LF, in order for Internal Audit to be engaged in a cooperation to provide a cost-efficient and coordinated coverage of an organisation's key risk areas and processes.

Generally speaking, the higher the level of maturity and formalisation in the 2LF, the higher the level of cooperation can be achieved, ranging from only being en-gaged in informal information sharing meetings to coor-dinated, combined risk coverage and reporting following common risk taxonomies.

In smaller organisations the complexity, especially of the formalisation elements, should be aligned to the size of the organisation, but all elements of both maturity and formalisation should be in place regardless of the size and complexity of organisations.

Finally, this should be coupled with Internal Audit's understanding of the expected level of cooperation required by its key stakeholders, primarily the management, audit committee and board, to assess whether this expectation is realistic and can be achieved.

Notes

[1] The IIA's Three Lines Model, The Institute of Internal Auditors, July 2020.

Compliancefunktionen i PFA-koncernen 2016 -2021

Sandie Thygesen Griepentrog, Chief Compliance Officer, PFA

Ulrik Knudsen, Senior Compliance Officer, PFA

Indledning

Artiklen vil give et billede af den rejse, som compliancefunktionen i PFA-koncernen har været på siden 2016, hvor etablering af compliancefunktionen blev et lovkrav for livsforsikringsselskaber.

Organisatorisk / referencer

Forud for 1. januar 2016 besluttede koncerndirektionen i PFA at etablere en compliancefunktion, som skulle agere som koncernfunktion og dermed dække de forskellige juridiske enheder i PFA-koncernen.

I de 5 år der er gået, har compliancefunktionen været organiseret i forskellige konstellationer med andre koncernfunktioner og har også skiftet reference til ressortdirektør undervejs. Aktuelt har PFA samlet de forskellige 2nd line funktioner i én organisatorisk enhed under Risk & Compliance, jf. **Figur 1** nederst på siden.

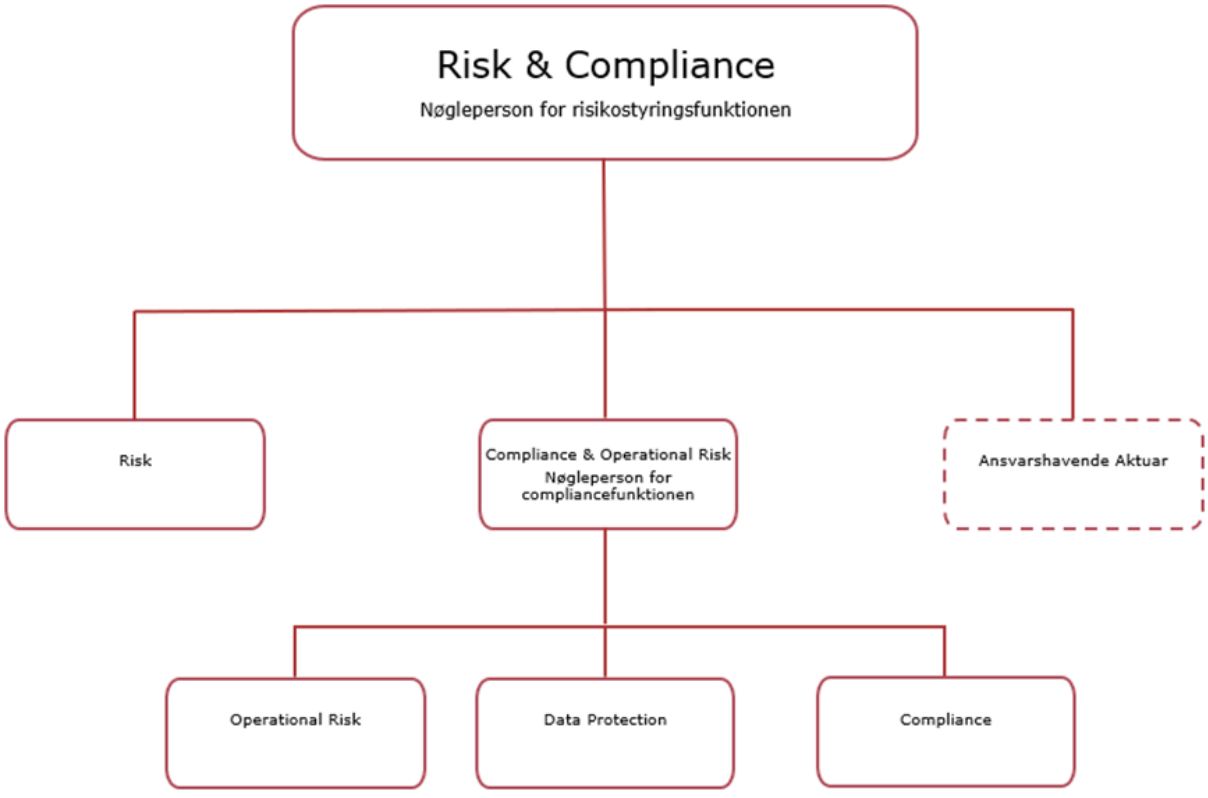
At compliancefunktionen indgår i et ressortdirektørs område, med andre ansvarsområder end compliance, og med en ledelsesmæssig reference til nøglepersonen for risikostyringsfunktionen betyder, at der løbende er fokus på, om eventuelle interessekonflikter kan materialisere sig, og der dermed kan sås tvivl om compliancefunktionens integritet og uafhængighed.

Det som der ikke har været ændret på siden 2016, er funktionens rapporteringslinjer. Der har altid været en direkte adgang og rapportering til både direktion og bestyrelse i de forskellige juridiske enheder, hvor Chief Compliance Officer selv præsenterer rapporter og analyser. Der afholdes løbende statusmøder med koncerndirektionen, og herudover afholdes der som minimum årlige møder mellem bestyrelsens koncernrevisionsudvalg og Chief Compliance Officer uden deltagelse af direktionen.

Ansvarsområder og ressourcer

Som en Group Compliance for en koncern der arbejder

Figur 1: Compliancefunktionens organisering



med livsforsikring, pension, investeringer og bankvirksomhed, er funktionens ansvarsområder forholdsvis velbeskrevet i lovgivningen samt i Finanstilsynets og de europæiske tilsynsmyndigheders fortolkning heraf.

Kort fortalt skal compliancefunktionen rådgive forretningen om dets compliancerisici i forbindelse med varetagelse af deres ansvarsområder og aktiviteter. Rådgivningen kommer til udtryk på mange måder. Eksempelvis er der i PFA nedsat en risikokomité, udvalg for juridiske risici og udvalg for operationelle risici samt flere produktfora, hvor compliancefunktionen er repræsenteret. Derudover bliver compliancefunktionen også involveret i større lov- og systemimplementeringer.

I PFA-koncernen er der formaliseret processer og procedurer for lovovervågning og lovimplementering. Men compliancefunktionen har et selvstændigt ansvar for lovovervågning for at sikre, at funktionen kan yde rådgivning, herunder at kunne sparre med og udfordre forretningen i relation til eksempelvis håndteringen af compliancerisici.

Derudover skal funktionen analysere og kontrollere, om de implementerede foranstaltninger anvendt af forretningen med henblik på at reducere compliancerisici på et givet område er tilstrækkelige og effektive. Resultatet heraf, herunder eventuelle anbefalinger, rapporteres til forretningen og ledelsen.

Ifølge lovgivningen må compliancefunktionen gerne varetage andre aktiviteter, der ikke har med compliancefunktionen at gøre, så længe funktionen ikke selv skal kontrollere håndteringen heraf og under hensynet til funktionens effektivitet. Det betyder også, at det nøje skal overvejes, hvis compliancefunktionen skal være ansvarlig for aktiviteter, som ikke har relation til compliancearbejdet.

I PFA har der været en proces med henblik på at identificere og vurdere om særlige ansvarsområder fortsat skulle varetages af compliancefunktionen. I den forbindelse er en række ansvarsområder og aktiviteter blevet flyttet fra compliancefunktionen til andre funktioner. Der er dog fortsat enkelte ansvarsområder, hvor det er vurderingen, at det giver værdi, at compliancefunktionen varetager disse ud fra en betragtning om, at det ikke påvirker funktionens integritet og/eller effektivitet.

På baggrund af lovgivningen har PFA-koncernen valgt, at medarbejdere i særlige funktioner og ansvarsområder er underlagt regler for personlige transaktioner af finansielle instrumenter, herunder en spørgepligt inden disse effektueres. Compliancefunktionen er ansvarlig for håndteringen af medarbejdernes handelsanmodninger, samt kontrol af efterlevelsen af og undervisning i reglerne.

I forbindelse med PFA-koncernens investeringsaktiviteter kan der opstå situationer, hvor der modtages intern viden om de selskaber, der investeres i. I de tilfælde har PFA valgt at registrere de selskaber, den interne viden drejer sig om på insiderlister, samt de medarbejdere der er vidende herom. På baggrund af forretningens tilbagemeldinger er compliancefunktionen ansvarlig for den systemmæssige registrering og administration af PFA's insiderlister.

PFA-koncernen er underlagt krav om at have en whistleblowerordning. I PFA er det compliancefunktionen, der er ansvarlig for håndtering og administration af samt undervisning i reglerne på tværs af de juridiske enheder.

Compliancefunktionen er bemandet med seks compliance officers, herunder Chief Compliance Officer, med en spredning på alder, uddannelsesmæssige baggrunde, erhvervserfaring samt faglige og personlige kompetencer. Compliancefunktionen anvender tidsregistrering, hvilket betyder, at alle i teamet registrerer deres tidsforbrug på forskellige aktiviteter for de respektive juridiske enheder. Det er med til sikre et overblik over, hvordan funktionen anvender dets ressourcer samt danner baggrund for vurdering af, om normeringen er passende.

Metodikker og håndteringen af Compliancearbejdet

Som noget af det første, der kom på plads i 2016 var en opdatering af den bestyrelsesgodkendte compliancepolitik i forhold til blandt andet kravene i Solvency II og en direktionsgodkendt funktionsbeskrivelse for compliancefunktionen. De to dokumenter var med til at sikre en forventningsafstemning med ledelsen om compliancefunktionens virke men også størrelsen af de compliancerisici, som direktion og bestyrelse kan acceptere.

Til at begynde med udarbejdede compliancefunktionen et overordnet risikobillede over forretningens compliancerisici. Det er en øvelse, som forudsætter en tillidsfuld og åben dialog med forretningen samt kendskab og forståelse for den lovgivning, markedsstandarder og interne regelsæt, som PFA-koncernen er underlagt. Efter compliancerisiciene var blevet identificeret, blev de enkelte risici vurderet i forhold til sandsynligheden for, at de kunne materialisere sig og konsekvensen heraf, hvis det var tilfældet. Risikobilledet ændres løbende som følge af ny og ændrede lovgivning, Finanstilsynets og de europæiske tilsynsmyndigheders fortolkning heraf, ændringer i de organisatoriske ansvarsområder i PFA, udefra kommende begivenheder eksempelvis domstols- og ankenævnsafgørelser samt klagesager etc. Som konsekvens heraf anvender compliancefunktionen flere ressourcer på løbende at

vedligeholde risikobilledet og dokumentere, hvad der ligger til grund for eventuelle ændringer.

Udgangspunktet for compliancefunktionen er, at alle compliancerisici skal gennemgås med en given frekvens. Rækkefølgen af gennemgangen er baseret på flere forhold, herunder input for forretningen, hændelser, risikoscoren og udviklingen i denne, funktionens egen vurdering og tidspunktet for den sidste gennemgang. På den baggrund udarbejdes der løbende aktivitetsplaner to år frem i tiden ud fra en risikobaseret tilgang og i dialog med forretningen, som efterfølgende bliver præsenteret for direktion og bestyrelse i de enkelte juridiske enheder. Når det er sagt, kan og vil der ske afvigelser i aktivitetsplanen, som følge af behovet for ad-hoc analyser, besvarelse af myndighedshenvendelser, håndtering af interne undersøgelser og hændelser m.v. I forbindelse med rapportering til ledelsen, vil afvigelserne til aktivitetsplanerne og forklaringer hertil blive præsenteret.

I PFA udarbejder compliancefunktionen hvert år en risikoanalyse af de enkelte juridiske enheders håndtering af compliancerisici, der fremlægges for direktion og bestyrelse. Analysen indeholder en detaljeret gennemgang af udvalgte compliancerisici og en mere overordnet vurdering af de øvrige compliancerisici.

Processen for analysens gennemførelse er fastlagt i en forretningsgang, som sikrer en ensartethed i planlægning, udførelse og afrapportering, herunder specifikke krav til compliance officers dokumentation for valg af teststrategi. Den fastlagte metode er med til at sørge for, at processen og slutproduktet er genkendelige for forretningen. At de enkelte compliance officers arbejder på en systematisk og ensartet måde er med til at sikre en effektiv compliancefunktion.

En detaljeret gennemgang af en udvalgt compliancerisiko starter med at nedbryde risikoen til nogle key risks, som opsamler de enkelte lovparagraffer på området og eventuelle fortolkningsbidrag. Det suppleres med en indsamling af eventuelle tidligere anbefalinger, eksempelvis fra Intern Revision, hændelser, klager, henvendelser fra Finanstilsynet samt tilsynsreaktioner og relevante afgørelser på området. I forlængelse heraf bliver de af forretningen registrerede risici, politikker, forretningsgange og kontroller ligeledes indsamlet. På den baggrund bliver gennemgangens omfang og afgrænsning fastlagt, og det bliver besluttet, hvordan gennemgangen skal gribes an, dvs. teststrategien. Det kan være i form af dokumentgennemgang, interviews, walk through, test af kontroller, dataanalyser, stikprøver eller en kombination heraf. Endelig bliver der estimeret et tidsbudget for gennemgangen. Det hele bliver indarbejdet i et planlægningsnotat. For hver enkelt gennemgang er der typisk udpeget en sagsbehandler og en kvalitetssikrer. Når disse to er enige om indholdet af planlægningsnotatet, præsenteres det for Chief Compliance Officer og dernæst involveres forretningen.

En detaljeret gennemgang af en compliancerisiko forudsætter dialog med forretningen, og der afholdes altid et opstartsmøde med forretningen, før gennemgangen påbegyndes. I den forbindelse anbefaler compliancefunktionen forretningen, at der udpeges en fagansvarlig, som funktionen kan gå til i forhold til den løbende afklaring af de mere specifikke forhold.

I løbet af gennemgangen forsøger compliancefunktionen at holde en løbende dialog med den fagansvarlige med henblik på blandt andet yderlige indsamling af informationer, men også præsentation af eventuelle observationer. Det er også med til at reducere risikoen for, at forretningen bliver præsenteret for fejlkonklusioner eller "ubehagelige overraskelser" i den endelige afrapportering.

De af compliancefunktionen indsamlede dokumenter, informationer og foretagne observationer holdes op imod de enkelte key risks og på den baggrund vurderes det, om der sker en passende mitigering eller, om der er behov for anbefalinger med henblik på at styrke området. Derudover registreres det faktiske tidsforbrug op imod det budgetterede og eventuelle afvigelser forklares til brug for den efterfølgende evaluering af processen. Det hele bliver opsamlet i et notat om udført arbejde, som gennemgås af kvalitetssikrer og efterfølgende præsenteres for Chief Compliance Officer. På den baggrund udarbejdes der en risikoanalyse til brug for rapporteringen til den ansvarlige områdedirektør, direktion og bestyrelse. Inden det kommer dertil, er compliancefunktionens observationer og eventuelle anbefalinger blevet præsenteret for forretningen med henblik på korrektion af eventuelle uklarheder/misforståelser.

Efter endt risikoanalyse afholder compliancefunktionen et internt statusmøde med henblik på en vurdering af forhold som opgaveplanlægning, udførelse af opgaven, rapportering, kommunikation med kunden og øvrige læringspunkter fra opgaven. Processen for gennemførelse af risikoanalysen bliver også drøftet med forretningen og Chief Compliance Officer.

Et halvt år efter færdiggørelsen af complianceanalysen udarbejdes der en compliancerapport, der indeholder en status på udviklingen i de forskellige compliancerisici, anbefalinger, ny lovgivning, undervisningsaktiviteter, hændelser, forhold der kræver ledelsens opmærksomhed,

tilsynshenvendelser samt vurdering af ressourcesituationen i compliancefunktionen.

Andre kontrolfunktioner og Intern revision

Den aktuelle organisering med de forskellige 2nd line funktioner som Risikostyring, Operational Risk, ansvarshavende aktuar, DPO'en og Compliance placeret i samme enhed, er et udtryk for ledelsens ønsker og forventninger om, at der kan høstes synergieffekter herved. Der er heller ikke tvivl om, at funktionerne kan lære meget af hinanden på forskellige områder. Alene det forhold, at det bliver nemmere at koordinere funktionernes aktiviteter med hinanden og anvendelse af en ensartet metodik og terminologi, vil komme både forretningen og ledelsen til gode. På lidt længere sigt er det også forventningen, at de forskellige funktioner på udvalgte område kan udføre fælles gennemgange.

Der afholdes periodiske møder mellem koncernrevisionschefen og Chief Compliance Officer som foruden koordinering af aktiviteter også kan søge afklaring af faglige problemstillinger. Mellem medarbejderne i de to funktioner er der også en velfungerende og løbende erfaringsudveksling, der er med til at fremme det gode samarbejde.

Take-aways

Baseret på fem års erfaring med compliance i PFA-koncernen er der blevet høstet en del erfaringer i forhold til, hvordan arbejdet kan/skal gøres og ikke gøres. Det har været en lærerig proces. Det vigtigste er i virkeligheden, at en stor del af compliancefunktionens virke har noget med mennesker at gøre og ikke blot en gennemgang af dokumenter og kontroller. Det vil nok være for omfattende i denne artikel, at redegøre for al den læring, som funktionen har samlet op siden 2016, hvorfor det kun er de tre vigtigste, der vil blive præsenteret.

Gør dit hjemmearbejde grundigt

Inden compliancefunktionen møder forretningen, er det bedste udgangspunkt for funktionen at være velforberedt. Det er blandt andet muligt, idet mange af de informationer, som anvendes i forbindelse med en risikoanalyse, herunder politikker, forretningsgange, kontroller- og kontrolresultater samt registrerede risici og hændelser kan findes i PFA's anvendte GRC-system. De observationer som sagsbehandleren har noteret sig i forbindelse med forretningens håndtering af compliancerisici, bliver også drøftet både med kvalitetssikrer og Chief Compliance Officer, herunder om det skal afstedkomme en konkret anbefaling eller et opmærksomhedspunkt, før de bliver præsenteret for forretningen.

Involvere forretningen

Det er vigtigt at have en løbende dialog med forretningen før, under og efter udførelsen af risikoanalysen. Det er dog en balancegang, så forretningen ikke opfatter compliancefunktionen som en "tidsrøver", selvom det kan være svært. I den forbindelse er det vigtigt, at compliance officeren udviser konduite og situationsfornemmelse for forretningens situation under hensyntagen til compliancefunktionens uafhængighed.

Få styr på din dokumentation

I forbindelse med en risikoanalyse bliver der typisk indsamlet meget information og også nogle gange for meget. Her er det vigtigt at være bevidst om, hvad dokumentationen skal anvendes til. Er det for at påvise mangler og utilstrækkeligheder, det modsatte eller som baggrundsstof til forståelse af forretningens aktiviteter? Sidstnævnte form for dokumentation har det med at fylde uforbeholden meget, og kan svække overblikket over den væsentlige del af dokumentationen. Derfor er det vigtig, at der tages hensyn til det i forbindelse med arkiveringen. Ligeledes er det vigtigt, at de enkelte observationer nemt kan genfindes eller reproduceres i dokumentationen. Det er både af hensyn til kvalitetssikringen, hvis risikoanalysen skal gentages på et senere tidspunkt og selvfølgelig også i forhold til eventuelle revisionsgennemgange.

Grænseflader mellem Compliance, Risikostyring og Intern revision

Benny Skjoldager, Intern revisor, Sparekassen Kronjylland

Mai-Britt Soo, Intern revisor, Sparekassen Kronjylland

Indledning

Emnet "Grænseflader mellem Compliance, Risikostyring, og Intern revision" synes at være relevant og interessant i går, i dag og i morgen – det er således et tema, som efter vores opfattelse ofte vil være aktuelt, da krav, forventninger og praksis på området hele tiden forandres og tilpasses.

Tanken med artiklen er at komme med et debatoplæg, som gerne skal bidrage til refleksion hos dig som læser – refleksion over egen situation i din organisation. Samtidig skal vi gøre opmærksom på, at artiklen er udtryk for vores egne oplevelser, observationer og erfaringer fra såvel nuværende som tidligere organisationer, som vi har været en del af.

Nogle af de temaer og problemstillinger, som vi gerne vil forsøge at sætte lidt lys på i denne artikel er:

- Oplevelsen af, at det i praksis er vanskeligt at finde de præcise snitflader, selv om vi hver især (de tre funktioner) synes, at vi har styr på det i teorien, herunder hvad kan årsagen hertil være.
- Vi vil også komme med nogle eksempler på, hvad vi gør i Sparekassen Kronjylland med henblik på at sikre bedst mulig afstemning af grænsefladerne de tre funktioner imellem.

Afgrænsning

Artiklen henvender sig primært til institutter med en Intern revision samt en selvstændig Risikostyrings- hhv. Compliancefunktion bestående af én eller få personer, da det er det udgangspunkt, vi selv kommer fra og dermed er grundlaget for vores debatafsnit og holdninger.

Institutter uden en Intern revision vil ikke have samme snitfladeproblematikker, mens institutter med større Risikostyrings- og Compliancefunktioner sikkert har yderligere problematikker, men også muligheder, som vi ikke er opmærksomme på.

Definitioner af funktionerne ud fra lovgivning

Det er vores vurdering, at en præcis og koordineret definition af hver af de tre funktioner danner det bedste grundlag og udgangspunkt for at kunne forstå forskellene mellem de tre funktioner. Derved er det også et bidrag til at tydeliggøre grænsefladerne mellem de tre funktioner, samt hvordan de tre funktioner bedst lykkes med at udfylde deres roller/funktioner til gavn for virksomhedsledelsen.

Ledelsesbekendtgørelsen[1] indeholder ikke en egentlig definition af de tre funktioner, men oplister en række krav til funktionerne. På tilsvarende vis har EBA guidelines[2] oplistet en række punkter, som funktioner bør (skal) udføre.

Finanstilsynet udsendte i februar 2020 notatet "God praksis for compliance og risikostyring i kreditinstitutter", hvori de har givet deres bud på en definition af de to funktioner. Det er nok det tætteste vi kommer på en formel myndighedsdefinition af de to funktioner. Definitionerne er gengivet nedenfor:

Compliancefunktion:
Compliancefunktionen skal fungere uafhængigt og kontrollere, at instituttet planlægger, organiserer og gennemfører sit arbejde indenfor gældende lovgivning, markedsstandarder og interne regler. Instituttets compliancefunktion skal have metoder og procedurer til at minimere risikoen for manglende regeloverholdelse.

Risikostyringsfunktion:
Kreditinstitutternes risikostyringsfunktion skal sikre, at alle væsentlige risici i instituttet bliver identificeret, målt, håndteret og rapporteret korrekt. Risikostyringsfunktionen skal have et samlet overblik over instituttets risikoeksponeringer for at kunne vurdere, om styringen heraf er betryggende.

For så vidt angår definition af intern revision fastslår Revisionsbekendtgørelsen[3], at Intern revision skal konkludere, hvorvidt instituttets risikostyring, compliancefunktion, forretningsgange og interne kontroller på alle væsentlige og risikofyldte områder er tilrettelagt og fungerer på betryggende vis. Et helt centralt element er, at intern revision skal være uafhængig af den daglige ledelse samt være objektiv i sin udførelse af opgaver.

IIAs definition er: "Intern revision er en uafhængig, objektiv, assurance- og konsulentaktivitet designet til at tilføre værdi og forbedre en organisations drift. Intern revision hjælper en organisation med at nå sine mål ved at bringe en systematisk, disciplineret tilgang til at evaluere og forbedre effektiviteten af risikostyring, kontrol og styringsprocesser (governanceprocesser)".

Som det fremgår ovenfor, er IIAs definition af Intern revision (i forhold til Revisionsbekendtgørelsen) bredere, hvor rådgivning og værdiskabelse er væsentlige elementer i Intern revisions rolle. En mulig årsag hertil kan efter vo-

res opfattelse være, at IIAs definition udspringer af en international kontekst, hvor begrebet operationel revision dækker bredere end det gør i Revisionsbekendtgørelsen.

Vores bud på definitioner af funktionerne

Med udgangspunkt i ovenstående er det vores forslag, at man dels kan forstå funktionerne ud fra deres forskellige afsæt i opgaver og dels ud fra forsvarslinjerne.

Vores bud på definitioner ud fra funktionernes afsæt i deres opgaver

- Compliancefunktionen: ansvarlig for at overvåge, om instituttet overholder gældende lovgivning, markedsstandarder og interne regler samt at rådgive[4] om, hvordan instituttet kan identificere og reducere compliancerisici
- Risikostyringsfunktionen: ansvarlig for overvågning og vurdering af instituttets evne til effektiv risikostyring samt at rådgive om risikobeslutninger truffet af organisationen og foreslå forbedringer af rammen for risikostyring og korrigerende foranstaltninger til at afhjælpe overtrædelser af risikopolitikker, -procedurer og -grænser
- Intern revisionsfunktion: ansvarlig for at give objektiv og uafhængig sikkerhed til instituttets bestyrelse og direktion om instituttets governance, risikostyring og interne kontroller

Vores bud på definition ud fra funktionernes placering i "forsvarslinjerne"

- 1. linje: Er ansvarlige for at identificere og styre risici på tværs af organisationen, herunder design, implementering og drift af effektive kontroller

  Den korte version: "Er risikoejere og udfører interne kontroller"

- 2. linje: Håndterer rammerne for risikostyring og udfører risikoovervågning. 2. line udgøres af Risikostyringsfunktionen og Compliancefunktionen. De standarder, politikker og metoder, som 1. line opererer under i relation til risikostyring og compliance, har 2. line typisk haft væsentlig indflydelse på. Anden forsvarslinje understøtter, udfordrer og er ansvarlig for risiko- og complianceovervågning af første forsvarslinje og er uafhængig af denne.

  Den korte version: "Overvåger og yder rådgivning til 1. forsvarslinje og er uafhængige af denne"

- 3. linje: Vurderer effektiviteten af risikostyring, kontrol- og governanceprocesser i relation til 1. og 2. forsvarslinjes interne kontrolmiljø og er uafhængig af begge forsvarslinjer.

  Den korte version: "Giver objektiv og uafhængig sikkerhed til instituttets bestyrelse og direktion om 1. og 2. forsvarslinje og er uafhængige af disse"

Efter at have undersøgt diverse lovgivning, vejledninger, best practice, myndigheder mv., har vi måtte konstatere, at det er vanskeligt at finde frem til en entydig definition af 2. linje funktionerne og Intern revision. Vi tror bl.a., at nedenstående forhold kan være med til at fastholde uklarhed omkring, hvad hver enkelt funktions rolle, ansvar og opgaver egentlig er:

- "Kontrolfunktion"
  EBA guideline[5] benævner alle tre funktioner som værende kontrolfunktioner, mens Revisionsbekendtgørelsen[6] eksplicit oplyser, at Intern revision ikke må udføre kontrolopgaver, da den interne revision skal kunne revidere instituttets interne kontroller.
  Vi fortolker Revisionsbekendtgørelsens ordlyd på den måde, at når Intern revision ikke må udføre kontrolopgaver, er det misvisende samtidig at benævne funktionen som værende en "kontrolfunktion". Det kan i hvert fald for andre dele af en organisation være med til at skabe uklarhed og forvirring om Intern revisions rolle.

- "Should (bør)"
  EBA guideline anvender "should" (bør) i sine afsnit omkring beskrivelsen af de tre funktioner (afsnit 20, 21 og 22).
  Det er vores vurdering, at anvendelsen af "bør" i stedet for "skal", kan give anledning til fortolkning og derfor også uklarhed omkring, hvad funktionerne rent faktisk skal og ikke skal. Vi tænker, at EBA anvender "should" i sine formuleringer på grund af proportionalitetskravet, men det ændrer ikke ved, at det efterlader uklarhed hos alle små og mellemstore institutter.

- "Rådgivning og/eller vejledning"
  Det er vores oplevelse, at "rådgivning og/eller vejledning" både af 2. linje funktionerne selv men også fra deres interessenter, er et væsentligt indhold i 2. linje funktionernes rolle.
  Jf. ledelsesbekendtgørelsen[7] er det dog alene vedr. investeringsservice og -aktiviteter, hvor det er et krav om rådgivning – og kun for Compliancefunktionen.
  EBA guideline anbefaler i mere generelle formuleringer, at 2. linje funktionerne også har en rådgivende/vejledende rolle.
  * For så vidt angår Risikostyringsfunktionen nævner EBA[8] således, at Risikostyringsfunktionen:
    - ikke bør hindres at indgå samspil med forretningsområder
    - bør levere rådgivning om forslag til risikobeslutninger truffet af forretningsområder eller interne enheder

  - kan foreslå forbedringer af rammen for risikostyring og korrigerende foranstaltninger til at afhjælpe overtrædelser af risikopolitikker, -procedurer, og -grænser
  - bør vurdere, hvordan det er muligt at begrænse risici, og rapporteringen til ledelsen bør omfatte forslag til hensigtsmæssige risikobegrænsende foranstaltninger
  - bør anbefale eventuelle afhjælpningsforanstaltninger

* For så vidt angår Compliancefunktionen nævner EBA[9], at Compliancefunktionen:
  - bør vejlede ledelsesorganet om foranstaltninger, der skal træffes for at sikre overholdelse af gældende love, regler, forskrifter og standarder

Vores bud på, hvordan man kan anskue funktionerne definitionsmæssigt samt de ekstra nævnte forhold, som kan skabe uklarhed, håber vi kan være et input i de følgende praktiske overvejelser.

Vores debatpunkter

Det er vores antagelse, at lovgiver i udgangspunktet ingen intention har haft om, at de tre funktioner skal udføre det samme stykke arbejde, eller at det samme stykke arbejde skal udføres af såvel 2. som 3. forsvarslinje. Det kan derfor ud fra vores synsvinkel være interessant at se lidt nærmere på:

1. Hvorfor er det svært at finde snitfladerne?
2. Hvorfor kommer vi til at udføre opgaver, som minder om hinanden?
3. Hvordan arbejder Sparekassens 2. linje funktioner og Intern revision i fællesskab med at sikre tydelige grænseflader og god koordinering?

Hvorfor er det i praksis svært at finde de præcise snitflader

Der er flere elementer, der kan spille ind i forhold til, hvorfor det opleves svært at få defineret nogle tydelige snitflader de tre funktioner imellem – og måske særligt mellem 2. linje funktionerne og Intern revision.

Vi tror på, at en afgørende forudsætning for at lykkedes med have nogle tydelige snitflader er, at man internt i en organisation har en klar definition af den enkelte funktion – en definition, som er konkret i relation til rolle, ansvar og arbejdsmetode. Ved udarbejdelse af definitionen af funktioner er det vores forslag, at man tager stilling til:

- metode for udførelsen af opgaverne, f.eks.
  - punkt for punkt gennemgang
  - egne analyser, test og vurderinger
  - test og/eller overvågning af 1. linje kontroller (test for design, implementering og effektivitet)
  - en kombination af ovenstående
- uafhængighed – overfor hvem og hvordan sikres/opretholdes uafhængigheden
- rådgivning og vejledning – hvordan, hvilket omfang og til hvem
- rapporteringsform og frekvens

Det er vores påstand, at hvis man undlader at tage stilling til ovenstående, vil det kunne resultere i, at funktionerne antager, at de ved præcis, hvad de selv står for, men også hvad de andre funktioner står for. Og hvis f.eks. Intern revisions opfattelse af sig selv ikke er i overensstemmelse med, hvordan Compliance- og/eller Risikostyringsfunktionen opfatter Intern revision, vil det kunne resultere i uklare snitflader mellem de tre funktioner.

Derudover er vores formodning, at i de institutter, hvor alle tre funktioner er små bemandingsmæssigt, vil alle udskiftninger af medarbejdere og måske især den ansvarlige, medføre en væsentlig risiko for, at samarbejdet og arbejdet med at afstemme snitflader, starter forfra. Med henblik på at imødegå og forhindre denne situation, er det derfor efter vores opfattelse vigtigt, at der sikres en løbende forankring i organisationen – forankring af de tre funktioners roller og ansvar.

I Sparekassen Kronjylland er vi bevidste om, at vi har en fælles opgave i løbende at have en dialog om grænsefladerne mellem 2. linje funktionerne og Intern revision. Den løbende dialog er formaliseret ved, at de tre ansvarlige for funktionerne har et månedligt statusmøde, hvor "stort som småt" bliver vendt, herunder også samarbejde og grænseflader. Det er er en god start og løser løbende driftsproblematikker, ligesom det giver vidensdeling. Det løser dog ikke alle definitionsmæssige forskelligheder, og disse bør efter vores vurdering derfor drøftes særskilt.

Hvorfor kommer 2. linje og Intern revision til at udføre opgaver, der minder om hinanden

Det er vores fornemmelse, at den øvrige organisation i nogle tilfælde har en oplevelse af, at 2. linje funktionerne og Intern revision udfører opgaver, som er meget ens, og vi tænker også, at det er tilfældet i nogle situationer. Det er helt sikkert ikke intentionen, men når det alligevel sker, er det vigtigt, at vi i fællesskab (de tre funktioner) målrettet arbejder med at finde frem til, hvad årsagerne hertil kan være. Vi har nogle bud på nogle mulige årsager:

- Manglende fokus på, med hvilket udgangspunkt, vi udfører vores opgaver – er det med et compliancefokus, risikostyringsfokus eller ud fra en revisionsbetragtning
- Manglende organisationsmodenhed i de tre funktioner -> risiko for manglede skarphed på, hvem gør hvad, hvorfor og hvordan
- Udvælgelse af områder/opgaver, der skal indgå i de tre funktioners årsplaner, sker ud fra "en væsentligheds- og risikobetragtning" -> det er ofte de samme områder, som de tre funktioner undersøger. Vi er opmærksomme på, at der lovgivningsmæssigt er krav om, at de tre funktioner skal kigge på nogle af de samme områder.

De to første punkter herover hænger sammen med afsnittet ovenfor omkring, hvorfor det i praksis kan være svært at finde de præcise snitflader. Derfor kan de ses som en mulig konsekvens af, at ens organisation til en vis grad mangler at få skabt en klar definition af den enkelte funktion.

Hvad kan være årsagen til, at vi oplever overlap – at vi udfører opgaver, som kommer til at minde meget om hinanden? Udvælgelse af områder, der skal undersøges sker ud fra en risiko- og væsentlighedsbetragtning, og derfor vil de tre funktioner ofte udvælge de samme områder (kredit, markeds, hvidvask, IT m.fl.).

Det er efter vores vurdering helt naturligt og berettiget, at de tre funktioner udvælger mange af de samme områder – netop ud fra en risiko- og væsentlighedsbetragtning. Men når det ofte er de samme områder, der udvælges, bliver det endnu tydeligere, hvis vi ikke i tilstrækkelige grad er skarpe på, hvilken arbejdsmetodik vi anvender ved løsning af vores opgaver. Og det er i disse situationer, at forretningen kan få oplevelsen af, at 2. og 3. forsvarslinje udfører (næsten) det samme.

Hvordan arbejder Sparekassens 2. linje funktioner og Intern revision i fællesskab med at sikre tydelige grænseflader og god koordinering af opgaver

I Sparekassen Kronjylland har 2. linje funktionerne sammen med Intern revision et årligt koordineringsmøde i starten af kalenderåret. Formålet med mødet er at få et overblik over, hvilke opgaver hver funktion har planer om at gennemføre det kommende år. Med udgangspunkt i dette overblik koordineres opgaverne med henblik på at undgå, at opgaver på samme område udføres på samme tid eller, om disse kan udføres samtidigt. Ligeledes drøftes formål og afgrænsning af de enkelte opgaver, således at det tilstræbes, at funktionerne løser opgaverne ud fra hver sit fokus.

Udover det årlige koordineringsmøde har de ansvarlige for de tre funktioner månedlige statusmøder, hvor bl.a. igangværende undersøgelser drøftes. De løbende statusmøder skal således også bidrage til en koordineret indsats fra de tre funktioner.

De løbende dialoger mellem de 3 funktioner har resulteret i, at vi har en ensartet skala, som vi anvender til afrapportering af resultater på vores undersøgelser.

Når de tre funktioner rapporterer resultatet af deres løbende undersøgelser, modtager de to andre funktioner ligeledes rapporteringen, således at funktionerne er bedst muligt orienteret om hinandens konklusioner og eventuelle anbefalinger på gennemførte undersøgelser.

I løbet af året, hvor opgaverne udføres, har de tre funktioner indbyrdes en aftale om, at de kontakter hinanden, inden opstart af en opgave. Et eksempel herpå er, at Intern Revision ved opstart af en revisionsopgave kontakter hhv. Risikostyringsfunktionen og Compliancefunktionen og hører dem, hvorvidt de har gennemført en undersøgelse af et givet område, f.eks. hvidvask.

Hvis Risikostyringsfunktionen og/eller Compliancefunktionen har gennemført en undersøgelse, modtager Intern Revision deres rapport og eventuelle arbejdsdokumenter. Intern Revision gennemlæser formål, afgrænsning og konklusion og vurderer, hvorvidt Intern Revision kan an-

vende deres udførte arbejde som bidrag til overbevisning til revisionen.

Den ovenfor beskrevet koordineringsindsats bliver løbende tilpasset og udviklet, og det er vores erfaring, at de tre funktioners evne til at koordinere indsatser og opgaver har stor betydning for resten af organisationens oplevelse og syn på os. En vellykket koordinering vil vise, at vi er bevidste om, at et godt og professionelt samarbejde er et vigtigt element til at lykkedes med at være værdiskabende for resten af organisationen.

Afrunding/opsummering

Det er vores håb, at artiklen har givet dig, som læser, et lille indblik i, hvorfor en løbende dialog og afstemning af grænseflader mellem 2. linje funktionerne og Intern revision er vigtig, men også hvorfor det kan opleves svært.
Vores påstand er, at en klar definition af hver af de tre funktioner er grundlaget for, at funktionerne kan have nogle tydelige grænseflader funktionerne imellem. Samtidig er det efter vores opfattelse vigtigt, at definitionerne er konkrete i relation til roller, ansvar og arbejdsmetoder. Hvis de tre funktioner i samarbejde lykkedes med dette, mener vi til gengæld, at der kan være ganske betydelige gevinster at hente for en organisation. Gevinsterne kan opdeles i, hvem der får glæde af den:

- instituttets ledelse
  - modtager tilstrækkelig og fyldestgørende rapportering i forhold til risikostyring og efterlevelse af love, standarder mv., herunder
    - modtager forslag til hensigtsmæssige risikobegrænsende foranstaltninger
    - modtager vejledning om foranstaltninger, der skal træffes for at sikre overholdelse af gældende love, regler, forskrifter og standarder
  - modtager en uafhængig og objektiv vurdering af risikostyring, det interne kontrolmiljø og governance

- instituttets øvrige organisation
  - vil undgå oplevelsen af, at de tre funktioner undersøger de samme ting på den samme måde
  - vil opleve, at de får en uafhængig vurdering af deres område – en vurdering, som kan give området en indikation af, om er behov for ændring i prioriteringer og/eller, om området er på plads med deres risikostyring, lovoverholdelse og/eller processer og interne kontroller
  - modtager rådgivning og vejledning fra 2. linje funktionerne om forhold omkring risikostyring og compliance

- 2. og 3. linje funktionerne
  - en mere effektiv anvendelse af deres ressourcer, da behovet for at sikre, at en af de to øvrige funktioner ikke har udført en tilsvarende undersøgelse, reduceres
  - vil opleve, at den øvrige organisation, vil modtage 2. og 3. linje funktioners besøg endnu mere positivt, da undersøgelserne udføres med forskelligt fokus og ud fra forskellige metodikker

Afslutningsvist vil vi gerne igen gøre opmærksom på, at holdninger, observationer, erfaringer og synspunkter, som fremgår af artiklen, er set ud fra Intern revision i Sparekassen Kronjylland.

Noter

[1] Ledelsesbekendtgørelsen, BEK nr. 1706 af 27/11/2020, Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl.
[2] EBA/GL/2017/11, Guidelines on internal governance under Directive 2013/36/EU
[3] Jf. Revisionsbekendtgørelsen, BEK nr. 1912 af 22/12/2015, Bekendtgørelse om revisionens gennemførelse i finansielle virksomheder m.v. samt finansielle koncerner
[4] LBEK §17, stk. 3 angiver, at Compliancefunktionen for den del af virksomheden, der vedrører værdipapirhandel, skal yde rådgivning af og bistand til de personer, der har ansvaret for at yde investeringsservice og udføre investeringsaktiviteter….
[5] Final Guidelines on Internal Governance (EBA-GL-2017-11)
[6] RBEK bilag 4, afsnit 1.1, side 50
[7] LBEK §17, stk. 3 angiver, at Compliancefunktionen for den del af virksomheden, der vedrører værdipapirhandel, skal yde rådgivning af og bistand til de personer, der har ansvaret for at yde investeringsservice og udføre investeringsaktiviteter….
[8] EBA, afsnit 20, punkt 166 og 169 og afsnit 20.1, punkt 180 og afsnit 20.4, punkt 181
[9] EBA, afsnit 21, punkt 192

70 years of IIA in the Nordics

Join the 70th Anniversary Celebration and Meet IIA President and CEO Anthony J. Pugliese

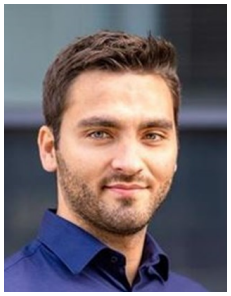
On 8 October 1951, IIA Denmark, IIA Norway and IIA Sweden met in Oslo to form The Scandinavian Chapter of the Institute of Internal Auditors; IIA Finland and IIA Iceland joined The Scandinavian Chapter a little later. The Scandinavian Chapter was the second institute to be formed outside the USA, making us one of the oldest institutes in Europe. Later, each country formed its own national institute.

The Nordic institutes invite all members to mark this 70th anniversary in a joint online event on Friday 8 October from 13.00-15.15 CET (add time zone here-time is different in Iceland and Finland), where you will also get the opportunity to meet IIA Global's new President and CEO Anthony J. Pugliese.

Registration: https://www.theiia.se/utbildningar_aktiviteter/#!educourse=523058

Skaber intern revision merværdi for virksomheder?

Andrias Solsker, Assistant, KPMG P/S



Petur Pauli Mikkelsen, Global Audit & Compliance Officer, Falck Danmark A/S

Denne artikel er baseret på vores kandidatafhandling på vores Cand.merc.aud. studie. Kandidatafhandlingen vandt IIA Prisens førstepræmie.

Motivation for at undersøge emnet

Under en forelæsning på vores Cand.merc.aud. studie på CBS blev der talt om intern revision og de fordele, en virksomhed kan opnå ved at etablere en intern revisionsfunktion. Herunder blev blandt andet nævnt den ekstra sikkerhed, som en bestyrelse kan få for, at virksomheden bliver drevet på en hensigtsmæssig måde fra en funktion, der, grundet sin organisatoriske placering, er mere uafhængig end en 2nd line of defence funktion, men samtidig opererer til dagligt i virksomheden, og dermed har en høj indsigt i virksomhedens drift. Dette ræsonnement syntes vi gav god mening, og baseret på det, var vores forventning, at danske virksomheder ville være tilbøjelige til at etablere en intern revisionsfunktion for at opnå disse fordele.

Ud fra grundlæggende økonomisk teori, vil enhver person altid søge maksimum tilførsel af værdi[1]. Hvis intern revision formår at tilføre merværdi for organisationen, burde der således være en selvregulerende mekanisme, hvor de virksomheder, der ser en værdi i intern revisions ydelser, vælger at etablere en intern revision på trods af, at det ikke er et lovkrav. Virksomheder, der ikke mener, at intern revision kan tilføre dem merværdi, vil fravælge at etablere sådan en funktion.

Ud fra denne forudsætning blev vi nysgerrige på, hvordan ovenstående ræsonnement med en værdiskabende intern revisionsfunktion kunne overføres til det danske erhvervsliv. Her kunne vi se, at mange danske industrielle virksomheder fravælger at etablere en intern revision på trods af, at professionen proklamerer sig selv som en værdiskabende funktion for virksomheder. Det er denne uoverensstemmelse mellem en værdiskabende funktion på den ene side, og fravalget af at etablere sådan en funktion fra virksomhedernes side, som vi gik i gang med at undersøge nærmere. Med udgangspunkt i dette blev vores fokus i afhandlingen at undersøge følgende:

Skaber intern revision merværdi for virksomheder, og hvordan defineres værdiskabelse?

Manglende forståelse af intern revision

Vores undersøgelse viste, at kun 5 ud af 20 industrielle virksomheder i det danske C25 indeks har valgt at etablere en intern revisionsfunktion, hvilket giver anledning til at sætte spørgsmålstegn ved intern revisions værdiskabelse.

Her fandt vi dog frem til, at problematikken med manglen på etablering af en intern revisionsfunktion blandt danske industrielle virksomheder, ikke nødvendigvis bunder i en manglende værdiskabelse, men at der eksisterer en misforståelse af, hvad intern revision er, og hvordan den kan skabe værdi. Derudover ligger en del af problematikken muligvis også på lovgivers side, hvor formuleringen i Revisorlovens § 31, stk. 3, nr. 3 muligvis medfører, at der hovedsageligt fokuseres på de områder, som flere professionelle interne revisorer forbinder med den mindste værdiskabelse, når det gælder intern revisions arbejdsområder – nemlig finansiel revision[2].

IIA's definition af intern revisions arbejdsområder er imidlertid langt bredere, hvor der fokuseres overordnet på følgende tre områder:

- Governance
- Risikostyring
- Interne kontroller

IIA lægger således ikke op til, at intern revisions primære arbejdsområde relaterer sig til det, som har med regnskabsaflæggelsen at gøre – altså finansiel revision, men lægger derimod op til, at en intern revisionsfunktion også kan tilføre merværdi ved at udføre operationel revision i bred forstand.

Den danske lovgivnings fokus på finansiel revision kan således medvirke til, at revisionsudvalg i danske virksomheder foretager vurderingen omkring nødvendigheden af etablering af en intern revisionsfunktion på et mangelfuldt grundlag, hvor man ikke får det fulde billede af, hvilken værdi intern revision kan tilføre virksomheden.

IIA's brede beskrivelse af intern revisions arbejdsområder er dog heller ikke uproblematisk, da det hurtigt kan blive uoverskueligt for revisionsudvalg og andre interessenter at se, hvordan en etablering af en intern revisionsfunktion kan se ud, og hvordan den kan tilføre virksomheden værdi.

Vi har derfor udarbejdet en definition af intern revision, som bedre beskriver, hvordan den skaber værdi for virksomheder. Formålet med definitionen er, at enhver beslutningstager i det danske erhvervsliv skal kunne forstå den interne revisions værdiskabelse, samt hvordan den adskiller sig fra andre sammenlignelige funktioner.

For at klargøre, hvorfor vi vurderer, at der er brug for en mere konkret definition af, hvad intern revision kan tilføre en virksomhed, vil vi, i det næste afsnit, vise, hvordan intern revision bruges i danske industrielle virksomheder med intern revision, samt hvad der forbindes med mest værdiskabelse.

Afslutningsvis vil vores definition af intern revisions værdiskabelse blive præsenteret.

Brug af intern revision

Vi har spurgt bestyrelsesmedlemmer, medlemmer i den daglige ledelse og revisionschefer i udvalgte virksomheder i Danmark, der har en intern revisions funktion, hvilke områder den interne revision bruger flest ressourcer på.

Arbejdsområderne er opdelt efter Finanstilsynets opdeling, hvor der skelnes mellem operationel revision, finansiel revision, risikostyring og compliance.

Figur 1 herunder viser, hvordan den interne revision benyttes i de responderende virksomheder, samt i hvilken grad den interne revision fokuserer på et givet arbejdsområde i virksomheden.

Vores undersøgelse viser, at revisionsfunktionerne i de adspurgte virksomheder hovedsaligt fokuserer deres ressourcer inden for operationel revision og compliance, efterfulgt af risikostyring og til sidst finansiel revision. Derudover kan det nævnes, at de besvarelser, der ligger i kategorien "Andre" også kan omfattes af operationel revision i bred forstand[3].

Resultaterne stemmer derfor godt overens med den trend, som anden litteratur også beskriver, hvor der viser sig at ske en rykning fra finansiel revision hen imod operationel revision.

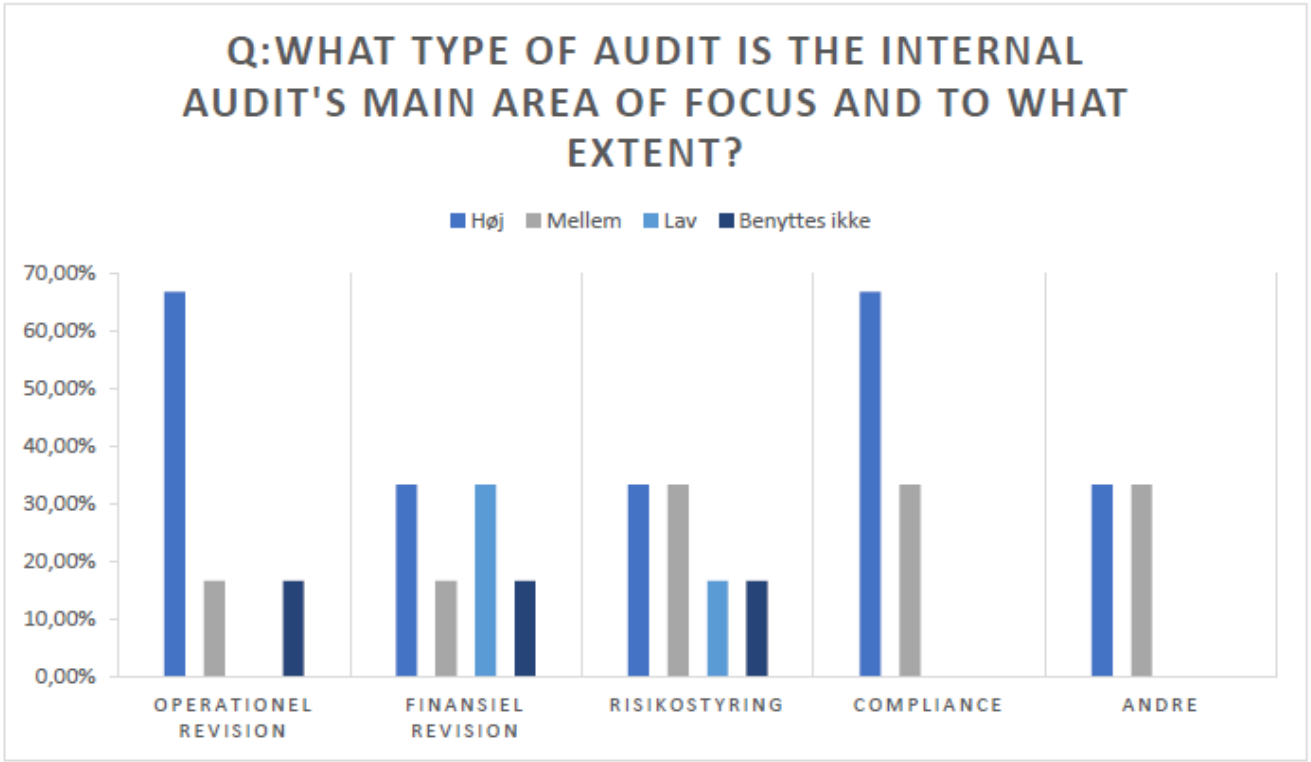
Hvilke områder kan intern revision tilføre mest værdi på:

Vi spurgte dernæst virksomhederne, hvilke områder, de mener, den interne revision skaber mest værdi på - Se **Figur 2** på næste side.

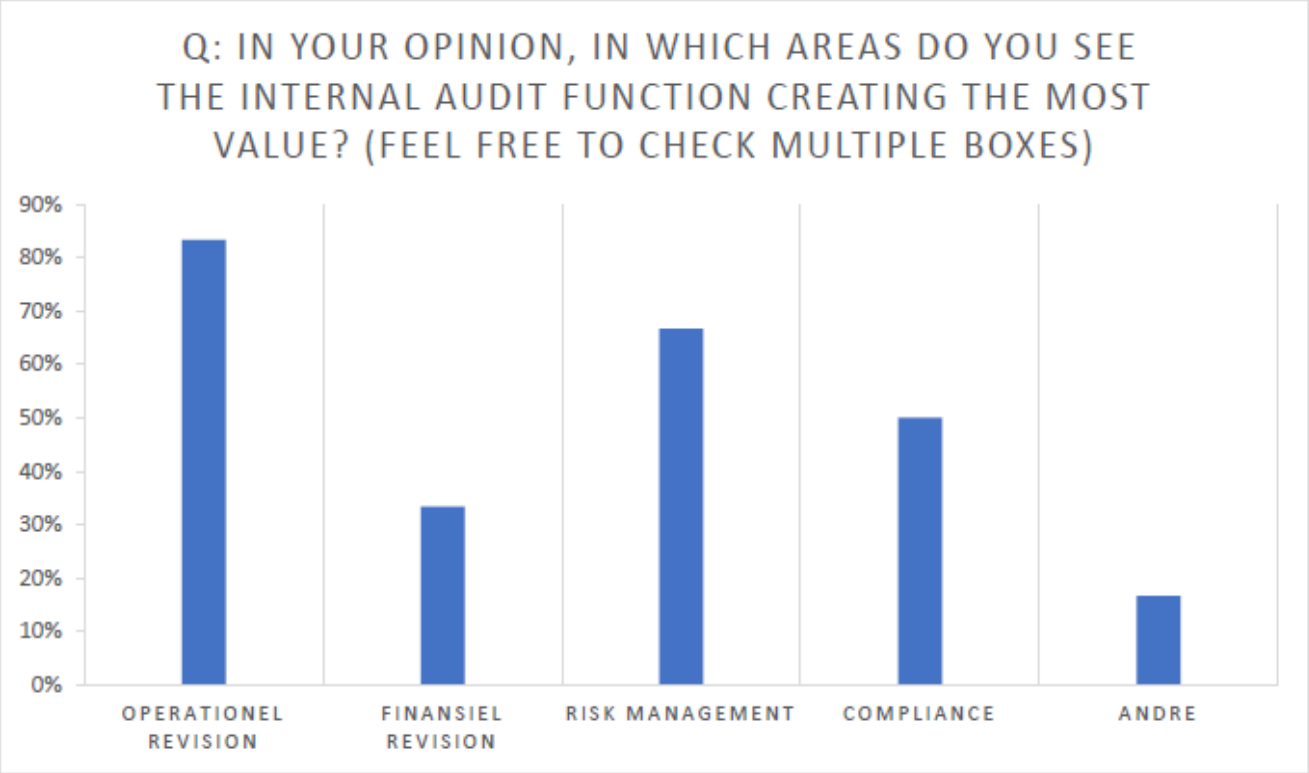
Figuren stemmer overens med det, vi har set gennem hele afhandlingsprocessen, hvor intern revisions værdiskabelse hovedsageligt vurderes at ligge inden for den operationelle revision. Af figuren ses, at størstedelen af respondenterne har svaret, at intern revisions værdiskabelse er inden for operationel revision. Færrest af de adspurgte mener, at finansiel revision er det område, som tilfører mest værdi. Dette giver også mening set i lyset af, at finansiel revision også bliver udført af den eksterne revision, hvilket begrænser nytteværdien af intern revision på dette område.

Ud over vores spørgeundersøgelse til bestyrelsesmedlemmer, medlemmer af den daglige ledelse og revisionschefer, havde vi et mere dybdegående interview med Mærsks revisionschef, som også deler denne holdning med hensyn til nytteværdien af finansiel revision:

Figur 1. Hvordan den interne revision benyttes



Figur 2. Hvilke områder, den interne revision skaber mest værdi på



And why I didn't select financial audit. Maybe I would put financial audit at the bottom. It is because we are also audited by external auditors. The incremental value we can provide is limited.

Ud fra de to figurer står det klart, at den interne revision skaber mest værdi ved at lave andet end finansiel revision. Vi har derfor undersøgt ved hjælp af faglitteratur og interviews hvordan den interne revision skaber værdi på følgende områder:

- Operationel revision
- Risk Management
- Compliance

Operationel revision
Operationel revision omfatter vurdering og gennemgang af de processer, virksomheden har opsat for at opnå sikkerhed for de af ledelsen fastsatte mål.[4] Mulighederne for at skabe merværdi ved udførsel af operationel revision afhænger hovedsageligt af, hvilke muligheder der er for profitoptimering i virksomheden gennem forbedring af virksomhedens efficiens og effektivitet. Man kan komme med flere praktiske eksempler på, hvordan den interne revision kan tilføre værdi igennem operationel revision, både igennem assurance og advisory[5]:

- Give uafhængig assurance omkring hensigtsmæssigheden og effektiviteten af de implementerede interne kontroller.
- Støtte virksomheden i at udvikle en omfattende ramme for evaluering af de interne kontrollers hensigtsmæssige design og effektivitet.
- Assistere den daglige ledelse i at fremme etisk adfærd og i at have en lav tolerance overfor ineffektive interne kontroller (tone at the top).
- Være fremadskuende og informere den daglige ledelse og bestyrelse omkring fremspirende risici.

Risk Management
Risk Management omfatter de aktiviteter, der iværksættes med hensyn til risikostyring, og som har til formål at skabe, bevare og realisere værdi. Igennem risikostyring kan intern revision tilføre virksomheden værdi ved at begrænse de risici, som virksomheden står over for.

Dette kan de gøre ved at assistere ledelsen i at overvåge både det interne og eksterne miljø for at identificere fremspirende risici. Som eksempel kan der ses på risici inden for IT-sikkerhed, hvor den interne revision kan assistere ledelsen i at overvåge og vurdere, om virksomheden har implementeret hensigtsmæssige foranstaltninger og retningslinjer, der begrænser risikoen for angreb fra hackere og virus mv., samt om foranstaltningerne er designet på en måde, der begrænser risikoen for menneskelige fejl. Dette vil under alle omstændigheder være ledelsens ansvarsområde, men den interne revision kan bidrage som sparringspartner over for ledelsen og samtidig give bestyrelsen uafhængig assurance på området.

Compliance
Compliance er et område, der ændrer sig hele tiden i og med, at nye reguleringer træder i kraft, der påvirker industrierne udefra. Den bedste sikkerhed imod risici, der kan opstå inden for complianceområdet, er først og fremmest en stærk compliancefunktion i virksomheden.

Som eksempler på ændringer inden for compliancelandskabet, der har haft stor påvirkning på mange virksomheder, kan nævnes GDPR og nye reguleringer imod korruption. Her kan intern revision, på samme måde som med risikostyring, agere som sparringspartner over for ledelsen og give uafhængig assurance til bestyrelsen med hensyn til overholdelse af love og reguleringer igennem såkaldte "Compliance revisioner".

Det kan være svært at måle intern revisions værdiskabelse på området, da formålet er at undgå økonomiske tab og skade på virksomhedens omdømme, som følge af overtrædelser af loven. I tider med en stærk compliance styring vil man således ikke kunne kvantificere værdien af intern revisions arbejde, men hvis der kommer for mange sanktioner og erstatningssager, kan dette virkelig skade virksomheden økonomisk og omdømmemæssigt.
Vigtigheden af at have fokus på compliance opsummeres meget godt af Mærsks revisionschef, som siger således:

…compliance is an area, where, if it goes well, the value addition is not high. But if it goes bad, then it is something that could really explode in your face.

Assurance og Advisory

Traditionelt set har den interne revision haft en tilbageskuende tilgang, hvor man har efterkontrolleret de begivenheder, der allerede er indtruffet. Dette har i sig selv også værdi, men sættes dette sammen med en proaktiv tilgang i form af advisory ydelser, hvor den interne revision kan komme ind og agere sparringspartner i et tidligt stadie på nye projekter og forretningsgange mv., er der et uforløst potentiale for den interne revisions værdiskabelse.

For at finde ud af denne værdiskabelse hos de danske virksomheder, har vi spurgt bestyrelser, ledelser og revisionschefer, hvorvidt deres interne revision udelukkende benyttes til at udføre de mere traditionelle assurance opgaver, eller om de også benytter den i forbindelse med advisory opgaver.

Vores undersøgelse viser en jævn fordeling mellem assurance og advisory. Dette giver en indikation om, at advisory-services, såvel som assurance-services, er en del af den interne revisions arbejdsopgaver, og at danske interne revisionsfunktioner i dag bruger flere ressourcer på advisory ydelser, end man tidligere har gjort, men samtidig har et stort fokus på de mere traditionelle assurance opgaver.

For at finde frem til den optimale fordeling mellem assurance og advisory, henvendte vi os til daværende præsident for IIA, Richard Chambers, der henviste til en global undersøgelse fra 2019, foretaget af The Global Internal Audit Common Body of Knowledge (CBOK), hvor netop den optimale fordeling mellem assurance og advisory services blev undersøgt. Interessenter fra i alt 23 lande deltog i undersøgelsen, som viste, at andelen af advisory services udgjorte alt mellem 7% og 40% af den samlede ressourcemæssige kapacitet for interne revisionsfunktioner. De fleste lå dog i et interval mellem 20-25% af det samlede ressourcemæssige forbrug, hvilket dermed kan være en indikation om en hensigtsmæssig fordeling mellem assurance og advisory. Revisionscheferne lægger vægt på, at på trods af, at der udføres advisory services, bevarer den interne revision en stærk forpligtelse over for uafhængighed, og at levering af assurance services stadigvæk har deres højeste prioritet.

Vi spurgte Mærsks revisionschef, hvordan fordelingen mellem assurance og advisory er hos dem, hvor han forklarer, at Mærsks interne revision inden for de seneste 3 år er begyndt at yde advisory services og ligger i dag på en fordeling på 10-15% advisory i forhold til den samlede ressourcemæssige kapacitet. Ifølge revisionschefen kan der gøres endnu mere ud af advisory services:

I think it could be slightly more and could go up to about 20-25% of advisory services. The maximum should be 25%. If we go over the 25%, then I would be concerned because of the threat to the independence as well as the fact that we should be giving assurance, because that's the kind of reliance that the Board can get towards the company being well run and managed.

Revisionschefen forklarer omkring ræsonnementet for deres beslutning om at yde mere advisory services:

We have made a conscious choice to do more advisory, because that's also from where we're providing our kind of input, in advance. Sometimes the IA (internal audit) provides assurance after the fact, which is not so helpful, because then the risk has already materialised, and the losses have incurred. So, we're thinking: How can we help the business reap more value from what we are doing.

CBOK-studiet viser, at fordelingen mellem assurance og advisory er meget varierende mellem virksomheder, hvilket gør det besværligt at komme med et generelt bud på, hvad en optimal fordeling mellem de to er. Dette giver også mening, da virksomhederne har forskellige behov, og det er forskelligt, hvad bestyrelsen ønsker at bruge den interne revision til. Der viser sig dog at være en enighed mellem CBOK-studiet og Mærsk om, at en hensigtsmæssig fordeling ligger på ca. 20-25% advisory. Vi kender ikke baggrunden for, hvorfor fordelingen i CBOK-studiet oftest ligger i dette interval, men det kan tænkes, at de fleste virksomheder også har samme overvejelser omkring problematikken med den interne revisions uafhængighed og objektivitet, hvis andelen af advisory overstiger 25%.

Sammenfatning af brug af intern revision

Baseret på vores egen undersøgelse af danske forhold, sammenholdt med internationale studier, kan vi konklu-

derende sige, at danske industrielle virksomheder benytter den interne revision til både finansiel- og operationel revision. Der er indikationer på, at der er et stigende fokus på den operationelle revision, da virksomheder har indset, at der er muligheder for den interne revision at tilføre mere værdi på dette område. Ekstern revision udfører allerede finansiel revision, hvorfor nytteværdien af, at intern revision også udfører denne form for revision, er begrænset. Derudover er der indikationer om, at danske industrivirksomheder er ved at indse, at intern revisions værdiskabelse kan optimeres ved at udføre en større andel advisory services for at komme risici i forkøbet og dermed reducere risikoen for tab. Der findes ikke en optimal fordeling mellem assurance og advisory, som passer til enhver organisation, da det afhænger af forskellige faktorer, så som den enkelte virksomheds omstændigheder, målsætninger og virksomhedens modenhed med hensyn til risikostyring og interne kontroller.

Egen definition af intern revisions værdiskabelse

Når der skal vurderes om behovet for en intern revisionsfunktion, bliver nødvendigheden af etablering af sådan en funktion ofte holdt op imod virksomhedens 2nd line of defence og den eksterne revision. Interessenter har svært ved at få øje på nødvendigheden af at etablere en intern revision, når alle virksomheder i forvejen har de to andre funktioner, som i høj grad kan udføre de samme arbejdsopgaver.

Med udgangspunkt i dette, har vi udarbejdet vores egen definition af intern revisions værdiskabelse.

Egen definition

Formålet med nedenstående formulering er at komme med en simpel definition, der indeholder kernepunkterne i forudsætningerne for intern revisions værdiskabelse, samt hvordan den adskiller sig fra andre sammenlignelige funktioner.

> *Intern revision er en funktion med dyb forretningsforståelse, som styrker organisationens governance, risikostyring og interne kontroller, med uafhængig og objektiv assurance og rådgivning til både bestyrelse og daglig ledelse.*

For at vende tilbage til de funktioner, som intern revision ofte bliver holdt op imod, kan man, som kritik af definitionen sige, at virksomheder allerede har en funktion, som styrker virksomhedens risikostyring og interne kontroller i form af deres 2nd line of defence, hvilket gør etablering af intern revision unødvendig. Virksomheden får derudover objektiv og uafhængig assurance og rådgivning gennem den eksterne revision. Spørgsmålet er så, hvad adskiller intern revision fra disse enheder?

Differentiering fra 2nd line of defence

En intern revision differentierer sig fra 2nd line of defence ved at have den højst mulige grad af uafhængighed i virksomheden, samt, at den organisatoriske placering og arbejdsfordeling gør, at den kan forholde sig objektivt til arbejdet. De forskellige controller-funktioner har sandsynligvis en dyb forretningsforståelse, men deres organisatoriske placering, hvor de er ansat af og rapporterer til den daglige ledelse, gør, at deres rapportering ikke kan anses som fuldstændig uafhængig og objektiv. En 2nd line of defence kan derfor have en tilbøjelighed til at rapportere på en måde, der tilfredsstiller den daglige ledelse fremfor at forholde sig fuldstændigt objektivt til eventuelle problematikker. Med den højst mulige grad af uafhængighed inde i organisationen kan den interne revision derimod forholde sig fuldstændigt objektivt til problematikker og rapporteringen heraf, da den ikke har et incitament til at tilfredsstille den daglige ledelse. Dette bør, alt andet lige, iklæde bestyrelsen til at kunne forholde sig mere kritisk til rapporteringen fra den daglige ledelse og derved sikre en forsvarlig organisation af virksomheden.

Differentiering fra ekstern revision

Virksomheden kan også få objektiv og uafhængig assurance fra eksterne parter. Her er der især fokus på den eksterne revision. Den eksterne revision har fokus på at revidere de områder, som påvirker regnskabsaflæggelsen og ikke på alle andre områder i virksomheden. Den interne revision har et bredere fokus, som også kan omfatte revision i forhold til regnskabsaflæggelsen, men ikke er afgrænset hertil, hvorfor det ville være forkert at sammenligne disse to enheder med hinanden. Vores undersøgelser viser dog, at bestyrelser har en tendens til at sammenligne intern revisions nytteværdi i forhold til ekstern revision, når der skal vurderes, om behovet for etablering af en intern revisionsfunktion. Igennem vores undersøgelser har vi kunnet påvise en indikation på, at denne tendens også er gældende i Danmark. Derfor er der et behov for at differentiere intern revisions værdiskabelse fra ekstern revision.

Etisk adfærd

Det kan være svært at måle intern revisions værdiskabelse, da ikke alt kan måles i kroner og ører. Til sidst er det også værd at nævne, at intern revision kan tilføre værdi ved at være med til at påvirke virksomhedens etiske adfærd med hensyn til governance, risikostyring og interne kontroller, og derved medvirke til en sund "tone at the top". Med tilstedeværelsen af intern revision som en uafhængig enhed, der samtidig har en dyb virksomhedsforståelse, stilles den daglige ledelse i højere grad til ansvar for deres handlinger, da intern revision kan forholde sig kritisk til måden, tingene gøres på i virksomheden, uden at frygte for mulige konsekvenser af sin kritiske holdning. Når den daglige ledelse i højere grad stilles til ansvar for deres handlinger, bør det, alt andet lige, føre til en mere forsvarlig drift af virksomheden, hvilket også vil påvirke virksomheden økonomisk på lang sigt.

Afrunding

I denne artikel har vi behandlet, hvordan intern revision kan tilføre danske virksomheder værdi. Artiklen er en kort version af en meget større og mere omfattende analyse, som vi har foretaget i vores kandidatafhandling.

Til sidst vil vi derfor fremhæve hovedpunkterne for, hvad læseren skal stå tilbage med efter at have læst artiklen, hvor fokus er at svare på det indledende spørgsmål til artiklen – *Skaber intern revision merværdi for virksomheder?*

Hovedpunkterne er følgende:

- Større fokus på operationel revision
- Mulighed for øget værdiskabelse ved advisory ydelser
- Løbende kommunikation af intern revisions værdiskabelse

Større fokus på operationel revision
For virksomheder, der i dag hovedsageligt benytter deres interne revisionsfunktion i forbindelse med finansiel revision, er der gode muligheder for at øge værdiskabelsen ved at have et større fokus på at udføre operationel revision i bred forstand. Med "bred forstand" mener vi, at dette også inkluderer ydelser inden for compliance og risikostyring.

Hermed påstår vi ikke, at udførsel af finansiel revision ikke også kan tilføre værdi til en virksomhed, men at nytteværdien af den interne revisionsfunktions ressourcer bliver forhøjet ved at dække områder i virksomheden, som ikke allerede bliver dækket af den eksterne revision. Ved at bryde fra den mere traditionelle finansielle revision, kan den interne revision også bedre påvise den værdiskabelse, som den tilfører virksomheden over for interessenter.

Mulighed for øget værdiskabelse ved advisory ydelser
Internationalt ser man en trend, hvor interne revisionsfunktioner vælger at bruge flere ressourcer end tidligere på advisory ydelser. Fordelen ved denne tilgang er, at man får mulighed for at agere sparringspartner på implementeringer af nye forretningsgange og projekter i et tidligt stadie og på den måde støtte virksomheden i at sikre, at de rigtige foranstaltninger foretages fra begyndelsen af.

Det skal dog gøres klart, at udførelse af assurance opgaver stadig er kerneydelsen for den interne revision, da det overordnede mål er at give bestyrelsen sikkerhed for, at virksomheden bliver drevet på en hensigtsmæssig måde. Med udgangspunkt i dette mener vi, at intern revisions værdiskabelse kan øges ved at have en hensigtsmæssig fordeling mellem assurance og advisory, hvor fordelingen ligger omkring 75 % assurance og 25 % advisory.

Kommunikation
For at få intern revision mere udbredt i Danmark er den største udfordring for IIA, at få kommunikeret denne værdiskabelse ud til dem, der skal træffe beslutningen om oprettelse af en intern revisionsfunktion. En adgang ind til landets bestyrelsesmedlemmer og C-suites er derfor vigtig for at have mulighed at kommunikere værdiskabelsen til beslutningstagerne.

Til bestyrelsesuddannelsen på CBS bliver der undervist i intern revision. Her opfordrer vi til, at man i undervisningen har fokus på, hvordan en intern revision differentierer sig fra de andre sammenlignelige funktioner, som vi har nævnt tidligere, samt hvilken værdi, dette medfører.
De interne revisionsfunktioner, som allerede er oprettet, spiller også en stor rolle for udbredelsen af den interne revisionsprofession i Danmark. Især revisionscheferne skal have fokus på at kvantificere funktionens resultater, hvor det er muligt sådan, at bestyrelser kan få leveret håndgribelige resultater, når der er mulighed for det.

Revisionscheferne skal derudover have løbende fokus på at kommunikere funktionens værdiskabelse til bestyrelsesmedlemmer og C-suites med henblik på, at disse, på baggrund af succesoplevelser, kan videreformidle budskabet om værdien ved at etablere en intern revision til deres øvrige netværk af beslutningstagere.

Konkluderende kan man sige, at der foreligger nogle spændende initiativer for udbredelse af den interne revisionsprofession i Danmark. Ansvaret for at få etablering af intern revision mere udbredt i Danmark ligger både hos IIA og de interne revisorer selv. IIA har taget et vigtigt initiativ for udbredelsen ved at introducere intern revision som et emne i bestyrelsesuddannelser, mens professionen selv skal have løbende fokus på at kommunikere værdiskabelsen til sine interessenter.

Noter

[1] Parkin et al., 2012
[2] Finanstilsynets opdeling af intern revisions arbejdsområder – Finansiel revision; Operationel revision, Riskostyring og Compliance
[3] Besvarelser inden for andre: Advisory on internal controls, processes and IT; Internal investigations, AC secretary; GDPR; IT
[4] Johansen et al 2016, s. 281
[5] Anderson et al 2017, s. 6-30

IIA-DK i dialog med Finanstilsynet omkring fornyelse af Revisionsbekendtgørelsen

Tobias Zorde, Afdelingsdirektør, Nykredit

"Foreningen af Interne Revisorer (IIA-DK) har foretaget gennemgang af BEK nr. 1912 af 22/12/2015 (Revisionsbekendtgørelsen) med det for øje at bidrage til den fortsatte positive udvikling af intern revisions rolle i finansielle virksomheder til gavn for finansiel stabilitet, forbrugerbeskyttelse og, ikke mindst, til gavn for bestyrelser i form af hjælp til beskyttelse af virksomhedens aktiver, omdømme og fortsatte drift. Gennemgangen er foretaget af Fagligt udvalg [for SIFI institutter] i regi af IIA-DK efter opdrag fra det Finansielle udvalg."

Således påbegyndes et notat sendt til Finanstilsynets kontor for Finansiel Rapportering fra IIA-DK's Finansielle udvalg. Notatet har været drøftet imellem repræsentanter fra samtlige SIFI-institutter i regi af det faglige udvalg samt repræsentanter for mindre pengeinstitutter og forsikringsvirksomheder i regi af det Finansielle udvalg.

Af notatet fremgår yderligere, at baggrunden for gennemgangen er den gradvise forskydning fra den såkaldte danske model til en mere international orienteret praksis og standard for den interne revisionsfunktion. IIA-DK har med notatet ønsket at henlede Finanstilsynets opmærksomhed på en række begreber i Revisionsbekendtgørelsen, der med fordel kunne adresseres for sikre, at der fortsat er sammenhæng mellem de anvendte begreber og den internationale praksis for intern revision i den finansielle sektor.

Begreberne udgøres bl.a. af:

- God revisorskik
- Høj-/begrænset grad af sikkerhed
- Væsentlighed
- Rapporteringsmæssige modifikationsbegreber, herunder: bemærkning, kommentar, supplerende forhold, supplerende information, forhold og forbehold

Det er IIA-DKs opfattelse, at disse begreber på afgørende vis er præget af forvirring hidrørende fra den danske model, som tager udgangspunkt i ekstern revision af regnskaber. Den manglende afklaring står således til hinder for, at intern revision kan aktualisere sig selv til fulde som en del af forsvarsværket. Begrebsligheden synes fortsat at være hentet fra ISA-standarder (revisionsstandarder for eksterne revisorer til brug for revision af regnskaber) snarere end at tage udgangspunkt i eksempelvis IPPF (IIA's begrebsramme) og de sektorspecifikke internationale guidelines fra eksempelvis BASEL, EBA, EIOPA, ESMA, ECB etc. Gennemgangen har givet anledning til konkrete anbefalinger på kort- og længere sigt (se **Tabel 1** herunder).

Dialogen med Finanstilsynet vedr. notatet foregår i regi af Det rådgivende revisionsudvalg, hvor IIA er repræsenteret. Det rådgivende revisionsudvalg sammensætter sig herudover af deltagere fra FSR og Finanstilsynet. Der har indtil videre været et enkelt møde, hvor dialogen har været imødekommende og konstruktiv. Det er IIA's opfattelse, at Finanstilsynet er lydhøre over for kommentarerne, som i første omgang vil være omdrejningspunkt for yderligere dialog til input og inspiration for kommende versioner af Revisionsbekendtgørelsen. Notatet kan findes i fuld længde på IIA's hjemmeside.

Tabel 1: Konkrete anbefalinger på kort og længere sigt

Kort sigt	Længere sigt
• Det anbefales at tydeliggøre, at intern revisions primære opdrag er revision af de risikofyldte områder (operationel revision), og at alle præciseringer omkring skik og krav til intern revisions arbejde udelukkende tager afsæt i dette formål. Det anbefales endvidere, at alle supplerende krav til interne revisioner, der påtegner årsregnskabet (finansiel revision) behandles særskilt evt. i separat bilag. • Det anbefales at indføre "Certified Internal Auditor" i kombination med en længere videregående uddannelse som alternativ adgangsgivende baggrund til bestridelse af posten som revisionschef. • Det anbefales at foretage diverse begrebsafklaringer og justeringer ift. konkrete detail-kommentarer, som fremgår af det fremsendte notat.	• Det anbefales at indsnævre anvendelsesområde for Revisionsbekendtgørelse til kun at omfatte krav til ekstern revision. Krav til intern revision inkorporeres i Ledelsesbekendtgørelsen m. separat bilag. • Som alternativ anbefales det at opsplitte revisionsbekendtgørelsen i to separate bekendtgørelser henvendt til henholdsvis intern og ekstern revision.

Gør dig selv den tjeneste - Gå ind og oplev Internal Auditor Magazine.

Er du ligeså glad for Ia (Internal Auditor) magasinet som os, så er det gratis tilgængeligt i en digital udgave via hjemmesiden InternalAuditor.org eller direkte via app til både iOS og Android. Så uanset hvor du er, så har du adgang. Bemærk dog at du først skal anmode om adgangen via dine medlemsoplysninger på www.iia.dk.

Artiklernes indhold er nu også linket til emner, så ønsker du viden inden for bl.a. Governance, Risk, Compliance eller Fraud – så er det virkelig nemt.

Ia magasinet er kåret som den førende kilde der leverer det mest relevante indhold til erhvervet Intern Revision i realtime, og med flere platforme og 24/7 adgang, er det lettere end nogensinde at holde trit med det udviklingen indenfor feltet intern revision.

Den digitale udgave af Ia er en fuld replikeret version af magasinet, så du kan se hele udgaver og bladre mellem siderne - ligesom den trykte udgave. Du finder en række navigationsværktøjer til at gennemse artikler samt bonusvideoindhold parret med udvalgte funktionsartikler.

Arkivet for den digitale udgave går tilbage til februar 2004 og er fuldt søgbare så du kan udnytte dets robuste søgefunktion for at identificere artikler af interesse.

www.InternalAuditor.org

www.theiia.org

The Institute of Internal Auditors

Making Internal Audit more dynamic, trusted and well-respected

Miguel Zorita Gil, MBA, Internal Audit Manager, Nordea

I still remember a quote from my early days in the banking sector: *"Organisations without a strong and well-respected audit function will run into problems, it's just a matter of time"*. In general terms, the internal audit function serves as a "safeguard" for organisations to ensure that their processes are run in a controlled and regulatory compliant manner so that risks and therefore potential losses are appropriately managed.

However, there are many different ways in which an internal audit engagement can be conducted. In this article, I would like to reflect upon the different practices during the audit engagement that I personally think are fundamental towards ensuring that the internal audit function keeps evolving into a more dynamic, trusted and well-respected unit.

In the following, the term *'audit'* refers to internal audit and auditors, unless otherwise stated.

We as auditors are not in possession of the truth

The audit function is complex by nature, as it demands a broad spectrum of expertise from auditors in order to enable them to give their opinion on different topics. As a result, sometimes the auditor's role is defined as 'generalist', based on the amount of knowledge the auditor should possess, which is not to the same degree as a specialist, to complete the work diligently.

Bearing that in mind, during all stages of the audit engagement but particularly during the planning stage, it is important to convey through our interactions a perception of willingness to learn about the different aspects of the auditee's work. In that respect, the first step is to acknowledge that we as auditors are not in possession of the truth, we need to prepare ourselves both before and during the audit. This is something we can be transparent about, as this will ultimately help us to build trust within the organisation.

The main reason why I think it is relevant for auditors to always keep this in mind is because it truly helps the auditees to perceive that the auditor is making a genuine effort to fully understand the audited area, as opposed to be simply looking for gaps based on previous experience. A good understanding of the audited area through open dialogue and a deep questioning exercise will in my view not negatively impact the image of the auditor. On the contrary, the auditor will be in a better position to use previous experience (either as an auditor or specialist) in the particular audited area.

Similarly, the auditee will feel the effort being made by the auditor to fully understand their processes, context, circumstances and / or challenges, and therefore will tend to empathise and consequently be more open to further discussions, which will ultimately lead to a more valuable audit outcome. The auditor is presumed to be professionally qualified, and therefore the interactions throughout the planning phase are not intended to cover a potential lack of knowledge, but rather to complement it.

Transparency

During the course of an audit engagement, there are different stages where I consider it fundamental to be fully transparent about the work we do and the way we do it.

First and foremost, our auditees should be absolutely clear on what is the objective of the audit engagement, how we expect to achieve it and what is the reason why the audit needs to be conducted in that particular area at that particular point in time.

What is transparency?

Transparency is primarily the practice whereby we disclose any relevant information regarding an audit, such as the justification for us to conduct the audit, the methodology that we intend to follow, the rationale as to why we believe something is a gap, the reasons which might be preventing us from providing assurance towards a specific area, etc.

This means that before anything is disclosed, an exercise needs to have been conducted within the audit engagement team to ensure that the audit scope, timeline, risks or testing strategies are justified and reasonable, so that we are in a solid position to deal with any potential challenge coming our way. Transparency serves as a method for auditors to reflect internally, identify weaknesses and correct them before anything is disclosed to the auditees.

What are the limits of transparency?
In my view, there should be no limits as to how transparent we can be as auditors. That does not mean we can't have internal discussions on how to position a specific aspect of an audit, for instance, but we should be prepared to share the rationale of each of our decisions. In that sense, through transparency, we as auditors can even build trust and credibility through error recognition.

It is not uncommon to realise that something that looked like a big gap at the beginning of an audit, might start to look like something minor or even negligible later on. If so, let's acknowledge it openly in front of the auditees, making them aware of the reasons that made us consider the gap as an issue initially, and why we consider it not to be a problem anymore.

Similarly, sometimes being open when we do not understand a process, a specific control design or even the rationale as to why something is being undertaken in a certain manner, can also help build trust in us, as this can generate discussions with the auditees that could make them reflect on why their own processes or controls are designed the way they are, and could therefore lead to potential improvements. Obviously that won't always be the case, but even when such an outcome is not obtained, being open and clear when we do not understand something is a fair approach to ensure that we can effectively provide assurance towards the audited area.

The most challenging form of transparency
Probably the transparency that we exercise towards ourselves is the most critical yet relevant form of transparency.

Inevitably, when we conduct an audit engagement, we look for either gaps or potential improvements to justify the work we do. This is partially driven by the general perception whereby the existence of the audit function is justified on the basis that it's able to identify such gaps. I won't say this is inaccurate, but I believe the audit function should be and is moving into a much more relevant and exciting role in the organisation.

As an auditor, I should not be scared of issuing an audit report with no issues or findings. This is a statement I keep repeating to myself to ensure I am absolutely transparent and honest to myself, the auditees and the audit function as a whole. It is definitely an extreme case, as normally there is always room for improvement (also in the way we do our audits), and therefore it is unlikely that no improvements or gaps will come out from an audit engagement.

But as a matter of principle, why should I be afraid of signing off on an audit with no gaps, if I truly believe I have done my work well and the audited area shows a well-designed control approach, for instance? On the contrary, in my view, the trust and recognition towards the audit function is damaged when issues that add no value are raised.

Being more transparent when sharing our findings
We can and we should be more transparent when sharing audit findings, as there are only benefits attached to it. Sometimes we tend to delay sharing our findings with the auditee in order to be absolutely confident that what we are raising is definitely an issue. In principle, I would not say that this is an incorrect approach, but there are definitely benefits associated with an early involvement of the auditees on this matter. It gives us more time to work with the auditees on the potential findings, and provides us with input which might allow us to enrich the content of the finding or maybe reconsider it, and which otherwise would have not been disclosed until at a later stage of the audit.

In addition, an early dialogue with our auditees on potential issues also prevents us from carrying an incorrect perception of something until the end of the audit, with the associated costs this may have in terms of time and resources, to finally realise that what we considered as an issue, is in fact not an issue.

The way we communicate is the way we are perceived

The work of an auditor is not only reflected in the final report, and therefore, care and attention should be given to every single interaction we have with our auditees throughout an audit project. Every single e-mail, meeting or phone call builds up the image of who we are and how the audit will be perceived, and will undoubtedly impact the final outcome of the audit and our future interactions.

Having recognised this fact, I spend a lot of time when I write an e-mail. I try to be clear and concise, I make sure my writing is kept professional whilst I also leave space to engage further and get to know each other better.

But most importantly, I try to put myself in the reader's shoes. Why should I not explain a bit about the reasons of my documentation request, if I know it will take the auditee a decent amount of time to compile it? Why not recognise the work the auditee is doing, even if it is part of his/her job to do it? Why not leave some room for the auditee to decide if a specific course of action is reasonable or not?

At the same time, as auditors, our verbal communication skills should be something we must work on and be mindful of throughout all our career. Verbal communication can be touched upon from many different angles, and there is not enough room in this article to cover all of them, so I will focus on the one aspect that I keep reminding myself of: Whenever I need to present something to my auditees, particularly during the reporting stage of the audit engagement, I need to keep it simple.

Am I able to explain this in simple terms? If I cannot, then I will assume I don't really understand what I am trying to raise, and therefore I should first of all re-evaluate the topic. Conversely, if before engaging with the auditees I am confident that I can explain the topic in

simple terms so that a third party not involved in the audit would understand it (e.g. a specific issue or gap related to an audit), then it means I have the facts clear and the conversation with the auditees is likely to be productive.

Poor communication can ruin all the good work done

All the good work and effort in an audit engagement can be ruined in a very short period of time, if we do not maintain a high standard of communication consistently and with no exceptions during all the stages of the audit.

This is particularly important to remember when disagreements arise, as it could potentially generate a more impulsive and less constructive way of communicating between the auditor and the auditee. When such an impulse arises, it is always important to take a step back, make an effort to understand the arguments on the table, and carry on with the same professional communication approach used since the beginning of the audit project.

There are many ways in which we can engage with our auditees and make the overall audit experience much better, and at the same time build up our personal and functional brand.

Listening with care is a 'must'

Over the years the role of the audit function has evolved significantly. Originally, the main expectation on the audit function was to provide assurance towards risks and controls and to preserve the organisation's value, which required a certain set of skills.

The overall role of the audit function is now expanding into a wider contribution towards the organisation, whereby auditors are also expected to provide input and add value from a more forward-looking perspective. That is what we know today as the advisory role of internal auditors. However, my objective is not to discuss the evolution of the role itself, but to emphasise how we as auditors can improve the way we work whilst still fulfilling our assurance duties.

Listening with care and the audit mission

Listening with care is, in my view, the capacity to truly listen to our auditees with attention and an open mind, so we can really understand the way they work, the challenges they face or the reasons behind potential weaknesses, whilst we leave behind any potential previous considerations which could unconsciously bias our judgment. The risk we run if we do not listen with care throughout the audit project end-to-end, is an incomplete or biased audit opinion or in the worst case scenario, even a wrong audit report.

Listening with care has always been important for providing assurance. But if the audit function is also to be focused on adding value from a more forward-looking perspective (e.g. providing counsel), it is even more important that we listen to our auditees fully and make sure we get all the facts right.

How to make sure we are listening with care

During the planning phase of an audit engagement the auditor will try to gather a high level overview of the audited area, in order to define the risks and controls which will be subject to testing activities during fieldwork. This is normally achieved through a series of walkthrough sessions held between auditor and auditee, and in which the latter will explain the area and will reply to the questions formulated by the auditor. It is in these walkthrough sessions that the auditor needs to listen with care in order to ask the right questions.

As indicated previously, due to the nature of the audit function, we are to some degree expected to identify gaps which might result in an issue, which will be raised in a report and subsequently fixed by the auditees. Whilst I think it is absolutely fundamental to have this in mind during the audit, I think we need to sometimes leave it aside and change our mindset, and walkthroughs during planning are a good example of this.

If we want to truly listen to our auditees, we can't keep only looking for the gaps whilst they explain the area. We need to just listen and make an effort to ensure that we understand what is being explained to us. The main objective whilst listening should be to understand and capture all the facts, not just flagging gaps as soon as possible, so we can dig into them. We should set aside time to do this, taking into consideration the tight deadlines and limited resources we might have to complete the audit project.

The difference between listening with care and just listening to find the gaps is that in the latter case, we will most likely miss the context, the nuances, the rationale or root cause as to why a potential gap or weakness exists. In the long run, that could eventually lead to less valuable audit outcomes and ultimately a damaged audit reputation.

Listening with care throughout the audit engagement

Even though I personally recognise planning as the audit

stage in which 'listen with care' is more important, that does not mean that during other phases of an audit 'listen with care' is less relevant.

It is common to have disagreements during the reporting phase, as this is when we would normally share our findings and proposed criteria to close a gap. When having those conversations it is important not to focus solely on 'defending' the reasons as to why the issue is being raised, but to carefully listen to the arguments which the auditee is putting on the table to potentially justify that the risk being flagged is already mitigated by the current processes.

Firstly, if during the planning phase we listened with care, the likelihood of having a fundamental disagreement during the reporting phase on how a risk is being dealt with is considerably lower. That does not mean it can't happen, but it will definitely reduce the probability.

Secondly, if for whatever reason there is a disagreement at the reporting stage, we must be transparent on the reasons that led us to consider that such a risk needed to be dealt with differently, as this will reveal any potential misunderstanding from our initial conversations.

Finally, we should listen carefully to the rationale given by the auditees, as we might have missed something important, or we perhaps gave too much weight to something, which in the proper context is not as relevant as we thought it was initially (e.g. the likelihood of the risk materialising is much lower than anticipated or the overall impacts are minimal based on the new explanations).

Having said that, we as auditors can still disagree even when we are fully transparent and listen with care, as it might well be that we still perceive that the risk is not being mitigated, or that a specific control is not strong enough. The difference is that if we have truly listened, the arguments to support our views on a specific topic will be much more robust, and we will likely end up in an agreement with the auditee. This is particularly evident in cases of disagreements caused by different views on very technical topics, as in those cases listening with care is even more relevant.

Overall, if the auditee believes that the auditor has listened, has been clear on the arguments and openly discussed them, a common ground will be reached and the trust in the audit function will have definitely improved.

It is important that the audit function is not seen as an isolated piece of the puzzle

As stated at the beginning of the article, I see the audit function, and in particular internal audit, as a fundamental pillar to keep an organisation healthy. In that sense, it is important that the audit function is not seen as an isolated piece of the puzzle, even if the reporting structures need to be carefully designed to ensure its independence. We need to make our auditees feel that we are part of the same team, and we should be seen as an opportunity to step back from the day-to-day and re-think the way we do things.

Besides, when conducting an audit engagement, we need to make our auditees feel that their risks are our risks, and the first step to achieve that is to truly believe that this is indeed the case. We should not see the risks or gaps that we identify as something completely separated from us, and we should approach the auditees with a mindset that conveys this idea to them.

We are part of the same team

It is fundamental to make the auditee feel that we as auditors have a genuine interest in mitigating a risk or closing a gap rather than simply raising an issue. The way I tend to approach this is through different techniques such as:

- Making it clear to the auditee throughout the discussions on a specific topic (e.g. a potential issue or risk identified), that there is no intention whatsoever of raising an issue if the risk or gap identified is finally assessed as immaterial or very unlikely to take place (for example), as the objective is to generate value and not additional work.
- Putting on the table different scenarios (e.g. from most to least likely or impactful), to jointly identify what will be the worst outcome, if the risks were to materialise.
- Substantiating our findings to evidence how things have already gone wrong due to the identified weaknesses.
- Sharing past experiences on how we have seen other organisations deal with a specific risk or gap and what type of consequences we have seen.

Ensuring that our auditees perceive us as equals and as part of the same organisation, albeit always maintaining strict rules to preserve our independence, will not only improve our professional brand as auditors, but will indirectly promote further collaboration from both sides. This will ultimately foster better and more productive discussions that will result in a more value-adding audit report and ultimately improvements to the business.

To sum up, even though the role of internal auditors (and probably the overall mission of the audit function as a whole) is constantly evolving, our auditees should always be at the centre of what we do, and we should constantly do our best to ensure the internal audit function is trusted, as the rest will come naturally.

De gode styredokumenter

Camilla Sabrina Kyed Overgaard, Manager, Deloitte

Baggrund

Arbejdsbeskrivelser, manualer, forretningsgange, politikker og forretningsmodeller. Der er dokumenter nok at holde styr på, når det kommer til styredokumenter.

Mens vi alle er klar over, at formålet med styredokumenter er at sikre en sikker og effektiv virksomhedsledelse, fortaber formålet sig alt for ofte, fordi vores styredokumenter slet og ret ikke er gode nok og ikke anvendes aktivt af organisationen. Styredokumenterne reduceres i disse tilfælde til skuffedokumenter, som hives frem fra skuffen, når tilsynsorganer, interne som eksterne, melder sin ankomst.

Skuffestyredokumenter er spild af både organisationens og tilsynsorganernes tid, så hvordan sikrer vi os, at vores styredokumenter er formålstjenestelige? For hvad er egentlig formålet med de enkelte dokumenter, og hvad kendetegner dem hver især? Hvad skal forretningsmodellen behandle, og hvad er den rigtige snitflade mellem forretningsgange og arbejdsbeskrivelser? Hvad er forskellen på en politik og en forretningsgang, og hvordan sørger man bedst for, at de mange styredokumenter får de bedste vilkår for at komme til at "leve" i organisationen?

Spørgsmålene vedrørende styredokumenter og disses sammenspil er mange og med rette. Indholdet af styredokumenter og rammen herom er nemlig fastlagt igennem praksis med den konsekvens, at det kan være vanskeligt at få et overblik over "best practice" og opskriften på de gode styredokumenter.

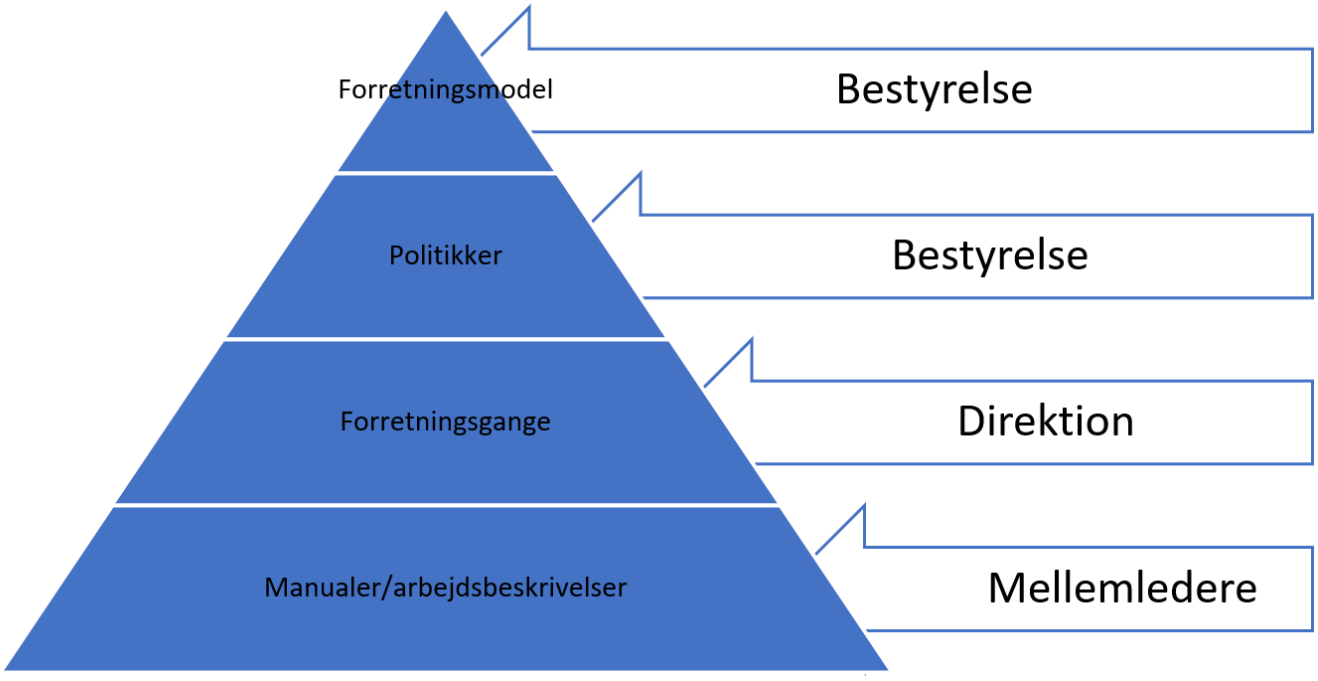
Hvis du vil du være klogere på de enkelte styredokumenter, så læs med.

Dokumenthierarkiets formål

Før en gennemgang af de enkelte styredokumenter giver det mening at træde et skridt tilbage og overveje, hvorfor styringen af virksomheder er fordelt over flere dokumenter.

Ledelsen af en virksomhed sker som bekendt på flere niveauer. Mens bestyrelsen tager sig af den overordnede og strategiske ledelse, inden for de lovgivningsmæssige rammer som virksomheden er underlagt, er det direktionens opgave at forestå den daglige ledelse med respekt for de rammer, som bestyrelsen har udstukket. Afhængig af virksomhedens størrelse vil direktionen have uddelegeret en række opgaver under den daglige ledelse til mellemledere.

Figur 1. Dokumenthierarki



Fordi bestyrelsen, direktionen og mellemledere har meget forskellige opgaver i forhold til virksomheden, bør de hver især fokusere deres tid og kræfter inden for de områder, hvor deres ansvar ligger.

Af denne grund er bestyrelsen pålagt opgaven med udarbejdelse af forretningsmodel, strategi og politikker, som fastligger de overordnede rammer for virksomhedens aktiviteter og de risici, som virksomheden ønsker at påtage selv.

Virksomhedens direktion udmønter bestyrelsens beslutninger, som disse er formuleret i forretningsmodel og politikker, i forretningsgange, som indeholder direktionens svar på, hvordan man efterlever de krav og målsætninger, der er fastlagt i politikken og forretningsmodellen. Som nævnt vil der afhængig af virksomhedens størrelse findes et lederniveau under direktionen, som i arbejdsbeskrivelser og manualer kan fastsætte et lavpraktisk værktøj til, hvorledes opgaverne i forretningsgangene løftes.

Opsummerende kan dokumenthierarkiet betragtes som en pyramide, hvor forretningsmodellen er øverst, politikkerne under forretningsmodellen, forretningsgangene under politikkerne og endelig arbejdsbeskrivelser og manualer under forretningsgangene - **se Figur 1** på foregående side.

Nedenfor følger en nærmere gennemgang af de enkelte styredokumenters karakteristika.

Styredokumenter - ejerskab og indhold

Forretningsmodel

- Ejes af bestyrelsen, som er ansvarlig for den overordnede og strategiske ledelse af virksomheden.
- Forretningsmodellen vil gå på tværs af områder og udgøre virksomhedens helt overordnede plan. Ofte vil forretningsmodellen være formuleret som målsætninger.
- For visse virksomhedstyper, fx finansielle virksomheder, er der en række krav til elementer, der skal behandles i forretningsmodellen.

Politikker

- Ejes af bestyrelsen og er en udmøntning af de beslutninger, som er truffet i forretningsmodellen.
- Skal indeholde overordnede strategiske mål for virksomheden. Politikkerne vil ofte være formuleret som krav.
- Skal være fastlagt for alle væsentlige risikoområder.
- Skal være målbare.
- For visse virksomhedstyper, fx finansielle virksomheder, findes der regulering, som specificerer kravene til indholdet.
- Skal fastlægge roller og ansvarsfordeling.

Forretningsgange

- Ejes af direktionen og skal udmønte krav og målsætninger i politikkerne. Det er direktionen der har ansvaret for at "sikre", at der findes nødvendige og tilstrækkelige forretningsgange. Direktionen kan dog uddelegere opgaven vedrørende udarbejdelse og vedligehold af enkelte eller alle politikker til relevante mellemledere (eller øvrige medarbejdere). Ved uddelegering skal direktionen sikre, at de mellemledere (eller øvrige medarbejdere), der uddelegeres til, besidder rette kompetencer og indsigt.
- Skal være fastlagt på alle væsentlige aktivitetsområder.
- Skal være operationelle og kunne fungere som et dagligt værktøj for de disponerende enheder, de er relevante for.
- Skal besvare, **hvilke** opgaver der skal løftes, **hvem** der skal løfte disse opgaver, **hvornår** disse opgaver skal løftes, og **hvordan** opgaverne skal løftes.
- Faktisk fastlæggelse af roller og ansvarsfordeling, herunder evt. krav til ledelsesrapportering.

Manualer/arbejdsbeskrivelser

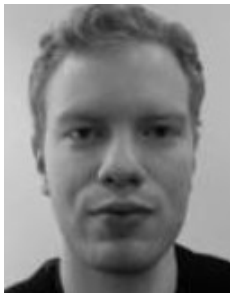
- Ikke krav om arbejdsbeskrivelser/manualer kan ud fra en konkret vurdering af virksomhedens størrelse og forhold give mening.
- Lavpraktisk værktøj eller step-by-step-vejledninger.
- Skal i sammenhæng med forretningsgange kunne stå alene, så en hvilken som helst medarbejder i princippet skal kunne udføre en opgave ved at følge manualen.

Afsluttende bemærkninger

På baggrund af ovenstående gennemgang kan det altså understreges, at det er afgørende at sikre, at der er sammenhæng hele vejen ned igennem dokumenthierarkiet eller pyramiden. Målsætninger i forretningsmodellen skal støttes af krav i politikkerne, som igen skal udmøntes i operationelle beskrivelser af handlepligter i forretningsgangene.

Derudover bør det sikres, at reguleringen af et givet forhold sker det rette sted i organisationen og dermed i dokumenthierarkiet. Opretholdes den korrekte snitflade ikke mellem de enkelte dokumenter, mudrer dette ansvarsfordelingen i organisationen. En rodet ansvarsfordeling medfører en mindre effektiv virksomhedsledelse, hvilket kan betyde højere administrative omkostninger og øget risiko for fejl, der kan medføre tab. Over tid kan dette afspejle sig i virksomhedens bundlinje. Denne årsag alene er så væsentlig, at den bør være begrundelse nok for, at en organisation prioriterer gode styredokumenter.

Nye regler for finansielle virksomheders outsourcing



Nicolas Damm Machholm, Fuldmægtig, cand.jur., Finanstilsynet

Indledning

Den teknologiske udvikling på IT-området muliggør en stadigt større brug af outsourcing, som i højere og højere grad bliver en integreret del af forretningsdriften for finansielle virksomheder. Udviklingen ses herhjemme såvel som på europæisk niveau. EBA (European Banking Authority) fastlagde i 2019 opdaterede retningslinjer for outsourcing, der i Danmark er blevet implementeret i bekendtgørelse om outsourcing for kreditinstitutter m.v. (outsourcingbekendtgørelsen), som trådte i kraft den 1. juli 2020.

Bekendtgørelsen erstatter den tidligere bekendtgørelse om outsourcing af væsentlige aktivitetsområder. Den medfører både en række nye krav og lempelser af de eksisterende krav til virksomhederne.

Formålet med reguleringen af outsourcing er at sikre, at virksomhedernes brug af outsourcing sker på en betryggende måde gennem tilstrækkelig ledelse, styring og kontrol i virksomhederne. Reglerne er dermed udtryk for god governance og kan ses i sammenhæng med reglerne i bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. (ledelsesbekendtgørelsen).

Derudover har Finanstilsynet netop offentliggjort en vejledning til outsourcingbekendtgørelsen. Vejledningen præciserer Finanstilsynets praksis og forståelse af bekendtgørelsens bestemmelser.

Bekendtgørelsens anvendelsesområde

Outsourcingbekendtgørelsen finder anvendelse på følgende virksomheder:

- Pengeinstitutter
- Realkreditinstitutter
- Fondsmæglerselskaber
- Investeringsforvaltingsselskaber
- Sparevirksomheder
- Fælles datacentraler
- Operatører af regulerede markeder
- E-pengeinstitutter
- Betalingsinstitutter
- Danmarks Skibskredit A/S.

Bekendtgørelsen finder også anvendelse på delkonsolideret og konsolideret niveau for de nævnte virksomheder med undtagelse af betalingsinstitutter og e-pengeinstitutter. Bekendtgørelsen finder ikke anvendelse på outsourcing, der er reguleret af andre regler på det finansielle område, dvs. når der er tale om *lex specialis*.

Ved outsourcing forstås enhver ordning mellem en virksomhed og en leverandør, i henhold til hvilken leverandøren udfører en proces, tjenesteydelse eller aktivitet, som outsourcingvirksomheden ellers selv ville udføre. Er en ordning klassificeret som outsourcing, følger en række krav til kontrakten og til virksomhedens styring og kontrol med outsourcingen.

Bekendtgørelsen opstiller desuden en række yderligere krav til ordninger, der klassificeres som "kritisk" eller "vigtig" outsourcing. Dette svarer i praksis til klassifikationen "væsentlig" outsourcing under det gamle regelsæt. Outsourcing skal anses som kritisk eller vigtig, hvis en fejl eller mangel ved dens udførelse væsentligt vil forringe et eller flere af følgende forhold for den outsourcende virksomhed:

- mulighed for at overholde betingelserne i sin tilladelse
- finansielle resultater
- mulighed for på forsvarligt grundlag at udøve sine aktiviteter.

Outsourcing af tilladelsespligtige aktiviteter vil per definition udgøre kritisk eller vigtig outsourcing. Ved kritisk eller vigtig outsourcing gælder bl.a. strengere krav til indholdet af kontrakten.

Endeligt gælder et proportionalitetsprincip for hele bekendtgørelsen. Det indebærer, at kravene i bekendtgørelsen kan lempes, hvis det er proportionelt med de konkrete karakteristika ved den enkelte virksomhed eller den enkelte outsourcingordning, eksempelvis en virksomheds størrelse, risikoprofil eller forretningsmodel, eller en ordnings kompleksitet, risici eller potentielle indvirkning på virksomhedens drift. Kravene til outsourcingvirksomheden kan lempes på baggrund af proportionalitetsprincippet, men de kan ikke fraviges helt.

Det centrale i de nye regler

Videreoutsourcing, særligt ift. cloudtjenester

Der er med den nye bekendtgørelse lempet på reglerne for videreoutsourcing. Under den tidligere bekendtgørelses regelsæt var det et krav, at den outsourcende virksomhed aktivt skulle godkende en væsentlig videreoutsourcing, inden en ny underleverandør kunne tages i brug.

Dette er fortsat en mulighed, men med den nye bekendtgørelse er det desuden muligt at aftale, at videreoutsourcing kan foregå efter en model med passiv godkendelse efter en notifikationsmekanisme. Under en sådan ordning vil virksomheden skulle notificeres af leverandøren, hvis leverandøren ønsker at videreoutsource en kritisk eller vigtig outsourcingordning til en underleverandør eller

ændre i en eksisterende videreoutsourcing. Derefter har virksomheden en periode til at vurdere, om den vil acceptere den foreslåede videreoutsourcing.

Notifikationsperioden skal være tilstrækkeligt lang til, at den outsourcende virksomhed som minimum kan vurdere risikoen ved den planlagte videreoutsourcing og reagere, før denne træder i kraft. Virksomheden kan gøre indvendinger ved eksempelvis at gå i dialog med leverandøren om genforhandling eller ved at mitigere de risici, som videreoutsourcingen medfører for virksomheden. Notifikationsperioden bør dermed også tage højde for, at virksomheden kan se sig nødsaget til at gennemføre et exit fra leverandøren indenfor den aftalte notifikationsperiode, hvis risici ikke kan mitigeres af virksomheden eller i samarbejde med leverandøren.

IT-outsourcing, herunder såkaldt cloud-outsourcing, skal efterleve bekendtgørelsen, inklusive reglerne for videreoutsourcing, på samme vilkår som gælder for øvrig outsourcing. Cloud-outsourcing betyder, at en virksomhed outsourcer en proces, tjenesteydelse eller aktivitet til en leverandør, som leverer ydelsen som en cloudtjeneste. Cloudtjenester skal som udgangspunkt forstås som tjenesteydelser leveret ved hjælp af cloudcomputing, dvs. en model, der tillader lettilgængelig og letanvendelig netværksadgang on demand til en fælles pulje af konfigurerbare computerressourcer (f.eks. netværk, servere, lagring, applikationer og tjenesteydelser), som hurtigt kan leveres og sættes i drift med et minimum af administration eller interaktion med leverandøren. Bekendtgørelsen indeholder dog kun ét specifikt krav til cloud-outsourcing, nemlig at en virksomhed skal registrere visse oplysninger i sit outsourcingregister, hvis en aftale indeholder brug af cloudtjenester.

Reglerne for videreoutsourcing gælder for alle outsourcingordninger, men har især været genstand for debat i forhold til cloud-outsourcing. Det skyldes, at et exit fra en cloudleverandør kan være en langvarig og kompleks proces for den outsourcende virksomhed. Det gør det svært at fastlægge en notifikationsperiode, som er realistisk for virksomheden, i tilfælde af at exit skulle blive nødvendig. Reglerne er udtryk for, at virksomheden skal kunne styre sine risici på en sådan måde, at der er tale om betryggende brug af outsourcing, hvilket er det grundlæggende formål med regelsættet. Virksomheden skal kunne tage konsekvensen af ændringer i outsourcingforholdet eller manglende kvalitet hos leverandøren og afslutte samarbejdet. Kan virksomheden ikke det, har den essentielt mistet kontrollen over sine risici. Det stiller desuden en virksomhed i en bedre forhandlingsposition overfor en leverandører, hvis den har mulighed for at træde ud af kontrakten.

Ledelsens opgaver og ansvar

Virksomhedens bestyrelse har ultimativt ansvaret for en betryggende brug af outsourcing. Den nye bekendtgørelse har dog åbnet for, at en virksomheds bestyrelse kan fastlægge klare rammer og betingelser, som direktionen kan indgå kritiske eller vigtige outsourcingkontrakter indenfor. Det var tidligere et krav, at bestyrelsen skulle træffe beslutning om hver enkelt aftale om væsentlig outsourcing. Der er altså tale om en lempelse af reglerne på dette punkt. Det påhviler direktionen at sikre, at brugen af outsourcing sker betryggende indenfor de rammer, som bestyrelsen har fastlagt.

Bestyrelsen tager konkret stilling til, hvor stor en kompetence direktionen tildeles. Det givne mandat bør være afgrænset og detaljeret, og der bør være taget stilling til virksomhedens risikovillighed, afgrænsning af, hvilke processer, aktiviteter eller tjenesteydelser der ønskes outsourcet, prisramme og vilkår for videreoutsourcing. Rammerne skal ikke forstås sådan, at bestyrelsen kun kan give et konkret mandat for hver enkelt aftale om outsourcing, men rettere sådan, at direktionen frit kan indgå eller ændre aftaler indenfor de klare rammer, som bestyrelsen har fastlagt. Ligger indgåelse af en kontrakt udenfor bestyrelsens mandat til direktionen, skal bestyrelsen give et nyt mandat eller selv træffe beslutning. Det kan eksempelvis være tilfældet, hvis en konkret outsourcing indbefatter risici, der falder udenfor den risikotoleranceramme, som bestyrelsen har fastsat.

Den nye bekendtgørelse indeholder derudover nye krav til outsourcingvirksomheden på området for ledelsens opgaver og ansvar.

Som noget nyt skal en outsourcende virksomhed udpege en ansvarlig for outsourcing, som har ansvar for styring, overvågning og kontrol af outsourcing og for at sikre dokumentationen af denne.

Den outsourcingansvarliges funktion skal som udgangspunkt forstås som en kontrol i første forsvarslinje. Det er ikke et krav, at den ansvarlige foretager de konkrete kontroller m.v. i første forsvarslinje i forhold til den enkelte kontrakt, da det typisk og mest hensigtsmæssigt vil ske i de enkelte forretningsområder. Det er dog den ansvarliges opgave at sikre, at outsourcingkontrakterne, rapporteringen, kontrollerne m.v. bliver udført i overensstemmelse med relevante politikker, forretningsgange etc.

Ud fra proportionalitetsprincippet vil opgaven hos mindre virksomheder kunne placeres andre steder i organisationen, eksempelvis i anden forsvarslinje med passende kompenserende foranstaltninger. Udgangspunktet for funktionen er dog, at der er tale om en funktion i første forsvarslinje. Den traditionelle anden forsvarslinjer (compliance- og risikostyring) bør under alle omstændigheder overvåge og kontrollere, om den ansvarlige er i stand til at identificere, styre og mitigere outsourcing-risici.

Der kan efter omstændighederne udpeges en fælles ansvarlig for outsourcing på koncernniveau, men for at modvirke interessekonflikter ved outsourcing bør virksomheder, der er individuelt omfattet af bekendtgørelsen, som udgangspunkt udpege deres egne ansvarlige.

Koncernforhold

Bekendtgørelsen gælder med de fornødne tilpasninger som nævnt også på konsolideret og delkonsolideret ni-

veau for de omfattede virksomhedstyper, med undtagelse af e-pengeinstitutter og betalingsinstitutter.

Det indebærer, at bekendtgørelsen, der gælder for individuelle virksomheder, også som helhed gælder for den koncern, som virksomhederne indgår i. Med konsolideret niveau skal forstås, at reglerne i bekendtgørelsen, der gælder for individuelle virksomheder, også som helhed gælder for den koncern, som virksomhederne indgår i. Koncernen skal i denne sammenhæng ses som en enkelt virksomhed. Med delkonsolideret niveau skal forstås konsolideret niveau for eksempelvis den del af koncernen, der udgøres af en modervirksomhed og dennes dattervirksomheder – uden at den pågældende modervirksomhed er den øverste modervirksomhed i hele koncernen.

En virksomhed, som ikke er omfattet på individuelt plan af bekendtgørelsen, kan dermed blive omfattet på konsolideret niveau eller delkonsolideret niveau, hvis modervirksomheden er individuelt omfattet. Ansvaret for, at bekendtgørelsen efterleves, vil i dette tilfælde ligge hos modervirksomheden. Det gælder også ved koncernintern outsourcing.

Modervirksomheder, som er individuelt omfattet, skal sikre, at brugen af outsourcing hos virksomheden og dens dattervirksomheder er konsistent, velintegreret og passende på alle niveauer i koncernen. Modervirksomheden skal altså være i stand til at vurdere koncernens brug af outsourcing på tværs af virksomhederne i koncernen og derved tage højde for de yderligere risici, der alt andet lige er på koncernniveau, som f.eks. den yderligere koncentrationsrisiko, der kan opstå, hvis flere virksomheder indenfor koncernen outsourcer til samme leverandør.

Bekendtgørelsen opstiller ikke særlige (lempelige) regler for koncernintern outsourcing, som derfor fuldt ud følger samme regelsæt som øvrig outsourcing.

Bekendtgørelsen muliggør desuden, at en koncern kan benytte sig af centraliseret overvågning og kontrol af outsourcing, et centralt styret outsourcingregister og centralt fastlagte exitplaner og beredskabsplaner for outsourcing. Vælger en virksomhed i en koncern at benytte sådanne ordninger, vil det skulle ske efter visse betingelser, som er fastlagt i bekendtgørelsen. Der vil være tale om koncernintern outsourcing, som i sig selv skal opfylde kravene i bekendtgørelsen. Virksomheden skal ved brug af centraliserede ordninger være særligt opmærksom på at identificere og afhjælpe eventuelle interessekonflikter, ligesom virksomheden til stadighed effektivt skal kunne udøve sine ledelsesbeføjelser.

Som tidligere nævnt opstiller bekendtgørelsen ikke betingelser for en outsourcingansvarlig på gruppeniveau, men en sådan kan, afhængigt af omstændighederne, stride imod bekendtgørelsens krav om at forebygge interessekonflikter.

Opsummering

Virksomheder, der er omfattet af reguleringen, bør altså sikre sig, at de til stadighed har tilstrækkelig ledelse, styring og kontrol med deres outsourcing, og at denne bruges betryggende. Finanstilsynet anbefaler derudover, at virksomhederne ved tvivl om bekendtgørelsens anvendelse orienterer sig i den nyligt udgivne vejledning.

De nye regler for outsourcing for finansielle virksomheder indebærer både en række nye krav og en række lempelser. Det gælder bl.a. muligheden for brug af passiv notifikation ved videreoutsourcing, proportionalitet og muligheden for, at bestyrelsen kan videregive noget af sin kompetence til indgåelse af kontrakter om outsourcing til direktionen. Lempelserne vil forhåbentligt gøre livet en smule nemmere for virksomhederne, men de indebærer også større krav til virksomhedernes styring.

Nye medlemmer

Nye medlemmer i IIA fra 2.4.2021 - 7.9.2021

Arbejdernes Landsbank
Gustav Pedersen

ATP
Mikkel Schøning

Coop amba
Lene Andersen

Danmarks Nationalbank
Deniz Demir

Danske Bank
Rikke Preisler Vilstrup

GF Forsikring
Ricki Søgaard

JN Data
Mogens Lund Petersen

Københavns Kommune
Páll Eysturoy

Landbrugsstyrelsen
Marianne Ørndrup

Lån & Spar Bank
Lise Meyer Brünnich

Nordea
Miguel Zorita Gil
Christopher Pommergaard
Steen Petersen
Johanna Viitanen
Jacob Thygesen

Nykredit
Jens Østergaard

Novo Nordisk
Lara Deleuran

Region Sjælland
Katalin Christensen

Ringkjøbing Landbobank
Mette Thesbjerg

Saxo Bank
Freya Nicky Pearce
Isabella Ørgaard Zöllner

Skatteministeriet
Viggo Jollmann
Rasmus Dybdal Pedersen
Martin Ginnerup-Nielsen
Malou Dall

Sparekassen Sjælland-Fyn
Nils Høj

Sydbank
Susanne Kopp Jensen
Lejla Mandzic

Takeda Pharma
Benjamin Koeie

TRYG
Jonas Møllegaard Larsen

Udenrigsministeriet
Jens Bech-Larsen

Uddannelsesaktiviteter

Er du opdateret på IIAs kursusudbud? Som altid findes datoer og emner for gå-hjem møder, kurser og konferencer på foreningens hjemmeside www.iia.dk under rubrikken "Uddannelse", hvor tilmelding til arrangementerne også foretages.

Nedenfor er fremhævet kommende planlagte kurser og møder, men listen bliver hele tiden opdateret, så det er bestemt værd at foretage et besøg på foreningens hjemmeside.

Kurser og gå-hjem møder

29.09.2021: Kursus for Forsikringsrevisorer
06.10.2021: Kursus for pengeinstitut– og realkreditrevisorer
08.10.2021: IIA Nordic 70 års jubilæum
27.10.2021: Revision af IT-applikationer
18.11.2021: Temadag for den finansielle sektor

"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.iia.dk eller til:

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

Jobannoncer

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

Certificeringer

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

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

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

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

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

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

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

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

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

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

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

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

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

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