INFO

Foreningen af Interne Revisorer
Nummer 79 | December 2021 | 26. årgang

Minitema: ESG

- Auditing ESG risks in financial institutions
- 5 Things You Need to Know About ESG

Mød Anthony Pugliese

Interview med IIA Globals President og CEO om Learning, Growth and Inclusion

Få løst revisionsopgaven

Anvendelse af konsulenter i Intern revision

Bkg. om ledelse og styring

Operationelle risici

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
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

Næste nummer
INFO 80 udkommer i april 2022.
ISSN: 1903-7341 (Elektronisk version).

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

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

Forsidefoto
UnknownNet

Redaktionens adresse

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

redaktionen@iia.dk

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

Indhold

Leder 3
Nyt fra redaktionen 4

Minitema: ESG
Auditing ESG risks in financial institutions 7
5 Things You Need to Know About ESG 12
Sidste nyt om ESG 17

Identifikation og risikovurdering af ikke-finansielle risici 19
Anvendelse af konsulenter i Intern revision 22
Internal Audit Assessment Tool for Audit Committees .. 25
Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. – Fokus på it-strategi, it-risikostyringspolitik og it-sikkerhedspolitik 27
Learning, Growth and Inclusion—Interview med Anthony Pugliese, IIA Global President and CEO 30
Nye medlemmer 35
Bagsmækken 36

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

Re-kalibrering

På grund af pandemien har mange organisationer prioriteret kortsigtede prioriteter for interne revisionsfunktioner, men nu er det også tid til at re-kalibrere for potentiel langsigtet usikkerhed og kompleksitet.

Den primære rolle for interne revisioner er at hjælpe beslutningstagerne med at beskytte organisatoriske aktiver og omdømme samt at understøtte operationel bæredygtighed. Med COVID-19-pandemien, der fører til en kraftig stigning i det hjemmebaserede arbejde, er aktivrisiciene steget, mens et driftsforstyrrende forretningsmiljø har skabt usikkerhed omkring omdømme og bæredygtighed.

Udfordringen for IA-funktionerne vil i det kommende år være at sikre, at de fortsat fører en sikker overvågning, samtidig med at de tilpasser sig et dynamisk risikolandskab. Intern revisors rolle skal i højere grad fokusere på, hvordan deres organisation forpligter sig til at opfylde offentlige behov og interesser som en del af sin kultur. Lovgiverne har også øget deres fokus på ESG-risici med initiativer i forbindelse med klimaændringer, aflønning af ledere, mangfoldighed og inklusion, arbejdsforhold og produktindhold, blandt andet.

Da risiciene er blevet mere og mere komplekse, er intern revisor nødt til at levere et større udvalg af tjenester. I nogle tilfælde – f.eks. i finansielle institutioner – har intern revisor også et ansvar med hensyn til styring, risikoappetit og kulturen med risiko og kontrol, som har været i fokus i de seneste år. I takt med at risikolandskabet er blevet mere komplekst er intern revisions funktionen nødt til at gennemgå deres nuværende set-up – og sikre, at de er udstyret til at revidere de nye områder herunder tilegne sig de nødvendige kompetencer.

Husk på at vores udgangspunkt er godt. Med intern revisions overblik på tværs af virksomheden kan interne revisorer vurdere en organisations ESG-risiko ud fra flere perspektiver og hjælpe med at forbinde punkter. For eksempel kan interne revisorer ved vurderingen af ledelse og politik overveje, om organisationen har skabt en ledelsesstruktur og kultur, der understøtter effektiv styring af klimarisici, og om der rapporteres oplysninger om klimarisiko til bestyrelsen osv. Vi kan revidere og vurdere risikostrategi og appetit, overveje om klimastrategi og risikoappetit hele tiden spredes over hele organisationen, og om der overvejes klimarelaterede risici i nye produkter og serviceydelser. Tilsvarende spørgsmål kan stilles med hensyn til yderligere ESG-risikostyringsområder som f.eks. risikovurderinger, overvågning og rapportering, porteføljeforvaltning og kapitalforvaltning, risikodata og -systemer samt risikostyringsmodel, medarbejdere og kultur.

Det er bestemt ikke nemt, men for dygtige og kompetente interne revisorer, er det bare endnu en dag på kontoret.

God jul, godt nytår og god læselyst.

Nyt fra redaktionen

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

Få indflydelse på indholdet af INFO

Fra redaktionens side er vi super stolte over, at vi med dette nummer af INFO kan krydre jeres juledage med artikler om aktuelle emner, som præger vores hverdag lige nu men forhåbentlig også jeres verden. Vi forsøger så vidt muligt at bringe artikler, som kan dække over alle vores læseres behov. Det er selvfølgelig en udfordring, og der vil være nogle, som kunne ønske sig artikler om andre emner.

Er du en af de personer, som har en masser ideer, om hvad der rører sig i vores branche og dermed en masse ideer til artikelemner, som vi ikke har dækket, har jeg alletiders tilbud til dig. Bliv medlem af redaktionen! Det kræver kun en kort mail til mig.

Redaktionsarbejdet er for de kreative. Arbejdet består af at holde sig opdateret med, hvad der sker i branchen, og komme med ideer til artikelemner. Herudover består arbejdet i at finde personer, som vil være forfattere til artiklerne. Arbejdet består som udgangspunkt ikke i at skrive artikler selv.

Ud over at være med til at bestemme indholdet af INFO får du som redaktionsmedlem også et netværk til interne revisorer i andre virksomheder.

Har du mod på at deltage i dette arbejde, så skriv en kort mail til mig på: bisv@bnpparibas-pf.dk.

Farvel og tak for indsatsen

Alting har sin ende. I dette nummer af INFO må jeg desværre sige farvel til Mai-Britt Soo, Sparekassen Kronjylland, som har forladt redaktionen. Mai-Britt har fået nyt arbejde uden for intern revision og jeg vil gerne benytte lejligheden til at takke Mai-Britt for hendes indsats i redaktionen. Hun har især bidraget til, at vi har fået en forståelse for, hvad der rører sig i mellemstore banker, herunder hvad der rører sig i de jyske pengeinstitutter.

Jeg ønsker Mai-Britt held og lykke i hendes nyt job.

Bliv en aktiv del af IIA!!!!

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

Læs om udvalg, netværksgrupper og meget mere på foreningens hjemmeside www.iia.dk, eller send en mail til kontakt@iia.dk.

IIA PRISEN

Prisopgave om intern revision

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

Minitema:
ESG

ESG! It's the talk of the town and it is headed our way. We may all be somewhat familiar with the main purpose and components of the ESG framework. We are also well aware that ESG is likely to impact our audit planning and priorities in the near future. However, I believe I speak on behalf of many internal auditors when confessing that ESG has left us somewhat challenged and confused. Despite our access to a wide array of literature, courses and advisory services, we are still left with many unanswered questions.

Luckily, Alexy Pozharny from Nordea has agreed to share with us his great knowledge and insights on ESG. In his article he provides valuable and tangible guidance on how to approach the audit strategy, risk assessments and resources, amongst other things. Although his main focus revolves around financial institutions, there is plenty of inspiration and many learning points to draw upon for readers who are not part of the financial sector.

Alexy's contribution is complemented by a recent article on ESG from the Internal Auditor magazine issued by the IIA. This article taps into the key questions and focal point which the internal auditor should address, when auditing the organisation's environmental, social and governance activities.

Collectively, we hope that these two articles may add value to the ESG-quest that many of us are embarking on.

Enjoy.

Auditing ESG risks in financial institutions

Alexey Pozharny, CIA, ACCA, Head of Audit ESG, People, Reputational Risk, Nordea

Introduction

Climate change negatively affects the real economy as well as the financial system. The financial sector is expected to play a key role in the transition to a low-carbon and more circular economy and climate change resistance. The transition entails both risks and opportunities for financial institutions.

The success of climate change resistance is dependent on the efficiency of the financial system, its ability to manage the risks and steer financial flows to a sustainable development, and is vital for the whole society. This drives the rapid evolvement of the society and also regulators' expectations towards the efficiency of the financial institutions and prudent risk management. Climate change resistance and sustainability have been incorporated into regulatory frameworks and supervisory expectations in a pace never seen before.

Therefore, internal auditors are facing increased demand and evolving expectations for the assurance work they provide, even though the guidelines and criteria are not sufficiently clear and keep developing fast. In this article I will share some ideas on how to adapt audit work to the changing and challenging environment, and how audit can add value to the sustainable development of the financial institution as well as serve stakeholders with due care.

ESG risks

The Environmental, Social and Governance (ESG) risks are *the risks of any negative financial impact on the institution stemming from the current or prospective impacts of ESG factors on its counterparties or invested assets*[1].

ESG factors are defined as *environmental, social or governance matters that may have a positive or negative impact on the financial performance or solvency of an entity, sovereign or individual*[2]. The examples of the ESG factors might be: energy consumption, waste production, impact on biodiversity, innovation in environmentally-friendly products, labour rights, health and safety, privacy, diversity and equal opportunity, supply chain management, codes of conduct and business principles, transparency and disclosure, bribery and corruption, community impacts and stakeholder engagement, etc.

Despite the developments at the EU level, the current policy framework still lacks common definitions of ESG factors, hence current market practice vary across institutions. This complicates the assessment of the ESG risk of the financial institution and its comparability, which is recognised by EBA. According to EBA, *a fundamental part of evaluating and measuring ESG risks in a comparable manner is to establish common definitions of ESG factors and to understand how these factors translate into financial risks that may impact institutions individually and the financial system as a whole*[3].

Financial institutions should expect further alignment of the common definitions of ESG factors, understanding the drivers and the ways how risk drivers impact the institutions (transmission channels). The main challenge for the financial institution and the auditor is the evolving determination of ESG risks, as well as developing methods and metrics to measure them. As a matter of fact, the auditor needs to act within a moving landscape and at a rapid pace of change. At the same time, it is an opportunity for the auditor to add value in the implementation of ESG risk management, for example by assessing the adopted definition of the risk factors, if it is complete and aligned to the institution's risk profile and exposures, as well as by assessing and challenging the institution's ESG implementation plans.

There are several other challenges that the auditor can turn into opportunities with the aim to keep adding value for stakeholders. A good starting point to tackle them is the audit strategy.

ESG audit strategy

The audit strategy for ESG risks should provide a comprehensive and structured analysis of the audit coverage needed for addressing increased stakeholders expectations. There are several factors to consider when developing the audit strategy.

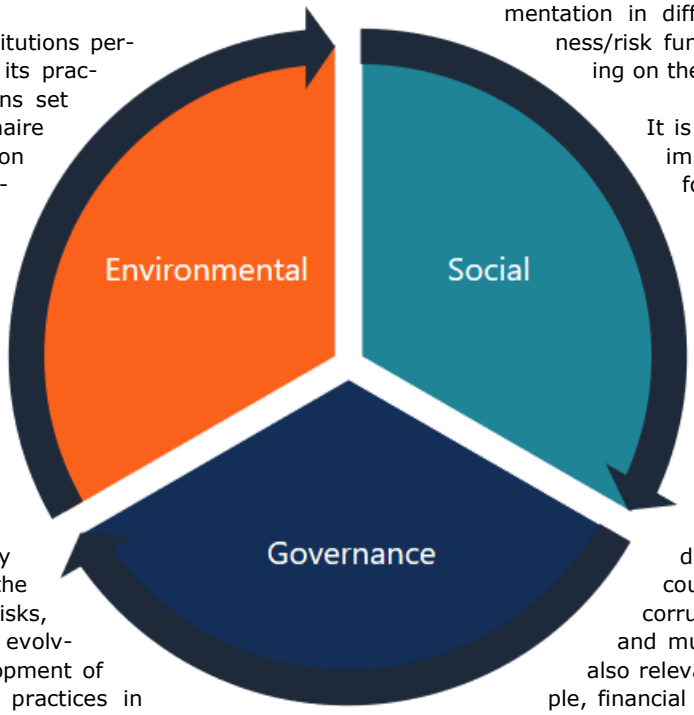
The auditor's challenge in providing sufficient risk coverage is that ESG risks arise from the core activities of the financial institution and materialise through the other risk

types. On the one hand, any ESG factor which impacts the institution or its counterpart will affect the institution through increased credit, market, reputational, operational and other risks. On the other hand, the way how ESG factors materialise in credit risk is different from e.g. liquidity risk. These drive the way how an institution will adapt the control environment for the other risk types to incorporate ESG risks in its risk management.

I would expect that the vast majority of institutions have launched initiatives to introduce ESG risk in the institution's exiting risk management framework and control environment, for example in the form of a programme.

The ECB Guide on climate-related and environmental risks (referred to hereafter as 'Guide') was published in November 2020[4]. It communicated the supervisory expectations related to ESG risk management and disclosure.

As a response, financial institutions performed self-assessments of its practices against the expectations set out in the Guide ('Questionnaire A') and its implementation plans to advance management of climate-related and environmental risks ('Questionnaire B') and submitted those to the Joint Supervisory Team (JST). The Guide as well as the responses to the questionnaires will serve as a basis for the supervisory dialogue with the institution.



Therefore, the audit strategy challenge is to address the evolving definitions of ESG risks, their broad scope as well as evolving audit criteria and development of the ESG risk management practices in the institution.

What should the auditor do when the requirements, plans, and results are evolving continuously? This is exactly the case when the real value of *agile* auditing tends to arise, *where there are high levels of uncertainty or the audit subject is moving at pace e.g. a programme that is using an iterative approach to solution design. It can quickly highlight areas which are not in a state to be fully audited, enabling the team to move on the other areas and return at an appropriate time*[5].

Thereby the auditor might apply a hybrid approach, combining traditional audit projects (as the institution should close the known gaps in ESG risk management) with an agile mindset (since regulations and methods to measure the ESG risks keep evolving).

It might be a valuable management practice to register the gaps identified by the institution's self-assessment ('Questionnaire A') as self-identified issues with stated due dates and issue closure criteria, in the issue-management systems used by the institution. This will help the auditor to plan the audit coverage of the phased deliveries of the institution's ESG programme, as well as not raise issues for known and escalated gaps.

I personally believe that an audit planning approach which is aligned with the institution's ESG implementation programme will be seen by management as adding value. The approach will challenge the delivered results to identify drawbacks and foster continuous improvement of the design quality. At the same time the auditor will be able to identify the drawbacks at an earlier stage, preventing deficiencies in the solution's rollout. Finally, knowing the closure status of the gaps will give the auditor flexibility in audit planning. As the speed of ESG risks implementation in different risk types and business/risk functions might differ depending on the significance of the gaps.

It is important to note that ESG implementation will be performed through the other risk frameworks in the institution. Therefore, the audit coverage of the ESG risk can be derived from the audit coverage of the other risk types, or at least partially leveraging them. It is important to remember that social and governance factors relate to human and labour rights, health and safety, diversity and inclusion, accounting and tax practices, corruption and bribery, ethics and much more. These factors are also relevant for the compliance, people, financial crime and reporting risks in the institution, and these might be already covered by the audit function outside of the ESG risks audit cycle.

All of the above call for a well-defined audit strategy for ESG risks coverage, to ensure the sufficiency and completeness of risk coverage in other risk types, as well as ensuring that ESG risks are included in scope of the audits for other risks. In these circumstances the ultimate ESG risks coverage might be blurry, due to unclear differentiation of the primary and secondary risk coverage by the different audit engagements. To keep the optics sharp on the ESG risks, the auditor should actively consider how to include ESG risks into the institution's risk assessment.

Risk assessment

According to the IPPF[6], risk assessment is *the identification and analysis (typically in terms of impact and likeli-*

hood) of relevant risks to the achievement of an organization's objectives, forming a basis for determining how the risks should be managed[7].

Risk assessment enables the development of the internal audit engagement plan, ensuring risk-based audit priorities.

The IPPF also states that: *Internal auditors may use management's information as one input into internal audit's organization-wide risk assessment*[8].

Institutions that have implemented Enterprise Risk Management (ERM) will have a comprehensive risk inventory and ESG risks should be part of it. The ECB Guide states: *Institutions are expected to develop a well-defined description of climate-related and environmental risks in their risk inventory that feeds into their risk appetite statement. The risk inventory is the result of the risk identification process and is expected to be based on the institution's internal risk taxonomy*[9].

A risk taxonomy is a common approach to categorising the risk types of an institution in the risk management framework. The approach helps to apply a common definition of the risks, helps with risk identification, and enables the risk aggregation.

According to EBA: *Institutions can incorporate ESG risks into their risk management frameworks as drivers of existing financial risk: Risks to capital (credit, operational, market) and risks to liquidity. Integrating ESG risks as a horizontal financial risk theme that can influence the traditional categories of financial risks should help ensure that the various impacts of ESG risks are identified and managed, whilst avoiding any double-counting effect*[10].

Many institutions incorporate ESG risks horizontally, that means that ESG risks are not standalone risks but part of the other risk types. The reason for such incorporation might be the organisational ownership of the risk frameworks in the institution. For example, it is the responsibility of the credit risk framework owner to integrate ESG factors in it, and credit units should develop and maintain controls for ESG risks in the credit processes. Therefore, horizontal incorporation of ESG risks in the institution will preserve the accountability for the implementation of ESG risks in relevant other risk types frameworks.

However, auditors might have their own approach to aggregation of risks, if it better serves the purpose of the risk-based audit plan development. *Auditable units may be any topic, subject, project, department, process, entity, function, or other area that, due to the presence of risk, may justify an audit engagement*[11]. Auditable units (AU) might not mirror the organisational structure of the institution, therefore auditor's risk aggregation might differ.

In addition, the auditor's risk assessment approach might be impacted by the granularity of the tools the auditor uses, e.g. how many risk-layers has the credit risk in the taxonomy. As a result the horizontal inclusion of the ESG risks in other risk types might make it illegible for understanding the severity of ESG risk in each AU.

For example, an AU is exposed to several risks (e.g. credit and reputational) which, in turn, are affected by ESG factors. Therefore ESG factors have multiple impacts on the AU's risk. As well as ESG factors might have different transmission channels for each AU's risk exposure. Consequently, it might be practically difficult to assess the whole ESG risks exposure of AU.

Also, I foresee a challenge with the assessment of the residual risk, as the state of controls might vary. For example, an AU exposed to credit risk might have satisfactory credit related control environment, but insufficient controls for the ESG factors affecting the credit risk. Also, the horizontal approach might complicate the depiction of the risk coverage. Depending on the organisation of the internal audit function, auditors focusing on the credit risk might have limited knowledge for assessing the ESG factors, or vice versa.

Therefore, I believe that having ESG risk as a stand-alone risk for risk assessment purposes will better enable an assessment of the severity of the risk for each AU in the institution's audit universe. It will also enable drawing the ESG heat map for the institution which could help the auditor in ranking coverage priority. This approach will help to have a comprehensive view of the institution's ESG risk exposure, as well as assess the level of the control environment in each AU. Otherwise, the ESG overview might be blurred due to delusion of ESG factors in other risk types.

Furthermore, the auditor will be able to juxtapose the ESG heat map with the ESG implementation plan of the institution, which will help setting the priority for audit coverage and effectively allocate audit resources. For example, the ESG risks related controls in credit risk might be under development and not ready to be audited. Therefore, the auditor should determine priority and areas of audit focus.

ESG audit focus

The auditor should independently and objectively provide assurance on matters related to the achievement of organisational objectives in accordance with Three lines model[12].

ESG risks should influence the financial institution's strategy and its business objectives. According to EBA: *ESG risks should be proportionately incorporated into the business model analysis, in particular with regard to the analysis of the business environment, the current business model, the strategy analysis and the assessment of the viability and sustainability of the business model*[13].

ESG risk management is the foundation of the sustainability of the business model, as it ensures long-term value creation. That is why it has so much attention from the various stakeholders. Many financial institutions have

incorporated sustainability targets aligned with global sustainability goals in their business strategy. Management is responsible for delivering business strategy under the board's supervision. *Because ESG strategy should align with business strategy and focus on material risks and business drivers, the full board will want to understand the ESG messaging and how those risks are being mitigated*[14]. Therefore, ESG matters in the institution's board agenda are not "nice-to-have", but necessary for the board to supervise ESG issues.

Nowadays it is nice to be "green", but institutions should be discreet and avoid the risk of been accused of 'greenwashing'. *Greenwashing is the practice of making an unsubstantiated or misleading claim about the environmental benefits of a product, service, technology or company practice*[15].

There are several indicators that the greenwashing and reliability of disclosures are receiving increased attention from the regulators and investors. For example, DWS (a German asset management company) shares slide 13% after greenwashing claims prompt BaFin (a German regulator) investigation[16], or over 70% of some of world's biggest corporate emitters failed to disclose the effects of climate risk in 2020 financial statements. 80% of their auditors showed no evidence of assessing climate risk when reporting[17].

Bearing in mind the attention and interest of various stakeholders in ESG matters, it would be advisable to plan a comprehensive audit coverage and key areas of ESG audit focus might be:

- alignment of the business goals with sustainability strategy,
- the governance and supervision of ESG risks, as ESG issues are relevant to all committees,
- measuring and reporting the progress against the sustainability targets,
- and also controls over the reliability of disclosures, ESG information and communications to stakeholders.

An efficient information gathering for these audit areas might be achieved by the auditor's observation procedures. It might be a sensible approach if the auditor participates as an observer in the steering committees of the institution's ESG change programmes, or other bodies accountable for the implementation of ESG risk frameworks and realisation of the sustainability strategy. Auditors will, in turn, understand the institution's ESG efforts, particularly how those efforts align with stakeholder expectations. Also, in institutions that lack ESG criteria and reporting, the auditor has an opportunity to help the institution to increase its ESG awareness. To be a valuable contributor to these dialogs, the auditor should possess relevant skills.

Audit resources

Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities[18]*.*

ESG risks are relatively new for the risk taxonomy and their scope is very broad, affecting all activities of the institution. That means that auditors covering ESG risks should have broad skills and knowledge on various topics, stretching from climate change to anti-bribery and labour rights.

These skills are needed to address only the ESG factors affecting the inherent risk, while in order to assess the control environment, these skills should be supplemented with knowledge of the credit risk, market risk and other risk frameworks.

There can be a challenge to staff the audit engagements with sufficient competences. I have identified several building blocks to consider when overcoming this challenge.

Firstly, the identification of the competence gaps in the audit function and finding the appropriate response, whether if it should be training, hiring or co-sourcing for the audits.

Secondly, I assume that the audit functions in large financial institutions are already staffed with auditors possessing the needed knowledge to cover other risk types, e.g. credit risk and market risk, which are impacted by ESG factors. Therefore, audit function's learning and development plan should include the training of these auditors in ESG factors and transmission channels relevant for those risks.

Thirdly, if the audit function hires or co-sources people with specific ESG/Sustainability skills, they can participate in the audits covering other risk types, thereby sharing their knowledge with the other team members. All in all this will help spreading and raising the knowledge of ESG risks across the entire audit function.

Finally, it is vital to found an ESG-forum in the audit function to share and collaborate between audit teams delivering audit engagements for different AUs and covering other risk types. This will enable a smooth coordination of audit effort and allocation of resources, as well as raise auditors' awareness of ESG across the audit function. This forum is also crucial for annual planning, as efficient audit coverage can be achieved through engagement synergies. For example, if the risk-based audit plan covers third-party risk management, ESG-assessment of the vendors' due diligence can be scoped into the planned engagement.

A few final remarks

When talking about ESG risks the key thing to keep in mind is the connection to sustainable development, which *is the development that meets the needs of the present without compromising the ability of future generations to meet their own needs*[19].

This means that ESG risks have vital importance both for society as a whole and for any institution, and the high level of attention will not diminish any time soon.

Society and institutions have started their ESG-journey which will last for decades. There will be new regulations, methods of measuring and increased comprehension of transmission channels, and overall evolving awareness.

This changing environment gives many auditors valuable opportunities to serve stakeholders by assuring the sustainable development. Auditors should develop a set-up which will help stay on top of ESG matters. The building blocks of the set-up should be: to learn and collaborate, be versatile and curious, and focus on stakeholders needs, governance, transparency and reliability.

It goes without saying that there are a lot of challenges in this evolving area. We should acknowledge the existing uncertainties, data gaps, imperfect measures, different speeds of change and other challenges, but these can never justify an auditor's inaction in promoting and facilitating continuous improvement.

We should act now. Therefore, I would conclude on the auditor's imperative regarding ESG risks in financial institutions with my favourite quote: *It takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that*[20]*!*

Noter

[1] Report on management and supervision of ESG risks for credit institutions and investment firms EBA/REP/2021/18
[2] EBA/REP/2021/18
[3] EBA/REP/2021/18
[4] Guide on climate-related and environmental risks. Supervisory expectations relating to risk management and disclosures, European Central Bank, November 2020
[5] Agile auditing. Mindset over matter. 2018, PwC
[6] The International Professional Practices Framework (IPPF)
[7] IPPF Developing a Risk-based Internal Audit Plan, May 2020, The IIA
[8] IPPF Developing a Risk-based Internal Audit Plan, May 2020, The IIA
[9] Guide on climate-related and environmental risks. Supervisory expectations relating to risk management and disclosures, European Central Bank, November 2020
[10] EBA/REP/2021/18 para 258
[11] IPPF Developing a Risk-based Internal Audit Plan, May 2020, The IIA
[12] The IIA's three lines model, July 2020
[13] EBA/REP/2021/18
[14] ESG oversight: The corporate director's guide, 2020 PwC
[15] https://whatis.techtarget.com/definition/greenwashing
[16] Financial Times 26 August 2021
[17] https://carbontracker.org "Flying blind: The glaring absence of climate risks in financial reporting"
[18] IPPF, Standard 1210 Proficiency, 2016, The IIA
[19] Report of the World Commission on Environment and Development: Our Common Future, 1987
[20] Through the Looking-Glass, Lewis Carroll, 1871

5 Things You Need to Know About ESG

Environmental, social, and governance (ESG) issues represent a growing area of focus among today's stakeholders. In the World Economic Forum's Global Risks Report 2021, businesses surveyed point to multiple ESG-related risks high in likelihood and impact, including extreme weather events, climate action failure, natural resource crisis, and infectious diseases. The report noted each as a threat not only to business activities, but to resilience of social infrastructure, emphasizing both economic and societal challenges.

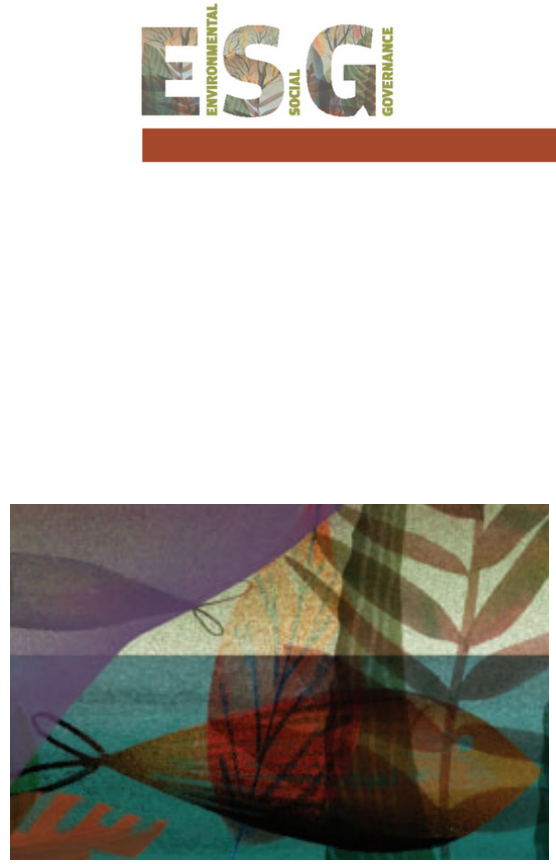
Business leaders, according to the KPMG 2020 Global CEO Outlook survey, face increased pressure to address these challenges. Nearly 80% of CEOs polled say their effectiveness in managing ESG risks and opportunities will play a role in determining if they can keep their job over the next five years. In fact, leaders are already called to account for the way they navigate these risks — and for their ability to turn them into strategic advantages.

But ESG risks are complex and dynamic, making them challenging to predict, monitor, and manage. They also are highly prolific, with the potential to impact business growth trajectories. An unanticipated severe weather event, for example, can cause physical damage to infrastructure, resulting in a standstill of business activities, job loss, stranded asset values, penalties from failure to deliver on contractual commitments, and even increased insurance premiums. The consequences can be severe and long-lasting.

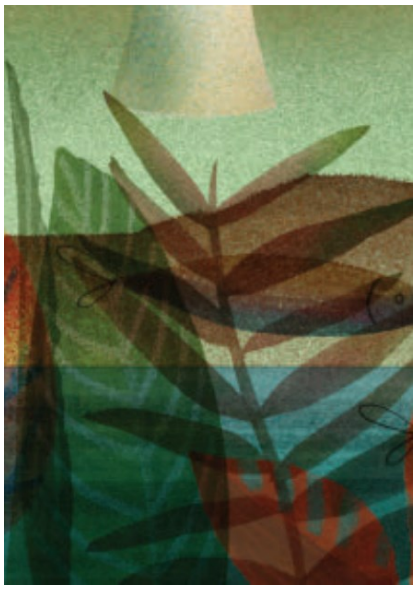
Internal auditors should consider several key questions when examining their organization's environmental, social, and governance activities.

Cherine Fok

Illustration by Sandra Dionisi



5 THINGS YOU NEED TO KNOW ABOUT ESG



Internal auditors must keep abreast of ESG developments and carefully consider their potential impact on the organization. The audit function plays an important role in ensuring ESG issues are cascaded down the organization's three lines (see "The IIA's Three Lines Model" next page) and acting as a steward for the relevance and reliability of ESG data. And because the audit committee regularly reviews internal audit's effectiveness, the committee's oversight extends to the processes for managing ESG information. With these considerations in mind, internal auditors must ask, and have answers to, five key questions regarding the organization's ESG-related activities.

1. Has the organization established a structured ESG framework? If so, how is it integrated with the Three Lines Model?

A structured ESG framework provides clarity on sustainability objectives and governance over topics that are material to an organization. Integrating the ESG framework with the existing risk management system reduces the risk that deficiencies may be undetected, as mismanagement of material ESG factors may cause organizations to deviate from achieving their strategic and operational objectives. For example, water often constitutes a material issue for food production companies. If the company secures a comparatively low cost for water use, it provides a strategic opportunity and a competitive advantage. At the same time, risks related to water include scarcity, which causes escalating water prices and disruption to supply.

Viewing risks through an ESG lens helps the organization and the internal auditor focus more acutely on the ESG implications of both new and existing risks. For instance, occupational health and safety is an ESG issue widely found in risk registers. It is not a new risk. However, applying an ESG lens draws attention to the wider social connotation of "occupational safety." For example, are safety practices in the workplace tracking local regulatory requirements and wider and emerging societal expectations such as mental wellness? An ESG perspective also helps stakeholders realize that managing this risk effectively can increase social capital, enhance enterprise value, and even allow the company to expand its socioeconomic contribution.

ESG risks should be closely monitored as part of the Three Lines Model. When examined in this context, ESG features prominently within each of the three lines:

- Line 1 — Management should take a proactive role in determining material ESG factors and actively seek to mitigate their potential impacts. This effort could include setting ESG policies and procedures that are aligned with the organization's sustainability objectives.
- Line 2 — Risk and compliance functions should provide tactical oversight, guidance, and challenge, and work closely with management on ESG-related matters.
- Line 3: The internal audit function needs to help ensure management is on the right track in managing material ESG factors.

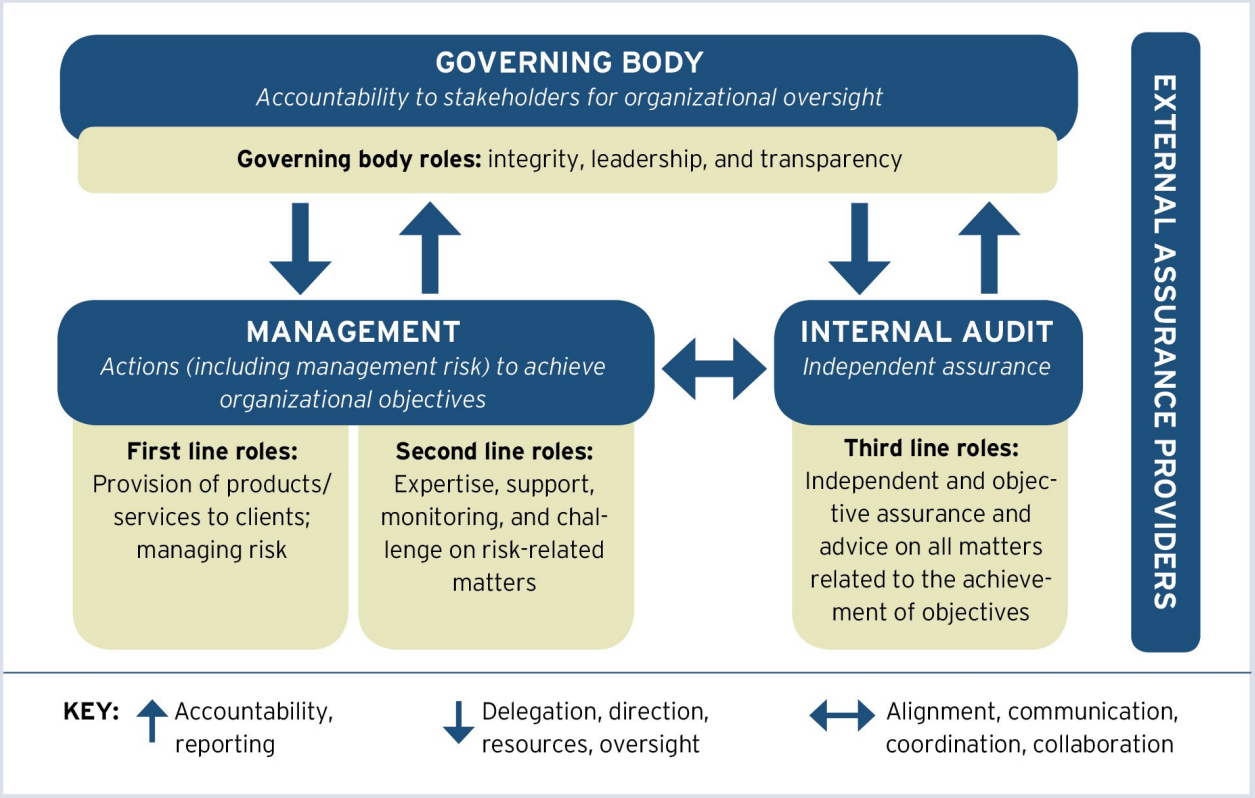
2. Does the organization possess the expertise, and a suitable culture, to manage ESG effectively?

While some ESG issues may fall within traditional functions, others may not be as clear cut. Areas such as green innovation, for example, may reside under strategy and research and development functions where outcomes are less defined. Or the procurement team may have been tasked with incorporating ESG considerations in its supplier policies despite knowledge gaps around technical understanding and evolving science. Internal auditors should assess whether additional expertise is necessary to supplement what an organization can accomplish in house. Moreover, preparedness to

More than 80% of managers and executives across the U.S., U.K., France, and Germany say their company has a formal ESG program in place, according to a recent Navex Global survey.

THE IIA'S THREE LINES MODEL

The Three Lines Model should encompass environmental, social, and governance (ESG) issues. Organizations can establish a sustainability function and provide suitable capacity building to support the management and oversight of ESG-related concerns, with internal audit providing independent assurance.



embrace sustainability may differ from one organization to another. Building ESG key performance indicators into balanced scorecards and remuneration frameworks can drive the success of ESG adoption.

A strong sustainability culture exists when leadership establishes a clear directive that ESG is integral to organizational purpose and values — and therefore core to business strategy. Everyone throughout the organization must understand that sustainability is an imperative, with each individual committed to the same vision and outcomes. Auditors can find evidence of this commitment in the establishment of ESG considerations within risk management processes, decision-making metrics, balanced scorecards, and remuneration frameworks. But these formal structures alone cannot drive sustainability. Practitioners also should make sure individuals are fully engaged on ESG topics and have adopted a growth mindset to embracing it.

3. Which ESG topics are being measured and reported, and why? Internal auditors should not set the organization's ESG strategy, but they must understand stakeholder priorities, material ESG issues, and most importantly, the intersection between the two. Ultimately, internal and external reporting should reflect both current state (what the organization is doing) and future state (what the organization intends to do), with metrics showing the efficacy of ESG initiatives. Internal auditors need to understand how ESG brings new risks to the organization's business model and opportunities for growth and transformation. Each organization will have its own mix of ESG priorities, encompass-

ESG ENVIRONMENTAL SOCIAL GOVERNANCE

5 THINGS YOU NEED TO KNOW ABOUT ESG

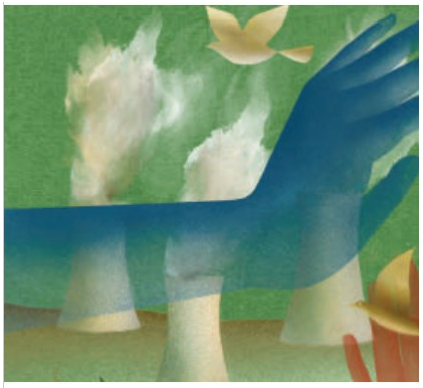
ing those that are key to its business success and important to stakeholders.

4. What processes and controls already exist over ESG data collection and reporting?
Data collection — especially in global, multiline businesses — can be challenging. For instance, many businesses currently report on their greenhouse gas emissions using the Greenhouse Gas Protocol, a global standard launched in 2001 by the World Resources Institute and the World Business Council for Sustainable Development. The protocol outlines a clear standard recognized by most investor groups. But tracking greenhouse gas emissions requires that each office, division, region, and business line is aligned on metrics, reporting style, cadence, and other areas. In addition, traditional approaches to risk management — even with horizon scanning to identify new and emerging risks — may not be sufficient for effective ESG management, as they typically examine the manifestation of risks within a predetermined time frame.

The Financial Stability Board's Task Force on Climate-related Financial Disclosures recommends the use of scenario planning, sensitivity analysis, and stress testing to ascertain an organization's resilience against climate risks. Those tasked with risk management and sustainability initiatives should harmonize their processes to facilitate cross-sharing of information and data control activities. Internal auditors should ask probing questions to understand the procedures and controls in place and assess their effectiveness.

5. What is the organization currently publishing in its ESG reporting?
Different reporting styles come with different levels of rigor. The data's importance to an organization's overall ESG strategy, risk appetite, and financial materiality should align with the corresponding regulations and levels of risk associated with the data. Thoroughly assessing these areas should help determine the reporting method. Likewise, ESG information included in a management analysis should be monitored with the same rigor as traditional financial metrics. A data-driven ESG approach helps make conceptual risks real and can more practically inform corporate strategy. Internal auditors should consider the risks associated with reporting strategies for certain metrics — especially as stakeholder demands rapidly increase — and help ensure the accuracy of disclosed data and measures.

KEEPING ESG ON TRACK
In an increasingly volatile environment, internal auditors play a critical role in helping the organization accomplish its goals by ensuring a systematic, disciplined approach to ESG. Material ESG issues should be addressed in the structured ESG framework — and when assessed to be of high impact and probability, these issues should be monitored through the organization's established enterprise risk management processes. Internal audit also should assess the risks that may not be covered in the framework, making sure adequate and effective measures are in place to address them. Using a thoughtfully considered approach, internal audit can help ensure the organization's overall ESG-related risk is managed effectively and that any residual ESG risks can be mitigated to an acceptable level.



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

Cherine Fok, CA, *is director, Sustainability Services, at KPMG in Singapore.*

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

SIDSTE NYT OM ESG

Finanstilsynet har offentliggjort konklusionerne fra sin temaundersøgelse af oplysningskrav under disclosureforordningen (art 3 om gennemsigtighed i forbindelse med politikker for bæredygtighedsrisici)

Finanstilsynet har gennemført to undersøgelser af implementeringen af disclosureforordningens artikel 3 blandt en række pengeinstitutter og pensionsselskaber.

Finanstilsynet finder, at implementeringen blandt disse virksomheder har betydeligt rum for forbedring på en række punkter, herunder især i forhold til nuanceret at identificere bæredygtighedsrisici specifikt for den givne virksomheds investeringer samt hvor og hvordan disse risici konkret integreres i investeringsbeslutningsprocessen henholdsvis investerings- eller forsikringsrådgivningen.

Finanstilsynet har opsummeret følgende punkter som de anser for best practice for, hvordan selskaberne opfylder art 3:

- Indeholder en klar vurdering af bæredygtighedsrisici, som defineret i disclosureforordningens artikel 2 stk. 22.
- Foretager en nuanceret og virksomhedsspecifik vurdering af, hvordan forskellige bæredygtighedsrisici, forstået som risikoen for en negativ indvirkning på værdien af en investering, gør sig gældende på tværs af den givne virksomheds typer af investeringer, således at slutinvestor får et fuldt billede af virksomhedens eksponeringer.
- Beskriver hvor og hvordan bæredygtighedsrisici integreres i investeringsbeslutningsprocesser henholdsvis investerings- og forsikringsrådgivning, således at slutinvestor informeres om, hvordan virksomheden konkret tager højde for de identificerede risici.
- Er lettilgængelige på virksomhedernes hjemmesider i form af en selvstændig politik for integration af bæredygtighedsrisici eller er klart afgrænset i et afsnit for integration af bæredygtighedsrisici i en mere overordnet politik på området
- I praksis bliver udmøntet i den pågældende finansielle markedsdeltagers investeringsbeslutningsprocesser samt når den finansielle rådgiver yder investerings- og forsikringsrådgivning.

Link til rapporten på Finanstilsynets hjemmeside

Sæt allerede nu kryds i kalenderen!

Identifikation og risikovurdering af ikke-finansielle risici

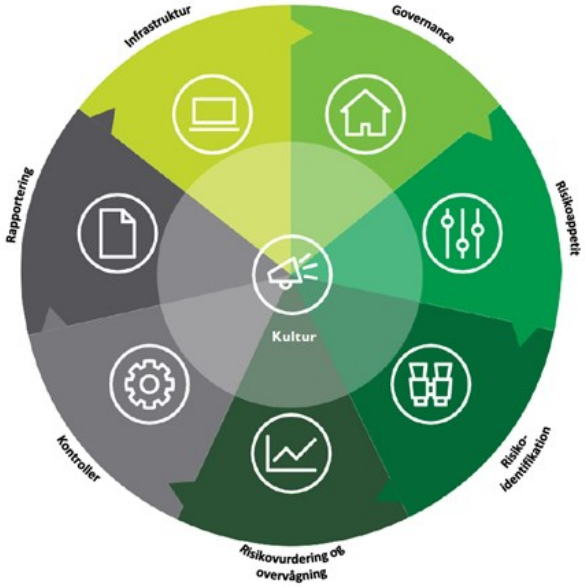
Christian Barrett, Manager, Deloitte

Martin Tripax, Senior Manager, Deloitte

Når puslespillet ikke kan samles af en funktion alene.

Indledning

I en verden som bliver mere og mere kompleks som følge af lovgivning, teknologi og begivenheder som Covid-19, er der kommet en erkendelse af, at det kræver en mere struktureret og målrettet indsats, hvis der skal ske en effektiv styring af risici. Dette vil omfatte implementering af et større rammeværk som omfatter alt fra governance til rapportering:



Et af de første skridt mod en mere sammenhængende tilgang til håndtering af ikke-finansielle risici er sikring af en fælles forståelse og begrebsramme for risici, således at der kan ske identifikation og risikovurdering af disse. De ikke-finansielle risici er identiske med de risici der i bilag 2 i ledelsesbekendtgørelsen hedder operationelle risici og IT-risici.

Kategorier af risici

For banker er det et regulatorisk krav at have en effektiv proces for identifikation af ikke-finansielle risici. I praksis er det dog en udfordring, fordi der mangler et fælles definition- og klassifikationssystem for disse risici.

I Deloitte benytter vi en fælles risiko-taksonomi, som her bliver gengivet i en forsimplet form for at give et bud på, hvad en sådan taksonomi kan indeholde. Den er delt op i to klasser. De finansielle risici og de ikke-finansielle risici.

Risikoklassen med finansielle risici er de traditionelle risici, som har en direkte effekt på virksomhedens finansielle situation, hvorimod risikoklassen med ikke-finansielle risici kan have en afledt effekt på de finansielle risici men de kan også have en effekt helt adskilt fra de finansielle risici. Et eksempel på det kan f.eks. være et stort hackerangreb. Dette er senest sket for den svenske bilfabrikant Volvo, som var ramt af et større hackerangreb, hvor der blandt andet blev stjålet data vedrørende forskning og produktudvikling.

De ikke-finansielle risici kan ofte være tæt forbundne, hvilket kan betyde, at en gennemgang fra compliance-funktionen ikke er tilstrækkelig. Et eksempel på dette kan være markedsmisbrug og fejl i den lovpligtige markedsovervågning. Her vil der være en compliance risiko i forhold til om lovgivning vedrørende markedsmisbrug overholdes, der vil være en IT-risiko i forhold til opsætning af markedsovervågning samt operationel risiko i forhold til manuelle fejl i den løbende overvågning.

Det kan også nævnes, at tendenser såsom brugen af Cloud kan medføre flere risici som har vidt forskellige karakter og tilsvarende vil være gældende for den øget brug af hjemmearbejdspladser.

De finansielle risici fremgår herunder:

Risiko-klasse	Kategori
Finansielle risici	Kreditrisiko
	Markedsrisiko
	Renterisiko på banking book
	Likviditetsrisiko

De ikke-finansielle risici defineres som værende øvrige risici end kreditrisiko, markedsrisiko, renterisiko og likviditetsrisiko. Det er altså alle de risici som ikke er finansielle risici.

De forskellige kategorier af ikke-finansielle risici kan ses på næste side:

Risiko-klasse	Kategori
Ikke-finansielle risici	Operationel risiko
	Compliance risiko
	IT-risiko
	Cybersikkerhedsrisiko
	Adfærdsrisiko
	Juridisk risiko
	Modelrisiko
	Tredjepartsrisiko
	Strategisk risiko
	Omdømmemæssig risiko

Til inspiration kan der nedenfor ses eksempler på risici der er tæt forbundne:

Eksempler på risici, som er tæt forbundne

- GDPR (compliance risiko), outsourcing (compliance risiko og tredjepartsrisiko) samt cybersikkerhedsrisiko
- Markedsmisbrug (compliance risiko) og fejl i den lovpligtige markeds-overvågning (IT-risiko eller operationel risiko)
- Manglende håndtering af kendte svagheder i kontrolmiljøet (operationel risiko) kan være relateret til forskellige former for compliance risiko
- Utilstrækkelig styring af adgangsrettigheder (cybersikkerhedsrisiko) og svindel (operationel risiko)
- Adfærdsrisiko og vildledning af kunder (compliance risiko)
- Fejl i aftalevilkår (juridisk risiko og/eller operationel risiko), tredjepartsrisiko samt omdømmerisiko
- Rapportering af mistænkelige transaktioner til SØIK (compliance risiko) og fejl i den forbindelse (operationel risiko)
- Kreditrisiko / markedsrisiko / forsikringsrisiko er forbundne til modelrisiko.

I konstant forandring

En risiko-taxonomi må ikke betragtes som værende statisk. Den vil være i evig forandring og ændre sig i takt med, at der kommer ny viden på områder, nye teknologier bliver introduceret og fænomener opstår.

Som nævnt tidligere kan f.eks. øget brug af hjemmearbejde medføre et kryds af flere kategorier af risici. Giver det en øget sandsynlighed for operationelle fejl når kommunikation i højere grad er digital, er der en større IT-risiko og eller cybersikkerhedrisiko når medarbejdere arbejder hjemmefra? Der kan eventuelt også være juridiske risici i forhold til arbejdsmiljø.

Det kræver et bredt kompetencesæt, hvis en medarbejder skulle afdække samtlige kategorier og kunne lave en fuldstændig risikovurdering af f.eks. hjemmearbejde. Dette skyldes at kategorierne spænder bredt og kræver indsigt i lovgivning, IT såvel som kendskab til virksomhedens processer og vurdering af konsekvenser ved operationelle fejl.

Det er vores anbefaling, at de tre forsvarslinjer og direktionen aktivt deltager i udviklingen af virksomhedens taxonomi. Dels for sikring af den fælles forståelse, men også for at sikre, at der sker udpegning af primær ejer for hver kategori. En ejer skal forstås som hvem der i 2. forsvarslinje har det primære ansvar for en kategori. Der vil forventeligt være mange ejere i 1. forsvarslinje for de enkelte kategorier.

En sådan øvelse vil sikre dels ejerskab på et område, men i lige så høj grad, at der gøres brug af de rette kompetencer således at juridiske risici og compliance risici bliver håndteret af en medarbejder med kvalifikationer indenfor dette.

Faldgruppen ved de ikke-finansielle risici er, at de ikke betragtes som værende komplekse, og vigtige perspektiver fra forskellige eksperter undlades. For eksemplet med hjemmearbejdspladsen kunne det være at risikoen udelukkende blev belyst ud fra et IT-perspektiv og juridiske perspektiver var undladt såsom arbejdsmiljø mm.

De fleste finansielle virksomheder har forøget deres udgifter til styring af de ikke-finansielle risici og nogle af de virksomheder vil også have bygget komplekse rammeværk til styring af de ikke-finansielle risici. Dette alene er dog ikke nødvendigvis nok. Det er vigtigt at virksomheden forstår sin risikoprofil i forhold til de ikke-finansielle risici, hvordan de er forbundet, hvordan de skal vurderes samt mitigeres. En velfungerende risiko-taksonomi kan afhjælpe dette, ved at understøtte identifikation og vurdering af risici. Dette kombineret med ejerskab bidrager til, at det er relevante medarbejdere som styrer de ikke-finansielle risici og dermed reflektere de stigende regulatoriske krav på området.

En fælles risiko-taksonomi vil blandt andet bidrage til:

- Der skabes en ensartet forståelse på tværs af virksomheden
- Der skabes et fundament for tildeling af ansvar og ejerskab, da det er muligt at identificere hvilken kompetencesæt der er nødvendige for en given risiko
- Der sker en reduktion i kompleksitet da underkategorier bliver fordelt ud til medarbejdere med de rette kompetencer.

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

Anvendelse af konsulenter i Intern revision

Morten Bendtsen, Koncernrevisionschef CIA, Alm. Brand, Bestyrelsesmedlem i IIA Danmark

Indledning

Den interne revision står over for en stadig mere kompleks forretningsmodel, nye risici og trusler, produkter og systemanvendelser og leverancemodeller hertil kommer, at reguleringen af den finansielle sektor er stadig stigende og omfangsrig.

Hvordan sikrer man, at den Interne revision er relevant og følger med den udvikling virksomheden udstikker?

I Alm. Brand besluttede vi at lukke en stilling i Intern revision ned og i stedet anvende budgettet på konsulenter. I december 2019 gik vi ind i en udbudsrunde.

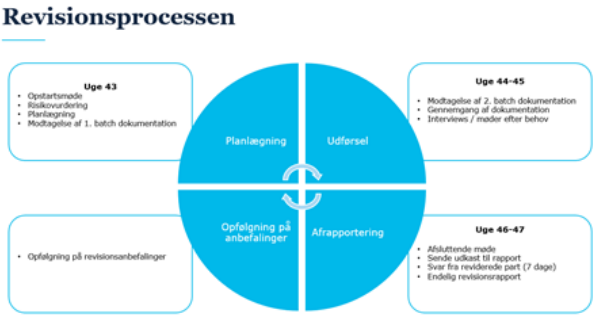
Udbud og operating model

Vi indbød EY, Deloitte, PwC og KPMG til at byde på opgaven, hvor vi bl.a. lagde vægt på følgende:

- En konkurrencedygtig og fleksibel prissætning
- Mulighed for op-/nedskalering af opgaver og timer
- Evnen til at bidrage med læring til Intern Revision
- Fag- og branchekendskab og bidrag med "Best Practice"
- Profiler og kompetencer

En anden væsentlig forudsætning bestod i, at Intern revision stadig skulle "eje" opgaven, og dermed at opgaverne ledes af Intern revision og løses i overensstemmelse med Intern revisions revisionsproces og rapporteringsformat.

Revisionsprocessen på en konkret opgave kan se således ud:



Konsulenter skal betragtes som insourcing af særlige kompetencer på teamet med det formål at øge værdiskabelsen af Intern revisions ydelser.

Løsning af opgaver skal kvalitetssikres efter revisionshuset gældende principper, hvilket skal dokumenteres overfor Intern revision.

Intern Revision skal modtage input til observationer og anbefalinger, jf. rapporteringsformat. Revisionsrapporten skrives eller færdiggøres af Intern revision og koncernrevisionschefen er underskriver på revisionsrapporten.

Intern Revision skal modtage dækkende dokumentation for det udførte arbejde, som bliver en del af Intern revisions dokumentation for opgaveløsningen.

Observationer og anbefalinger registreres i Intern revisions bemærkningsdatabase, og der kører kvartalsvis opfølgning og rapportering til direktioner, koncernledelse og revisions- og risikoudvalg.

For ledelsen og revisions- og risikoudvalg er der således ingen forskel på om opgaven løses med bidrag fra konsulenter eller alene af medarbejdere i Intern revision.

Valg af samarbejdspartner

Processen for udbud, udvælgelse og kontraktindgåelse blev foretaget med assistance fra Indkøb og jf. koncernens indkøbsproces i øvrigt.

Vi valgte at gå med EY, og aftalen indbefattede en tidsramme på 650 timer til konkret opgaveløsning.

Som udgangspunkt ønskede vi assistance til følgende opgaver:

- Selvbetjeningsløsninger for indtegning og produktændringer
- Digitalisering af skadesbehandling
- Mikrotarifering og prisændringer
- Agil udviklingsmodel
- Robotter
- Overvågning af investeringsrammer og beregning af rammeudnyttelse
- Intern kontrol og datakvalitet i Aktuariatet
- Funktionsundersøgelse af Compliance (udført af Deloitte opfølgning fra 2019)

I 2020 endte vi med at udnytte 580 timer i rammen og løse 5 opgaver i samarbejde med konsulenter. Arbejdet medførte, at vi udgav 7 revisionsrapporter og vi oplyste heri at " Revisionen er udført med assistance fra E&Y, Financial Services" eller " Deloitte, Audit & Assurance, Compliance Team", ellers lignede alt sig selv.

I 2021 valgte vi at gå med Deloitte, da EY blev vores valgte revisor. Vi så det som et problem, at EY skulle udtale sig om intern revision jf. revisions-bekendtgørelsen § 8 og med den anden hånd være bidragsyder til opgaveløsningen i intern revision.

Grundet frasalg af Alm Brand Bank blev tidsrammen reduceret til 440 timer.

Deloitte skal yde assistance til følgende opgaver:

- Agil udviklingsmodel (over flow fra 2020)
- Cloud
- Cyber
- Chatbots (robotter)
- PEP og sanktionslister (ibrugtagning af nyt system)

I 2021 har vi valgt at have fokus på teknologisiden i og med det er der Alm. Brand har en række strategiske fokusområder fx ønsker virksomheder at opgive sin egen infrastruktur (datacentre m.v.) og flytte i "skyen", men også at områderne indeholder nye risikobilleder, som forretningen skal tage højde for og være opmærksomme på.

Revisions- og risikoudvalg samt bestyrelser udviser ligeledes stor interesse for fx Cyber og Cloud og har en forventning om, at vi har emnerne som fokusområder og en del af vores revisionsaktiviterne.

Arbejdsdelingen på en konkret opgave kan se således ud:

Alm Brand

- Sikring af overblikket over processen
- Faciliterer møder omkring processen
- Input til afslutningsmøde plancher og revisionsrapport
- Sparring omkring opgaven
- Færdiggørelse af afslutningsplancher og revisionsrapport

Deloitte.

- Planlægning samt sikring af overblikket over processen
- Risikovurdering
- Kontroloverblik
- Test af kontroller
- Gennemgang af dokumenter, såsom forretningsgange
- Stikprøvetest af dokumentation
- Best practice
- Udarbejdelse af udkast til afslutningsmødeplancher
- Udarbejdelse af udkast til revisionsrapport

I år er det vores forventning at alle opgaver løses.

Erfaringer m.v.

Første og meget vigtige punkt er, at vi er lykkedes med at integrere konsulenterne fuldt ud i Intern revision både internet i vores metodik og rapportering og udadtil i forhold til forretningen. Det er helt afgørende, at konsulenterne ikke står ved siden af Intern revision og kører deres eget løb, men er en ligeværdig bidragsyder til den interne revisionsydelse ligesom øvrige medarbejdere i Intern revision.

Samarbejdet med konsulenter har dernæst givet os adgang til kompetencer, som vi som mindre revisionsafdelingen ikke kan "drifte" selv, og vores produkt palette af revisionsydelser er i princippet nu ubegrænset.

Samarbejdet har ligeledes givet os en sparringspartner på øvrige opgaver, som kan agere som supplement til vores i øvrigt gode samarbejde med vores valgte revisor (EY).

Der, hvor vi fremadrettet skal have øget fokus, er "bidraget til læring i Intern Revision" bredt set. Vi skal sikre at alle i Intern revision føler sig trygge ved at bevæge sig ind på nye områder sammen med konsulenterne. Det vil kræve en tidsmæssig investering.

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

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

50+ Sessions

16 Language Translations

100+ Speakers From Around the Globe

17-20 July 2022

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

Why should I attend?

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

Internal Audit Assessment Tool for Audit Committees

Miguel Zorita Gil, MBA, Internal Audit Manager, Nordea

Introduction

The Institute of Internal Auditors (IIA) has in January this year published a paper[1], which describes how the audit committee (AC) can assess the internal audit function (IA). The objective of this article is to provide a summary of the content of the referenced publication, as a way of introduction to the topic.

In line with the three lines model, IA is responsible for providing independent and objective assurance on the adequacy and effectiveness of internal processes. To that end, the company board of directors and their audit committees (AC) rely on IA to provide them with good quality input across all the areas subject to review from an IA perspective (such as governance and risk management).

Figure 1: The Three Lines Model

As a result, IA needs to be subjected to regular scrutiny and review to ensure that the work undertaken by auditors is of the expected quality, to enable the AC to fully rely on their work, and also for the AC to better understand the overall quality of the services provided by IA, as well as its level of independence, objectivity and skepticism.

What are the main benefits of monitoring the performance of IA?

Some of the benefits of a robust monitoring of the IA function include:

- Improving the understanding of IA effectiveness and efficiency of its work.
- Ensuring that the efforts of IA support the strategic objectives of the company, board and AC.
- Providing the AC with valuable input on key topics such as the effectiveness of controls and risk management.
- Identifying opportunities to improve the efficiency and/or effectiveness of the IA activity.
- Finding ways to improve the relationship with external auditors or other third parties.
- Allowing basis for an honest dialogue between IA, the AC and the board.

Besides these questions, members of the board and the AC should also consider including questions related to their own oversight of the IA activity to the assessment tool, to make the assessment more tailored to the organisation's needs and/or characteristics (for example, is the assessment effective in helping leadership and IA activity leaders understand the role of IA in the organisation and the need or opportunities for changes in its role?)

The IA assessment tool also prevents that the AC or the board assume that all is well under control, as this could result in the failure to identify potential weaknesses or further opportunities for improvement within the IA function, and subsequently, within the organisation.

What are the main targets to be achieved with the Audit Assessment Tool?

The key objective of the assessment tool is to provide the AC and the board with a clear evaluation of:

- The quality of the services and sufficiency of resources provided by IA.
- The robust and constructive dialogue between IA and the AC.
- The balance between IA's independence and its role as a key resource for the organisation.

The IIA assessment questionnaire is organised into 3 sections to cover the above areas.

Quality of the services and sufficiency of resources provided by IA

Overall, the aim of the different questions in this section is to ensure that there is a robust process in place to guarantee a good quality of the IA services, by considering the AC's ability to evaluate the IA function, its adherence to internal and/or external standards, the quality of its reports, its general impact towards the organisation or its use of the available resources. amongst others.

In order to have a detailed evaluation of the quality of the services provided, the audit assessment tool includes a sample of questions across different areas, such as "Performance and Expectations", "Adding Value" or "Team qualifications and makeup", amongst others. These are intended to cover the key areas on which the

AC should have a clear view, in order to have a good quality oversight of the IA function.

The questions below are examples of questions that can be used as part of the audit assessment tool, across the above-referenced areas, respectively:

- Were matters IA brought to the ACs attention relevant?
- Is the audit plan organised so that issues can be detected in a timely fashion and audits can be completed as expected?
- Does the IA activity lend its expertise to key implementation initiatives, such as compliance with new laws and regulations, an unexpected event like the COVID-19 pandemic, or the organisation's implementation of enabling technology?
- Is the AC aware of whether IA has the right resources and competency to do its work competently and deliver on the AC's goals?

Communication and interaction with the IA team

Having a robust and constructive dialogue between IA and the AC is fundamental to ensure a good oversight of the IA function by the board and AC. There are two main areas in which the assessment should focus, "The Working Relationship" and "Quality of Communications".

The questions below are examples of questions that can be used as part of the audit assessment tool across the areas referred to above, respectively:

- Does IA feel comfortable bringing up important and sometimes difficult issues? Does the AC have executive sessions with the CAE without management?
- Are IA communications well-organized and clear? Does the AC consider these to be high-impact reporting with high-quality visuals?

Auditor independence, objectivity and professional skepticism

IA independence is normally achieved through a dual reporting relationship, to management from an administrative perspective, and to the AC for strategic direction and accountability. Ensuring the balance between being independent whilst still playing an important role in the organisation can be achieved by asking the right questions across areas such as "Best Practices", "Independence", "Objectivity" and "Skepticism".

The questions below are examples of questions that can be used as part of the audit assessment tool across these areas, respectively:

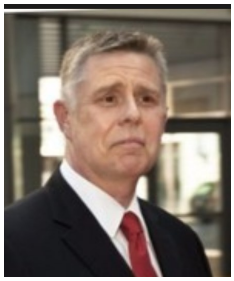
- What is the rationale for the team's organisational structure and is there a need to consider realigning the structure within the CAE's strategic vision of the department?
- Are there continuous development plans for staff members?
- Is the independence of the IA activity accepted and respected? Is the IA activity considered trustworthy and confidential? Is the IA activity able to resist pressure to minimise or limit audits or to succumb to other favors asked by management?
- Have IA team members been able to maintain an unbiased and impartial mindset in all engagements?

To sum up, the assessment tool should be utilised by ACs to better understand if IA is playing a valuable role for the company and whether room for improvement might still exist. The questionnaire in the IIA paper provides ample inspiration for the ACs in designing their own assessment tool.

Notes

[1] "Internal Audit Assessment Tool" for Audit Committees; IIA, January 2021. Link to the article: https://na.theiia.org/about-ia/PublicDocuments/Internal-Audit-Assessment-Tool.pdf

Bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. – Fokus på it-strategi, it-risikostyringspolitik og it-sikkerhedspolitik



Kim Stormly Hansen, Special Advisor, Nykredit

Indledning

Den 26. juni 2021 trådte den nye bekendtgørelse om ledelse og styring af pengeinstitutter m.fl. i kraft. Specielt bilag 5 vedrørende it-strategi, it-risikostyringspolitik og it-sikkerhedspolitik er blevet væsentligt opdateret, primært som følge af indarbejdelse af kravene i EBAs retningslinjer om Information Communication Technology (ICT) and Security Risk Management.

Det er Finanstilsynets holdning, at der herved ikke er sket en skærpelse af kravene, idet disse krav allerede indgik som fortolkningsgrundlag under de eksisterende regler. Finanstilsynet har oplyst, at kravene er blevet konkretiseret, så de bliver mere eksplicitte og dermed nemmere at gå til for de omfattende virksomheder.

Ser man imidlertid på de svar der er afgivet i forbindelse med bekendtgørelsens høring, betragter stort set alle høringsparter kravene som væsentligt skærpede. Om der er tale om skærpede krav, skal jeg ikke vurdere, men hvis virksomheden anvender ISO2700x som referenceramme til strukturering og styring af it-anvendelsen og eksempelvis it-sikkerhedshåndbogen er struktureret herefter og revisor derfor tidligere har anvendt ISO 2700x som referenceramme i relation til revisionen, er der en række områder, man ikke i samme omfang vil dække i relation til kravene i bilag 5. Det er min identifikation og vurdering af de væsentligste af disse punkter, jeg vil gennemgå i det følgende.

Indledningsvis vil jeg dog lige berøre proportionalitetsbestemmelserne i relation til bilag 5. Tilsynet skriver, at *"proportionalitet indebærer, at den enkelte skal overholde bestemmelserne på en måde, der står i et rimeligt forhold til og tager hensyn til virksomhedens størrelse, dens interne organisation og anvendelse af en fælles datacentral. Desuden skal det stå i et rimeligt forhold til omfanget, kompleksiteten og risikoen ved de tjenesteydelser og produkter, som virksomheden leverer eller har til hensigt at levere."*

Ved anvendelse af en fælles datacentral lægges der vægt på, i hvilket omfang virksomheden får leveret sin forretningskritiske IT fra en fælles datacentral. Det skal i den forbindelse sikres, at der er klare aftaler og grænseflader mellem datacentralens opgavevaretagelse for virksomheden og de kontrol- og sikringsforanstaltninger, som virksomheden selv varetager for at kunne opfylde bestemmelserne.

Erfaringsmæssigt er det dog ikke altid sikkert, at virksomheden og tilsynet fortolker proportionalitet ens. Mere om proportionalitet kan ses i "Høring over udkast til bekendtgørelse om ledelse og styring af pengeinstitutter m.fl af 10. februar 2021"

Det er vigtigt, at man forstår Finanstilsynets definition af 2 centrale begreber i bilaget:

IT-risikostyring: er bl.a. at identificere og synliggøre de aktuelle risici, og imødegående kontrol- og sikringsforanstaltninger, over for ledelsen og sikre, at virksomheden ikke påtager sig større risici, end hvad der er acceptabelt. At medvirke til at ressourcer kan prioriteres mest effektivt mv.

Trusler, sårbarheder og risici ændres løbende, hvorfor vurderingen af risici også er en løbende proces, der skal forankres i og på tværs af organisationen.

Finanstilsynet lægger i sin vurdering af virksomhedens IT -risikostyring bl.a. vægt på, at:

- metoden for udarbejdelsen af IT-risikoanalyser og vurderinger er dokumenteret, sådan at de endelige vurderinger kan kvalitetssikres
- eksterne og interne interessenter bliver inddraget (f.eks. sparring med IT-sikkerhedseksperter, forretningens funktioner mv.)
- relevante trusler er synliggjort og IT-risici identificeret, bl.a. med udgangspunkt i tilgængelighed, fortrolighed og integritet. Finanstilsynet tager her hensyn til væsentlighed i forhold til virksomhedens systemiske vigtighed og kompleksiteten i virksomhedens IT-anvendelse
- sammenhæng mellem risici og de etablerede imødegående tiltag er tydeligt dokumenteret
- identificerede sårbarheder er synliggjort og vurderet i IT-risikoarbejdet på en måde, så konsekvensen og vurderingen af dem tydeligt fremgår af den samlede vurdering
- virksomheden har vurderet, om dens politikker, forretningsgange samt kontrol- og sikringsforanstaltninger er tilstrækkelige og imødegår IT-risici. Den tilbageværende restrisiko skal være tilstrækkelig synliggjort.

IT-sikkerhedsstyring: er bl.a. at sikre, at der med afsæt i organisationens IT-risikobillede er etableret tilstrækkelig og effektive tiltag, forankret hos topledelsen.

Udvalgte emner

It-strategi

It-strategi var en naturlig del af de områder, der skulle revideres jf. den "gamle" revisionsvejledning 14, men er

ikke et fokus i ISO 2700x. It-strategien er eksplicit nævnt i det nye bilag 5. Dette vil sandsynligvis betyde, at revisionen vil have mere fokus herpå i den fremtidige revision.

It-risikostyring og it-risikostyringspolitik
Begrebet it-risikostyring blev også brugt i det det tidligere bilag 5, men af det nye bilag 5 fremgår det eksplicit, at virksomheden skal have en politik for it-risikostyring. Begrebet er defineret af tilsynet ovenfor.

De sidste års tilsynsbesøg har resulteret i en række påbud på området, hvilket betyder, at virksomheden og dermed revisor bør have øget fokus på dette område.

Test af it-sikkerhed
I pkt. 50 i det nye bilag 5 fremgår det, at "direktionen skal sikre, at der gennemføres løbende og gentagne test af sikkerhedsforanstaltningerne. Kritiske it-systemer skal testes mindst én gang om året. Ikke-kritiske systemer skal testes regelmæssigt og inden for en periode på minimum tre år". Begrebet test og kritiske it-systemer er ikke defineret, men det er mit gæt, at dette vil betyde, at virksomheden skal udvide testomfanget- /frekvensen.

It-projektstyring
Det nye bilag 5 har et afsnit om it-projektstyring. Projektstyring skal også behandles i it-sikkerhedspolitikken. Det er igen mit gæt, at ikke alle revisioner har omfattet dette forhold.

Identificering af funktioner, processer og aktiver
Det nye bilag 5 indeholder krav om, at direktionen skal sikre identificering af forretningsfunktioner, roller og understøttende processer for at kunne vurdere betydningen af de enkelte elementer og deres indbyrdes afhængighed i forhold til it-risici og sikre, at kortlægningen heraf holdes opdateret.

Virksomheden og hermed revisor skal nok have en øget fokus på forretningsdelen og applikationer.

Kryptering af data i hvile
Dette er ikke et nyt krav, men det har vist sig i praksis, at kravet giver visse udfordringer – ikke mindst i relation til performance. I tilfælde hvor kryptering af data i hvile ikke er etableret, bør revisor som minimum have fokus på eventuelle kompenserende risikomitigerende tiltag. (Dette er dog min personlige holdning og ikke nødvendigvis Tilsynets)

Beredskab
Dette afsnit er væsentligt udvidet og specificeret i det nye bilag 5 og et område, der har Finanstilsynets fokus. Der er givet en række påbud på område i de seneste år. Afsnittet er underopdelt i:

- Styring af forretningskontinuitetet (Business Continuity Management, BCM),
- Forretningskonsekvensanalyser (Business Impact Analysis, BIA)
- Forretningskontinuitetsplaner (Business Continuity Plans, BCP), herunder krav til stillingtagen til det maksimale tidsrum, inden for hvilket et system eller en proces skal genoprettes efter en hændelse (Recovery Time Objective, RTO) og det maksimale acceptable datatab, mål i tid (Recovery Point Objective, RPO).

  Disse krav er ikke nye, men det er mit gæt, at denne specifikation giver anledning til (mindst) 2 ting.

  1. at der skal ske en stærkere koordinering mellem det forretningsmæssige beredskab (hvordan udføre forretningsaktiviteter videre uden it) og det tekniske beredskab (hvordan reetableres it).
  2. at der skal ske en styrkelse af specifikke krav i servicemålaftaler (SLA), der indgås med fælles datacentraler eller andre leverandører.

- Genopretningsplaner (Disaster Recovery Plans, DRPs)
- Test af planer (Her er der også krav om, at kritiske funktioner, understøttende processer, it-aktiver og disses indbyrdes afhængighed skal testes mindst én gang om året, herunder, hvis relevant, dem der leveres af tredjeparter.)
- Krisekommunikation

Risikostyringsfunktionens og den risikoansvarliges opgaver på it-risikostyringsområdet
Dette forhold har fået sit eget afsnit i det nye bilag 5. Der har igennem en tid været drøftet organisering af 2nd line i relation til it-risikoen. Er it-sikkerhedsafdelingen en 1st line eller en 2nd line enhed eller måske begge dele, og hvad er den risikoansvarliges ansvar, og hvordan sikres dette?

Finanstilsynet har tilkendegivet, at de betragter it-sikkerhedsafdelingen primært som en 1st line, mens risikostyringsfunktionen er den primære 2nd line enhed. Dette stemmer også godt overens med den skærpede fokus på risikostyringsfunktionen og den risikoansvarlige i bilag 5, men vil nok betyde en del tilpasninger i de enkelte virksomheder.

Afslutning

Ovenstående er på ingen måde udtømmende, og de enkelte områder er ikke dybdegående analyseret, men det er en række emner, som jeg har hæftet mig ved. Det er min opfordring, at man hver især – alt efter behov – foretager en grundig gennemlæsning af bilag 5 med henblik på at identificere områder, hvor der er behov for en styrkelse af revisionsindsatsen. Denne identifikation kan med fordel tage udgangspunkt i en gap-analyse foretaget af virksomheden.

Der er som nævnt ikke klare definitioner på en del begreber eller en entydig beskrivelse, hvordan kravene skal efterleves. Der er imidlertid ved at danne sig en tilsynspraksis på området og en indikation på, hvordan tilsynet fortolker de enkelte krav.

Learning, Growth, and Inclusion

Lauressa Nelson

Photographs by Phelan Ebenhack

Just weeks after accepting his position as IIA president and CEO, Anthony Pugliese's schedule was jam packed with IIA-related activities. He arrived bright-eyed and smiling at IIA Global Headquarters for meetings, interviews, and a photo shoot amid a whirlwind schedule.

That whirlwind will no doubt intensify as Pugliese officially takes the helm, replacing longtime leader Richard Chambers. He says he is enthusiastic about the potential for a more vibrant, innovative, and future-ready internal audit profession — and IIA. His vision prioritizes new approaches to learning and training; technological advancement and acumen; human intelligence skills; and diversity, equity, and inclusion (DE&I) — all vital to internal audit's long-term growth and relevance, he says.

"Internal auditors get to see the whole organization in a way that not many others do," Pugliese says. "That can be challenging, but it's also exciting because it never stops changing and our profession gets to be in the middle of it, advising management and giving assurance to shareholders and audit committees."

Pugliese's broad experience includes seven years at Deloitte, 21 years at the Association of International Certified Professional Accountants (AICPA), and more than two years in his most recent position, president and CEO of the California Society of CPAs (CalCPA), the largest state CPA organization in the U.S. The IIA's Global Executive Search Committee selected him after a meticulous, stakeholder-informed global search. "Anthony has the breadth, depth, and scale of experience, business acumen, and strategic thinking that will facilitate the growth of The IIA and ready it for the future of the internal audit profession — from membership and global advocacy to digital transformation and technological innovation," says Mike Joyce, Blue Cross Blue Shield Associa-

New IIA President and CEO Anthony Pugliese sees many opportunities for moving the profession forward and positioning The Institute for long-term success.


"The primary role of any professional association is to make sure that its members stay relevant."

LEARNING, GROWTH, AND INCLUSION

tion vice president, chief auditor and compliance officer, who chaired the committee.

Turning Vision Into Action

When digging into his new role at The IIA, Pugliese asked individual stakeholders open-ended questions, allowing themes to emerge organically. He takes in data "constantly and quickly," he says, combining intuition and judgment, grounded in the facts he has available. "I don't like to get bogged down, and I try to find the common themes," he notes. "Complex problems can often be simplified with questions like, 'Why do we do that?' or 'What are we trying to fix?'"

vision and being able to drive it through is a critical leadership skill," says Charlie Wright, Jack Henry & Associates chief risk officer, who served on the committee. "Anthony is a seasoned association leader who has a strategic focus on running a business, which will be critical to taking The IIA from where it is today and bringing us into tomorrow. He has very creative ideas about partnerships, our approach to training, how to respond to disruptive technology, and how to advance our digital transformation process."

Responding to Change and Disruption

A key priority for Pugliese is ensuring the internal audit profession remains relevant in today's highly disruptive

Pugliese's ability to consume information quickly and distill it into a clear strategy has been noted throughout his career. "Anthony has a superhuman ability to synthesize information from across the organization, connect ideas and people, and drive collaboration and results — all with a sense of humor and wit that makes working with him feel like fun," says Heather Pownall, a management consultant for (ISC)2, who worked in business development under Pugliese's leadership at the AICPA. "He was the connective tissue, understanding everything that was going on across the organization and unifying the executive team."

The IIA's Executive Search Committee noted that Pugliese exuberantly takes on challenges and develops vision, strategy, and actionable plans. "Establishing a

business environment. Internal auditors must keep moving beyond their comfort zones, he says. They must consistently seek to expand their awareness and update their competencies through continuing education and training, especially in the areas of technology; human intelligence; and environmental, social, and governance (ESG). "The primary role of any professional association is to make sure that its members stay relevant," he explains. "The world is at a point where change is so fast that the people coming out of colleges and universities have more knowledge than the people mentoring and supervising them, so it's really incumbent upon our members to keep up. That is why I think education is so important."

While internal auditors hold the responsibility for

seeking opportunities to learn, Pugliese also recognizes that The IIA must continually produce training on timely, relevant topics and design training platforms that attract members and give them something valuable. "We have to figure out a way to make learning fun so that people want to do it and that it's relevant to the issues we want to solve," he says. "Successful training means members walk out knowing how to do something versus just being able to remember what they heard."

Pugliese also says internal auditors need to be on the leading edge of awareness about technological developments and trends. "Technology has gone from being a way of increasing efficiency to something that is far more transformative across business and surely across every profession," Pugliese told Richard Chambers in a February edition of Chambers' IA Insights and Advice video series. "Embracing some of the disruptive aspects of business today and being able to guide management and boards and audit committees through things like technological disruption is going to be huge in positioning us for ongoing relevancy."

Going Beyond Technology

But internal auditors should not limit their continuing education to technology, Pugliese says. ESG is a burgeoning area that internal auditors are well-positioned to address. "Measuring and assessing nonfinancial indicators of success is really exciting, and internal auditors are very well-situated to do that kind of work, in fact better than almost any other profession," he says. "It's one of the biggest opportunities I've seen for internal audit to add value in a tangible way, not just to management and the board, but to everybody."

Human intelligence competency is also important for internal auditors. "Those skills you don't necessarily consider critical to a job — perception, intuition, and teamwork — actually are becoming more important," Pugliese says. "Internal auditors have to rely on many different people in the conduct of their work; they can't possibly know it all. So being able to assemble and lead a team is vital. Sometimes those skills are natural or innate, but often you can acquire them."

A self-described extrovert, Pugliese counts humor among his human intelligence skills. "Sometimes people can be overly serious when the situation doesn't warrant it," he says. "I found out early on that if you've got a good knack for using the right kind of humor and the right timing, it can defuse a lot of tension and anxiety."

While a love of people and a quick wit seem to come naturally to Pugliese, self-awareness, which he defines as understanding the way one is perceived by others, is more hard-won. "That's actually very important for any job, but particularly in the CEO role, much of what you do is to motivate people," he says.

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

Cultivating An Inclusive Culture

Pugliese is known for his ability to engage and empower people — key ingredients for building an inclusive culture. Terry Grafenstine, global chief auditor for technology at Citi, is a longtime IIA volunteer and member who met Pugliese while serving on the AICPA's board. As a public sector internal auditor, she was worried about fitting into a group dominated by private industry CPAs. "Anthony made me feel so welcome, like the things that I contributed were different and meaningful," Grafenstine recounts. She says Pugliese was instrumental in the AICPA's merger with the U.K.-based Chartered Institute of Management Accountants (CIMA) and that he brought together individuals from different cultures, backgrounds, and industries, and motivated them around a common vision. "He made us feel like what we each had to say was important, and as a result, he got more out of the sum than the parts," Grafenstine explains.

Demonstrated effectiveness as a driver of inclusive culture was important to the executive search committee and the stakeholders surveyed by the committee at the onset of the process. The business benefits include increasing collaboration between IIA Headquarters and global affiliates and members, which ensures global voices feel equally heard and valued and maximizes the sharing of intellectual capital, according to Joyce. "We want to support diversity and inclusion throughout The IIA, both in the workplace and among our membership globally, so we probed all the candidates about their experience and engagement around that," Joyce explains.

Taking Action on Diversity

Pugliese says people often avoid the topic of diversity because they don't understand what to do with it. "It can be uncomfortable for some people," he says. "Yet when you talk to someone in an underrepresented population, it's really not that uncomfortable, because people want to talk and to give their point of view. And you just have to be respectful."

Pugliese has proven his willingness to tackle such issues directly, with measured thought and action. Following the death of George Floyd, a Black man who died while being restrained by Minneapolis police last year, Pugliese issued a DE&I statement to the membership of CalCPA, committing to form a member-led DE&I committee responsible for establishing goals and practices to identify and address racial inequities. Additionally, CalCPA and the Institute of Management Accountants jointly issued a survey-driven report that exposed troubling disparities in the senior ranks of the accounting industry. "We have gotten a little bit better on hiring, in terms of bringing in underrepresented populations, but we haven't done much better in terms of bringing those individuals all the way up into key senior management roles," Pugliese explains. "And I sense the same concerns are here in the internal audit profession, so we're going to continue this work."

In addition to being the right thing to do, the survival of the profession is contingent upon underrepresented groups seeing themselves in business roles like internal auditing, Pugliese adds. "Diversity, equity, and inclusion are business decisions as much as they are ethical decisions," he says, noting that changing demographics alone make diversity "intrinsically important" to the pipeline of future auditors.

Pugliese says having a global board of directors with members from underrepresented groups will lead this progress. "They get it, including me; for the LGBTQIA population, I get it," he says. Leveraging personal experiences will foster multiple approaches to success, he notes, but the process of trying various plans of attack prompts an urgency in getting started. "There's not one magic program."

Embracing Change

As organizations face a whirlwind of change, technologically and socially, internal auditors must be ready to go all in on the unique opportunities at their fingertips. Pugliese is palpably enthusiastic about ensuring The IIA is the dynamic and inclusive authority, educator, and advocate to help the profession seize those opportunities globally. "His energy is clearly contagious," says Jenitha John, CEO of the Independent Regulatory Board for Auditors and IIA Global Board chair, who served on the search committee. She and others laud Pugliese's insight, foresight, and fresh perspectives as well as his ability to parlay them into a vision for The IIA. "Anthony demonstrates the caliber and attributes we require in the next CEO," she says. "We look forward to his expertise and wisdom."

Lauressa Nelson *is a content writer and technical editor, Standards and Professional Knowledge, at The IIA.*

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

Nye medlemmer

Nye medlemmer i IIA fra 7.9.2021 - 7.12.2021

ATP
Johan Schleimann
Ali Radi Zarif

Bankdata
Linkajan Nadarajah James

Danske Bank
Line Skaarup Schøndorff
Pia Stonor Dyrholm Groot
Majken Jørgensen Bonde
Rodolfo Gonzalez Alves

Deloitte
Maria Foged
Maja Marie Nyvang Hansen
Jacques Peronard

Energistyrelsen
Poul-Erik Kristensen
Mads Mølgaard Nielsen
Katrine Strøm
Ásbjørg Abrahamsen
Sanne Hansen

GF Forsikring
Jeanette Lindevang

Hempel
Philip Hertz

Landbrugsstyrelsen
Niels Hegelund
Erik Schultz Bonde

NKT Cables Group A/S
Cæcilie Risholt

Novo Nordisk
Anastasia Sheriff
Aitzol Nubla Arto

Nykredit
Falentin Eliaz Valentino

PWC
Michael Kayser Vestergaard

Saxo Bank
Sinan Dasdemir
Niels Christian Østergaard Mouritsen

Sydbank
Adelina Istrate Hansen
Christoffer Øvrebø McIntosh

Udenrigsministeriet
Dan Winther Rasmussen

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.

Kommende kurser og gå-hjem møder

04.05.2022 Kursus for forsikringsrevisorer
10.05.2022 IIA Årsmøde 2022

"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