INFO

Foreningen af Interne Revisorer
Nummer 72 | September 2019 | 24. årgang

Dual Rating
- Hvordan og hvorfor?

Business partnering
- Værdi for dig og din virksomhed

Chief Digital Risk Officer
Har din virksomhed brug herfor?

Bæredygtig långivning
Introduktion, risici og revision

Tips til overvågning af ikke-revisionsydelser

INFOs redaktion

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

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

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

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

Afdelingsdirektør, CIA
Tobias Zorde
Nykredit
☎ 21 18 54 97 ✉ tzo@nykredit.dk

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

Næste nummer
INFO 73 udkommer i december 2019.
ISSN: 1903-7341 (Elektronisk version).

Indlæg til INFO
Artikler i INFO påskønnes med en vingave.

Forsidefoto
UnknownNet

Redaktionens adresse

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

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

Indhold

Nyt fra bestyrelsen

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

www.iia.dk

Leder

Jesper Siddique Olsen, Audit Director, Danske Bank

For nylig kunne IIA Global konstatere, at IIA globalt har mere end 200.000 medlemmer. Ud af disse er ca. 600 medlemmer her i Danmark. Disse tal viser med alt tydelighed at vi er nødt til at følge og hente inspiration fra vores globale netværk. Derfor en opfordring til at besøge IIA Global's hjemmeside for at indhente inspiration.

Bestyrelsen i IIA Danmark vil sammen med vores globale netværk rundt om i verden kæmpe for at fremme den værdi, som intern revision bringer til styrkelse af risikostyring, intern kontrol og virksomhedsstyring. Overalt i verden fremmer IIA intern revision som en vigtig del af organisatorisk succes. Vi forsvarer behovet for at bevare uafhængighed og objektivitet. Vi opretter og plejer forhold til interessentgrupper og andre ligesindede for at fremme IIA's internationale standarder for den professionelle praksis inden for intern revision.

Jeg tænkte for nylig på, hvorfor jeg oprindeligt begyndte frivilligt at arbejde med IIA. Jeg kan ikke huske et "aha-øjeblik", andet end jeg bare følte, at det var vigtigt at være involveret i den organisation, der understøtter mit valgte erhverv. I 2010 startede jeg med at deltage i forskellige netværksgrupper, deltage i kursusaktiviteter og senere i 2014 med bestyrelsesarbejde. Når jeg tænker på, hvad jeg personligt får ved arbejde med IIA, finder jeg listen omfattende. I virkeligheden, efterhånden som jeg bliver mere involveret med IIA, får jeg faktisk lige så meget, hvis ikke mere, til gengæld end det, jeg faktisk har lagt i det. Et par højdepunkter inkluderer muligheder for at netværke, udvide mine lederegenskaber og påvirke fremtiden for den interne revisions profession i Danmark.

Med hensyn til netværk er der så mange måder, at jeg har udvidet mit netværk gennem involvering i IIA. Nu har jeg et globalt netværk af kolleger og venner. Når jeg møder problemer og udfordringer dagligt, kan jeg komme i kontakt med andre IIA-medlemmer, der har lignende problemer og udfordringer, uanset hvor de befinder sig.

På grund af tidligere forhold til disse mennesker gennem netværk, er det let at nå ud og bede om et andet perspektiv. Desuden har jeg gennem disse aktiviteter mødt nogle vidunderlige mennesker, der spænder over masser af baggrunde og perspektiver. Jeg vil gerne benytte denne mulighed for at takke to af disse, Poul-Erik Winther og Kim Stormly Hansen. Både Poul-Erik og Kim valgte tidligere på året at fratræde fra vores bestyrelse. Jeg vil på bestyrelsens vegne gerne takke for den kæmpe indsats de begge indtil nu har bidraget med. Heldigvis fortsætter både Poul-Erik og Kim med at være involveret i IIA-regi og på denne måde fortsætte med at styrke vores erhverv.

Vi vil i bestyrelsen fokusere på at påvirke erhvervet og vores medlemmer og få vores stemme hørt. Jeg tror, at dette i sidste ende vil hjælpe med at forme erhvervets fremtid. Vi havde for nyligt vores første bestyrelsesmøde efter generalforsamlingen og jeg må indrømme at energien og motivation er endnu større efter at have deltaget i dette møde. At se så mange passionerede medlemmer, der brænder for intern revision, er fantastisk. Jeg fandt mig selv nærende af lidenskaben fra disse fantastiske frivillige, som også er så engagerede i de medlemmer, de tjener.

Som nævnt i "Nyt fra bestyrelsen" har vi udvalg og netværksgrupper som altid har brug for ny inspiration, så derfor vil jeg gerne opfordre alle til at række ud og aktivt deltage i IIA's arbejde.

I dette nummer af INFO er der en række artikler, som viser hvor vigtigt der er for os at fortsætte med at omfavne innovation. Herunder ESG, dual rating, business partnering osv. Omfavnelse af innovation og udnyttelse af teknologi er nøglen til, at blive en succesrig intern revision i det 21. århundrede. Personlig er jeg bekymret for, at erhvervet ikke holder trit: Lave adoptionshastigheder for næste generation af teknologi, såsom automatisering ved robotter, data driven assurance, kunstig intelligens, og små ændringer i årtier gamle revisionsprocesser antyder, at vi falder bag innovationskurven.

Så lad os alle fortsætte kampen og god læselyst!!

Nyt fra redaktionen

Birgitte Rousing Svenningsen, ansvarshavende redaktør

Endnu et nummer af INFO er nu på gaden. Jeg håber, at du vil finde artiklerne spændende og relevante. Bladet kommer dog ikke på gaden uden en del arbejde fra det aktive redaktionsudvalg. Jeg vil benytte denne lejlighed til at sige tak for indsatsen til alle medlemmerne af redaktionsudvalget.

En særlig tak skal lyde til Lea Kehlet Halsø (Nykredit) og Tobias Zorde (Nykredit), som begge har valgt at træde ud af udvalget. Stort tak til jer begge for jeres indsats med at optrævle aktuelle artikler og med bidrag som forfattere til enkelte artikler.

Lea udtræder da hun er skiftet til et compliancejob. God vind i sejlene med det.

Tobias udtræder for at fokusere mere på andre opgaver i foreningen herunder bestyrelsesarbejde og hjemmesiden. Jeg glæder mig til at se den udvikling af vores hjemmeside, som Tobias kommer til at drive.

Intet er jo så skidt, at det ikke er godt for noget. Tobias' udtræden har givet plads og lyst til, at et af vores "gamle" redaktionsmedlemmer indtræder i redaktionen igen. Det er mig en ære at kunne sige velkommen tilbage til Lars Geisler (Nykredit) i redaktionen. Jeg ser frem til et godt samarbejde og ved, at Lars allerede har sadlet hesten og er på jagt efter aktuelle og interessante artikler.

Nyt fra arbejdet med netværksgrupper

Anita Damgaard Laugesen, Internal Audit Manager, CIA, Nordea

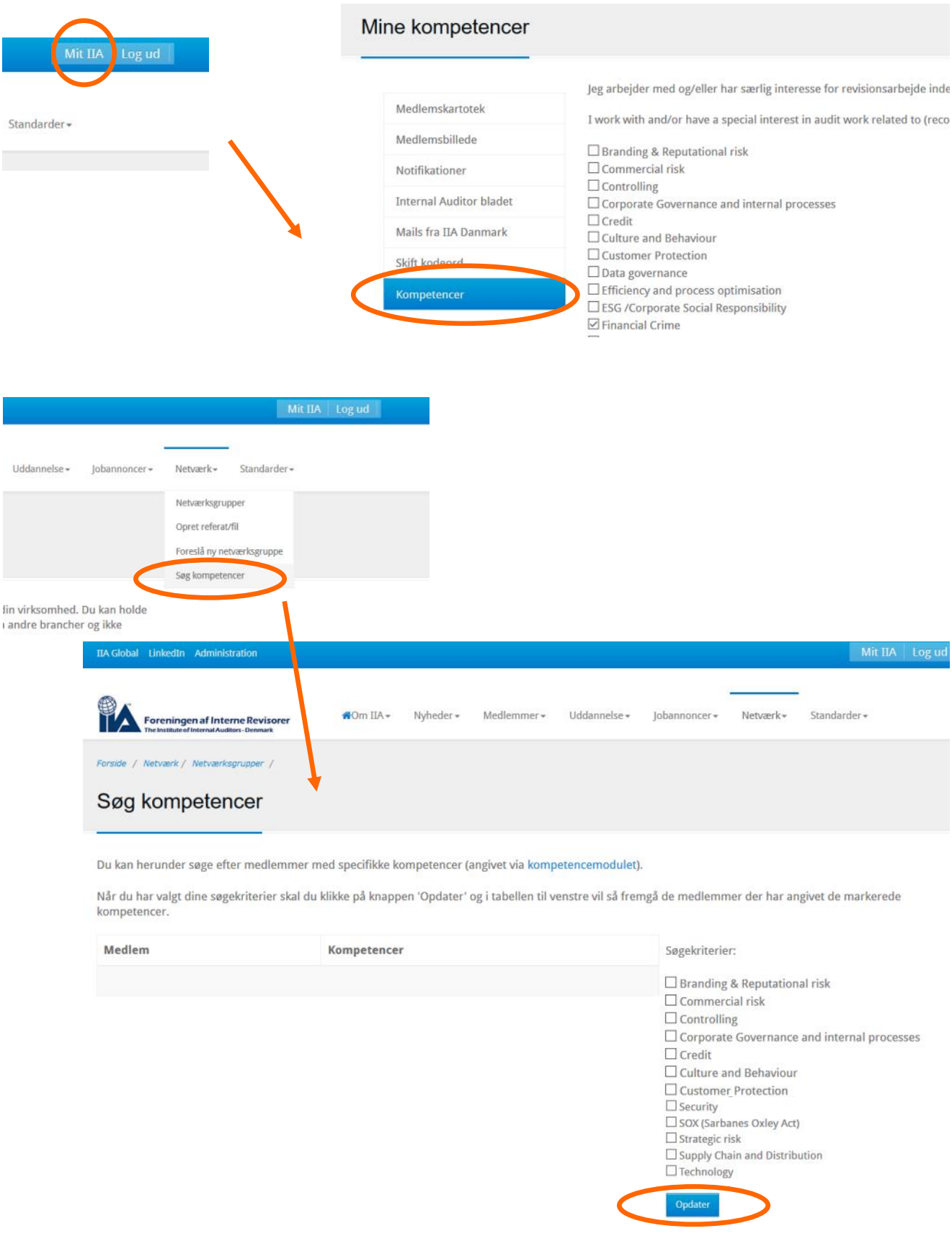
For at gøre det lettere at bruge det netværk, vi har i IIA i det daglige til sparring mv, er der på IIA Danmark's hjemmeside under **Mit IIA/Kompetencer** nu en funktion, hvor man kan udfylde sine primære kompetencer og interesser. Denne funktion giver mulighed for, at alle medlemmerne under **Netværk/Søg kompetencer** kan søge blandt de øvrige medlemmers kompetencer og derved identificerer de medlemmer, der arbejder med et specifikt område og tage kontakt, hvis der er brug for oprettelse af netværksgrupper, sparring om et specifikt område eller blot konkrete spørgsmål, man mangler hjælp til.

For at gøre denne funktion så værdiskabende som muligt opfordres alle medlemmer til at gå ind på sin profil og udfylde sine kompetencer. Og del meget gerne gode historier med jeres kollegaer, når I har brugt denne funktion til at udbygge jeres netværk.

På næste side er en kort vejledning til hvordan du bruger den nye funktion.

"Netværk er fremtidens valuta"

- Citat Susie Lynge og Morten Vium


Mit IIA
Log ud
Standarder
Mine kompetencer
Medlemskartotek
Medlemsbillede
Notifikationer
Internal Auditor bladet
Mails fra IIA Danmark
Kompetencer
Jeg arbejder med og/eller har særlig interesse for revisionsarbejde inde
I work with and/or have a special interest in audit work related to (reco
Branding & Reputational risk
Commercial risk
Controlling
Corporate Governance and internal processes
Credit
Culture and Behaviour
Customer Protection
Data governance
Efficiency and process optimisation
ESG /Corporate Social Responsibility
Financial Crime
Mit IIA
Log ud
Uddannelse
Jobannoncer
Netværk
Standarder
Netværksgrupper
Opret referat/fil
Foreslå ny netværksgruppe
Søg kompetencer
lin virksomhed. Du kan holde
andre brancher og ikke
IIA Global
LinkedIn
Administration
Mit IIA
Log ud
Foreningen af Interne Revisorer
The Institute of Internal Auditors - Denmark
Om IIA
Nyheder
Medlemmer
Uddannelse
Jobannoncer
Netværk
Standarder
Forside / Netværk / Netværksgrupper /
Søg kompetencer
Du kan herunder søge efter medlemmer med specifikke kompetencer (angivet via kompetencemodulet).
Når du har valgt dine søgekriterier skal du klikke på knappen 'Opdater' og i tabellen til venstre vil så fremgå de medlemmer der har angivet de markerede kompetencer.
Medlem
Kompetencer
Søgekriterier:
Branding & Reputational risk
Commercial risk
Controlling
Corporate Governance and internal processes
Credit
Culture and Behaviour
Customer Protection
Security
SOX (Sarbanes Oxley Act)
Strategic risk
Supply Chain and Distribution
Technology
Opdater

Nyt fra bestyrelsen

Birgitte Rousing Svenningsen, CIA, CISA, bestyrelsesmedlem af IIA

Konstituering

På generalforsamlingen den 16. maj blev Kim Klarskov Jeppesen (CBS), Tobias Zorde (Nykredit) og Christoffer Max Jensen (ATP) nyvalgt til foreningens bestyrelse. Bestyrelsen har efterfølgende konstitueret sig på følgende måde:

Formand:	Jesper Siddique Olsen, Danske Bank
Næstformand:	Michael Ravbjerg Lundgaard, DSB
Kasserer:	Morten Bendtsen, Alm Brand
Sekretær:	Anita Damgaard Laugesen, Nordea.

Udvalg

Foreningens aktiviteter drives i høj grad af en række stående udvalg bestående af både bestyrelsesmedlemmer og andre medlemmer. For hver af udvalgene er der tilknyttet et eller flere bestyrelsesmedlemmer. I disse udvalg er der løbende udskiftning af medlemmerne, og har du lyst til at yde en indsats i et af udvalgene, er du velkommen til at kontakte det bestyrelsesmedlem, som har kontakten til udvalget. De stående udvalg er:

Udvalg	Kontaktperson
Uddannelse og medlemsmøder	Pia Sønderlund Nielsen
Den finansielle sektor	Morten Bendtsen
Industrisektoren	Johan Bogentoft
Den offentlig sektor	Pia Sønderlund Nielsen
Hjemmesiden	Tobias Zorde
Redaktionsudvalg INFO	Birgitte Svenningsen

Under uddannelsesudvalget har foreningen tre underudvalg:

1. Årsmødeudvalg
2. Udvalg for penge- og realkreditinstitutter
3. Udvalg for forsikring

Disse udvalg arrangerer vores årsmøde og uddannelsesdage specifik for interne revision i pengeinstitutter og forsikringsselskaber. Du kan komme i kontakt med disse udvalg, enten ved at kontakte et af medlemmerne af udvalgene eller ved at kontakte Pia Sønderlund Nielsen, som er ansvarlig for uddannelsesudvalget generelt.

Hjemmesideudvalget har også et underudvalg, som udarbejder foreningens nyhedsbreve. Tobias Zorde er ansvarlig for dette udvalg.

Tilsyn, brancheorganisationer mv.

Foreningen har også repræsentation i nogle udvalg under Finanstilsynet og FSA. Her arbejdes der med at fremme foreningens og professionen som intern revisors interesser.

Dette omfatter følgende udvalg under Finanstilsynet, hvor bestyrelsen er repræsenteret af følgende personer:

Udvalg	Kontaktperson
Finanstilsynet rådgivende revisionsudvalg	Christoffer Max Jensen
Finanstilsynet rådgivende regnskabsudvalg	Morten Bendtsen

Du er altid velkommen til at kontakt disse medlemmer, hvis du har nogle spørgsmål til deres arbejde.

Foreningen er tillige repræsenteret med følgende personer i FSRs udvalg:

Udvalg	Kontaktperson
Cyber Security	Kim Stormly Hansen
IT sikkerhedskonference	Bethina Hamann

Hvis du har input til deres arbejde eller spørgsmål hertil er du også velkommen til at kontakt dem.

Nye certificeringer

Heinrich Ringsgart, Nordea (CIA)
Per Graabaek Ventzel, Danske Bank (CIA)
Thomas Bang van Dijk, Saxo Bank (CRMA)
Marcin Winiarczyk, Danske Bank (CFSA)

Et stort tillykke med certificeringen !!!!

CONFERENCE #ECIIA2019
Luxembourg, 18-20 September 2019

Embrace Change and Innovation in Internal Audit

institute of internal auditors luxembourg
ECIIA
LUXEMBOURG LET'S MAKE IT HAPPEN

IIA PRISEN

Prisopgave om intern revision

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

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

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

Hovedopgaven skal omfatte et emne og en problemformulering, som er relevant for forståelsen af intern revisions arbejde og betydning for de virksomheder, som har eller overvejer at etablere(t) en intern revisionsfunktion. For at komme i betragtning skal hovedopgaven være afsluttet i perioden 1. august 2018 til 31. december 2019.

Ansøgningen indsendes elektronisk til bisv@expressbank.dk. Ansøgningen skal indeholde

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

Ansøgningsfristen er 15. januar 2020. De nærmere ansøgningsbetingelser fremgår af foreningens hjemmeside www.iia.dk.

Prisoverrækkelsen vil ske på IIA's årsmøde i maj 2020 i Kolding. Bedømmelsesudvalget består af Dorthe Tolborg (Danske Bank), Kim Klarskov (CBS) og Birgitte Rousing Svenningsen (Express Bank).

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

Foreningen af Interne Revisorer
The Institute of Internal Auditors - Denmark

Dual rating: Management Risk Awareness and Response

Maibritt Skovmand Løvbjerg,
Audit Director, Danske Bank

Introduction

In this article, I will share why Danske Bank's Group Internal Audit (GIA) introduced a Dual Rating framework including an assessment of 'Management Risk Awareness and Response'. I will also elaborate on how we introduced the concept and lessons gained during the implementation.

The Management Risk Awareness and Response assessment has a dual purpose, to gain insight into:

1. Whether the core values are embedded; and
2. The risk and control culture.

The assessment of Management Risk Awareness and Response makes GIA able to identify areas within the Group where risk awareness and response is weak and therefore should be subject to management and/or audit attention.

The outcome of an audit activity is two specific ratings as part of our Dual Rating framework:

1. Governance, risk management and control assessment rating
2. Management's risk awareness and response assessment rating.

If the audit activity covers more than one business unit/function, one overall Management Risk Awareness and Response rating is given. The summary of the audit report may then elaborate on the differences observed across the business units/functions covered.

As to the issues on governance, risk management and controls, the audit report does not include audit observations or recommendations followed by action plans, deadlines and owners on issues related to Management Risk Awareness and Response.

Table 1 shows the rating scale we use regarding Management Risk Awareness and Response.

How to ensure objectivity

The design of the framework to assess Management Risk Awareness and Response needs to address how to ensure objectivity when performing subjective assessments.

Therefore, GIA has defined ten areas to assess in order to be able to conclude on Management Risk Awareness and Response. The auditors need to have the ten areas in mind during the audit and conclude on these before finalising the audit report.

When assessing the ten areas the auditors have to consider the following:

- Not all ten areas are necessarily relevant for each audit activity. Normally this will be the case, but there may be exceptions.
- For each of the ten areas, the auditor needs to conclude whether the area is Strong, Adequate or Weak. In addition, the rationale for the conclusion needs to be documented.

In **Table 2** on the next page I have included an overview of the ten areas that we assess in order to conclude on Management Risk Awareness and Response.

Implementation and challenges

A pilot was performed in 2017 before we implemented the framework. Based on feedback from our audit customers, the framework was adjusted and implemented in 2018. We decided to use the framework on approximately 20% of our audit activities in 2018 to gain additional lessons learned before implementing it within all audit activities in 2019. As part of the annual planning process, we therefore decided which audit activities to include in the Dual Rating Framework in 2018 across business units/functions and managers.

Table 1: Rating scale regarding Management Risk Awareness and Response

	Management risk awareness and response:
Strong	Meet key components in a strong manner
Adequate	Pass but with room for improvement
Weak	Need improvement

In 2018, we issued a separate Management Risk Awareness and Response report, which was prepared after having finalised the audit activity and after having issued the audit report. The aim was to include our assessment of collaboration with GIA throughout the entire audit process and until the final audit report was issued. However, this caused some practical difficulties and inefficiencies in gathering all stakeholders for debriefing twice – first regarding the audit report, and later on regarding the Management Risk Awareness and Response report.

In addition, lessons learnt included that an 'Unsatisfactory' rated audit report was easier to accept by the audit customer if delivered in combination with a strong/adequate Management Risk Awareness and Response rating. Amongst others because it then becomes clearer if gaps are already known by the audit customer and with appropriate plans for mitigating the risks.

Also, other audit customers were somewhat critical towards the Management Risk Awareness and Response rating setup - especially if rated 'Weak' – primarily because the rating only covers the specific audited area and hence not necessarily the Manager's full area of responsibility.

Therefore, communication towards our audit customers on the setup of the framework is key to avoid misinterpretations of the outcome of our assessments.

Impact on the audit

The business is not required to prepare further documentation in order for GIA to be able to do the assessment. This has helped the business to easily on-board the Management Risk Awareness and Response assessment.

Further, the Dual Rating framework has helped improving the collaboration between the business and GIA. For instance, one important point of the assessment is whether the risk awareness and response is proactively articulated by the business. This entails that the business is transparent about identified gaps and plans in place to mitigate those, which makes the audit more efficient.

Conclusion

In all, 2018 was a year of learning how to develop and use the Dual Rating framework. The framework changed from two separate reports to one combined audit report, and overall positive feedback on insights gained during 2018, resulted in that all 2019 audits will have a dual rating covering i) Governance, risk management and control; and ii) Management's Risk Awareness and Response.

Table 2: Overview of the ten areas of Management Risk Awareness and Response assessment.

1	Key risks and controls influencing the business unit/function's end to end process are articulated
2	Risk identification processes result in timely risk management and there are no surprises within risk identification activities
3	Metrics or measures are implemented on Operation, Performance and Controls, including monitoring and follow up
4	Control gaps are managed proactively and action plans are detailed and address known exposures and risks
5	If full remediation is not possible or inappropriate, management determine whether risk acceptance should be the approach
6	Cross-functional risks are recognised and integrated, e.g. Operations, Technology, Information Security and Shared Services
7	Significant issues are escalated to Senior Management in a timely manner
8	Observations and similar from Group Compliance and other control functions are adequately addressed
9	Procedures are in place to benchmark against Industry Standards
10	Collaboration with GIA support that audit activities are completed timely. This include employee availability, discussion of potential concerns with open mind, comprehensive action plans to mitigate identified risks and appropriate target dates

What is Business Partnering?

Nicoleta Mehlsen, Head of Internal Audit, Danfoss

Introduction

Business Partners are members of a function who acts as a connector, a bridge, linking functions to ensure that the expertise they have to offer is offered and accepted within the current challenges encountered in the business and it creates value for the company, directly or indirectly. These individuals have the potential to greatly optimize transactions and processes, drive performance and ensure compliance within the organization. They maximize the timely deployment of the functions' skills and expertise and match that with the company's priorities and are aligned with its strategy. Business Partnering therefore, requires a high degree of relational mastery and business acumen, to sit alongside technical expertise and experience. Therefore, a focus on general consulting skills is an effective lens for business partners as they are often acting in the capacity of a consultant to their business unit (s).

And this is where Internal Audit fits perfectly into the business partnering role. Danfoss Internal Audit, with our focus on ensuring compliance with local rules and regulations, international accounting standards, with deep understanding of the processes the company is running, plays an unique role in business partnering.

Internal Audit Teams holds incredible knowledge of the business: They are often involved in internal investigations, and they monitor the effective implementation of internal controls and ERM. All this knowledge places the Internal Audit in the situation where big impact can be generated by addressing the change from within, by sharing the knowledge Internal Audit team has with the organization, and by being advisors to the business – thus moving its mindset from "audit view" to "company view". I often advise my team to forget that you lose an argument with the business over an audit observation!

Is it about understanding why we lose? Is it because we did not fully understand the business and our recommendation does not add value? Or is it because we have not made ourselves worthy of being trusted partners? It is not about winning or losing a heated argument in the closing meeting, it is about ensuring that the end result adds value to the business, and that we take this learning from the conversation and improve our approach in the future.

One time, in one of the closing meetings, such a situation happened, where I had to ask "John, please forget for a second that this is an audit issue. Do you have this problem I am mentioning or not? If we could imagine for a moment that this observation would not appear in an audit report, would you then recognize the problem and discuss improvement? If the answer is yes, then we should rather start thinking 'Danfoss' and work together towards finding the appropriate improvement – for the company's sake".

Business partnering is about both parties winning from the trade. The trade/exchange in this case is knowledge of best practices to ensure compliance. This trade cannot happen if there is no acceptance from the business that the recommendation adds value to him/her, or the receiving party do not feel that they can trust the business partner.

As you can see, business partnering is nothing different than any other successful relationship. Every trade partnership has in common the exchange of currency for a benefit. The key to every partnership is to define what this currency is.

The easiest way to business partnering is to understand where your partner is experiencing challenges and evaluate how you can help, with the knowledge and resources you have; and sometimes, at absolutely no gain for you alone, but at times just for the other party. In Danfoss, one of our behaviors is "think Danfoss" – therefore, we continuously challenge ourselves to step out of "what is in it for me" and "think Danfoss" instead.

Internal Audit is in a unique position in a company, as it can business partner with all functions, across segments, countries, regions. The only danger in this outreach is how to ensure that business partnering is not pushing Internal Audit into becoming operational, hence putting Internal Audit at risk of losing its independence and objectivity. Segregation of duties have to be ensured, as Internal Audit cannot audit a process which they have helped designing. Therefore, business partnering must follow a structured framework.

How can you become an effective business partner?

Take a minute to reflect upon this. Think about the Business Partners that you have worked with. Have you ever partnered with someone who you have found to be particularly authentic and influential, without any sense of being manipulative or acting solely on their own agenda? These people are able to relate to you in a deeper and more generative way. What's more important is that these relational skills can be learned and become embedded in your practice over time. Why is this important? Because they are powerful levers to establish and sustain deep and true partnerships.

Below are a few steps inspired by our journey:

A. Clearly define the role you want to play

Business Partners can play multiple roles, but the following are roles which we have taken on:

Creators of Business Value – we have deep insights and contribute to the bottom line for the short and long term rather than detracting from it.

Enabler of Policy Implementation – we have the ability to simplify the policy into compliance points and, in an effective way, build commitment and acceptance from the business, rather than resistance. By doing so, we drive sustainable, compliant and ethical results.

Technical Specialist – we have more than one core expertise, and we strive continuously to expand the knowledge we have, based on the changing business environment and latest trends (such as automation, robotics, smart tools etc).

Intermediator – we have an extended network and we use this network either directly, or we facilitate other people in our network to connect in order to share best practices.

B. Business Partnering skills

I consider the following two skill-sets as being the most important:

1. Advisory skills

Being a good listener: Listening to understand what is being communicated, without judgement – purely open minded.

Working with unstructured information: Being willing to sit with ambiguity for longer than may feel comfortable, to truly "sense" into the situation without a need for immediate resolution of the issue (real or perceived).

Challenge the information received and understand the dynamics and drivers of what and why (it) happened in the past, which created the current situation.

Business knowledge: Having business insight relevant to the work areas and ensuring this is current and continuously improving.

Share best practices learnt from other businesses inside the organization or from outside: Benchmark with others in order to get the best outcome.

2. Self-control

This refers to your ability to maintain independence of thought and action for the sake of a better business outcome. The challenge is being able to hold the functional line while understanding and interpreting all information objectively, and saying "No", when appropriate, and "Yes" when alignment is reached. The shift in being able to have difficult or confronting conversations internally, produces a higher level of respect, mutual understanding and thus builds trust - an essential element of any effective relationship.

Your business impact will come from the change in the nature of the conversations that you have inside the team, with others and with the business.

C. Business partnering journey – welcoming constructive criticism

A few years ago, we performed an internal survey on how Internal Audit was seen by our stakeholders. To our surprise, we heard the business units complaining that we are operating in our own narrow agendas and do not "understand" the business.

Without properly understanding the business, how can Internal Audit make proper recommendations, build alignment and receive buy-in that by implementing this recommendation, it would add value to the counterpart?

So it is vital that people and teams find shared purpose, build alignment and get commitment when building individual and organizational capability, and powerfully engage senior leadership from the very beginning. The goal is to close the gap between the functions and use common agendas for progress for everyone, and not for one party only.

We took in these comments, sat together and developed what we called "how to add value to our stakeholders". Below are some examples of their comments:

***Hard truth #1**: "When Internal Audit performs an audit, it should be more of a two-way communication rather than an "interrogation". We felt uneasy talking to Internal Audit, so we only answered their questions to the minimum."*

Our actions to improve:

- Ask open questions; soft way of asking questions, more active listening, let people talk and explain the process, communicate effectively, be more empathetic.

- State that it is a "fact finding" task and not "fault finding"
- Communicate in a constructive way and remember to praise the good practices
- Recommend a solution to their audit issue.

We also provided training to the team in cultural awareness and interviewing techniques.

Hard truth #2: *"Sometimes it took so long to receive the audit report after Internal Audits visit (more than two months), so we don't remember all the details or remediation actions became obsolete."*

Our actions to improve:
- Create KPI to show Report delivery time (see below).

We managed to reduce the report delivery time from 62 days (in 2016/2017) to 18 days average (2018/current).

Hard truth #3: *"We were told we were doing fine, but when the audit report was released, it contained a couple of "major" highlights which were never shared with us at the conclusion meeting."*

Our actions to improve:
- Ensure audit observations are fully aligned with the control owners before the meeting.
- Leave the conversation open for learning new information during the closing meeting, should the entity provide further evidence.

Hard truth #4: *"Be more flexible and tolerant with minor deviations from the "rule book", as long as it is still in the framework of Danfoss policies, or the risk is immaterial."*

Our action to improve:
- We acknowledge and are mindful in our approach and recommendations.

Hard truth #5: *"Internal Audit should be more visible to stakeholders, be available for training, information sharing, and telling about compliance at entity level."*

Our actions to improve:
- Be more visible. Be part of some strategy meetings, have direct information sharing with the segments, procurement, shared services, and all other functional areas where new risks or new processes would come into place.
- Training from corporate functions were given to the Internal Audit team (such as new IFRS and the plans for implementation in the company, including methodology, transfer pricing (high level), export controls training, ethics training, anti-money laundering training, etc) – and development or tailoring of audit programs to match their new processes or risks.

How do we measure business partnering?

In my view, business partnering is about making a difference in the organization and being accepted as a trusted partner to the business.

Therefore, below are some KPIs I would recommend, which would indicate the extent to which we are on the right track:

- **Number of recommendations/suggestions accepted:** Please note that I am not saying "audit observations". A positive development in Business Partnering is represented by an increasing trend year over year.
- **Report on time (days)**, measured as number of days from Face-to-Face visit to the audit report issuance day. A positive development in Business Partnering is represented by a decreasing number of days (average) year over year.
- **Number of management requests**: This represents the number of times management reached out to Internal Audit requesting a focused audit in a particular area or where some flags of non-compliance where raised. A positive development in Business Partnering is represented by an increasing trend year over year.

Business partnering is a mindset, an attitude. This was our journey, which started a few years back. It requires patience, passion and dedication, as its results are not immediate.

IIA Årsmøde 2020

Afholdes
27.5.2020-28.5.2020

på Hotel Comwell, Kolding

Sæt allerede nu kryds i kalenderen

Hvad laver en Chief Digital Risk Officer - og har dit selskab også brug for en?

Janus Friis Bindslev, Chief Digital Risk Officer, PensionDanmark

Indledning

Mange virksomheder – og måske især de finansielle – har indset, at digitalisering er en af de væsentligste nøgler til fortsat at være konkurrencedygtig. Både effektivitetsmæssigt og i forhold til at levere services og oplevelser så hurtigt, personligt tilpasset og let tilgængeligt – og på de platforme – som kunderne ønsker og forventer. Det kræver, at data er øjeblikkeligt tilgængelige på tværs af stort set alle kundevendte forretningsprocesser – og at intelligent automatisering og selvbetjening skal kunne ske i hele værdikæden. En proaktiv stillingtagen til de muligheder – og de risici – som digitaliseringen og den smarte teknologianvendelse, af fx cloud, robotics m.v., medfører, må derfor være en central del af hele beslutningsprocessen vedrørende nye tiltag.

Samtidig har større hacker-sager, datalækager og persondatalovgivning bragt "cyber-truslerne" helt op på toppen af den ledelsesmæssige opmærksomhedsskala, og både persondata- og cybersikkerhed har været et fokus- og investeringsområde i mange selskaber. Og spørgsmålet er, om det – i den digitale og datadrevne verden – overhovedet giver mening at se disse emner som adskilte fagområder. Personligt mener jeg det ikke.

Det er her, at "digital risikostyring" kommer ind i billedet. Digital risikostyring defineres i PensionDanmark som en forretningsdrevet tilgang, der har som mål proaktivt at håndtere de forretningsmæssige risici, der følger med datadrevne, digitaliserede processer, inklusive cybersikkerheds- og persondatamæssige risici, såvel som de relaterede overvejelser i relation til fx lovgivning, automatisering og etik. Jeg vil i det følgende prøve at give et indblik i, hvordan det fungerer i praksis, herunder samarbejdet på tværs af de tre forsvarslinjer.

Jobbeskrivelsen og væsentligste ansvarsområder

Jeg har titel af "chief digital risk officer", hvilket måske lyder lidt buzzword-agtigt, men kort fortalt handler det om at tage ansvar for, at information beskyttes tilstrækkeligt, og at medlemmer og forretning ikke påvirkes negativt af digitale hændelser, uanset hvor i PensionDanmarks it-netværk eller digitale økosystem, de måtte opstå. Altså at sørge for, at der hele tiden er den rigtige balance mellem risici og udnyttelsen af digitaliseringens muligheder. Hos os omfatter det også at varetage rollen som DPO eller databeskyttelsesrådgiver i henhold til persondataforordningen.

Mere formelt formuleret er det væsentligste succeskriterium at understøtte opnåelsen af forretningsmæssige mål, hvor forretningsprocessen er afhængig af teknologi, gennem at identificere, vurdere og rapportere på digitale risici på en måde, der lever op til compliance og lovmæssige krav – så ledelsen kan sikre balancen med PensionDanmarks risikoprofil og -appetit. Værktøjskassen til at styre disse risici er for en stor dels vedkommende processer, der allerede findes – men et konstant ændrende risikobillede kræver hurtig tilpasningsevne og beslutningsdygtighed. Derfor har jeg opstillet følgende principper for arbejdet:

- Fokus på risikobaseret beslutningstagen i stedet for "checkboks-compliance"
- Fokus på at beskytte forretningsprocesser frem for teknisk infrastruktur
- Styr på informationsanvendelse frem for fokus på kontrol af informationskilden
- Anerkendelse af teknologiens begrænsninger og nødvendigheden af fokus på den menneskelige faktor
- "Perfekt beskyttelse" findes ikke – men beredskab og detektion gør.

Generelt er målet, at den digitale risikostyring skal være en ressource, og ikke en autoritet, og at fokus er på at skabe overblik over risici – frem for "bare" at undgå regelbrud (selv om det selvfølgelig også er et mål). Dialogen med organisationen er derfor fokuseret på pragmatisk rådgivning mere end "compliance-politi".

De væsentligste ansvarsområder er beskrevet nedenfor:

- Understøtte forretningsudvikling og transformation gennem en rolle som sparringspartner og beslutningsstøtte for forretning og it i relation til digital udvikling og risiko
- Sikre forståelse for og prioritering af digitale risici og databeskyttelse på tværs af PensionDanmark, fx ved rådgivning i forbindelse med udarbejdelse af konsekvensanalyser og ved at underrette og rådgive interessenter og de ansatte om databeskyttelse
- Etablere og drive processer for vurdering, imødegåelse og løbende overvågning af digitale risici
- Dokumentere og vedligeholde model for digital risikostyring som beslutningsstøtte for at sikre værdiskabelse og omkostningseffektivitet af etablering af digital platform og services
- Udarbejde vejledninger, metoder, standarder og værktøjer for vurdering og adressering af digitale risici

- Beskrive regler og rammeværk for integreret sikkerhed i PensionDanmarks digitale set-up
- Bidrage til overholdelse af lovmæssige krav i relation til teknologi, sikkerhed og databeskyttelse, herunder som DPO at overvåge overholdelsen af interne regler for persondatabeskyttelse i PensionDanmark og lovgivning på området, samt samarbejde med Datatilsynet, Finanstilsynet og andre myndigheder på vegne af PensionDanmark i det omfang, der måtte være behov
- For brud på persondatasikkerheden er DPO bindeled mellem PensionDanmark, Datatilsynet samt de registrerede (dvs. typisk medlemmerne)
- DPO har også ansvaret for henvendelser for så vidt angår GDPR, medmindre ansvaret på bestemte områder er delegeret videre i organisationen i PensionDanmark, fx at den primære medlemskontakt sker i Medlemsrådgivning for indsigtsbegæringer og HR for ansattes forespørgsler.

Samarbejdsflader

PensionDanmark har en høj digitaliseringsgrad og arbejder fortsat med at transformere forretningsmodellen gennem blandt andet fokus på automatisering af processer og meningsfuld anvendelse af robotics og machine learning. Derfor foregår en stor del af arbejdet i udviklingsorienterede projekter, som jeg samarbejder tæt med. Eksempler på aktuelle projekter er:

- Digital dialog, som sender individuelt tilpassede og relevante budskaber til medlemmer på deres foretrukne kanal
- Videreudvikling af portaler til cloud-baseret drift
- Udbredelse af robotics og machine learning til flere medlemsprocesser
- Chatbot.

Ud over at deltage i projekterne, er andre daglige kontaktflader it-organisationen, både udvikling og drift, hvor også de tekniske it-sikkerhedskompetencer er organiseret, og reelt er jeg i regelmæssig dialog med hele forretningen på tværs af rådgivning, økonomi, investering, HR m.v.

Organisatorisk er jeg placeret med daglig reference til PensionDanmarks COO, og jeg er medlem af PensionDanmarks risikokomité, hvor de væsentligste risici behandles. Det løbende arbejde med digitale risici drøftes minimum kvartalsvist i den digitale risikokomité, som jeg driver. Bestyrelsen er også generelt opmærksom på cybertrusselsbilledet, og har ønsket regelmæssigt at blive briefet herom.

Formelt fungerer jeg altså primært som en "anden forsvarslinje", men jeg er placeret organisatorisk meget tæt på "første forsvarslinje", hvilket gør det daglige samarbejde meget effektivt og smidigt. Det er derfor også et erklæret mål, at håndteringen af både digitale og persondatarelaterede risici håndteres og indarbejdes som en naturlig del af de daglige forretningsprocesser i stedet for at blive "separate specialistområder".

Som eksempel herpå er både dokumentation af digitale risici, kontroller og den GDPR-relaterede behandlingsfortegnelser indarbejdet i samme værktøj som PensionDanmarks generelle proces- og it-dokumentation. Dermed undgås den parallelle vedligeholdelse af et separat "compliance-system", der i praksis ofte vil føre til, at det system kommer ud af sync med virkeligheden.

Samarbejdet med dels compliance-funktionen dels med intern revision som "tredje forsvarslinje" er også velfungerende, og vi holder regelmæssige koordineringsmøder, hvor vi drøfter væsentlige risikoområder samt fokusområder, afgørelser og nyheder fra diverse tilsyn mv. Vores erfaring viser, at disse regelmæssige drøftelser kan give nyttigt input til fokuseringen af fx intern revisions it-revision. Samtidig opfattes det meget positivt i organisationen, at der er sammenfald mellem de risici, der arbejdes med at adressere både i nye projekter og i "driftsarbejdet" med fx opdatering af forretningsgange, og i de risici, intern revision adresserer i sit tilsynsarbejde og fokusområder.

På et område som leverandørstyring er der et tæt samarbejde i forhold til fx indhentning af og opfølgning på revisionserklæringer fra væsentlige samarbejdspartnere, således at indhentninger af "almindelige" it-revisionserklæringer og persondata-erklæringer sker i samme arbejdsgang.

Har din virksomhed også brug for en Chief Digital Risk Officer?

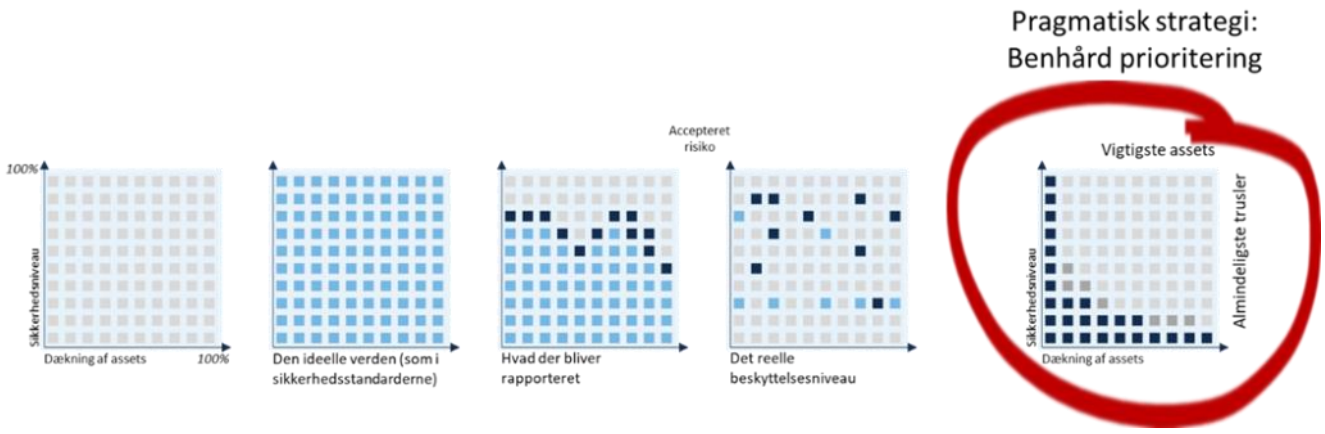
PensionDanmark er på nogle områder en digital frontløber og har arbejdet fokuseret med at integrere teknologi og forretning i digitale forretningsprocesser i store dele af forretningen. Som følge heraf har risikobilledet (og forretningsmulighederne) ændret sig. Dette er dog nok en beskrivelse, mange andre selskaber også kan nikke genkendende til. Baseret på min erfaring – også som mangeårig rådgiver inden for cyber-risici og cybersikkerhed – er det dog en udfordring i mange virksomheder, at cyber-, privacy- og andre digitale risici på forskellig vis behandles i siloer rundt omkring i organisationen.

Digitaliseringen sker måske "isoleret" i en særligt innovationsfokuseret enhed, persondatasikkerhed er placeret som et compliance-ansvar, mens it-sikkerhed er placeret i it-organisationen med reference til it-chefen eller it-direktøren. Det, mener jeg, ikke giver mening mere. Disse risici er nødt til at blive behandlet af et samlet – eller integreret – team i en governance-model, der tillader direkte rapportering til ledelse og i andet led til bestyrelse.

Hvorvidt det direkte nødvendiggør en "chief digital risk officer" i organisationen vil jeg ikke sige – og faktisk kan jeg godt lide, at jeg indtil videre vist nok er den eneste i hvert fald i Skandinavien med den titel. I stedet mener jeg, at det vigtige at fokusere på er, at man etablerer den nødvendige, tværgående forståelse af risiciene på tværs af hele forretningen. Ikke bare ud fra et compliance- eller risikominimerende perspektiv, men ud fra et perspektiv om, at en integreret tilgang til og involvering af de rigtige kompetencer tidligt i digitale transformationsinitiativer gør det muligt at levere disse hurtigere.

I flere selskaber har jeg set it-sikkerhedsteamet fået malet sig selv op i et hjørne, hvor de opfattes som konstante nej-sigere, og derfor bliver kørt ud på et sidespor – hvilket selvsagt ikke er konstruktivt – ligesom det heller ikke er konstruktivt blot at bruge penge på it-sikkerhedsudstyr uden at det er baseret på en vurdering af de konkrete risici. Der findes mange sikkerhedsfirmaer, der mener at have en "silver bullet", men den findes altså ikke, og bare at følge med i det nyeste trends er nærmest en disciplin for dig.

Jeg noterer mig, at flere af de store rådgivningsfirmaer også er begyndt at slå på tromme for "digital risk" som disciplin og for at integrere cybersikkerhed, privacy og digitalisering på tværs af siloerne. Og det er nok også det allervigtigste råd, jeg vil give videre: stop med at tænke "ekspert-siloer", tænk på forretningen først. Måske med inspiration i nedenstående tegning: Hvis du kender dine vigtigste processer og data og dine risici, så har du det overblik, der er nødvendigt for at kunne tage hurtige, men velunderbyggede beslutninger. Og det er nødvendigt, hvis du vil være en digital vinder. Det tager lang tid at vinde kundernes digitale tillid – men at miste den igen kan ske hurtigt...



Bæredygtig långivning - en væsentlig del af bankers fremtidige forretningsmodel

Cecilie Stegenborg-Andersen, Chief ESG Analyst, Danske Bank

Dorte Kurek, Head of Wholesale Credit Governance, Danske Bank

Indledning

Bæredygtige banker, grønne banker og sociale banker er ikke rigtige banker. Sådan var holdningen blandt mainstream banker for bare fem år siden. I dag arbejder langt de fleste banker på at få bæredygtighed indarbejdet i deres kerneprocesser og beslutninger.

I Danske Bank har vi mange års erfaring med kreditvurdering af vores kunder, mens bæredygtighedsvurdering er noget nyere i udlånsprocesserne. I denne artikel fortæller vi lidt om vores tilgang til at arbejde med bæredygtig långivning. Vi ved, at vi har meget at lære om bæredygtighed i den sammenhæng – og det er en rejse, vi glæder os til.

Samfundsudviklingen viser klart, at bæredygtighed generelt optager folk. Det er især drevet af FN's Paris aftale om at holde den gennemsnitlige globale temperaturstigning under 2 grader sammenlignet med niveauet før industrialiseringen[1]. I EU har EU-kommissionen sat sin egen handlingsplan i gang, hvor der blandt andet stilles krav om, at bankerne rapporterer på deres klimapåvirkning – også for deres udlån, samt at der anvendes en fælles EU-definition af, hvad der anses for bæredygtige aktiver[2].

Flere og flere investorer efterspørger også bæredygtige investeringsmuligheder. Larry Flint, CEO for Blackrock – verdens største investor – har annonceret, at bæredygtigheden skal være i orden for samtlige investeringer hos Blackrock[3]. De største rating bureauer har allerede integreret vurdering af bæredygtighed i deres ratings.

Bæredygtighed skal være konkret

Begrebet bæredygtighed bruges i mange sammenhænge og når vi arbejder med bæredygtig långivning i praksis, er det vigtigt med en præcis afgrænsning. I Danske Bank har vi valgt at arbejde med bæredygtig långivning ved at integrere ESG . E står får Environmental (miljømæssig), S står for Social (sociale) og G står for Governance (styring og ledelse). ESG definerer en række konkrete og kvantificerbare målepunkter, som gør det klart, hvad vi præcist forstår ved bæredygtighed ved bevilling af lån, og gør det nemmere at sammenligne virksomheder på tværs, jf. **Figur 1**.

Når vi analyserer miljømæssige og sociale forhold, selskabsledelse og finansielle faktorer får vi en bedre forståelse af vores erhvervskunder. Deres forretningsmodel, deres position i markedet og de risici og muligheder, de står over for. ESG hjælper os derfor med at lave bedre kreditbeslutninger til gavn for både kunden og os.

Danske Bank har fokus på bæredygtig udvikling

I Danske Bank har vi en ambition om at skabe bæredygtig udvikling og have en positiv indvirkning på det samfund, vi er en del af. Vi integrerer bæredygtighed i vores tilgang til at drive virksomhed og anvender ESG til at vurdere bæredygtighed i virksomheder, som vi investerer i, udlåner til eller anvender som leverandører. Vi tror på, at ESG perspektiver og bæredygtige produkter er nøglen til

Figur 1. Definition af ESG

at lave langsigtet værdiskabelse for kunder, investorer og samfund.

Vi begyndte at arbejde med ESG i långivningen i 2015, hvor vurdering af ESG blev integreret i vores kreditpolitik, og vi fik defineret nogle få sektorer, som vi anså for særligt risikofyldte. Vi har siden arbejdet på at integrere ESG i de eksisterende udlånsprocesser på lige fod med vurdering af f.eks. finansielle nøgletal.

Vi konstaterede hurtigt, at det kan være svært for bankmedarbejdere at forholde sig til bæredygtighed ved vurdering af udlån – uden konkrete værktøjer og relevant træning. Vi udviklede derfor en række værktøjer til at føre principperne i kreditpolitikken ud i praksis. Og vi gik i gang med at træne vores kolleger i at bruge værktøjerne. Samtidig besøgte vi nogle af de større europæiske banker for at lære, hvordan de arbejder med bæredygtighed i långivningen. Endelig samlede vi vores input fra træningsessionerne og fra besøg hos andre banker i en ny bæredygtig udlånsstrategi, som vi er i gang med at rulle ud.

Et væsentligt element i strategien er at udvikle en intern ESG-score af vores kunder, der gør det muligt at vurdere de enkelte kunders styrker og svagheder i forhold til andre virksomheder i samme sektor. Vi har desuden nedsat en komité for bæredygtige udlån, der løbende tager stilling til, hvilke bæredygtighedskrav der skal stilles for enkelte sektorer, samt bankens holdning til en række principielle dilemmaer.

Interessen for ESG og bæredygtig långivning er steget betydeligt blandt medarbejdere i banken. Der er stor efterspørgsel på træning og viden omkring bæredygtighed. Og omvendt er antallet af samtaler om, hvorfor banken skal beskæftige sig med bæredygtighed faldet markant i samme periode. Så vi er på rette vej.

Vi bygger ovenpå de eksisterende kreditprocesser i banken

Vores fokus lige nu er derfor på at få opbygget en basisforståelse af bæredygtig långivning i organisationen og integrere det i vores processer. ESG indgår som en del af vores kreditpolitik og er derfor en del af vores kreditprocesser.

For os handler ESG i kreditprocessen om at få en bedre forståelse af kunden – er kunden for eksempel selv opmærksom på bæredygtighed, og hvilken historik og governance har kunden indenfor ESG.

Med hjælp fra en ekstern dataleverandør screener vi også for, om der har været problemer relateret til ESG hos vores kunder. Det kan være alt fra kemikalieudslip og CO_2-udledninger til dårlige arbejdsforhold og børnearbejde i supply chains. Hvis der har været et issue, er vores første skridt at tage en dialog med kunden og høre, hvordan de arbejder med at udbedre skaden. ESG handler ikke om, at der ikke må laves fejl, men om hvordan risici kan minimeres, og hvordan man kan lære af fejl.

Vi er ved begyndelsen af en spændende rejse

Arbejdet med at indføre bæredygtig långivning i Danske Bank er en lang og spændende rejse. Problemstillingerne inden for bæredygtighed er komplekse, og det er særdeles sjældent, at virksomhederne i vores portefølje har top performance på samtlige ESG-kriterier. Ligesom vi kender det fra kreditvurdering af kunder, er det i praksis nødvendigt med en helhedsvurdering af kunden, og mange spørgsmål kan kun opklares i tæt dialog med kunden.

Vi vil gerne sikre, at bæredygtig långivning bliver en almindelig del af vores forretningsmål. Derfor har vi valgt at bygge bæredygtighed ind i vores almindelige arbejdsprocesser, f.eks. indgår vurdering af ESG som et fast punkt i vores Kreditkomité, vores sektoranalyser er udvidet med en ESG-vurdering, og ESG vil også blive indbygget i vores etableringsproces for nye kunder i banken. Vi starter med et minimumsniveau i alle relevante processer, og bygger på derfra.

Noter

[1] Parisaftalen er en international aftale inden for FN's klimakonvention UNFCCC, som drejer sig om begrænsning af udledning af drivhusgasser gennem grøn omstilling, klimatilpasning og finansiering heraf. Aftalen blev indgået på COP21-klimakonferencen i Paris i december 2015, og den træder i kraft i 2020. 195 lande underskrev aftalen, som pr november 2017 er ratificeret af 171 lande. Aftalen forpligter landene til at modvirke den globale opvarmning ved at holde den globale temperaturstigning under 2° C i forhold til det førindustrielle niveau, og stræber mod en temperaturstigning på kun 1,5° C.[3]

[2] https://en.wikipedia.org/wiki/Paris_Agreement
https://ec.europa.eu/info/sites/info/files/180308-action-plan-sustainable-growth-factsheet_en.pdf

[3] I sit årlige brev fra 2018 skrev Larry Fink, CEO i BlackRock (verdens største investor) at "… a company's ability to manage environmental, social, and governance matters demonstrates the leadership and good governance that is so essential to sustainable growth, which is why we are increasingly integrating these issues into our investment process". https://www.blackrock.com/corporate/investor-relations/larry-fink-ceo-letter

Revision af ESG

Per Graabæk Ventzel, Audit Director, Danske Bank

Ann Christina Kristensen, Danske Bank

Som betroet finansiel partner har Danske Bank som mål at understøtte den bæredygtige udvikling i samfundet. For at kunne det, er det afgørende at koncernen er i stand til at håndtere 'Environmental, Social and Governance' (ESG) risici som en del af låneprocessen.

For ESG er der ikke tale om regulær lovgivning med specifikke instrukser mv. men hensigtserklæringer og forventningerne, og dertil uden entydig sammenhæng mellem kravene i revisionsbekendtgørelsen og bl.a. FN's klimamål og Paris-aftalen.

Informationsindsamling og specifik videnssøgning er i højsædet og revisionen af ESG som tema åbner en unik mulighed for at øge "vidensbanken". Der er i større grad tale om basis for fortolkninger og dialog omkring "baseline. Der er ikke noget med to streger under og kildedatabasen indeholder ikke tidligere afgørelser fra Finanstilsynet.

Vurdering af de iboende risici på kreditområdet er primært drevet ud fra en regulatorisk eller finansiel tilgang. Ved revisionen af ESG inddrages "omdømme-risiko" i højere grad. Således er det i bankens 'Social Impact & Sustainability Policy' anført:

> *We do not conduct business with customers whom we believe disregard or deliberately violate UN-based principles on environmental protection, human rights, labour rights and anti-corruption.*

Helt overordnet var vores approach at vurdere tilstrækkeligheden af politikker og direktiver samt 'oversight'-rollens implementering til sikring af ovenstående.

At revidere ESG var som udgangspunkt ikke metodisk forskelligt fra den måde vi reviderer andre processer og kontroller. Metodisk har vi haft den samme tilgang; med udgangspunkt i walk-throughs lavede vi en vurdering af design og implementering, dernæst test af O/E af designet.

Vi formulerede det i to overordnede risici:

- Insufficient development and maintenance of the policies in 2nd line of defense regarding ESG risks
- Insufficient oversight and support by 2nd line of defense regarding ESG risks.

For at kunne vurdere og teste ovenstående, blev der derfor indledningsvist læst en del litteratur om emnet. Dernæst skulle vi stifte bekendtskab med bankens tilgang hertil, tilføjelser i Kreditpolitikken, offentliggjorte direktiver og endelig tilføjelser til den bestående kreditproces. Dertil interviews. Masser af interviews.

Qua de ovennævnte risici, havde vi primært kommunikation med 2nd line of defense, der så vores revision som en løftestang til at få endnu mere fokus i koncernen på udfordringerne ved at modne og implementere procedurer til at supportere en mere bæredygtig udvikling. Og dertil en mulighed for at drøfte udfordringer, fortolkninger mv. med en "udenforstående". Således fra vores perspektiv et godt udgangspunkt for samarbejde og vidensdeling.

Vores væsentligste take-away fra revisionen var en åbenhed i koncernen omkring den rejse man er påbegyndt og en erkendelse af ikke at være i mål endnu, men på vej. Meget endnu skal fortolkes, vurderes og implementeres. Vi forventer derfor også at skulle have ESG på planen de næste par år.

Som interne revisorer i Danske Bank er vi også på en rejse – vi har taget vores "værktøjs- og videnskasse" med os, og vi forventer at fylde den op med ny læring og viden omkring revision af ESG og omdømmerisici generelt. Det har givet god mening at være med på bankens rejse fra dag et, således at vi på den måde kan supporte banken med "timely" vurdering af det forventede/ igangsatte kontrolmiljø.

Mere til dig

PFA
Mere til dig

Vil du være en del af en intern revisionsafdeling med høj faglig standard og høj kvalitet, hvor vi arbejder tæt på forretningen? Måske er du den interne revisor, vi søger, i PFA, hvor du tager hul på en karriere med mere mening og opgaver, der giver dig masser af gode kolleger og udvikling af dig, personligt og fagligt.

Du skal stå for revisionsopgaver - bl.a. med fokus på it-sikkerhed
Du bliver en del af den interne revisionsafdeling i PFA. Vores opgave er at udføre revision i overensstemmelse med funktionsbeskrivelsen og de lovgivningsmæssige krav og standarder. Vi har fokus på operationelle forhold, risikostyring og regeloverholdelse. Desuden deltager vi i udvalgte områder af den løbende finansielle revision og i revision af regnskabsaflæggelsen i samarbejde med PFA's eksterne revisor. Som intern revisor får du et tæt samarbejde med de øvrige medarbejdere i Intern Revision og med chefer og medarbejdere i de områder, der revideres. Dine nøgleopgaver er at:

- planlægge og udføre revisionsopgaver
- deltage i og udarbejde revisionsrapporter
- deltage i opstartsmøder og afmelde revisioner over for de reviderede
- bidrage til den løbende udvikling af vores metodik og arbejdsdokumentation.

"Vi leder efter dig, der er åben og observant, og som trives med et bredt samarbejde internt i koncernen. Det er også vigtigt, at du har en vis robusthed, så du kan holde hovedet koldt i de pressede situationer, vi nogle gange oplever," siger Louise Claudi Nørregaard, der er koncernrevisionschef.

Du har flere års erfaring med revisionsopgaver

Vi forventer, at du:

- besidder og udlever en høj faglig og metodisk standard
- har flere års praktisk erfaring med revisionsopgaver, herunder it-revisionsopgaver
- arbejder struktureret, har altid fokus på at forstå og fortolke data korrekt og vægter højt, at detaljer er i orden
- er god til at udtrykke dig kort, klart og præcist, uanset om det er på skrift, i dialog eller i præsentationer
- bruger som en selvfølgelighed de nødvendige it-systemer på højt niveau og har interesse for eller erfaring med databehandling og dataanalyse
- har en relevant kandidatgrad.

Det er et plus, hvis du allerede har erfaring med revision af liv- og pension. Som del af jobbet tilbyder vi årlig efteruddannelse, så du kan udvikle dig til specialist i revision af operationelle forhold, risikostyring og regeloverholdelse.

Dit nye team venter på dig
Du bliver en del af et mindre team. Vi har forskellige kompetencer inden for revision, og vi prioriterer højt at lære af hinanden. Vi vægter godt kollegaskab højt, og vi har fokus på at skabe rammer, der betyder, at du får energi af at gå på arbejde. Du vil opdage, at vi har række tilbud, der giver dig mulighed for at udvikle dig selv fagligt og personligt samt at udforske din fysiske og mentale sundhed. PFA har en samfundsmæssig opgave, men ligeså vigtigt er vores ansvar for dig og dine kolleger. Vi synes selv, at vi har sammensat en attraktiv ansættelsespakke, der tager hensyn til din økonomi, familietid og din nutidige og fremtidige trivsel.

Er du klar til at blive en del af holdet?
Så send din ansøgning senest den 20. september 2019. Vil du vide mere om stillingen, er du velkommen til at kontakte koncernrevisionschef Louise Claudi Nørregaard på 61558488.

En karriere i PFA
PFA er et pensionsselskab, men vi er langt mere end det. Udover pension og forsikring tilbyder vi opsparing i vores bank for privatkunder og en række løsninger inden for sundhed og boliger. Vi er ejet af vores mere end 1,3 millioner kunder, og vi blev stiftet i 1917 for at sikre danskerne frihed til at leve det liv, de ønsker. Vores arbejde har betydning for danskernes liv, og vi tager samfundsansvaret alvorligt - bl.a. med afsæt i FN's udviklingsmål. Selvom vi er 100 år, er vi i konstant forandring og går efter at være i front med teknologi og digitalisering, og al den værdi vi skaber, sender vi tilbage til kunderne.

Monitoring of non-audit services - what is all the fuss about?

Morten Vilstrup Olesen, MSc in Business Economics and Auditing, Internal Audit Manager, Nordea

Introduction

From time to time the external auditor of a company provides other services than the statutory audit, these are in general categorised as 'non-audit services', and for Public interest Entities (PIE), there are certain limitations to the provision of these services.

In 2014 the European Parliament and the Council drafted the regulation on specific requirements regarding the statutory audit of public-interest entities [1] (the 'regulation'). The regulation contains, among other things, specific measures for non-audit services of relevance for the statutory auditor, the audit committee of the 'PIE' or 'company' and thus also of relevance for the internal audit function of the PIE.

While most parts of the regulation have been in force for years now and thus do not have any significant news value, new or enhanced focus on compliance with especially Article 4 is needed from 2020.

This article will have its focus on Article 4 and 5 in the regulation, which is regarding non-audit services. The article will provide you with an introduction to the content and interpretation of Article 4 and 5, how to manage non-audit services in line with the regulation, and which questions to ask yourself when monitoring non-audit services. Also, links and references to the regulation and where to find further guidance is included.

Regulation

The regulation is called *'Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities'* and is closely related to the EU directive *'on statutory audits of annual accounts and consolidated accounts'* no 43/2006.

Scope

In scope of the regulation are:

1. Statutory auditors and audit firms carrying out statutory audits of PIE's, and
2. PIE's.

Within the PIE, the regulation is deemed of relevance for the audit committee and the department having the day-to-day interaction with the statutory auditor, e.g. the finance department.

Having knowledge of the regulation becomes relevant for the internal audit function, when internal audit supports the audit committee and provides independent assurance on the non-audit service reporting from e.g. the finance department and overseeing the reporting from the statutory auditor.

Purpose

The purpose of the regulation is to promote the independence of the statutory auditor and avoid the occurrence of conflicts of interest.

The regulation introduces a strict approach to the independence of statutory auditors or audit firms with a list of prohibited non-audit services (Article 5) and a financial cap on the audit fees for non-audit services (Article 4). Please also note that the Member States may apply more stringent requirements than set out in the regulation. The intention by setting strong independence measures is to achieve a high level of consumer and investor protection to the customers and investors of the PIE's.

Impact

The regulation prohibits certain services and sets a limitation on the volume of non-audit services. The limitations of non-audit services delivered by the statutory auditor is specified in the sections below regarding Article 4 and 5.

Entry into force

The regulation entered into force on the twentieth day following its publication. Hence it became applicable on June 17th, 2016 and applies to financial years starting on or after this date. However, the cap on non-audit services specified in Article 4 will have its impact from 2020 onwards.

The regulation has binding legal force throughout the EU and should be aligned/incorporated in national law. The regulation will override national law where there is a conflict.[2]

Non-audit services

The statutory auditor can provide the PIE, its parent undertaking and its controlled undertakings non-audit services. However, certain limitations and responsibilities lie on the statutory auditor, the audit firm and the audit committee of the PIE.

Article 5(4) stipulates; *The statutory auditor may provide the audited entity, its parent undertaking or its controlled undertakings non-audit services other than the prohibited non-audit services, subject to the approval of the audit committee after it has properly assessed threats to independence and the safeguards has been applied.*[3]

Hence, some non-audit services are prohibited, and all others are subject to an assessment of the 'threat on independence' and approval by the audit committee, prior to being carried out. In practice, a list of common, non-complex services, up to a certain value, can be issued and pre-approved by the audit committee, to lighten the approval burden.

The regulation has strong ties to the general principle of independence for auditors. Hence regarding non-audit services, the responsibility for being independent and in compliance with the limitations and cap of non-audit services also lies on the statutory auditor. However, this should be overseen by the audit committee of the PIE [service receiver].

The audit committee shall "*review and monitor the independence of the statutory auditor or audit firm, and in particular the provision of additional services to the audited entity*".[4] In practice the internal audit function can support the audit committee by conducting independent review and monitoring of the services delivered by the statutory auditor and provide independent reporting to the audit committee.

First and foremost, monitoring requires knowledge of the type of services and common categories of the services provided.

Audit and non-audit services
In the context of monitoring audit services and fees, three common categories can be used:

1) Statutory audit,
2) Non-audit required by law, and
3) Other non-audit services.

1. Statutory audit (also known as 'audit services') means audit of annual accounts or consolidated accounts insofar as required by Community law.[5]

2. Non-audit required by law (also known as 'audit related') are assurance services, which are not part of the statutory audit engagement, but required by EU or national legislation.[6] These are fully allowed non-audit services, however, still subject for approval by the audit committee.

3. 'Other non-audit services' are all other services provided by the statutory auditor, which do not fall into the categories of 'statutory audit' or 'non-audit required by law', and which are not prohibited cf. Article 5.

Other non-audit services are allowed, subject to the approval of the audit committee following an assessment of the threats to independence and the safeguards in place to mitigate or eliminate those threats. However, the volume of other non-audit services is limited cf. Article 4(2).

In addition to the services in the three categories are the prohibited non-audit services.

Article 5: Prohibition of the provision of non-audit services

Article 5 of the regulation introduces a 'blacklist' of some non-audit services, which the statutory auditor or audit firm is prohibited in providing. A list of prohibited services, as listed in the regulation, is presented below:

Article 5 (partial extract): Prohibited non-audit services shall mean;	
(a)	Tax services relating to:
(i)	preparation of tax forms;
(ii)	payroll tax;
(iii)	customs duties;
(iv)	identification of public subsidies and tax incentives unless support from the statutory auditor or the audit firm in respect of such services is required by law;
(v)	support regarding tax inspections by tax authorities unless support from the statutory auditor or the audit firm in respect of such inspections is required by law;
(vi)	calculation of direct and indirect tax and deferred tax;
(vii)	provision of tax advice;
(b)	Services that involve playing any part in the management or decision-making of the audited entity;
(c)	Bookkeeping and preparing accounting records and financial statements;
(d)	Payroll services;
(e)	Designing and implementing internal control or risk management procedures related to the preparation and/or control of financial information or designing and implementing financial information technology systems;
(f)	Valuation services, including valuations performed in connection with actuarial services or litigation support services;
(g)	Legal services, with respect to:
(i)	the provision of general counsel;
(ii)	negotiating on behalf of the audited entity; and
(iii)	acting in an advocacy role in the resolution of litigation;
(iii)	cost control.

(h)	Services related to the audited entity's internal audit function;
(i)	Services linked to the financing, capital structure and allocation, and investment strategy of the audited entity, except providing assurance services in relation to the financial statements, such as the issuing of comfort letters in connection with prospectuses issued by the audited entity;
(j)	Promoting, dealing in, or underwriting shares in the audited entity;
(k)	Human resources services, with respect to:
(i)	management in a position to exert significant influence over the preparation of the accounting records or financial statements which are the subject of the statutory audit, where such services involve: – searching for or seeking out candidates for such position; or – undertaking reference checks of candidates for such positions;
(ii)	structuring the organisation design; and
(iii)	cost control.

The list of 'prohibited services' is wide ranging and only applies within the EU. Subject to general principles of independence, an auditor (other than the statutory auditor) should be able to provide any non-audit service outside of the EU. However, special rules may apply, hence it is recommended to become acquainted with those.

Article 4: Audit fees

Article 4 of the regulation introduces a 'fee cap' for the volume of 'other non-audit services' which a statutory auditor or audit firm is allowed to provide to a PIE, its parent undertaking or its controlled undertakings. The services are limited to no more than 70% of the fee for the statutory audit, averaged over the prior three years.

Article 4(2):
"When the statutory auditor or the audit firm provides to the audited entity, its parent undertaking or its controlled undertakings, for a period of three or more consecutive financial years, non-audit services other than those referred to in Article 5(1) of this Regulation, the total fees for such services shall be limited to no more than 70 % of the average of the fees paid in the last three consecutive financial years for the statutory audit(s) of the audited entity and, where applicable, of its parent undertaking, of its controlled undertakings and of the consolidated financial statements of that group of undertakings."

The fee cap applies to the PIE group i.e. the public-interest-entity, its parent undertaking and its controlled undertakings.

PIE Groups
A public-interest-entity is defined in the audit directive[7], while a PIE group can be defined as the PIE, its parent undertaking and its controlled undertakings.

A larger financial group can easily consist of several PIE groups, e.g. by having credit institutions, mortgage- and insurance companies within the group, and maybe even in several countries. The PIE group and the PIE sub-groups are all individually applicable to the regulation of non-audit services.

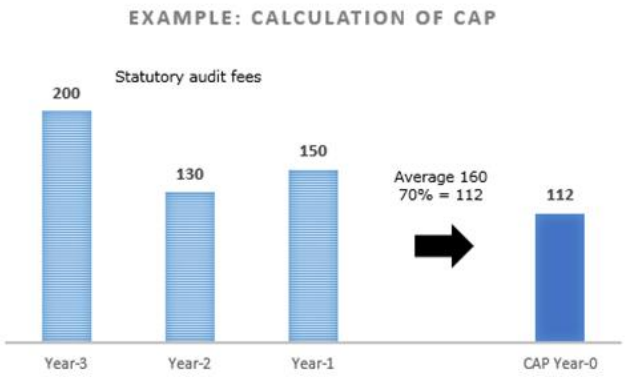
Figure 1 on the next page presents a group structure with 15 companies and four branches in total, including three PIE's. Each PIE shall have an audit committee and review and monitor the independence of the statutory auditor, i.e. by following the amount and type of non-audit services provided by the statutory auditor.

In the example, there are three PIE groups:
1) Red sphere; the overall 'Group' here determined by the main (mother) company, which here is identified as a PIE.
2) Green sphere; 'PIE-sub-group 1', and
3) Purple sphere; 'PIE-sub-group 2'.

If there are more than one PIE within a group, a cap shall be determined for each PIE-sub-group.

The calculation of the fee cap
When calculating the cap for other non-audit services, a three-year average of the statutory audit fee is used as the denominator. For example, statutory audit fee for the fiscal years since the regulation entered into force, 2017, 2018 and 2019, will be the basis for the cap calculation in 2020. Thus, there is the need for enhanced focus on the regulation and the cap in 2020 and going forward.

$$NAS\ year\text{-}0 \leq 70\%\ of\ \frac{\sum(year\text{-}3;\ year\text{-}2;\ year\text{-}1)}{3}$$



The exercise of calculating the fee cap should be done for each PIE in a group.
The cap will only apply in the fourth consecutive year; the clock will be reset if in one year no non-audit services were provided. Hence, during the first three consecutive years under the legislation, no cap applies. However, the fee cap can used by the audit committee as a threshold for 'independence' and be implemented as a static limit for non-audit services.

The calculation of utilisation of fee cap
Knowing the fee cap, the next step is to monitor the utilisation of the fee cap for other non-audit services, to make sure the limit is not breached.

Services required by national or EU legislation are exempted from the calculation of the cap (referred to as 'non-audit services required by law'), thus only fees for 'other non-audit services' is used in the calculation.

The utilisation is monitored per fiscal year, normally following the calendar year. The calculation is simple if one has a good overview of the approved (and delivered) other non-audit services, as they constitute the numerator of the calculation. The denominator is the three-years average of statutory audit fees, as presented above.

$$\frac{\textit{Other non-audit services}}{\textit{3 years average statutory audit}}$$

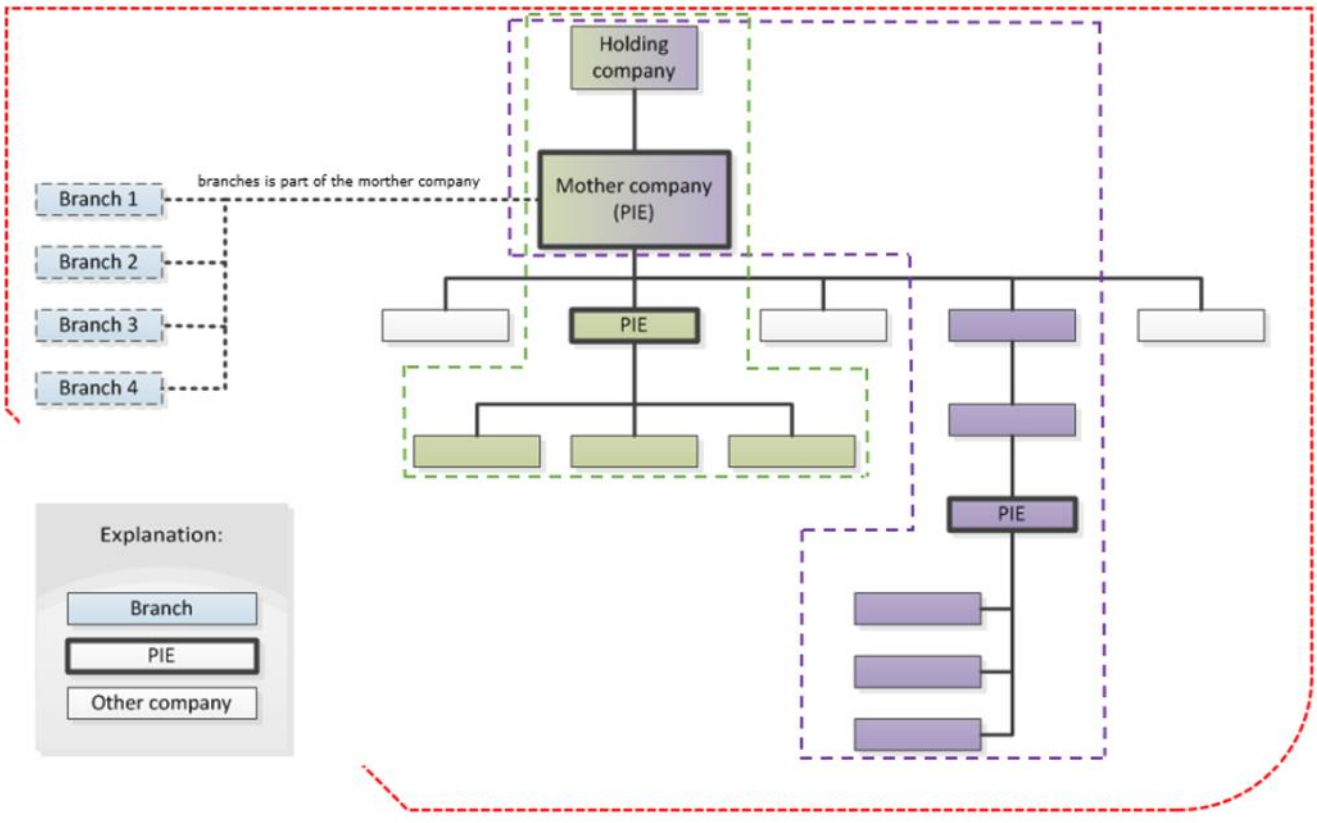
The utilisation ratio shall be less than 70%, cf. Article 4 (2).

NAS from AC and IA perspective

AC involvement and practical handling
The audit committee (AC) is required to monitor the independence of the statutory auditor, and hence also to be involved in the monitoring of non-audit services (NAS). The provision of permissible non-audit services is subject to an assessment of the threats to independence and safeguards applied to mitigate or eliminate those threats, followed by an approval by the AC.

Depending on the volume of non-audit services provided to the PIE, it can – from a practical point of view – be relevant for the AC to pre-approve certain services, e.g. reoccurring non-audit services up to a certain amount, to be able to focus on the more rare, complex and special cases of services. The pre-approval can be established in a policy/internal guideline with mandate to the CFO, head of accounting or similar, to procure common non-audit services within a certain monetary limit, while other non-audit services and high amount services shall still be approved by AC. The AC should have the approval and monitoring of non-audit services on the agenda of the AC meetings and the approvals should be documented, e.g. in meetings minutes.

Figure 1. Group structure with companies and branches



Focus points for internal audit (IA) assurance work
In order to provide assurance to the AC, the internal audit function (IA) can perform ongoing review of the non-audit services and the reporting to the AC. In the review the internal auditor should have focus on:

- **Completeness**
  Are all entities and all fees included in the approval and reporting process? And do the approved amounts agree with the actuals recorded in the general ledger?

- **Accuracy**
  Do the records of purchased services correspond to the list of services from the statutory auditor and the reporting to the AC? And does the aggregated amount reconcile to the figures used for calculation of utilisation of fee cap?

- **Classification**
  Is the classification of the services set correctly? Is it 'non-audit services required by law' or 'other non-audit services'? Or is the service listed in Article 5 and thereby prohibited?

Other food for thought, for the auditor working with review or monitoring of non-audit services:

- Is the company a PIE?
- Does the group consist of several PIE groups?
- Do we have full oversight/overview of entities and fees in the group? Do all have the same statutory auditor? And do even the smallest entities in the group know about the regulation and the restrictions, and do they comply?
- Does the AC have approval procedures for non-audit services?
- Which kind of reporting does one get from the statutory auditor? And do the figures agree with ours?
- Which kind of monitoring does the audit committee perform?
- How to reconcile actuals with approved fees, if there are months in between the approval of a maximum fee and the one invoiced?

This introduction to the regulation and how to monitor non-audit services, as well as the open questions above, hopefully provide you with a better understanding of the regulation and the approach to take when monitoring or providing assurance on non-audit service reporting.

Where to find further guidance

Committee of European Auditing Oversight Bodies (CEAOB) has issued guidance, called 'Monitoring the fee cap of non-audit services'.[8]

The European Contact Group (ECG), which is an informal grouping of the six large accounting networks in the EU, have produced a FAQ document on the EU Audit Legislation[9], also covering this topic.
Also, some audit firms have issued small memos on the topic.

Notes

[1] EU Regulation no. 537/2014 (the 'regulation')
[2] The regulation is incorporated in national law, e.g. Revisorloven § 31(2) in the Danish legislation.
[3] EU Regulation 537/2014, Article 5(4)
[4] EU Directive 2006/43/EC, Article 41(2), item (d).
[5] EU Directive 2006/43/EC, Article 2 no 1.
[6] EU Regulation 537/2014, Article 4(2)(2).
[7] EU Directive 2006/43/EC, Article 2 no 13.
[8] CEAOB Guideline on monitoring the fee cap of non-audit services, issued 21 September 2018.
[9] ECG FAQs – February 2018

External Assessment - Internal Audit i Ørsted A/S

Christian Aslo-Petersen, Senior Audit Specialist, Ørsted

Martin S. Petersen, Lead Audit Specialist, Ørsted

External Assessment generelt

Ifølge IIA's "International Standards for the Professional Practice of Internal Auditing" (standarderne), skal der minimum hvert femte år foretages en "external assessment". Kravet, der fremgår af standard 1312, kan opfyldes på to måder idet der enten foretages:

- Full external assessment, eller
- Self-assessment with independent validation.

Begge metoder kræver en uafhængig ekstern assessor, som kan foretage vurderingen (full external assessment) eller validere den foretagne self-assessment.

Der er fordele og ulemper ved begge metoder. En af fordelene ved 'full external assessment' er, at den interne revision skal anvende færre interne ressourcer. Omvendt vil metoden medføre, at tidsforbruget for den eksterne assessor bliver større.

En af fordelene ved 'self-assessment with independent validation' er, at medarbejdere i den interne revision opnår et solidt indblik i efterlevelse af standarderne og Code of Ethics samt selv identificerer eventuelle forbedringsmuligheder. Metoden kræver flere interne ressourcer, da der er mange områder, som skal vurderes, og disse vurderinger skal dokumenteres. En ulempe ved metoden kan være, at den eksterne assessor ikke opnår samme kendskab til den interne revision, og der er derfor en risiko for, at nogle forbedringsmuligheder ikke bliver afdækket.

IIA's 'Quality Assessment Manual' indeholder 4 skemaer, som skal udfyldes for at dokumentere den foretagne self-assessment. Temaerne i de fire skemaer er 'Governance', 'Staff', 'Management' og 'Process', og de dækker dermed alle områder i standarderne og Code of Ethics således at det sikres, at alt bliver vurderet. Herudover er der et skema, som oplister det materiale, som skal foreligge til den eksterne assessor.

Erfaring med external assessment i Ørsted Internal Audit

Internal Audit i Ørsted blev etableret i sin nuværende form i 2013. Ca. 12 måneder senere fik vi foretaget en ekstern assessment. Årsagen til, at vi valgte at få foretaget en ekstern assessment er, at det er vigtigt for både bestyrelsen, daglig ledelse og os selv at sikre, at vi efterlever standarderne samt Code of Ethics, og dermed udfører vores revisions- og konsulentarbejde i overensstemmelse med anerkendte internationale standarder. Hvis vi fortsat vil leve op til standarderne, skal vi have foretaget en ny external assessment senest i 2019. Den fik vi foretaget i løbet af Q1 2019, og resultatet heraf er blevet drøftet med den daglige ledelse og bestyrelsen.

I forhold til valg af metode, valgte vi at foretage en 'self-assessment with independent validation", da det er vores vurdering, at arbejdet giver et godt indblik i, hvorvidt standarder og Code of Ethics efterleves i Ørsted Internal Audit. Samtidig giver arbejdet et værdifuldt input til det 'Quality Assurance and Improvement Program' (QAIP), som er en del af kvalitetsstyringen i Ørsted Internal Audit. Det er derfor vores vurdering, at de interne ressourcer er givet godt ud. Et råd til andre, som påtænker at foretage en ekstern assessment er, at det er vigtigt at starte processen i god tid, da indsamling af materiale, udarbejdelse af self-assessment skemaer, planlægning af møder med stakeholders m.v. tager tid. I vores tilfælde blev der brugt ca. to uger for to fuldtidsressourcer til dette arbejde.

Vi valgte at indgå en aftale med et eksternt revisionsfirma om, at de skulle validere den self-assessment, som vi udarbejdede. Som en del af deres valideringsarbejde interviewede det eksterne revisionsfirma udvalgte stakeholders i Ørsted for at få disse personers vurdering af det arbejde og den værdi, som bliver skabt af Ørsted Internal Audit. Denne del af processen tog sammenlagt ca. en uge at gennemføre.

Resultaterne af vores "Self-assessment with independent validation" er, at vi fortsat efterlever standarderne samt Code of Ethics. Dette har vi som nævnt kommunikeret til ledelsen, ligesom vi fortsat medtager information herom i al vores rapportering. Det er vores vurdering, at information om at vi efterlever standarderne og Code of Ethics, har betydning for vores stakeholders, da de dermed har sikkerhed for, at vores arbejdsmetoder følger internationale standarder.

Nogle gode råd til de interne revisioner, som overvejer at få foretaget en ekstern assessment:

- Start i god tid, så der også er tid til at overveje hvilken af metoderne, der er bedst for din interne revision
- Besøg IIA Global's hjemmeside, hvor der er vejledninger m.v. som bør studeres inden arbejdet igangsættes, jf. https://na.theiia.org/services/quality/Pages/Quality-Assurance.aspx
- Baseret på valg af assessment metode skal der udvælges en uafhængig assessor. En tidlig dialog med as-

sessor, hvor der forventningsafstemmes og planlægges, er med til at sikre, at den eksterne assessment kan foretages på en effektiv måde uden for mange tilbageløb

- Udpeg de medarbejdere, der skal sikre, at den eksterne quality assessment bliver foretaget. Samtidig skal det sikres, at der afsættes tid til arbejdet, og at medarbejderne har adgang til IIA's 'Quality Assessment Manual' samt relevant internt materiale
- Der bør være ledelsesmæssig fokus på opgaven, så det sikres, at den prioriteres ligesom de øvrige planlagte revisions- og konsulentopgaver.

Reflektion

I artiklen '*Trials and Transformation'*, der er publiceret i februar 2019 udgaven af 'Internal Auditor' fremhæver Richard Chambers, at niveauet for overholdelse af standarderne kan forbedres ved at sikre at der foretages en ekstern assessment (siderne 26 – 27).

Det er vores vurdering, at den eksterne assessment er med til at sikre, at vi kontinuerligt er opmærksomme på at efterleve standarderne samt Code of Ethics. Endvidere giver den eksterne assessment et godt indblik i, hvorvidt der er områder, som kan forbedres. De interne revisioner, som endnu ikke har fået foretaget en ekstern assessment, bør derfor nøje overveje, om det er et kvalitetsstempel, som er relevant. Dette for at sikre, at den interne revision og det udførte arbejde lever op til standarderne samt Code of Ethics.

Nye medlemmer

Nye medlemmer i IIA fra 28.3 – 1.9.2019

A.P. Møller-Mærsk
Richard Engström
Siddharth Kehr

Banknordik
Kirstin Sigvardsen

Betri Banki
Erland Berg Danielsen

Codan Forsikring
Stina Kjellström
Mats Andersen

Danfoss
Stine Juhl-Hansen

Danske Bank
Jouliana Marjane Afroukh
Marta Szymaszek

Ernst & Young P/S
Anders Houmann

Finansministeriet
Ahmed Shuheibar
Diana Holm

Forsvarsministeriets Interne Revision
Søren Tang Møller

Jyske Bank
Lena Lykkegård

KPMG P/S
Tobias Kristensen

Københavns Kommune
Marie Neergaard Hald
Irena Wolowicz

Landbrugsstyrelsen
Rasmus Brøndt
Barnabas Czomba

LEO Pharma
Mengtan Li

Lån & Spar Bank
Maja Lundbye

MAN Energy Solutions SE
Natalie Lebel Kessler

Nordea
Per Hansen
Trine Møller Ovesen

Novo Nordisk
Peter Ulrich

Nykredit
Anne-Mette Buus Jensen

PwC
Mads Skovgaard Larsen

REVI-IT
Thomas Tscherning

Solar
Christina Liljegren

Ørsted Services
Pia Elkjær Bay
Lars Aaes Nielsen
Paul Barchard

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

01.10.2019: Kursus for Forsikringsrevisorer
07.10.2019: Operational Audting - Influencing Positive Change
13.11.2019: Temadag for den finansielle sektor
27.05.2020 - 28.05.2020: IIA Årsmøde 2020 i Kolding

"Bagsmækken"

Foreningens adresse

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

CVR nr. 73954215

Indmeldelse i foreningen

Indmeldelse i foreningen foretages på www.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, Internal Audit Manager, CIA, Nordea
☎ 31 18 38 01 ✉ heino.hansen@nordea.com

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

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

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

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

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

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

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

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

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

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

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

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