INFO

Foreningen af Interne Revisorer
Nummer 65 | April 2017 | 22. årgang

Minitema:

- ***COSO og interne kontroller***

Think Outside the Box - Part III • **CIA forberedelseskurser**

INFOs redaktion

Ansvarshavende redaktør
Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
Europæiske Rejseforsikring
☎ 33 27 84 82 ✉ brs@europaeiske.dk

Øvrig redaktion
Seniorspecialist
Lea Kehlet Halsø
Nykredit
☎ 44 55 93 01 ✉ lea@nykredit.dk

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

Intern revisor
Maria Lyngbek
PFA Pension
☎ ✉ mly@pfa.dk

Revisionschef
Louise Claudi Nørregaard
PensionDanmark
☎ 33 74 80 13 ✉ lcn@pension.dk

Manager
Monica Vestergaard Rasmussen
Skatteministeriet
☎ 72 37 99 67 ✉ mvr@skm.dk

Senior Audit Manager, CIA
Tobias Zorde
Nordea
☎ 21 18 54 97 ✉ tobias.zorde@nordea.com

Næste nummer
INFO 66 udkommer i september 2017.
ISSN: 1903-7341 (Elektronisk version).

Indlæg til INFO
Artikler i INFO påskønnes med en vingave.

Forsidefoto
UnknownNet

Redaktionens adresse

Foreningen af Interne Revisorer (IIA)
Att.: Seniorspecialist Glenn Thunø
Intern revision
Nykredit
Anker Heegaards Gade 4-6
1780 København V

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

Indhold

Nyt fra bestyrelsen

Referater fra bestyrelsesmøder lægges på foreningens hjemmeside umiddelbart efter mødernes afholdelse.

Du kan her løbende holde dig opdateret på bestyrelsens arbejde på hjemmesiden under "Nyheder".

www.iia.dk

Leder

Neil Jensen, Regional Chief Auditor, CIA, CISA, RSA Scandinavia

COSO – ikke blot en døgnflue

Det er i år 25 år siden at COSO rammeværket for intern kontrol, Internal Control – Integrated Framework, blev publiceret. Rigtig mange virksomheder anvender også i dag dele af eller hele det ajourførte (2013) rammeværk i måden, hvorpå virksomhedernes interne kontrolsystem organiseres. Og med god grund. COSO organisationen har gennem årene været i stand til at opdatere og udgive nye, relevante publikationer med retningslinjer og begrebsrammer, som spejler ændringerne i det omgivende samfund og de risici, som virksomhederne agerer i.

I 2004 udkom Enterprise Risk Management – Integrated Framework, som konceptualiserer, hvad vi i dag anser for værende god Risk Management, og så sent som i 2015 udkom publikationen "COSO in the Cyber Age", som beskriver hvorledes, det oprindelige kontrolrammeværk kan anvendes som rammeværk for håndteringen af cyber ricisi. COSO er altså ikke blot en døgnflue, og derfor er det relevant med et minitema om COSO rammeværket og interne kontroller i denne udgave af INFO.

COSO rammeværkerne har været genstand for flere artikler i vores eget medlemsblad, hvilket på fornem vis illustrerer COSO's relevans for blandt andet, hvorledes et relevant internt kontrolmiljø etableres gennem virksomheders organisering i forhold til roller, ansvar og processer. I dette nummer af INFO er der mulighed for at genopfriske COSO kuben, de 5 kontrolelementer og de 17 principper for god intern kontrol i perspektiv af risikostyringskonceptet "de tre forsvarslinjer".

Jesper Granstrøm (EY) og Heino Hansen (Nordea) har skrevet en inspirerende artikel, som på glimrende vis forklarer, hvordan vi som interne revisorer kan anvende COSO rammeværket som grundlag for vurderingen af roller og ansvar i forhold til kontrolmiljøet, ved design af revisionshandlinger, samt ved vurderingen af kvaliteten af virksomhedens kontrolmiljø.

Det kan således anbefales, at betragte revisionsopgaven i perspektiv af de 5 kontrolelementer, og opbygge sine revisionshandlinger med udgangspunkt i de underliggende principper for kontrolelementerne.

INFO 65 indeholder også en interessant artikel baseret på et case study om sammenhængen mellem implementeringen af nye kontroller og de svagheder, som intern eller ekstern revision identificerer. Ikke uventet eksisterer der en sådan sammenhæng, men undersøgelsen viser samtidig, at virksomheden/klienten anerkender behovet for nye kontroller, og at kontroller blandt andet opfattes som et forebyggende værn i forhold til eventuelle påtaler fra Finanstilsynets undersøgelser af efterlevelsen af gældende regulering i finansielle virksomheder. Derfor bliver processen med management letter og revisionsprotokol en fælles proces mellem ledelse og revision, og forfatteren af artiklen, Leif Christensen (CBS), rejser spørgsmålet om, hvorvidt de regulatoriske myndigheder bør overveje en mere principbaseret regulering, frem for den nuværende regelbaserede tilgang til compliance.

Ask Ransdal Hansen (PwC) har i sin kandidatafhandling taget temperaturen på Intern Revision i Danmark med henblik på at finde ud af, hvilke professionelle standarder (ISA, IPPF eller INTOSAI), der anvendes som referenceramme for revisionsfunktionernes arbejde, og hvilke risikostyringsmodeller virksomhederne anvender.

Det viser sig, at en langt overvejende del af revisionsfunktionerne anvender IPPF, hvilket illustrerer et ændret fokus for Intern revisions arbejde, idet en undersøgelse fra 2006 viste, at den primære referenceramme var ISA standarderne. Det ses samtidig, at virksomhederne overvejende anvender COSO eller COSO-lignende modeller for risikostyring.

INFO 65 indledes med afslutningen på artikelserien fra Yves Froude (The World Bank) om kreativ og nytænkende dataanalyse som redskab til at bringe revisionsarbejdet til "næste niveau". Genbrug er godt, og artiklen handler om, hvordan man med fordel kan anvende data og resultater fra tidligere dataanalyser i andre revisionsopgaver, samt værdien af god dokumentation af dataanalyser. Den handler også om at tænke "ud af boksen" ved anvendelsen af dataanalyse i revisionsarbejdet, og giver eksempler på nye datatyper og analyseværktøjer som kan indgå i overvejelserne ved planlægningen af nye revisionsopgaver.

Rigtig god læselyst!

Nyt fra redaktionen

Birgitte Rousing Svenningsen, Revisionschef, CIA, CISA, Europæiske Rejseforsikring

Som haveelsker glæder jeg mig hvert år til det tidspunkt, hvor løgplanterne begynder at titte frem. De bringer de første forårstegn og skaber optimisme. Jeg kigger hvert år efter, om der er kommet nogle nye planter, enten fordi de har formeret sig, eller fordi jeg sidste år lagde nogle nye løg i jorden. De nye løgplanter giver nye farver og ny inspiration. En vis rotation er heller ikke af vejen. Disse ord er skrevet om min have, men de kunne også have været skrevet om en revisionsafdeling eller om INFOs redaktion.

Nye personer i en revisionsafdeling giver typisk ny energi og inspiration. Sådan har vi det også i INFOs redaktion. Vi håber på en løbende udskiftning af medlemmerne, således at vi bevarer engagementet og gejsten hos de enkelte medlemmer, men vi lægger også vægt på, at der er nogle gamle rotter til at holde bladet på rette kurs. Jeg mener, at vi har en god balance mellem gamle rotter og nye inspirationsskabende medlemmer.

Arbejdet i redaktionen er til tider tidskrævende, og det er derfor både med sorg og glæde, at jeg kan meddele, at Morten Bendtsen har valgt at træde ud af redaktionen. Det er for mig med glæde, idet det betyder, at han kan lægge flere kræfter i arbejdet som foreningens kasserer. Det, synes jeg, er fantastisk. Morten har i sine år i redaktionen arbejdet hårdt på fremskaffelse af gode og interessante artikler, og han har på redaktionsmøderne bidraget med kontante holdninger til bladet indhold. Jeg har værdsat Mortens indsats meget højt. Jeg ser meget frem til også i fremtiden at kunne arbejde sammen med Morten i foreningens bestyrelse.

Et farvel til et redaktionsmedlem er et goddag til et andet redaktionsmedlem. Et goddag til et nyt og inspirerende medlem. Således har Maria Lyngbek fra PFAs interne revision taget i mod tilbuddet om at blive nyt redaktionsmedlem. Maria har flere års erfaring fra intern revision i Finansielt Stabilitet og Politiet og har også nogle års erfaring fra ekstern revision. Det er min forventning, at Maria med sin baggrund vil kunne bidrage med inspiration til interessante og aktuelle artikler inden for et bredt felt. Jeg er sikker på, at vi kommer til at se Marias bidrag til bladet, som erantis der bliver større og større og breder sig mere og mere for hvert år, der går. Jeg ser meget frem til et godt samarbejde med Maria.

Fra mig og resten af redaktionen skal der med erantis på forsiden lyde de bedste forårsønsker til alle vores læsere.

Generalforsamling

Foreningens generalforsamling afholdes den 1. juni i forbindelse med årsmødet i Aarhus. På generalforsamlingen er halvdelen af bestyrelsesmedlemmerne på valg. Det er Morten Bendtsen, Jesper Jæger Granstrøm, Neil Jensen, Pia Sønderlund Nielsen og Jesper Siddique Olsen. Alle fem medlemmer er villige til genvalg. Har du lyst til at blive medlem af bestyrelsen og yde en indsats for foreningen, er du velkommen til at kontakte foreningens formand Kim Stormly Hansen på ksh@nykredit.dk senest den 1. maj. Du bedes sende os et kort CV og en beskrivelse af, hvad du brænder for i bestyrelsen, således at vi har mulighed for at udsende denne information til alle foreningens medlemmer sammen med indkaldelsen til generalforsamlingen.

Nye certificeringer

CIA (Certified Internal Auditor)
Jesper Hagild, Nordea
Sarah Nørholm Straarup, Nordea
Elsebeth Ankjær, DSB
Anna Carolina Zourdis Cederblad

CFSA (Certified Financial Services Auditor)
Thomas Bang van Dijk, Saxo Bank

Et stort tillykke med certificeringen !!!!

Nyt fra uddannelsesudvalget

Heino Hansen, Internal Audit Manager, CIA, Nordea

Peer Højlund, Chefspecialist, Nykredit

BLIV CERTIFICERET INTERN REVISOR (CIA) OG BLIV BEDRE RUSTET TIL DE STIGENDE KRAV!

Bestyrelsen har i sin strategi for IIA fastlagt en målsætning om, at foreningen skal medvirke til en høj faglig standard blandt interne revisionsafdelinger ved at gennemføre relevant, udviklingsorienteret og målrettet uddannelse. Et af de områder, som har høj prioritet, er ønsket om at øge antallet af certificerede interne revisorer blandt foreningens medlemmer.

Vi er netop nu i tæt dialog med IIA Global om et samarbejde, som betyder, at vi 2017 i Danmark vil tilbyde et forberedelseskursus til del 1 af CIA certificeringen. Kursets varighed vil være 2 dage med en professionel instruktør, som vi på forhånd har sikret os vil tage direkte udgangspunkt i IIAs CIA Learning System.

Du vil, i forbindelse med tilmelding til kurset, få mulighed for at købe CIA Learning System til en forventet reduceret pris på ca. **4.300,-** (normalpris er ca. 6.300,-), således, at du kan forberede dig til eksamen både før og efter kurset. Bemærk at et gyldigt købt CIA Learning System er en forudsætning for at kunne deltage på forberedelseskurset.

Der bliver naturligvis udstedt kursusbevis efter gennemført kursus, som vil give CPE points i henhold til antallet af undervisningstimer (2 dage = 16 point).

Hvis ikke du ønsker at gå op til eksamen, vil der stadig være et stort udbytte af kurset, hvor du får en indføring i de vigtigste områder og begreber indenfor:

- IIAs professionelle standarder
- Intern kontrol og risikostyring
- Intern revision - metode, teknik og værktøj.

Når først du har gennemført det første kursus, og måske også valgt at gå til eksamen på del 1 af CIA certificeringen, har du sikkert fået blod på tanden. Og godt begyndt er som bekendt halvt fuldendt. Så hvorfor stoppe her?

Vi planlægger at tilbyde forberedelseskurser til del 2 og 3 af CIA certificeringen i 2018, henholdsvis forår (2 dage) og efterår (3 dage), hvor timingen ikke er endeligt afklaret, men det ligger fast, at målet er kursus i alle tre dele inden for et år, med forbehold for at opbakningen i form af tilmeldinger er tilstede.

HVAD OMFATTER CIA EKSAMENEN?

Der har indtil nu været tale om eksaminer af 2 - 2½ times varighed, hvor man skal besvare 100 - 125 multiple choice spørgsmål inden for forskellige områder, jf. nedenstående oversigt.

<u>Part 1: Internal Audit Basics</u>

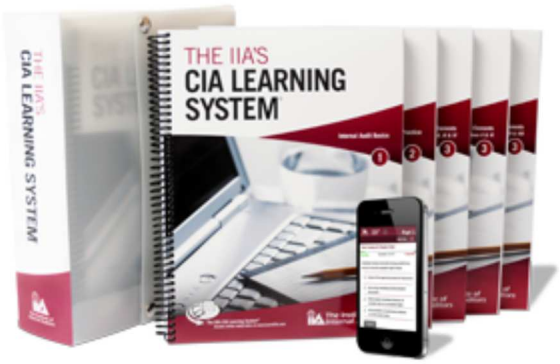
- Mandatory Guidance (35% - 45%)
- Internal Control and Risk (25% - 35%)
- Conducting Internal Audit Engagements—Audit Tools and Techniques (28% - 38%).

<u>Part 2: Internal Audit Practice</u>

- Managing the Internal Audit Function (40% - 50%)
- Managing Individual Engagements (40% - 50%)
- Fraud Risks and Controls (5% -15%).

<u>Part 3: Internal Audit Knowledge Elements</u>

- Governance/Business Ethics (5% - 15%)
- Risk Management (10% - 20%)
- Organizational Structure/Business Process and Risks (15% - 25%)
- Communication (5% to 10%)
- Management/Leadership Principles (10% - 20%)
- IT/Business Continuity (15% to 25%)
- Global Business Environment (0% - 10%).



"The IIA's CIA Learning System teaches the entire global 3-Part CIA Exam syllabus. You can study this content with printed books or e-reader files."

HVORDAN KVALIFICERER OG TILMELDER MAN SIG TIL CIA EKSAMEN?
For at kunne indstille sig til eksamen skal man kunne dokumentere, at man har bestået, hvad der svarer til en bachelorgrad. Herudover kræver certificering, at man har minimum 24 måneders erhvervserfaring som intern eller ekstern revisor.

Man kan godt gå op til CIA eksamen, selvom man endnu ikke har den krævede erhvervserfaring, men man opnår først status som Certified Internal Auditor, når man kan dokumentere de relevante 24 måneders erhvervserfaring.

Tilmeldingen til eksaminerne sker via IIA USAs hjemmeside (https://na.theiia.org/certification), hvor man indskriver sig i CIA-programmet i det såkaldte "Certification Candidate Management System" (CCMS). Her vil du også kunne finde IIA Certification Candidate Handbook, hvor du kan læse mere om CIA-eksamen. Selve eksamen foregår hos Global Knowledge ApS på Stamholmen 110, 2650 Hvidovre. Der er ingen faste eksamensdatoer, så man bestemmer selv, hvornår man vælger at gå til eksamen. Se mere på http://www.iia.dk.

Proceduren vedrørende eksamenstilmelding og hjælp til samme, vil kunne tilbydes i forbindelse med forberedelseskurser, ligesom der vil blive mulighed for at danne læsegrupper, hvis det ønskes.

HVAD KOSTER KURSUS, MATERIALER OG EKSAMEN?
Kursusafgiften vil være 3.500 pr. kursusdag, dvs. for del 1 vil prisen være 7.000,-. Prisen for del 2 (2 dage) vil også være på 7.000,- og prisen for del 3 (3 dage) vil være på 10.500,-. Med forbehold for at opbakningen i form af tilmeldinger er tilstede, vil en samlet pris for kursusforløbet - inkl. et gyldigt CIA Learning System til ca. 4.300,- og eksamensgebyrer - være ca. 30-32.000 kr.

TIDSFORBRUG
Man skal påregne 4-5 ugers (inklusive en on-line pretest) selvstudie inden et forberedelseskursus og 2-3 ugers selvstudie efter et forberedelseskursus, inden man går til eksamen. Der skal også påregnes noget forberedelse mellem de enkelte dage på forberedelseskurserne.

HVORNÅR OG HVOR AFHOLDES FORBEREDELSES KURSERNE?
Forberedelseskurset til CIA del 1 forventes at blive udbudt i slutningen af september 2017 på en central lokation i København. Vi forventer som sagt at kunne udbyde alle 3 forberedelseskurser inden for godt ét år.

HVAD SÅ NU?
Så snart detaljerne om forberedelseskurset til CIA del 1 er fastlagt, vil det blive annonceret via mail og på IIA DK's hjemmeside.

Har du spørgsmål til ovenstående, er du velkommen til at kontakte Heino eller Peer, jf. kontaktoplysningerne herunder:

Heino Hansen, Internal Audit Manager, CIA, Nordea
Tlf. 31183801
Mail: heino.hansen@nordea.com

Peer Højlund, Chefspecialist, Nykredit
Tlf. 44559314
Mail: phc@nykredit.dk

ERFARINGER MED CIA CERTIFICERING I DAGLIGDAGEN

Anita Damgaard Laugesen, relativt "nycertificeret" kollega i Group Internal Audit i Nordea:

"Efter et lærerigt og fagligt krævende CIA certificerings forløb, som jeg afsluttede med eksamen på del 3 i 2014, følte jeg mig i høj grad bedre rustet til opfylde både formelle krav fra min arbejdsgiver samt de stigende faglige krav, som stilles i mit virke som intern revisor i en kompleks finansiel virksomhed. CIA certificeringen er også en god måde at få papir på sine kompetencer som intern revisor og få dette på CV'et. Materialet og eksaminerne er alt sammen på engelsk, og det er min erfaring, at man hurtigt kommer ind i terminologen og emnerne ved grundig brug af det tilhørende CIA Learning Systems mange muligheder. Jeg har siden certificeringen i 2014 valgt at specialiserer mig i intern revision inden for AML området, og i den forbindelse har færdighederne, som jeg har tilegnet mig via CIA, fortsat været relevante og lagt et solidt grundlag for efterfølgende yderligere certificeringer indenfor mit nuværende arbejdsområde."

IIA årsmøde 2017

31. maj – 1. juni 2017

Årsmødet afholdes på Hotel Comwell Aarhus

Der er nu mulighed for at tilmelde sig årsmødet 2017 på www.iia.dk.

Tilmeldingsfristen er: **d. 3. maj 2017**.

Igen er det lykkedes at engagere en række spændende og inspirerende foredragsholdere og programmet er bredt sammensat så alle foreningens medlemmer - uanset arbejdsområde - vil kunne drage nytte af de mange inspirerende og varierede foredrag. Se www.iia.dk for yderligere information om årsmødet og programmet.

Prisen er 4.750 kr. for hele arrangementet, inklusive 1 overnatning fra d. 31. maj - 1. juni 2017, forplejning begge dage, rundvisning og middag d. 31.5 på ARoS Kunstmuseum.

Under middagen vil der være underholdning, og kaffen vil blive serveret i ”Your Rainbow Panorama”. Efter kaffen er det ”Aarhus by Night” på egen hånd og for egen regning.

Think Outside the Box! - How Creative & Unconventional Audit Analytics can help you take your Audits to the "Next Level" (Part III)

Yves S. Froude, CIA, CISA; Data Analytics Officer – The World Bank, Washington DC

Introduction

Greetings, fellow out-of-the-box-thinkers, and welcome to the third and final article of this series.

*As you may recall, in **Part I** we introduced the basic concepts of "Innovative Analytics", demonstrated its value with some basic examples and introduced an applicable framework to be used in challenging situations.*

***Part II** was our most technical part of the series and delved deeper into this approach, by using more complex, real-life scenarios (such as password sharing).*

*With **Part III**, we will naturally continue with more practical examples, as the best way to learn, train and develop a creative mind remains trough regular practice and a frequent exposure to new and original concepts.*

In this part though, we will show how to build upon past tests, and also use a different angle, to illustrate what can be done when things don't work your way. We will finally close this series by addressing the planning and governance aspects of injecting unconventional analytics in your audit projects.

Building Up on Past Successes

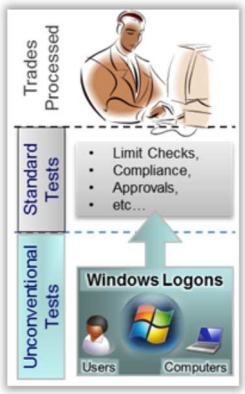
This is an extremely important chapter! Some of you may have been discouraged or intimidated by the complexity in some of the examples shown in these articles, so I really want to emphasize on this point: **the more you do it, the easier and quicker it gets!** This is not a "spend", it is truly an investment.

So… Now that we have invested so much time and effort into building such complicated tests, how can we continue to reap the benefits?

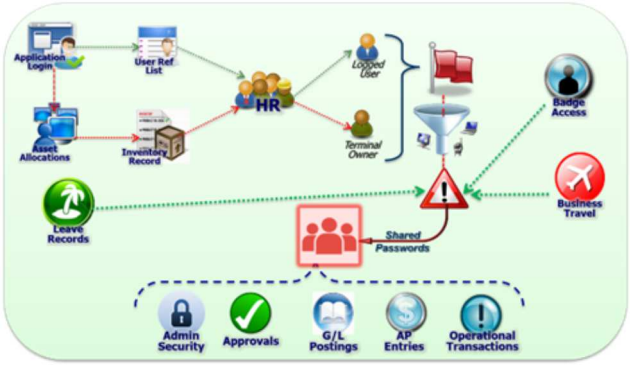
Well, if you have archived your data and documented your processes and interfaces properly, it should all be come **quite easy** going forward.

Let us first review our past successes:

In **Part I**, we showed the example of a test mixing IT controls with financial audit. We showed how to reconcile a trader's transactions with their Windows logon records (to ensure they were really the ones processing the transaction).



We also closed **Part II** by showing all the steps that took us to the intricate test for password sharing:



By now, you should realize that the amount of data and the diversity of tables gathered so far can be reused in new tests for a variety of audits. Oftentimes, I find myself called in the middle of audits that I was not involved in, and asked to offer a quick solution, which would not be possible if I didn't already have a solid base archived in my back pocket.

Therefore, one of the most important aspects of everything you do is **document** your tests, detailing all processes, systems, data and key contacts, and don't forget to save your code & comments.

So what can you reuse? Naturally all functions and algorithms you have built, but most of the time, your main advantage is reuse **data**, either (a) within previous test files or (b) between different tests.

(A) Reusing Data within previous test files

I was called once during a Travel Audit, when whistle-blowers had claimed that some staff were abusing corporate travels. Apparently, short international training or business trips were allegedly used by staff to pay for their own vacations.

Without any warning, I was suddenly pulled into the engagement and asked if I could build an analytics test to check the allegation. Luckily, I had already dealt with both **travel** and **leave** data previously when doing the password sharing test, I had it all documented, and the interfaces were still functional, so I was even able to quickly refresh the data with the latest update.

Those two files (leave and travel data) were originally difficult to find and extract (located on different systems) and extremely difficult to match (the layouts were completely different, from the user keys to the date format). Yet, this test was done in a record time thanks to the fact that all those technical issues had been addressed already during a previous engagement (from "password sharing" tests).

Within half a day, the test was built. By the end of day one, we already had an overall write-up of what the issue would be and what the magnitude of the problem was. We spent the rest of the week just tweaking, adding other data points (destination country and nationality of traveler) and cleaning up.

In the end, several cases were found where expensive international professional trips systematically coincided with the travelers Leave-requests. The most common pattern was when the majority of a trip duration was spent on leave days, whereas the business part of the trip was extremely short (1-2 days), which did not justify such a high expense. Another common factor was that the country destination was often the same as the nationality of the traveler.

This audit was deemed as extremely successful, due in great part to the efficient use of analytics.

(B) Reusing Data between different tests

On this example, the decision to use audit analytics was also made very late in the process, when the audit testing phase was already well underway.

During a wireless security audit, the team found that the wireless signal extended much further than the physical walls of the company's building. It was also found that the local administrator account on company laptops could be compromised, since local administrator accounts were the same on all builds – coming from the same image.

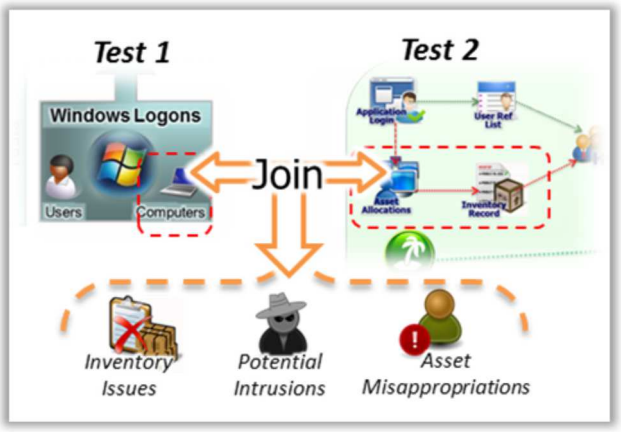
Since certificate-based security is used for laptops, the wireless network automatically authenticates computers first (computer access is required in order for the user credentials to be checked against the domain controller).

(Note: although hacking the laptop would not grant user-level access to the domain -e.g. Shared-drives, active-directory; it does provide with an internal IP address…)

The improvised audit test was simple: the risk being that a laptop falling into the wrong hands could be used to access the company's network (at least partially), we needed to ensure that administrators terminate all computers that are no longer in use.

[By the way, if you ever do this simple test in your environment (check if terminated computers are removed from the network), you are very likely to find numerous exceptions: Administrators are usually very diligent removing terminated users, but terminated machines are often left out (considered a house-keeping issue). This is as mistake though, since such machines could still be used to access the network if not removed.]

In any case, I was asked to test for "terminated laptops" with access to the network; and again, the fact that I had worked with similar data in the past was of great help. I had to mix data from two different tests to achieve the result: the 'trader-logon access' data, to get the list of all laptops allowed on the network, and again the 'password sharing' test data, to translate those computer IDs into asset number, and match with the inventory to check what their physical status was.



The findings exceeded expectations. We first noted that **hundreds** of authorized laptop had long been flagged in inventory as lost, stolen, scrapped, sold, decommissioned, etc…

What was more alarming was that dozens of them seemed to **have accessed the network** since their "retirements". Most of those ended up being false positives though, which highlighted an issue with inventory record accuracy (poor control).

A handful eventually seemed to be **potential intrusion** attempts from misappropriated laptops, and were blocked immediately. Finally, the test also showed an unexpected finding: some of those machines reported lost or stolen were actually being used to connect by… the very same users who had reported them lost/stolen (possible internal fraud case)!

This was another great example on how well documented can cases keep "paying dividends" in the long run, so don't be hesitate to take one complex tasks, because you may be enjoying the benefit of your work for many years.

But enough about successes…

Dealing with Failure

Throughout this series, I have been proudly sharing my success stories, but let's be honest: it was not all roses and fairy dust. I had more than my fair share of bitter disappointments, and I believe I have been honest about it from the very beginning! You may recall that I started this series by stating that this series was not about "picking the low-hanging fruits", but rather about "sniffing out the truffle".

Right from the introduction in Part I, I even wrote: "(…) *Why take the risk of going for added complexity, higher failure rates, longer turn-around time, uncertain results, and being out of your comfort zone, all-the-while fighting against your hierarchy to try and sell your ideas? Well, because the amazing opportunity offered by getting that unique, unexpected insight will really make all the difference."*

Although I mentioned "higher failure rate", I then spent the rest of my articles showing you all the good things that can happen to those who take their chances, but now I also owe it to you to show you the other side of the medal: while it is true that you could be "the hero who finds solutions where none seemed possible", you are still stepping into the unknown, trying to do something that has never been done before, and hence you are adding a lot more uncertainty into your chances of success.

So let us address the elephant in the room: **What can you do when things don't work your way?**

There are several ways that you could still get value out of this exercise, and we will focus on **Four** Key Points:

1. Document, Document, Document!
2. Turn a Test Failure into an Audit Success
3. Keep Trying…
4. Think Outside the Box!

Now I can imagine some of you rolling your eyes as you read this. Yes I know, it does look like oversimplified trivial concepts, but there is actually a lot more depth to each of those – let us go over those with concrete examples:

1. Document, Document, Document!

This probably just sounds like what you have been hearing continuously from your managers and supervisors from the very first day you started working as an auditor: "Make sure you **document** everything!"…

If you have been using data analytics techniques in your audits, you know that this old wisdom rings even truer, and you have to be extremely disciplined about it: document the systems and data table names, how you extracted them, what tools, teams or people helped you in obtaining it, etc...

For instance, even if I had failed the 'password sharing' test because of some missing logon data, I would still have been able to have some success later on with other tests (such as the "travel fraud" or "stolen laptops" examples we saw in the last section).

But in order to succeed there, I would have still needed a well-documented environment, to know where to find the files and how to match them.

Remember that whenever you uncover new areas, you expand your knowledge and push the boundaries of your audit capabilities for all future engagements, even if you may not always be able to use it right away.

Also, it is very likely that whatever piece of the puzzle was missing at the time could become available at a later stage; so it would be important to have the test documented and ready to be rolled out if or when that happens.

So always document well to make sure that the efforts invested do not go to waste.

2. Turn a Test Failure into an Audit Success

This one actually refers specifically to a situation when a key file is missing.

Some time ago, as I was presenting my methodology on "password sharing" during a lecture, I remember a member of the audience came to me afterwards and said "your method would not work in our environment… I tried something similar once, but the IT-Admin told us that we do not have the application login data, so we had to give up…"

My immediate reaction was "No login data?? This is great! Your audit report is just writing itself, you have just put your finger on one major issue, now you simply need to go write down your findings".

It is never OK for any system to **not** know who logged onto it. This is actually a double-winner in some way.

- First, you are issuing a recommendation that will be implemented, and thus improve the control environment.
- Second, thanks to you, the log has now been switched on, so… just wait till next year, and then you can actually finally do the test you wanted to do in the first place!

3. Keep Trying…

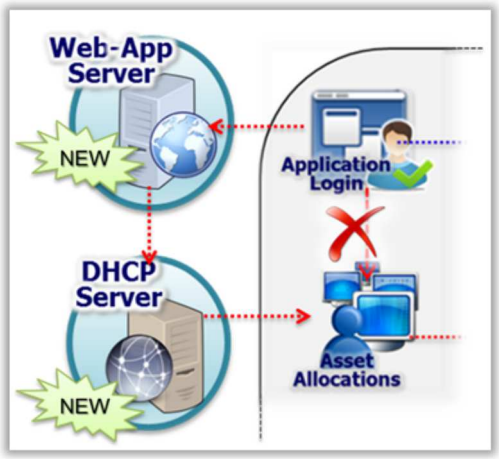
This is the one that usually gets the most "eye-rolls". I must admit it sounds a bit like your old gym teacher at school who would scold you for "not trying hard enough".

In reality, it is meant in a much more constructive way: this is about cycling a bit longer through the last two stages of our 7-step methodology introduced in **Part II**: the "*Add-On*" and "*Expansion*" phases. In other words, asking the questions "**What other data exists**" and "**What else should I know**". (If you are unfamiliar with this, refer back to the last article).

It is easy to get discouraged when all your hard work do not produce a result right away, but you should always makes sure that you have envisaged all possible avenues.

For instance, I had a challenging situation once when trying to apply the same complex password sharing test onto a new environment. I quickly realized that my standard methodology would not work, because in that specific case, there was no actual "Application Login": it was a web-based application (a more and more common occurrence these days), and the authentication was managed by the web-server, and therefore outside the application's control. I had to rethink my whole process and take a holistic look at what information I would need to succeed ("what should I know"), and how to obtain it from the data-points available in that specific environment ("what other data exists"). In the end, following the same careful method, I was able to determine:

- *"What I should know"*: The **IP address** (i.e. the actual "network address") of the users' PCs; and
- *"What data I can use"*: the **reference table** showing all IP addresses and their corresponding physical device.



I could obtain the first one from the **web-server**, and the second from the **DHCP server** (without going into technical details, this is the server on your network that 'distributes' IP-addresses to all devices connecting to it, and therefore "knows" what address belongs to whom/what).

There were other tricks and tweaks along the way that I will spare you, but in the end, I had a solid test that was even bigger and more complex than the original, but still worked properly.

Important: make sure that you also go through the *"consolidation/cleanup"* phase again, as you may have inserted new false-positives when you added those new files, and you will therefore need to adapt the **filter** accordingly. From experience, the more files you add to a chain of linked files, the higher the rate of false-positives, and hence the more careful you have to be when applying your filters.

(Just FYI – In the example above: since DHCP is a 'Dynamic' process, the IPs can sometimes get reassigned; therefore I had to add a filter to ensure that the IP allocation was older than the logon event I was trying to tests).

4. Think Outside the Box!

Of course, this is the main theme of my articles so I have to close the loop with that one, but you may wonder "Outside the Box? Isn't this what we have been doing so far?" Yes, but this time I want to push is just a nudge: let's think 'outside every box'.

During my articles, I have encouraged you to walk off the beaten path, by using systems that nobody analyzed before, or by reconciling systems from completely different universes. So what more can we do?

Well… what if I told you that sometimes, those very systems could actually be the box?!

The Solution is not always in the system! There are several other ways that you could go about it.

For instance, you may look at the **transactions in the files** themselves, to see if there was any pattern and try to find some deviation from that pattern.

Alternatively, you may look at the **business processes**, and see if something looks like out of the regular workflow.

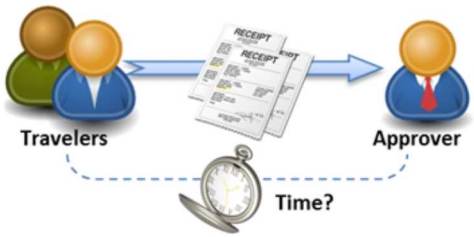
Finally, why not just look at what is happening in the **real world**? Is there some action or behavior that could give you a hint that something is weird?

Here is another example to illustrate this new concept: I was once able to prove the occurrence of password sharing without even having to extract all the files and go through the complex process we described in **Part II**.

By first looking at the **transaction** data, I could feel that something was off. I noticed a curious pattern on the timing of transactions: Most approvals would take hours or days, but some would occur almost instantly after the transaction.

Then I looked at the **flow description** for this **business process**: it was a standard "Travel and Expense Reimbursement" process, and it showed the steps that the manager had to take to approve the expenses, which included reviewing the document and ensuring that all receipts were properly filed.

Finally, I observed how this process actually happened in **real life**, and this is when it hit me:



In order for the process to complete normally, it would take some **time** for the travelers to file all their receipt after submitting their claims. Then it would take some more **time** for these receipts to be transferred to the managers for approval, and then even more **time** for the managers themselves to sort through and review all the documents until they could finally approve.

In this case, after manually repeating the steps myself, I determined that anything approved under 4 hours should be deemed as suspicious. Then, going back to the transactions file, I flagged all the "quick approvals", and was able to clearly make the case that there was no way those went through a 'real' approval process: they were probably done by the submitters themselves, using a shared password. (I later added some travel and logon data to highlight that some of those were indeed processed while the manager was not even present and/or connected).

This "timing test" has worked for me on other environments as well, for instance with traders who needed to submit a manual signed list of orders for the manager to approve them as a batch (a heavy control that always raises the temptation to break the rules in a fast-pace treasury environment).

The actual time taken will depend on your process and your organization, but whether it is a few hours or a day, it is a reliable indicator of fraud.

So as you can see, when I say 'think outside the box', I really do mean '**outside all the possible boxes**': systems, processes or transaction. We should never allow to limit ourselves in any way, it is important to always keep an open mind when looking for solutions.

To summarize, always keep those key questions in mind:

- Are you focusing on the big picture (business process, approval workflow, etc…)?
- Do transactions have to follow a certain sequence?
- Is the transfer of manual documents required for approvals?
- Is timing important?

Let's Talk Planning

How do you plan for "out-of-the-box" thinking? Can you really forecast creativity? Well in my humble opinion, you cannot!... not really at least; not in the classical sense of annual audit plan.

So why broach the subject, you may ask? Because allowing for flexibility, in an otherwise rigid and resource constrained process is an extremely important aspect of making unconventional analytics a success! Let us take a look at how **"standard" planning** would look like:

Every team may have slightly different ways to define their audit universe, identify risks, etc… but let's keep it simple for the sake of the argument.

In a nutshell, your **annual audit plan** will define the audits that you will do throughout the year, which will guide what **business processes** you will be reviewing in each of those, which in turn outline what **key controls** you will be looking into. This will be used to describe your **control testing** procedures, and consequently dictate what **data** you will need to request from your clients.

This is all neat, wrapped up properly, without surprises, in a way that clients, management and audit executives usually favor. Since the workload and resources have been laid out from the start, it makes the engagement easier to budget and clients have time to prepare the data ahead of time.

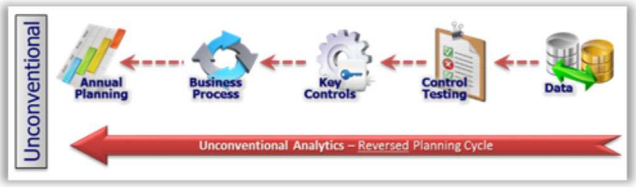
Now, what happened when "Unconventional" audit analytics concepts are injected into this perfectly oiled machine? Well, with unconventional analytics, the cycle is usually much shorter: the process is more Reactive rather than Proactive, and it often occurs when the Tests have already started, and something unexpected came up.

It can usually go two ways: Either a significantly shortened planning cycle (1), or a completely reversed planning cycle (2).

1. Shortened Planning Cycle

This usually happens when some unexpected issue seems to emerge early in the test, which leads to a "Eureka" moment and causes the auditor to completely rethink the direction of the test and the data needed to achieve it. This is basically what happened in our earlier examples on "travel fraud" or "stolen laptops". The team never planned for those tests, the issues came out of nowhere during the engagement and new tests just "appeared" and took a life of their own. The cycle is shortened, because it started simply with a **testing** idea which led straight to new **data** requirement.

2. Reversed Planning Cycle



This one is probably going to challenge your auditor's habits the most. Sometimes, either in the course of an audit, or when sorting through past engagements, you come across some **data** that is so good, just so good, that you realize it can tell you many stories, beyond whatever tests you had originally planned. You realize that you can actually **test** for something else, which turns out uncovering an unexpected **control** failure somewhere, on a **business process** that was not even on your radar. If you want to follow through on your finding, you may need to create a new **audit** and will eventually

have to add it to the **annual planning**. Although such cases are not common they do exist, and if you believe in the power of creative analytics, if you are flexible enough to endorse this approach and are ready to follow through that path, you should accept that it is okay sometimes to let your data affect your annual plans!

Let us look at our final example for this series. For this instance, we will be using **ALL of the data files** we have used in our examples so far (password-sharing, trader access, stolen laptop, travel, etc…)

Now just take a step back, and imagine what you could do if you could get all that data together.

Just contemplate the massive amount of intelligence you could get out of all those data files... and try to realize the amount of information you have about all users in the company… you could literally tell **everything** about them: **when** they worked, **how, where, on what, with whom, for how long?**...

Now it is not my opinion that auditors should play "big brother" with all employees in the company. There is a question of trust, ethics, and a core principle that those aspects should be the responsibility of their management.

But isn't there one specific cohort of the working population in your company for whom we may want to apply higher standards?

If you said **"Consultants"**, you are right!

All the data available from these tests can help you determine who was working on a certain day and who was not, which is extremely useful when trying to monitor expenses while managing a large portfolio.

For instance, on a major multi-year system implementation project, this technique was used to determine that the vendor had charged all of their consultants full-time, month after month, although a thorough review indicated that:

- Several of them had not been on premises for several weeks at a time.
- There was no record of their logging to windows or any other major system.
- Their computers had not been connected to the network.
- There was no trace of them on the remote access logs.

Presented with those findings, the consulting firm had to readjust their fees accordingly.

Although the client was happy for the efficiencies gained that day, the auditors did not really know how to handle the situation, especially if they wanted to eventually present their findings to the board.

This is a typical case of great data that produces a case of reverse-planning:

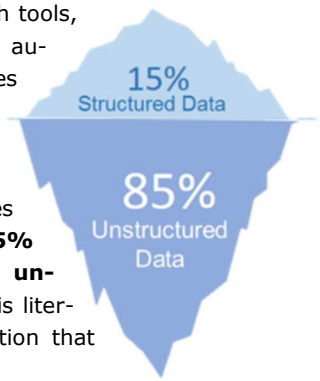
1. The data at hand was used to "improvise" a test
2. This quickly showed instances of vendor overbilling (control issue)
3. This led audit management to revise the annual plan during the mid-year review
4. It was finally decided to add a "Third Party Management Audit" to the annual plan, so that the issue could be officially communicated, and the risk be addressed globally.

The Future of Auditing

With the constantly evolving technology landscape, it is exciting to look forward to what technical capabilities we will have tomorrow that seem out of touch for now.

When I started my auditing career, concepts such as *text-mining, speech recognition, face recognition, geo-tagging or even web-mining* seemed liked a distant dream, and went far beyond what we considered our personal computers capable of doing. Nowadays though, I have all those functionalities conveniently fitting in a small phone in my pocket (many of them are even available on my wrist)!

It would be a shame not to consider what could be done with such tools, if we were to apply them on audits. After all, our examples so far only applied to **structured data**, which is really just the tip of the iceberg. In most companies nowadays, an estimated **85% of all data available is unstructured**, and thus there is literally a gold mine of information that remains unused.



Let us briefly go through some of those new technologies, and see how they could be applied in audits. The following is not intended to offer full solutions, but to show a few concepts or ideas that either I have tried personally, or that other "innovators" have shared with me.

1. Text-Mining

Text-Mining (i.e. the extraction of useful information from text documents) is now one of the most common use of unstructured data. It basically consists in processing long text narratives in a way that would allow us to eventually use it like one would do with a structured table, using various techniques (such as categorization, clustering, or summarization).

Many libraries are available in Python or R, and I actually even had some success by simply using Excel to do it. The applications are almost limitless, but I have personally used it most successfully for parsing through large-scale survey comments. This allows you to obtain some issues and concerns out of thousands of open-text comments, that were simply not available by looking simply at the easily-analyze multiple choice questions. I have also seen the technique used by peers to audit medical claims, or to review resumes from candidates among others.

2. Speech Recognition

Machines have become a lot better at transcribing speech into written text in recent years, and are capable of doing so in several languages, and working through loud background noises and thick accents.

Several years ago, I was pulled into a Treasury audit, where a policy required traders to call the broker within 5 minutes of passing a trade (to confirm, over a certain threshold). All phone calls from trading rooms being recorded and logged on a server, I tested this control by checking simply if the trader had made **one call** in the same timeline as the trade. This however was just a partial test, since I had no way of knowing if the call was to the right person, or for the right reason (so it was just about checking for exceptions – of which I found plenty).

Nowadays, the phone calls are not only recorded, they are also **directly transcribed**; so the speech recognition is already done for you. All that would be left to do is parse through that transcript using some of the text-mining techniques described above. Given the large amount of business still conducted exclusively by phone worldwide, it is easy to see the value that such a technology could bring to your audits.

3. Face Recognition

This technique has been used for years at security checks and customs to catch criminals, in casinos to spot known cheaters, etc… such systems have now become affordable, and have even been mainstreamed as alternative authentication mechanisms for many private devices (i.e. your computer recognizes you, so you do not need to enter a password).

As for audits and forensic practices, I have seen this technique used in special projects, when checking for racial bias and discrimination. Many companies do not hold records on ethnicity on their employees, and certainly not on their clients, but most will have a scanned portrait of the person. Such techniques have a success rate generally over 98%, which is quite impressive, but you would still need to account for false positives.

4. Geotagging

Geotagging tools can turn most physical addresses on earth into geographical coordinates (longitude & latitude).

This is extremely useful, since it allows you to accurately determine the distance between addresses.

I used this technique to check for address proximity between debarred vendors. Sometimes, companies that were flagged as fraudulent (and thus barred from doing business with us) would just reappear under a new name, with an address just around the corner. Geotagging was instrumental in testing for such patterns.

The same technique was used by peers at an insurance company, where they managed to uncover rare cases of collusion between agents and clients (false claims). The team would just sample all claims where agent and client lived within a couple of blocks of one another, as these had much higher probability of being fraudulent, yet were rare enough to reduce the population down to an easily testable size.

Of course, another classic use of geotagging is when looking at 'Mileage Reimbursement' in personal expense claims. When employees charged for a certain number of miles/km (when driving to clients), the test would check that the actual distance would be within a reasonable size (e.g. if the driven distance was more than three times the 'straight-line' distance, the record would be flagged for manual review).

5. Web-Mining

What if you could apply all of your amazing analytics skills on the largest source of data ever made available to mankind: the World Wide Web?…

This is what Web-mining is about!

Whereas the previous four categories were associated with the 'submerged part of the iceberg', I would actually define Web-mining techniques as "drinking the ocean". This is not necessarily a technique for 'unstructured' data, as a matter of fact I have been using it mostly for very precise, structured data point – but it is in a category of its own due to the sheer size, scope and extent of the data available to you.

So what can you do with all that?

Have you ever had to work on a file that had transactions in different currencies? How frustrating was it when you realized that the exchange rates were missing, and that you could not ever possibly copy-paste the rates per date manually on thousands of transactions, and thus your test had failed before even starting…

…unless you can think outside the box and find a way to automated such data import!

It is not even complex or expensive: This can be done now even via simple macros in Excel! Basically, any webpage accessible without login can easily be grabbed. This can be used to get currency exchange rates of course as mentioned, but also:

- Get number of fans, followers, subscribers, or views on FB / twitter / YouTube…
- Get WHOIS information for domain names
- Get Stock quotes and underlying Financial data
- Get definition of a word from Google.

I even had a colleague build a whole Web Scanner to check the company's web-site quality according to very specific internal criteria (typos, broken-links, wrong use of the company's acronym, etc…)

These are just a few ideas, but the possibilities are virtually endless.

You can probably think of several other examples yourselves on all of these techniques (and if you do, please do drop me a line, I love hearing innovative ideas from others too!)

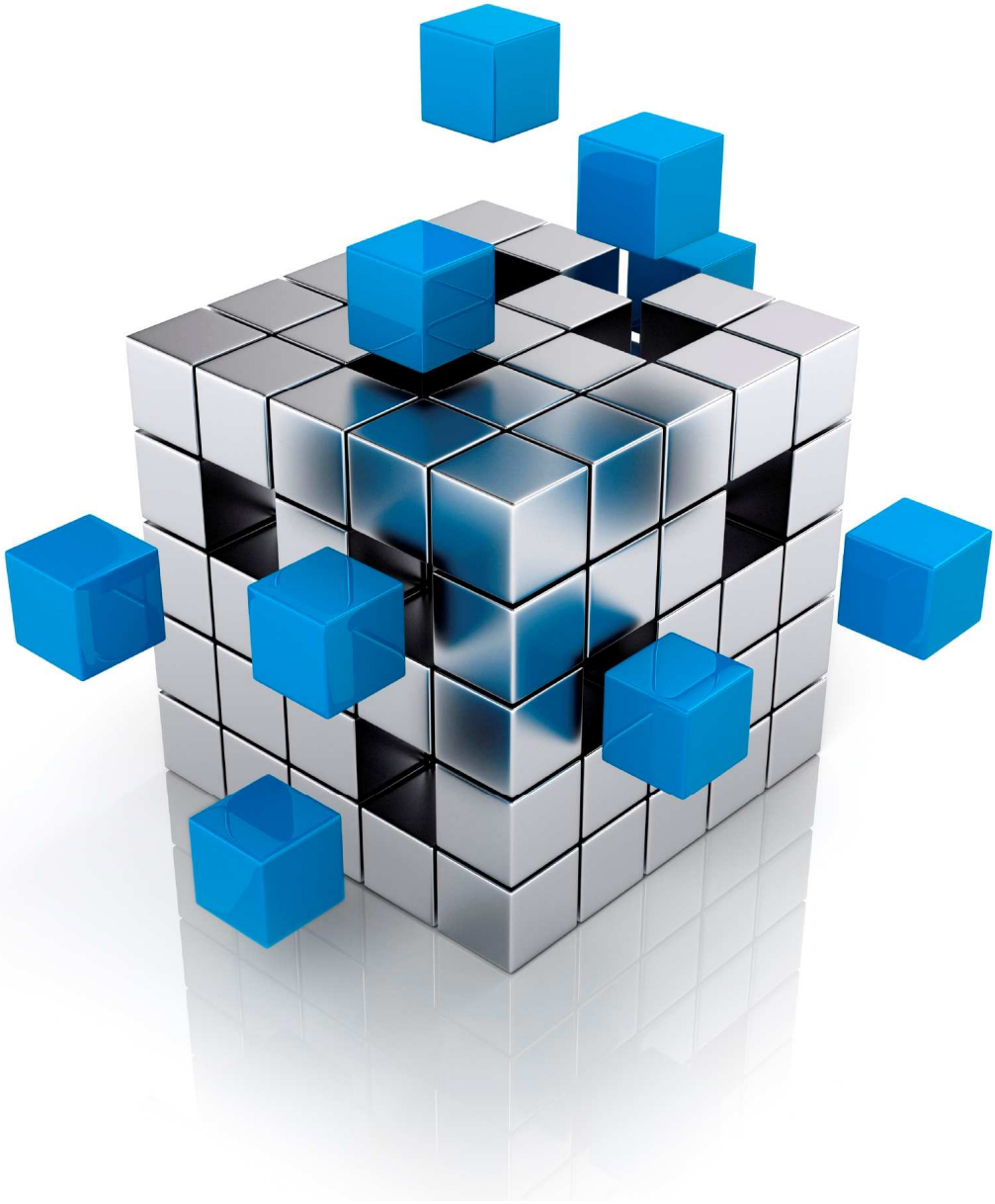
Series Conclusion

As this series comes to a close, I hope that its content was of value to you, and was perhaps able to 'plant a seed' in your mind, and hopefully some of the examples and methodology highlighted in those articles will someday inspire you to try something new and challenging, and help you to take on some informed risks.

As always, I love the opportunity to exchange new ideas and experiences, so feel free to contact me at YSF.data@gmail.com if you feel like sharing your own special stories, or if you have any questions or comments.

Thank you!

Minitema: COSO og interne kontroller



Udelukker en governance model baseret på de tre forsvarslinjer brugen af COSO? Er revisionsarbejdet i sig selv en motiverende faktor for eksistensen af interne kontroller? Hvilke standarder og risikostyringsmodeller læner interne revisorer sig op ad i Danmark? Disse tre spørgsmål danner omdrejningspunktet for dette nummers minitema, hvor vi skal se nærmere på COSO og interne kontroller.

God fornøjelse.

COSO og de tre forsvarslinjer – hvad betyder det egentlig for Intern Revision?

Jesper Jæger Granstrøm, Executive Director, CIA, CRMA, CFE, Ernst & Young P/S

Heino Hansen, Internal Audit Manager, CIA, Nordea

Som interne revisorer anvender vi ofte både COSO og de tre forsvarslinjer (3LoD) som helt naturlige begreber, der er med til at "definere" Intern Revisions rolle og de kriterier, der anvendes til at vurdere de kontrolsvagheder, som vores arbejde måtte afdække. Men ser man lidt nærmere på de to referencerammer og samspillet mellem disse, så er der flere forhold som kan have betydning for Intern Revision og måden vi udfører vores arbejde på.

The IIA udgav i juli 2015 publikationen "Leveraging COSO across the three lines of defense", hvilket er et væsentligt grundlag for denne artikel. Vi har i denne artikel ikke inkluderet en detaljeret redegørelse af de skærpede regulative krav, der gælder for den interne revisionsfunktion i finansielle virksomheder.

Er 3LoD og COSO Corporate Governance værktøjer?

IIA's standarder indeholder følgende definition af governance[1] og risiko:

*"Governance is the combination of **processes and structures** implemented by the board in order to **inform, direct, manage and monitor** the activities of the organisation toward the **achievement of its objectives**."*

*"The possibility of an event occurring that will have an impact on the **achievement of objectives**. Risk is measured in terms of impact and likelihood."*

For finansielle institutioner i EU, er der i GL44[2] fremsat specifikke krav til governance, idet der heri er anført, at alle kreditgivende finansielle virksomheder skal besidde en **robust governance struktur**, hvilket inkluderer:

- *a clear organisational structure with well defined, transparent and consistent lines of responsibility,*
- *effective processes to **identify, manage, monitor and report the risks** it is or might be exposed to,*
- *adequate **internal control mechanisms**, including sound administrative and accounting procedures, and*
- *remuneration policies and practices that are consistent with and promote sound and effective risk management".*

Selvom 3LoD ikke nævnes specifikt i ovenstående ses det dog tydeligt, at et væsentligt aspekt af governance er risikostyring. Dermed bliver 3LoD også et naturligt corporate governance værktøj for ledelsen, da formålet hermed er at styrke forståelsen af risici og kontroller på tværs af virksomheden. Tilsvarende ses det, at der er en tydelig kobling mellem ordvalget i ovenstående definitioner og de fem kontrolkomponenter i COSO's rammeværk for intern kontrol – og dermed kan COSO rammeværket også anses som et naturligt corporate governance værktøj for ledelsen.

Samspillet mellem COSO og de tre forsvarslinjer

Helt grundlæggende kan man sige, at de tre forsvarslinjer og COSO er to rammeværk, som er nært forbundne, når man ser på deres respektive formål. Modellen med de tre forsvarslinjer har til formål at styrke den generelle forståelse af risikostyring og intern kontrol gennem en tydelig fordeling af roller og ansvar på tværs af de tre forsvarslinjer. Tilsvarende har COSO's rammeværk for intern kontrol til formål at understøtte et effektivt design i virksomhedens kontrolaktiviteter baseret på de risici, der er identificeret. Man kan dermed sige, at COSO er "værktøjskassen" og de tre forsvarslinjer er den organisatoriske struktur, som understøtter, hvem der har ansvaret for og hvem der skal anvende de enkelte elementer i værktøjskassen. Tydelighed og transparens i forhold til de enkelte komponenter og samspillet herimellem er fundamental for en effektiv implementering heraf i virksomhedens corporate governance, og dermed også i relation til ledelsens mulighed for at dokumentere, at de har etableret en solid governance struktur i virksomheden.

[1] "Glossary" til IIA standarderne

[2] GL 44: Internal governance for institutions in the European Community is covered by Article 22 of Directive 2006/48/EC

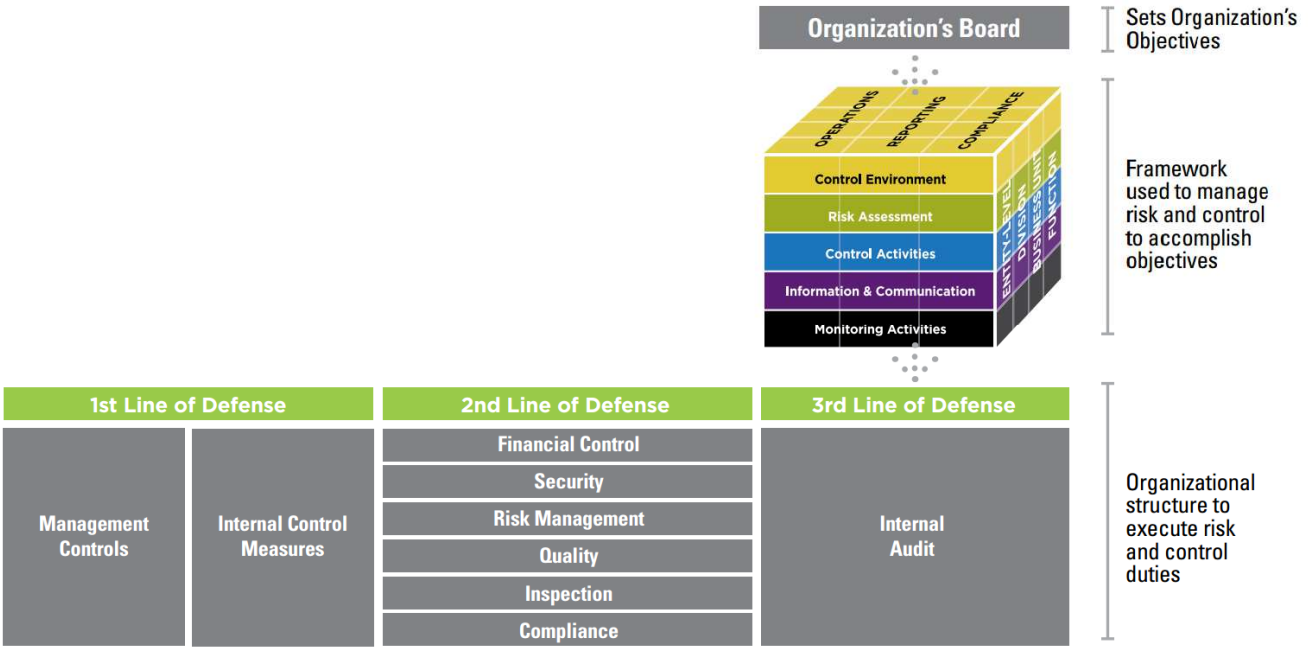
Samspillet mellem de to rammeværk bør dermed også anvendes af Intern Revision, som inspiration i forhold til såvel indhold som omfang af revisionsopgaver, ligesom det kan være en hjælp i den "root cause" analyse, som bør være en integreret del i formuleringen af de revisionsbemærkninger, som arbejdet måtte give anledning til.

Intern Revisions rolle

Modellen med de tre forsvarslinjer er velkendt for de fleste interne revisorer og anvendes af mange som en naturlig referenceramme i forhold til at beskrive intern revisions rolle i virksomhedens governance struktur. I modellen er de enkelte forsvarslinjers ansvar beskrevet på følgende måde:

1. Ejer og håndterer risici og tilhørende kontrolaktiviteter (operationel ledelse). Den første forsvarslinje medvirker også til, at det er de rette risici, der tages som del af den daglige drift. Reelt skal første forsvarslinje kunne stå alene, hvilket betyder, at de udførte kontrolaktiviteter til afdækning af virksomhedens væsentligste risici, i deres design ikke må være afhængige af, at aktiviteter udført af anden forsvarslinje afdækker en del af den identificerede risiko.
2. Monitorerer håndteringen af risici og kontrolaktiviteter på vegne af ledelsen (indsætter risikostyrings-, kontrol- og compliancefunktioner). Anden forsvarslinje skal støtte ledelsen gennem deres særlige ekspertise og procesindsigt på tværs af organisationen, således at de (sammen med første forsvarslinje) medvirker til at sikre, at risici og kontroller håndteres og styres effektivt.
3. Leverandør af uafhængig revisionsoverbevisning vedrørende effektiviteten i håndteringen af risici og kontroller til brug for bestyrelsen og virksomhedens øverste ledelse. På mange måder har tredje forsvarslinje samme opgave som anden forsvarslinje, dog med den særlige forskel, at tredje forsvarslinje skal forholde sig til, om første og anden forsvarslinje opererer i henhold til bestyrelsens forventninger. Herudover er en vigtig præmis, at tredje forsvarslinje er uafhængige af ledelsen, hvilket også er med til at sikre objektivitet i det udførte arbejde.

Modellen med de tre forsvarslinjer er fleksibel forstået på den måde, at virksomhedens størrelse, kompleksitet, branche mv. vil have stor betydning for, hvilke funktioner der vil være behov for at indsætte, ligesom afgrænsningen mellem de enkelte forsvarslinjer kan variere (eksempelvis vil anden forsvarslinje i nogle virksomheder også have ansvaret for direkte kontrolaktiviteter og i andre virksomheder vil første forsvarslinje også udføre monitorerende aktiviteter). De særlige "krav" til tredje forsvarslinje i modellen i forhold til uafhængighed og objektivitet bevirker dog, at denne forsvarslinje som udgangspunkt ikke kan påtage sig opgaver, som ligger i første eller anden forsvarslinje, hvis rollen som uafhængig



Figur 1: Samspillet mellem COSO og de tre forsvarslinjer
Kilde: The IIA: "Leveraging COSO across the three lines of defense"

"Assurance provider" skal opretholdes til fulde. Dermed ikke sagt, at det ikke vil være værdiskabende for en virksomhed, hvis de har en intern revisionsfunktion, som ikke lever op til modelkravene, enten som følge af rapporteringslinjer, der ikke er direkte til bestyrelsen, eller at den interne revisionsfunktion er tættere på nogle af opgaverne i anden forsvarslinje. En sådan praksis øger bare de iboende risici for, at tredje forsvarslinje ikke vil levere den overbevisning til bestyrelsen og den øverste ledelse, som er tiltænkt gennem modellen. På den anden side vil en fuld efterlevelse af modellen heller ikke give nogen sikkerhed som sådan, hvis kulturen og integriteten blandt de ansatte i tredje forsvarslinje ikke lever op til den forventede standard.

For finansielle virksomheder medfører de regulatoriske krav, at det ikke er muligt for virksomheden at anvende "hybrid løsninger", hvor tredje forsvarslinje påtager sig opgaver, som omfatter andet end revision. I øvrige virksomheder giver IIA standarderne i deres 2017 opdatering mulighed for, at revisionschefen kan påtager sig opgaver/ansvar, som ligger udenfor intern revision, hvorfor en "hybrid løsning" ikke er et brud på kravene til intern revision. Dette fremgår af den nye standard 1112:

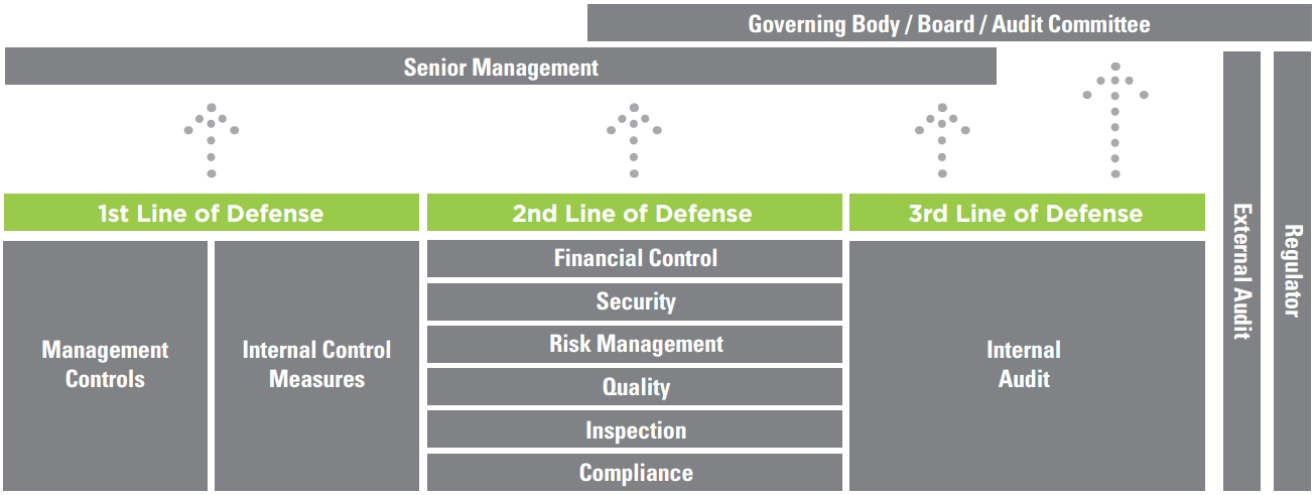
"Where the chief audit executive has or is expected to have roles and/or responsibilities that fall outside of internal auditing, safeguards must be in place to limit impairments to independence or objectivity."

I fortolkningen til standarden er det anført, at sådanne opgaver eksempelvis kan være, at revisionschefen også påtager sig ansvaret for compliance- og risikostyringsopgaver. Som eksempel på "safeguards" der kan begrænse indvirkningen på intern revisions uafhængighed og objektivitet er anført, at dette kan bestå i bestyrelsens overvågning og gennemgang af rapportering samt periodisk evaluering af rapporteringslinjer og ansvar.

Det er vores vurdering, at den nye IIA standard samt tilhørende fortolkning bygger på en forudsætning om, at såvel bestyrelsen som virksomhedens øverste ledelse har en solid forståelse af 3LoD modellen, da det ellers ikke vil være muligt for dem reelt at tage stilling til, hvornår intern revisions uafhængighed og objektivitet er kompromitteret i forhold til de forventninger der er til compliance - og risikostyringsaktiviteterne i de tilfælde, hvor dette ansvar varetages af chefen for intern revision.

Sammenfattende kan man således sige, at modellen med de tre forsvarslinjer skal medvirke til at give en tydeligere struktur i forhold til, hvordan virksomhederne gennem deres daglige drift tager de rigtige risici, og at de risici der tages også håndteres og kontrolleres på en effektiv måde. Det overordnede mål om at give værdi til virksomheden, uanset hvilken forsvarslinje man er i, betyder også, at der altid vil være et vist spændingsfelt mellem de enkelte forsvarslinjer i forhold til, hvem der skal gøre hvad. Det er også den fleksibilitet, der som tidligere nævnt, er i modellen, da den skal implementeres under hensyntagen til virksomhedens størrelse, struktur og kompleksitet, og efterhånden som virksomheden udvikles kan det også give ændringer til såvel opgaver, roller og ansvar for de enkelte forsvarslinjer.

Og hvad betyder dette så for intern revisions rolle? Nogle interne revisionsfunktioner kan stadig være påvirket af den tilgang, som den eksterne revision har i forhold til sikring af, at virksomhedens regnskab er retvisende. For at de eksterne revisorer er i stand til at påtegne årsrap-



Figur 2: De tre forsvarslinjer
Kilde: The IIA: "Leveraging COSO across the three lines of defense"

porten er de nødt til at få deres egen overbevisning om, at de kontroller, der understøtter regnskabet, fungerer effektivt og afdækker de krævede revisionsmål. Men dette er ikke den rolle, som tredje forsvarslinje har i henhold til modellen. I modellen er det ledelsens ansvar, gennem første og anden forsvarslinje, at risici identificeres og at der implementeres de nødvendige kontroller, og at disse er effektive. Det er således ikke en forudsætning i modellen, at intern revision skal opnå overbevisning om kontrollers effektivitet gennem egne test, men derimod foretage vurderingen af, om ledelsen er i kontrol givet de aktiviteter, der udføres af første og anden forsvarslinje. For at kunne give denne overbevisning vil det være naturligt, at intern revision udfører et antal test af kontroller for at validere resultaterne fra første og anden forsvarslinje.

Det betyder også, at intern revision som tredje forsvarslinje skal forholde sig til, hvordan ledelsen har "designet" deres monitorerende funktioner i anden forsvarslinje, således at første og anden forsvarslinjes samlede virke understøtter, at det er de rigtige risici, der påtages, og at de påtagne risici håndteres og kontrolleres i overensstemmelse med bestyrelsens forventninger hertil. Hverken bestyrelsen eller den øverste ledelse er som sådan en del af de tre forsvarslinjer, men den øverste ledelse har det direkte ansvar for de to første forsvarslinjer, og bestyrelsen har en tilsynsrolle i forhold hertil, hvor de kan anvende tredje forsvarslinje som et værktøj til at udøve denne tilsynsrolle.

Koblingen til COSO's rammeværk for intern kontrol

Den øverste ledelses ansvar for, at første og anden forsvarslinje fungerer effektivt giver også koblingen over til COSO's rammeværk for interne kontroller og komponenten "control environment" med de dertilhørende fem "guiding principles".

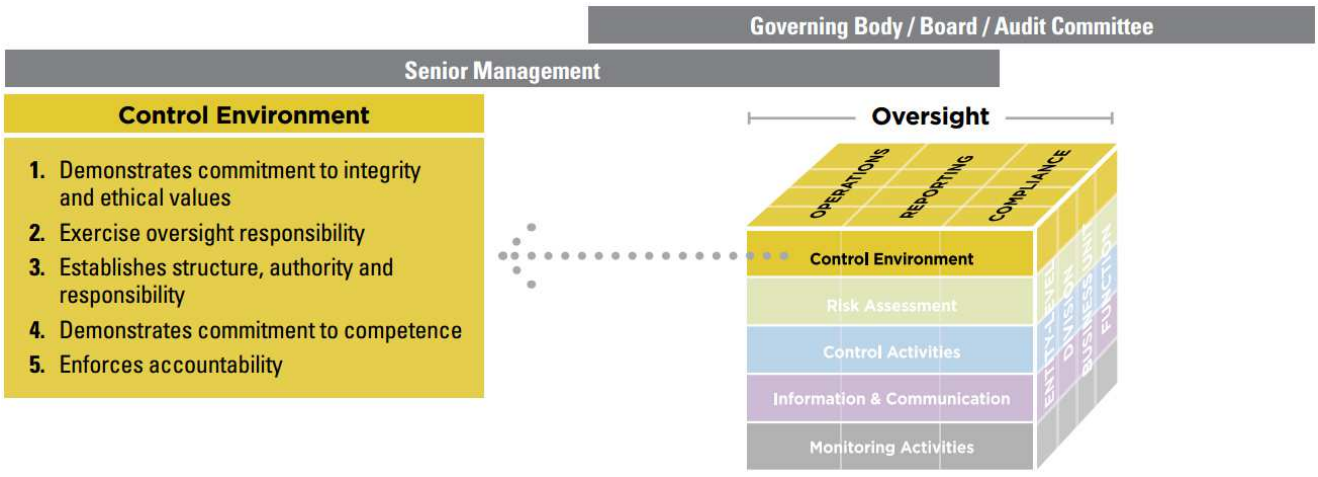
Indledningsvist bemærkes det, at de fem "guiding principles" i COSO's rammeværk harmonerer med den definition af kontrolmiljø, som fremgår af ordforklaringen til IIA standarderne:

"Control Environment. The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- *Integrity and ethical values.*
- *Management's philosophy and operating style.*
- *Organizational structure.*
- *Assignment of authority and responsibility.*
- *Human resource policies and practices.*
- *Competence of personnel."*

Ser man på de fem "guiding principles", som understøtter komponenten "control environment", så giver det stof til eftertanke i forhold til, hvad det betyder for intern revisions arbejde og rolle som tredje forsvarslinje. Det betyder alt andet lige, at intern revision gennem sit arbejde skal tage stilling til, om den øverste ledelse lever op til "kravene" i de fem "guiding principles", hvilket kan være svært at revidere, og i nogle situationer også vil udfordre ledelsens måde at varetage deres hverv på.

For intern revision betyder de fem "guiding principles", at det ikke er tilstrækkeligt alene at se på, om der er de



Figur 3: Komponenten "control environment" og de fem tilhørende guiding principles
Kilde: The IIA: "Leveraging COSO across the three lines of defense"

fornødne politikker og forretningsgange, om roller og ansvar er tydeligt definerede, etc., som ofte er nogle af de elementer der ligger til grund for vurderingen af kontrolmiljøet, da dette primært kan henføres til princip 3.

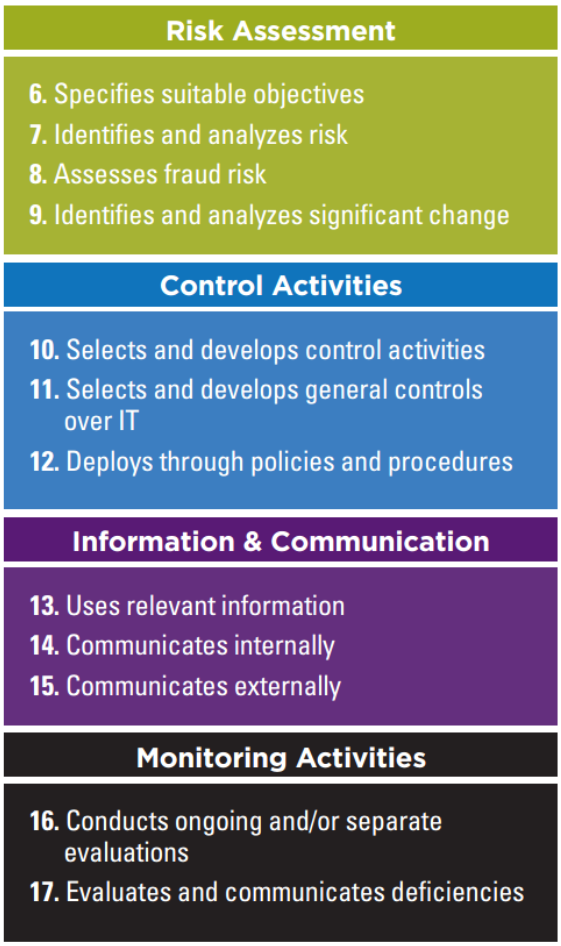
Men skal intern revision lave særskilte revisioner af virksomhedens etiske værdier og hvordan de efterleves i organisationen, og er intern revision i stand til at udtale sig om, hvordan det etiske miljø er i virksomheden? Svaret må være, at der i henhold til IIA standardernes definition af kontrolmiljø er en begrundet forventning om, at disse begreber inkluderes i udførelsen af intern revisions arbejde samt at intern revisions metodik omfatter disse aspekter, således at intern revision kan inkludere dette i rapporteringen til bestyrelsen og/eller virksomhedens øverste ledelse. At det ligger som en forventning i IIA standarderne betyder dog ikke, at det er en let opgave at løfte for intern revision.

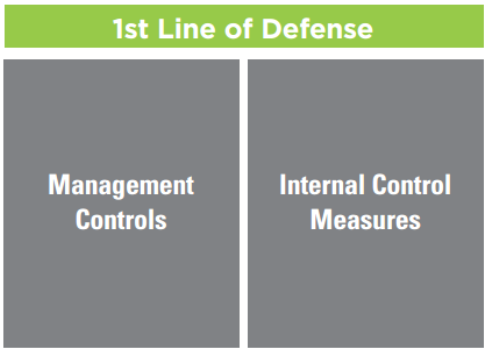
Lettere er det nok at forholde sig til efterlevelsen af princip 4, da det kan gøres gennem vurdering af virksomhedens HR politikker, rekrutteringsproces, programmer for kompetenceudvikling, anvendelse af successionsplaner, mv., som også er konkrete elementer i definitionen af "control environment" i IIA standarderne.

Dvæler man lidt mere ved princip 4, så er det værd at bemærke, at dette princip lægger op til, at bestyrelseskomiteer skal forholde sig til, om de funktioner de overvåger, besidder de fornødne kompetencer. Det må således betyde, at eksempelvis intern revision overfor revisionskomiteen skal vise, at deres kompetenceprofil modsvarer dels de opgaver, som intern revision skal løse i henhold til deres funktionsbeskrivelse, men også i forhold til den revisionsplan, som fremlægges til godkendelse.

Første forsvarslinje

I forhold til COSO's rammeværk for intern kontrol har første forsvarslinje en rolle i alle kontrolkomponenterne, med undtagelse af "control environment", der som nævnt ovenfor er bestyrelsens og den øverste ledelses ansvar.





Figur 4: COSO og første forsvarslinje
Kilde: The IIA: "Leveraging COSO across the three lines of defense"

Ser man på de "guiding principles", som ligger i de øvrige kontrol komponenter, og hvad det betyder for intern revisions arbejde, så er der enkelte, som det er værd at fremhæve. I forhold til "risk assessment", er det en grundlæggende forudsætning i princip 6, at alle der er en del af virksomhedens interne kontrolsystem, har en forståelse af virksomhedens strategi og målsætninger. For intern revision betyder det, at der som en del af revisionen skal tages stilling til, om medarbejderne i første forsvarslinje også besidder en tilstrækkelig og relevant forståelse af virksomhedens (væsentligste) risici, da det er en forudsætning for, at den fastlagte risikoappetit og risikotolerance reelt kan efterleves. Tilsvarende er det en forudsætning for at forstå formålet med de implementerede kontrolaktiviteter (et element i princip 14 under "information & communication") – og dermed kunne bidrage aktivt til kvaliteten i/resultatet af de udførte kontroller.

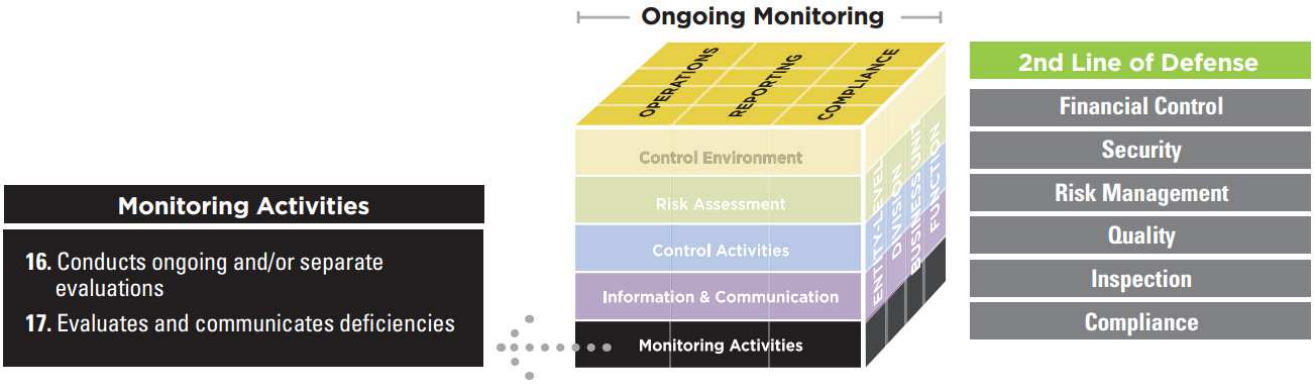
Det vil med andre ord sige, at det ikke er tilstrækkeligt at se på, om interne kontroller er dokumenteret i nødvendigt omfang. Man skal også (eksempelvis via interview) opnå overbevisning om, at de udførende af kontrollen reelt forstår, hvorfor den udføres og hvad den skal afdække. Tilsvarende kan det være relevant at se på, hvorledes de der udfører kontrolaktiviteterne, "eskalerer" muligheder for optimering af kontrolaktiviteten (princip 9).

Herudover er princip 17 under "monitoring activities" også interessant i forhold til intern revisions vurdering af, hvordan dette håndteres af første forsvarslinje. Såfremt der har været kontrolsvagheder, hvordan har første forsvarslinje så arbejdet hermed, herunder hvilke kompenserende aktiviteter der er iværksat som følge af de identificerede svagheder? Er svagheder eskaleret til rette ledelsesniveau og er der foretaget de fornødne vurderinger af, om der er tale om en enkeltstående hændelse, eller om det er mere systematisk, hvilket kan kræve, at første forsvarslinje udfører yderligere undersøgelser for at afdække omfanget af svagheden. Der er også en kobling til princip 10 under "control activities" – tages der fornyet stilling til kontrollers design, hvis der konstateres svagheder, herunder etableres nye (re-designede) kontroller i de tilfælde, hvor en hændelse ikke er modvirket af de eksisterende kontroller? Har første forsvarslinje argumenteret med, at en kontrolsvaghed kompenseres gennem en aktivitet udført af anden forsvarslinje, er der reelt tale om, at første forsvarslinje ikke kan stå alene, og de eksisterende kontroller i første forsvarslinje skal derfor udbygges og/eller re-designes.

Anden forsvarslinje

Det vil som udgangspunkt alene være kontrolkomponenten "monitoring activities" som er direkte koblet til anden forsvarslinje, da de forskellige riskostyrings-, intern kontrol- og compliancefunktioner, som ledelsen etablerer, netop har til hensigt at understøtte ledelsens overvågning af, at første forsvarslinje tager de rette risici, og håndterer og kontrollerer de tagne risici effektivt.

Da intern revision som tredje forsvarslinje skal give bestyrelsen en uafhængig vurdering af den samlede effektivitet i håndteringen af risici og kontroller, betyder det også, at intern revision bør forholde sig til de etablerede funktioner i anden forsvarslinje og deres virke. Dvs. om de pågældende funktioner, i deres måde at tilrettelægge arbejdet på, reelt lever op til formålet med den pågældende funktion. Implicit må det også betyde, at intern revision skal forholde sig til, om der er "huller" i den samlede monitorering, som de forskellige funktioner i anden forsvarslinje udfører, eller om der er unødige overlap mellem det de ser på.

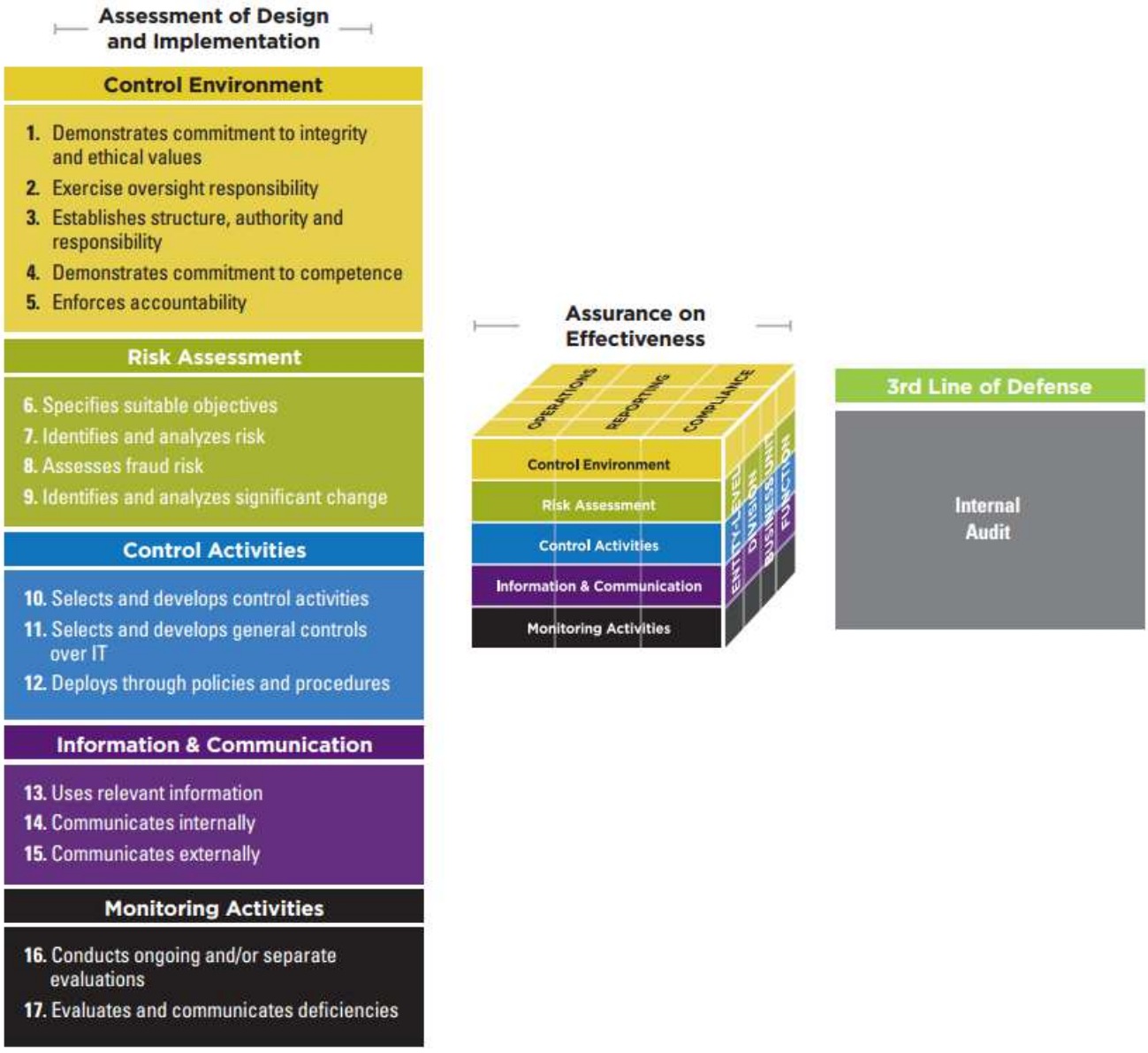


Figur 5: COSO og anden forsvarslinje
Kilde: The IIA: "Leveraging COSO across the three lines of defense"

Selvom funktioner i anden forsvarslinje principielt ikke er uafhængige (i forhold til virksomhedens ledelse), så er der stadig en vis grad af uafhængighed i forhold til de aktiviteter, som første forsvarslinje udfører. For virksomheder i den finansielle sektor er der et formelt defineret krav til, at der skal være etableret risiko- og compliance funktioner i anden forsvarslinje. Funktionerne i anden forsvarslinje spiller derfor også en vigtig rolle i forhold til, at den øverste ledelse kan leve op til deres overordnede ansvar for den samlede håndtering af risici i virksomheden. Har de forskellige funktioner i anden forsvarslinje ikke den fornødne "respekt/integritet" i organisationen, vil der være en iboende risiko for, at de pågældende funktioner ikke er stand til at udfylde deres rolle effektivt. Skulle det forekomme kan det derfor være et naturligt (påkrævet) punkt for intern revision at fremhæve, som del af deres samlede vurdering, konklusion og rapportering.

Tredje forsvarslinje

Intern revision skal som del af sit arbejde forholde sig til samtlige elementer i COSO's rammeværk for intern kon-



Figur 5: COSO og tredje forsvarslinje
Kilde: The IIA: "Leveraging COSO across the three lines of defense"

trol. Det helt særlige kendetegn ved tredje forsvarslinje – uafhængigheden af den daglige ledelse og den direkte rapporteringslinje til bestyrelsen – gør tredje forsvarslinje i stand til at give en objektiv vurdering af, hvordan ledelsen er i kontrol i forhold til de risici, som er forbundne med at drive virksomheden, og om håndteringen heraf lever op til bestyrelsens forventninger hertil.

I de foregående afsnit er der givet eksempler på, hvordan koblingen mellem COSO's rammeværk for intern kontrol, kan have betydning for intern revisions arbejde. Når man ser på modellen med de tre forsvarslinjer og koblingen til COSO er det essentielt, at man altid har for øje, at det er ledelsens ansvar, at virksomheden tager de rette risici, og at de påtagne risici håndteres og kontrolleres effektivt. Som intern revision er det derfor relevant, at man forholder sig til "modenheden" i ledelsens håndtering af dette ansvar. Dette kan man eksempelvis gøre gennem anvendelse at selv-evalueringer i forhold til såvel identificering af risici som vurdering af kontrollers design og effektivitet, som den operationelle ledelse skal udfylde. Intern revision kan som del af deres vurdering forholde sig til, hvor god/pålidelig den operationelle ledelse er hertil i forhold til såvel fuldstændighed som nøjagtighed.

Resultatet af sådanne vurderinger af ledelsens selvevalueringer vil være gode indikationer på, om der reelt er den fornødne indsigt og forståelse af både risici og kontroller. Intern revision kan i denne forbindelse overveje, om en todimensionel konklusion, hvor der dels vurderes på effektiviteten i det etablerede kontrolmiljø og dels "modenheden" i kontrolmiljøet / risiko- og kontrolkulturen, vil øge informationsværdien for virksomhedens øverste ledelse og bestyrelse.

Koordinering mellem de tre forsvarslinjer

I forhold til IIA standarderne er det et krav, at der sker en aktiv koordinering på tværs af de forskellige forsvarslinjer (og med ekstern revision), jf. IIA standard 2050. Formålet hermed er, at "dobbeltarbejde" skal reduceres mest muligt. Overordnet set har alle tre forsvarslinjer det samme ultimative mål – at hjælpe virksomheden til at nå de besluttede målsætninger, bl.a. gennem en effektiv håndtering af risici. En effektiv koordinering vil også hjælpe bestyrelsen, idet dette øger sandsynligheden for, at der kun er en version af "sandheden" på tværs af de forskellige forsvarslinjer.

Intern revision bør således også bygge på det arbejde, som udføres af anden forsvarslinje i det omfang, det er muligt. En forudsætning herfor er naturligvis, at de pågældende funktioner har en vis modenhed, og at deres opgavetilgang og anvendte metoder har den fornødne kvalitet. En forudsætning for, at intern revision kan vurdere modenheden og opgavetilgang og metode hos funktionerne i anden forsvarslinje er selvsagt, at der er foretaget en egentlig revision af de pågældende funktioner, hvilket som udgangspunkt også vil omfatte test (re-performance) af anden forsvarslinjes kontroller/ monitorering.

Afslutning

Selvom både COSO's rammeværk for intern kontrol og modellen med de tre forsvarslinjer virker som ganske naturlige begreber at anvende for os som interne revisorer, så er det stadig værd at tage et fornyet kig på elementerne i de to rammeværk og forholde sig til, hvad det betyder for arten og omfanget af vores arbejde givet det stade, som virksomheden er på nu – og ud fra hvordan intern revision har udviklet sig. Det kan klart anbefales at læse IIA's publikation "Leveraging COSO across the three lines of defense", som denne artikel bygger på. Publikationen indeholder et appendiks, hvor der for hver af de 17 "guiding principles" i COSO er lavet en kobling til, hvad dette princip betyder for de enkelte forsvarslinjer, hvilket også kan give god inspiration til, hvordan man som intern revision kan knytte de forskellige "guiding principles" op på den "root cause" analyse, som bør udføres i relation til identificerede svagheder i det etablerede kontrolmiljø.

Link til Publikationen:
https://www.coso.org/Documents/COSO-2015-3LOD.pdf

I hvilket omfang, hvordan og hvorfor påvirker system- og procesrevisionen omfanget af de interne kontroller

Leif Christensen, Assistent Professor, CBS

Nedenstående artikel er baseret på en del af min PhD-afhandling: "Quality of information – The role of internal controls and materiality".

http://research.cbs.dk/da/publications/quality-of-information(009a3613-c75c-461e-8b54-5141668423e0).html

Introduktion

Det har gennem en længere årrække været dokumenteret, at der af forskellige årsager har været et pres på virksomhederne for at etablere nye og forbedre eksisterende interne kontroller. Det har ligeledes i lang tid været antaget, at både intern og ekstern revision spiller en central rolle i forhold til disse overvejelser. Holdningen er således, at revisorerne lægger pres på virksomhederne for etablering af yderligere kontroller.

Revisorernes anbefalinger om interne kontroller bliver typisk rapporteret i management letters. Da jeg arbejdede som ekstern system- og procesrevisor, fik jeg ofte kommentarer til vores arbejde, f.eks. fra en CFO i en stor dansk virksomhed:

"I anbefaler altid forbedringer og implementering af nye kontroller i jeres management letters - så I er faktisk den primære årsag til det stigende antal kontroller."

Der er måske en vis sandhed i dette udsagn, da der er et pres på revisorerne for at være synlige overfor klienten (anbefale forbedringer) og dermed demonstrere værdi af revisionen.

Selvom intern revision anses som en vigtig spiller, har de generelt set ikke en veldefineret rolle i forhold til intern kontrol. Der er således en begrænset dokumenteret viden om intern revisions betydning for og påvirkning af de interne kontroller. For at etablere viden herom er det som en del af min PhD-afhandling derfor blevet undersøgt:

- I hvilket omfang,
- hvordan og
- hvorfor system- og procesrevisionen påvirker omfanget af interne kontroller.

Undersøgelsen er baseret på empirisk materiale indsamlet fra et casestudie af en intern revisionsafdeling i en stor finansiel virksomhed. Den interne revisionsafdeling i denne virksomhed er i al væsentlighed bemandet og arbejder på samme måde som ekstern revision, hvilket er understøttet af regulatoriske krav fra Finanstilsynet.

Disse krav omfatter bl.a. at intern revision udelukkende rapporterer til bestyrelsen, og at der årligt udarbejdes en aftale, der fastlægger fordelingen af arbejdsopgaver mellem intern og ekstern revision.

Endvidere skal ekstern revision foretage en kvalitetskontrol og gennemgå de arbejdshandlinger, som intern revision har udført. Dette kan i henhold til gældende praksis ske som en fælles revision af afgrænsede områder. De nævnte forhold betyder, at resultatet af undersøgelsen ikke blot er gældende for intern revisions arbejde med interne kontroller, men også for tilsvarende arbejde udført af ekstern revision.

I hvilket omfang påvirker system- og procesrevisionen interne kontroller?

Et management letter er en almindelig anvendt form for formel rapportering af anbefalinger og bemærkninger fra revisor til klienten, herunder resultatet af revisionen af virksomhedens interne kontroller.

For at afdække i hvilket omfang system- og procesrevisionen påvirker de interne kontroller, blev der, som en del af casestudiet, foretaget en detaljeret analyse af management letter rapporteringen for perioden 2008 - 2012. I denne periode blev der i alt afgivet 404 anbefalinger omkring interne kontroller.

Anbefalingerne er i management letter rapporteringen klassificeret i tre kategorier, der kan sammenfattes til 1) væsentlig svaghed, 2) betydende svaghed og 3) mindre svaghed. Denne klassifikation svarer i al væsentlighed til den globalt anerkendte klassificering som f.eks. er defineret af AICPA.

De revisionsmæssige anbefalinger fordelt på år og kategori fremgår af **Tabel 1** på næste side.

	Klassifikation			
År	1	2	3	I alt
2008	10	61	12	83
2009	15	75	10	100
2010	8	51	12	71
2011	8	55	17	80
2012	6	54	10	70
Total	47	296	61	404

Tabel 1 – Anbefalinger fordelt på år og klassifikation

Bortset fra 2009 er niveauet af anbefalinger 70 – 80 årligt. 2009 er påvirket af den finansielle krise og den følgende skærpede opmærksomhed omkring vigtigheden af velfungerende interne kontroller, hvilket er understøttet af en række nye regulatoriske krav fra Finanstilsynet.

Billedet er stort set det samme, hvis der udelukkende fokuseres på anbefalinger om etablering af nye kontroller, jf. **Tabel 2**.

	Klassifikation			
År	1	2	3	I alt
2008	7	13	1	21
2009	8	33	4	45
2010	1	9	2	12
2011	1	14	6	21
2012	3	14	2	19
Total	20	83	15	118

Tabel 2 – Anbefalinger om nye kontroller fordelt på år og klassifikation

Med hensyn til den ledelsesmæssige håndtering, resulterer samtlige anbefalinger om etablering af nye kontroller i en efterfølgende implementering af tiltag, der afdækker de kontrolmæssige svagheder. Der kan dog være en tidsmæssig forskydning mellem rapporteringen af anbefalinger og implementeringen af løsninger. Den væsentligste årsag er, at hvis det er nødvendigt at implementere en ny systemmæssig løsning med tilhørende re-design af understøttende processer, så vil der i praksis medgå en længere periode, før denne er effektiv.

Der blev ligeledes foretaget en tekstmæssig analyse af rapporteringen for at afdække naturen af de enkelte anbefalinger. På baggrund heraf kan det konstateres, at anbefalinger begrundet i lovgivningsmæssige- eller regulatoriske krav udgør ca. 40%. I den forbindelse tegner Finanstilsynets skærpede opmærksomhed omkring værdien af udlånsporteføljen sig specifikt for ca. 25% heraf. De resterende 60% er begrundet i en revisionsmæssig vurdering og dækker typisk over forhold som manglende funktionsadskillelse, rapporteringsmæssige svagheder og utilstrækkelig dokumentation.

Sammenfattende kan det konstateres, at der i gennemsnit implementeres ca. 20 nye kontroller som følge af revisorernes anbefalinger. Baseret på en gennemgang af anbefalingerne i management letters kan det derfor konstateres, at system- og procesrevisionen påvirker omfanget af virksomhedens interne kontroller.

Hvordan påvirker system- og procesrevisionen interne kontroller?

For at se nærmere på hvordan denne påvirkning sker, blev der etableret et traditionelt flow-chart med en beskrivelse af management letter processen, og herunder blev det identificeret i hvilke faser af processen, der er formelle møder mellem revisor og klienten. Der blev i alt identificeret fem formelle møder med fokus på følgende emner af management letter rapporteringen:

A. Revisors observationer
B. Anbefalinger
C. Samlet udkast til detailbemærkninger
D. Udkast til sammenfatning
E. Udkast til revisionsprotokol.

De enkelte møder blev herefter analyseret på grundlag af en teoretisk model til beskrivelse af interaktionen mellem revisor og klient. Ifølge modellen kan revisors og klientens adfærd på møderne hver for sig klassificeres som:

- Insisterende,
- argumenterende eller
- eftergivende.

Endvidere klassificeres den kombinerede adfærd som:

- Udveksling af information,
- diskussion eller
- forhandling.

Resultatet af mødet vurderes og klassificeres som et:

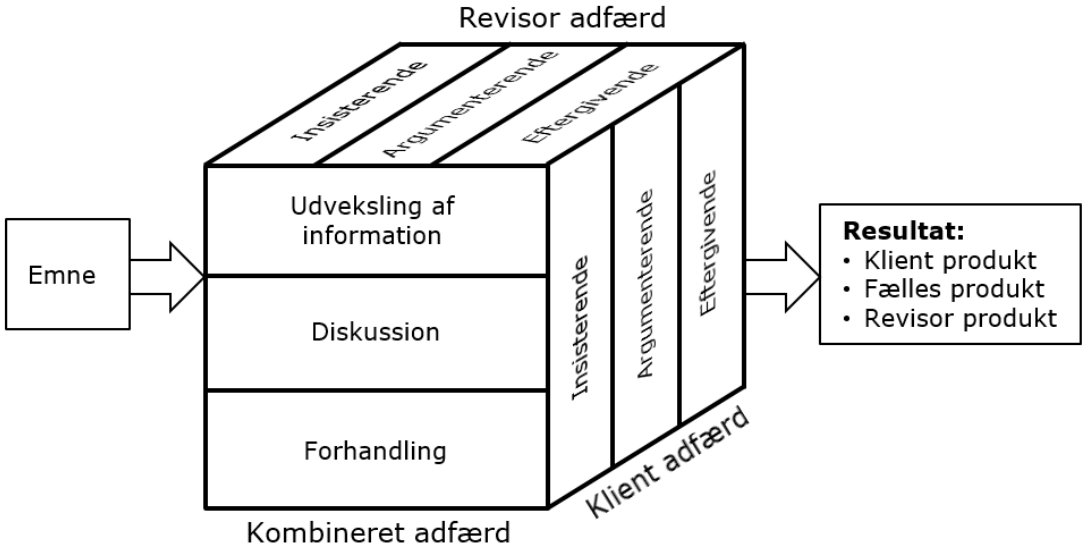
- Klient produkt,
- fælles produkt eller
- revisor produkt.

Modellen er illustreret i **Figur 1** på næste side.

Resultatet af analysen af behandlingen af de enkelte emner er beskrevet i nedenstående afsnit.

A - Revisors observationer

Revisionen resulterer typisk i en række observationer, som bliver dokumenteret i skemaform, der indgår som appendiks til management letter. Disse observationer er emnet for det første møde mellem revisor og klient. For-



Figur 1 – Kombineret revisor / klient interaktionsmodel

målet med mødet er at afklare eventuelle misforståelser, og om den skriftlige præsentation af observationen svarer til de faktiske forhold. Baseret på interview af revisormedarbejderne, suppleret med en gennemgang af udkast til observationer, arbejdspapirer og endelig rapportering, er der ikke identificeret uafklarede uoverensstemmelser omkring observationerne. Dette understøttes af to repræsentanter fra virksomheden, der i fælleskab beskriver situationen:

"Hvis revisorerne har fået et forkert indtryk af en procedure, er de villige til at lytte til begrundede argumenter."

Hvis der er forskellige synspunkter, er det således op til klienten at præsentere yderligere dokumentation. Mødet er derfor en argumenterende udveksling af information, og resultatet – de endelige observationer – kan klassificeres som et fælles produkt.

B - Anbefalinger

Herefter udarbejder intern revision en risikovurdering og anbefaling til de enkelte observationer, som ligeledes indarbejdes i appendiks til management letter. Anbefalingerne er emnet for det næste møde mellem revisor og klient.

Set fra revisorernes synspunkt er formålet med anbefalingerne at forbedre kontrolniveauet, og dermed opnå revisionsbevis fra test af kontroller, når forbedringen er gennemført. Ifølge revisionschefen er de åbne overfor ændringer til de foreslåede anbefalinger:

"Med hensyn til anbefalingerne er det af mindre betydning, hvordan problemet bliver løst - så længe det virker. Men anbefalingen bør mindske risikoen - ellers må vi prøve igen. Vi er nødt til at lukke observationen, men hvordan det sker er af mindre betydning."

Denne praktiske tilgang understøttes også af den måde, som klienten håndterer anbefalingerne på. Da det er klientens ansvar på et senere tidspunkt at gennemføre en løsning, går medarbejderne ofte til ledelsen for at blive enige om en løsning.

Både revisorernes og klientens adfærd kan primært klassificeres som argumenterende. Der er dog tegn på, at revisorerne kan blive insisterende, hvilket understøttes at kommentaren "… anbefalingen bør mindske risikoen", som angiver et minimumskrav til løsningerne. Den kombinerede adfærd er dog stadig en diskussion, der har til formål at fastlægge en anbefaling, der både kan implementeres og samtidig opfylder de revisionsmæssige krav. Resultatet af interaktionen er derfor et fælles produkt, da begge parter deltager aktivt i løsningen.

C - Samlet udkast til detailbemærkninger

Som afslutning på arbejdet med detailbemærkningerne foretager revisor en prioritering af observationerne. Der er ingen formelt definerede kriterier for prioritering, men de er baseret på en "professionel bedømmelse" og svarer som tidligere nævnt til globalt anerkendte klassificeringer. Klassificeringen har dog interesse fordi prioritet 1 anbefalinger, ifølge praksis i den finansielle sektor, altid rapporteres i revisionsprotokollen. Der er endvidere det specielle forhold i en finansiel virksomhed, at revisionsprotokollen skal fremsendes til Finanstilsynet.

Samtidig udarbejder klienten et oplæg til kommentarer til de enkelte observationer og anbefalinger, hvilket inkluderer fastlæggelse af deadlines for implementering af forbedringer. Begge forhold indarbejdes i udkast til appendiks til management letter, der er emnet for det næste møde.

Specielt prioriteringen af anbefalinger er vigtig for klientens medarbejdere, dette understreges af en bemærkning fra revisionschefen:

"Medarbejderne har ikke noget imod vores anbefalinger, og de foretrækker at have velkontrollerede forretningsprocesser. Hvis vi er rimelige med vores anbefalinger, så bliver de umiddelbart opfyldt. De er dog ikke glade for prioritet 1 observationer, da disse via revisionsprotokollen bliver rapporteret til bestyrelsen og Finanstilsynet."

En af klientens afdelingsledere er enig i dette synspunkt:

"En prioritet 1 anbefalinger kan føre til reaktioner fra bestyrelsen, som kan forårsage unødig uro i organisationen. Det er en situation, vi af indlysende grunde ønsker at undgå, men generelt er anbefalingerne fra intern revision rimelige."

En sammenholdelse af udkast til detailbemærkninger med den endelige version viste, at antallet af prioritet 1 anbefalinger bliver reduceret. Revisionschefen forklarer at:

"… vi kan måske nogle gange blive enige om en prioritet 2 i stedet for 1. Det er dog en forhandlingssituation – hvis vi ændrer prioritet fra 1 til 2, kan vi måske også blive enige om at fremskynde fristen for implementering af en løsning på problemerne."

Adfærden hos både revisor og klient er argumenterende i retning af insisterende, og den kombinerede adfærd har karakter af en forhandling. Dette er primært begrundet i den potentielle eksponering overfor bestyrelsen og Finanstilsynet. Samtidig kan dette ses som et eksempel på "tone at the top", hvilket indikerer, at bestyrelsen ønsker velkontrollerede processer.

Detailbemærkningerne skal godkendes af begge parter, og begrundet i det aktive samspil omkring prioriteringen af anbefalingerne og fastlæggelse af deadlines for implementering af forbedringer, anses denne fase af management letter processen for et fælles produkt.

D - Udkast til sammenfatning

Baseret på detailbemærkningerne udarbejder intern revision en sammenfatning, der primært er bestemt til koncernledelsen. Udkast til sammenfatning med tilhørende appendiks er emnet for mødet mellem intern revision og koncernledelsen.

Da koncernledelsen har det samlede overblik over forretningen, er der mulighed for, at de ønsker at foretage ændringer i prioriteringen af de tiltag, som medarbejderne har besluttet til afhjælpning af de kontrolmæssige svagheder. Dette kan f.eks. være tilfældet, hvis det er nødvendigt at foretage en prioritering af ressourcerne til forskellige implementeringsprojekter. En anden mulighed er, at de er bekendt med større fremtidige implementeringsprojekter, der kan ses som løsningen af en eller flere af de rapporterede svagheder. Intern revision er opmærksom på dette:

"Det er en ledelsesmæssig beslutning, hvordan ressourcerne skal prioriteres – og det er helt klart ikke vores opgave at være involveret i denne proces. Vi accepterer disse beslutninger og planlægger vores revision i overensstemmelse hermed."

Dette ses som en eftergivende holdning hos revisorerne, der er baseret på en faglig forståelse af roller og ansvar, herunder potentielle uafhængighedsproblemer.

Da de eneste ændringer til udkast til sammenfatning er initieret af ledelsen, er den endelige sammenfatning klassificeret som et klient produkt.

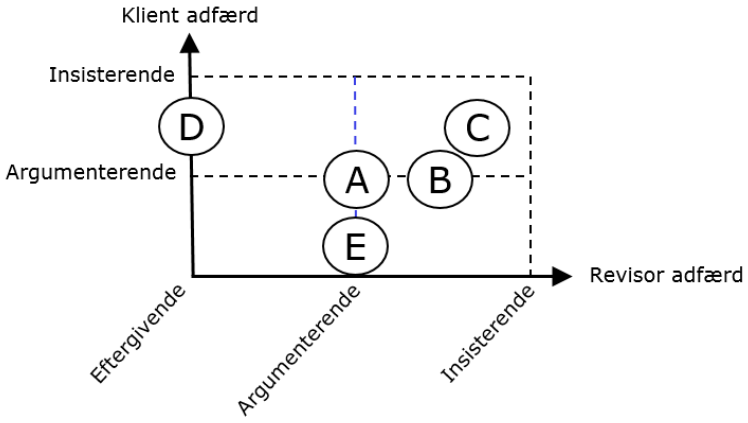
E - Udkast til revisionsprotokol

Det sidste emne i management letter processen er udkast til revisionsprotokol, der bl.a. indeholder en overordnet beskrivelse af prioritet 1 anbefalingerne. Udkast til revisionsprotokol sendes til revisionsudvalget og præsenteres på et møde. Ifølge revisionschefen har mødet en formel karakter:

"Det er vores dokument og vores professionelle ansvar. Vi har desuden været involveret i hele processen, og det er derfor ikke acceptabelt, hvis revisionsudvalget ændrer vores faglige vurdering."

Dette kan ses som udtryk for, at revisorernes adfærd er argumenterende i retning af at være insisterende, og mødet kan klassificeres som en udveksling af oplysninger. En sammenholdelse af udkast og endelige revisionsprotokoller viste ingen væsentlige ændringer. Dette indikerer, at adfærden hos revisionsudvalget er eftergivende.

Denne adfærd kan også forklares med, at revisionsudvalget først bliver involveret i management letter processen på et sent tidspunkt, hvor alle andre parter er blevet enige om detaljerne. Resultatet er det endelige revisionsprotokollat, som bliver underskrevet af bestyrelsen. Doku-



Figur 2 – Revisors, klients og deres kombinerede adfærd i management letter processen

mentet er et revisionsprodukt, da revisorerne både har det formelle og faktiske ansvar for indholdet.

Sammenfatning
Resultatet af analysen af management letter processen kan sammenfattes som illustreret i **Figur 2**.

Som det fremgår, er intern revisions adfærd argumenterende i retning mod insisterende og klientens gennemsnitlige adfærd argumenterende, når de træffer beslutninger om interne kontroller. Den kombinerede adfærd er primært en udveksling af oplysninger, hvor kvaliteten af oplysningerne afgør udfaldet af samspillet. Der er dog to undtagelser: Den overordnede prioritering af de ressourcer, der kræves for at forbedre eksisterende eller gennemføre nye kontrolforanstaltninger og revisionsprotokollen. Prioriteringen af ressourcer er et ledelsesansvar og dermed et klient produkt. Revisionsprotokollatet er derimod revisorernes ansvar og deres uafhængige rapportering til bestyrelsen. I den forbindelse ser det ud til, at bestyrelsen respekterer management letter processen og tager resultatet heraf til efterretning.

Det kan også ses som et resultat af en management letter proces med stærke interne kontroller, der er påvirket af bestyrelsens "tone at the top" og et overordnet ønske om velkontrollerede forretningsprocesser.

Resultatet af management letter processen, som er en beslutning om implementering af nye eller forbedring af eksisterende kontroller, er baseret på et argumenterende samarbejde og kan derfor betragtes som et fælles produkt.

Hvorfor påvirker system- og procesrevisionen interne kontroller?

Som det sidste element i case studiet er det analyseret, hvorfor system- og procesrevisionen påvirker de interne kontroller. Denne del af analysen er dels baseret på en teoretisk model, der beskriver de kontekstuelle forhold, der påvirker management letter processen, dels en vurdering af specifikke anbefalinger til forbedring af den interne kontrol.

De kontekstuelle forhold er grupperet på følgende måde:

- Regulatoriske- og lovgivningsmæssige forhold
  - Ufravigelige krav
  - Krav undergivet ledelsesmæssige skøn
  - Risikoen for bøder, påbud eller henstillinger
- Interne forhold i virksomheden
  - "Tone at the top", herunder overholdelse af ledelsesgodkendte politikker
  - Personlige mål
- Revisor / klient forhold
  - Erfaringer fra tidligere samarbejde
  - Kompetenceniveau
  - Historiske erfaringer i forhold til det emne der behandles
  - Væsentlighed af det emne der behandles.

Med hensyn til de specifikke anbefalinger blev der udvalgt 10 eksempler, som både fra et revisionsmæssigt og forretningsmæssige synspunkt vurderes som væsentlige. Udover en vurdering af den kontrolmæssige svaghed omfattede udvælgelseskriterierne tillige, at implementeringen af en løsning kræver betydelige ressourcer.

Regulatoriske og lovgivningsmæssige forhold
Alle aktiviteter i koncernen er underlagt obligatoriske tilsyn fra Finanstilsynet. Et tilsynsbesøg dækker normalt et forretningsområde, og der gennemføres i alt 4 - 6 inspektioner årligt. Rapporterne fra Finanstilsynet skal offentliggøres på koncernens hjemmeside. Som følge af de regelmæssige tilsynsbesøg er medarbejderne bekendt med dette og betragter dem som "nødvendige, men tidskrævende og besværlige". Der er generelt set bekymring over Finanstilsynet, og det kommer til udtryk på flere måder, her i en kommentar fra en afdelingsleder:

"De (Finanstilsynet, red.) hænger over os som en sort sky. Der er næsten ingen grænser for, hvad de kan bede om af specifikationer og rapporter - vi må da håbe, at det er nyttigt."

Denne holdning betyder, at der er en opmærksomhed omkring velfungerende kontroller:

"Uanset hvordan vi ser på det, så har vi brug for at have de nødvendige interne kontroller på plads - for at beskytte os mod tilsynsbesøg."

Dette pres fra Finanstilsynet ses også hos intern revision, der via netværksgrupper mv. er meget opmærksomme på hvilke temaer Finanstilsynet aktuelt beskæftiger sig med:

"Baseret på oplysninger fra bl.a. netværksgrupper er vi meget opmærksomme på, hvilke områder som Finanstilsynet har arbejdet med i andre banker. Baseret på disse oplysninger tilpasser vi revisionen, så den udover det traditionelle revisionsmæssige formål tillige udgør en form for forsvar mod Finanstilsynet. Vi bør undgå en situation, hvor vi har gennemført revision af et område, og Finanstilsynet efterfølgende identificerer væsentlige svagheder på samme område. Vi foretrækker at have et godt omdømme hos Finanstilsynet - det gør tingene meget nemmere."

For mere konkret at vurdere effekten af Finanstilsynet gennemgik vi 10 udvalgte anbefalinger med både intern revision og klienten. Som forventet var der eksempler på anbefalinger, som primært ses som et forsvar mod Finanstilsynet:

"Det her er et typisk eksempel på en anbefaling, der primært kan tilskrives Finanstilsynet. Kontrollen udføres, som den skal, men er ikke dokumenteret "tilstrækkeligt". Fra et forretningsmæssigt synspunkt gør det ingen forskel - men vi accepterer anbefalingen, og ser det som et forsvar, når vi har inspektioner fra Finanstilsynet."

De fleste anbefalinger vurderes dog at have en forretningsmæssig værdi. En afdelingsleder forklarede:

"Disse anbefalinger – og vores håndtering af risikoen – er helt uafhængig af Finanstilsynet. Afdækningen af risikoen er væsentlig set fra et forretningsmæssigt synspunkt. Hvis dette problem var blevet identificeret ved et tilsynsbesøg, havde det utvivlsomt medført et helt berettiget påbud. Nu så vi det selv først – og så bliver det naturligvis håndteret."

Spørgsmålet om hvor meget ekstra arbejde med interne kontroller, der bliver udført – direkte eller indirekte begrundet af Finanstilsynet – blev rettet til revisionschefen:

"Det er umuligt at måle, hvor meget ekstra arbejde vi udfører af denne årsag, men alle de 10 udvalgte anbefalinger ville have været rapporteret – også i en verden uden Finanstilsynet. Enkelte af anbefalingerne ville dog nok have fået en lavere prioritering, hvis der udelukkende blev lagt en revisionsmæssig vurdering til grund."

Selvom presset fra Finanstilsynet blev nævnt flere gange, vurderes det, at de anbefalede forbedringer af eksisterende eller implementering af nye interne kontroller, tilføjer værdi både fra et revisionsmæssigt og forretningsmæssige synspunkt.

Interne forhold i virksomheden
Overholdelse af gældende lovgivning og god praksis har en høj prioritet for bestyrelsen, hvilket kommer til udtryk i "tone at the top". Selvom det ikke fremgår af en specifik ledelsesgodkendt politik, så finder bestyrelsen ikke, at det er acceptabelt, hvis der er problemer med at overholde krav fra Finanstilsynet. Et af bestyrelsesmedlemmerne forklarede det på følgende måde:

"Specielt dem der sidder i flere bestyrelser er meget opmærksomme på ikke at blive eksponeret for kritik fra Finanstilsynet."

Problemstillingen er naturligvis forstærket af at både det interne og eksterne revisionsprotokollat, efter godkendel-

se af bestyrelsen, skal sendes til Finanstilsynet. Endvidere er det et regulatorisk krav, at revisorerne skal følge op på og rapportere, om anbefalinger og påbud fra Finanstilsynet bliver fulgt. Denne praksis betyder, at problemer med interne kontroller er kendte for både bestyrelsen og Finanstilsynet. Hensynet til bestyrelsen og Finanstilsynet bruges da også nogle gange som argument af intern revision:

"Nogle gange henviser vi både formelt og uformelt til bestyrelsens holdning, når vi argumenterer for en anbefaling."

Dette argument forstærkes af at "tone at the top" ikke blot er en holdning, men også kan komme konkret til udtryk. En afdelingsleder forklarede:

"Jeg fik et meget klart budskab fra et bestyrelsesmedlem: 'Vi ønsker ikke lån, der konflikter med vores retningslinjer - slet ingen'. Det er vel overflødigt at sige, at dette gav anledning til en intern præcisering af kravene overfor vores medarbejdere."

Overordnet set er der et pres fra bestyrelsen, hvilket kan forklares med et ønske om at opfylde god praksis og krav fra Finanstilsynet. Selvom der ikke er en formel politik om overholdelse af myndighedskrav, har "tone at the top" en betydelig påvirkning på både medarbejdere og intern revision.

Revisor / klient forhold

Samarbejdet mellem intern revision og klientens medarbejdere er baseret på gensidig respekt, både på det personlige og faglige niveau. Interviewene af både revisionsmedarbejdere og klientens medarbejdere beskriver samarbejdsrelationerne som gode. Dette understøttes også af den seneste kundetilfredshedsundersøgelse, hvor intern revision sammenfattende vurderes som: "… gode samarbejdsrelationer - en konstruktiv og objektiv partner". På revisorsiden understøttes den faglige respekt tillige af, at både revisionschefen og en række nøglemedarbejdere har mere end 10 års anciennitet i koncernen. Hertil kommer at intern revision er aktiv hos Foreningen af Interne Revisorer, Danske Revisorer, og underviser på Copenhagen Business School.

Samtidig søger intern revision også at finde en balance mellem den potentielle forbedring af de interne kontroller og det samlede antal anbefalinger. En af revisormedarbejderne forklarede:

"Hvis vi får et rimeligt resultat (afhjælpning af svagheder), er der ingen grund til at gå videre. Vi skal jo også tage hensyn til det fremtidige samarbejde."

Dette indikerer, at revisorerne overvejer hvornår "nok er nok" med det formål at støtte de langsigtede relationer. Revisionschefen er meget opmærksom på dette forhold:

"Vi skal undgå at rapporterer mindre detaljer, det vil bare irritere forretning, og vi vil sandsynligvis have problemer med at komme igennem med vigtige findings."

Det ser ud til, at den afbalancerede strategi vedrørende antallet af anbefalinger påvirker samarbejdet og er en del af forklaringen på hvorfor klienten umiddelbart accepterer alle anbefalingerne i management letters.

Konklusion og diskussion

Baseret på et case study af en intern revisionsafdeling i en stor finansiel virksomhed er det undersøgt i hvilket omfang, hvordan og hvorfor system- og procesrevisionen påvirker omfanget af interne kontroller.

Som en indledende del af undersøgelsen blev det konstateret, at anbefalingerne i management letters i gennemsnit har resulteret i implementeringen af 20 nye kontroller årligt. Isoleret set støtter dette således de anekdoter som siger, at revisorerne er skyld i det stigende antal af interne kontroller.

Der blev herefter foretaget en kortlægning af management letter processen og en analyse af de formelle møder der er mellem revisor og klient. På grundlag heraf kan det konstateres, at beslutningen om implementering af nye eller forbedring af eksisterende kontroller er baseret på et samarbejde mellem revisor og klient – og at resultatet er et fælles produkt.

Dette resultat understøtter således ikke de anekdoter som siger at revisorerne er skyld i det stigende antal af interne kontroller.

Hvad er så begrundelsen for dette samarbejde og den fælles holdning til implementering af nye kontroller? Umiddelbart forekommer det som om, at respekten for Finanstilsynet er den væsentligste årsag. Dette resulterer i en holdning om at velfungerende interne kontroller er en form for forsvar mod Finanstilsynet.

Denne holdning er måske ikke overraskende, da væsentlige anbefalinger via revisionsprotokollatet rapporteres til Finanstilsynet. Samtidig er det dog også en bekvem forklaring på, hvorfor det er nødvendigt at bruge betydelige ressourcer på at forbedre eksisterende og gennemføre implementering af nye kontroller. Det tyder dog på at påvirkningen fra Finanstilsynet primært er af indirekte karakter, f.eks. ved at intern revision deler erfaringer med kollegaer – og tilpasser revisionen herefter.

En detaljeret analyse af udvalgte væsentlige anbefalinger viser dog, at disse tiltag både har en revisionsmæssig og forretningsmæssig værdi. Resultatet viser således, at forbedringerne sandsynligvis ville være gennemført uafhængigt af Finanstilsynet.

Denne konklusion giver anledning til overvejelser omkring det hensigtsmæssige i, at de regulatoriske myndigheder fastholder den mangeårige praksis med at compliance skal baseres på en regelbaseret tilgang. Det kan derfor overvejes om et skift i fokus til en mere principbaseret regulering er mere hensigtsmæssig. Dette synspunkt støttes af at klienten – trods klager over Finanstilsynet – respekterer de interne kontroller, hvilket er supporteret af en uformel politik fra ledelsen i form af "tone at the top", der har en betydelig påvirkning på både medarbejdere og intern revision.

Den analyse der ligger til grund for nærværende artikel har været fokuseret på management letter processen. De klager over Finanstilsynet der er observeret som en del af processen, har derfor ikke været hovedfokus for analysen. For at opnå en dybere forståelse af de regulatoriske myndigheders påvirkning på de interne kontroller, kan det derfor være interessant af foretage en nærmere analyse heraf. I den forbindelse kan det være interessant at få afklaret om klagerne – i stedet for krav om interne kontroller - reelt set er begrundet i stigende krav til rapportering, likviditet og kapital, der er en direkte følge af skærpet lovgivning og regulering efter finanskrisen.

Hvis dette er tilfældet er spørgsmålet om niveauet for virksomhedens interne kontroller primært er et anliggende mellem revisor og klient. Som følge heraf vil det derfor være dem der fastlægger niveauet og bestemmer hvornår ”nok er nok”.

Hvilke standarder bruger intern revision ?

Ask Ransdal Hansen, Associate, PwC

Intern revision er i gang med at rykke sig. Det viser hovedkonklusionen af mit speciale på cand.merc.aud ved CBS. Et speciale, der tager temperaturen på intern revision i Danmark med udgangspunkt i en række interviews med danske interne revisionschefer.

Indledning

Min vejleder Kim Klarskov Jeppesen skrev i 2006 en artikel i samarbejde med Marika Arena om intern revision i Danmark. Denne artikel endte blandt andet med at konkludere, at intern revision dengang i vid udstrækning udførte finansiel revision baseret på ISA'erne. Dette startede en undren hos mig. Som cand.merc.aud. studerende havde jeg taget valgfaget intern revision og var derfor klar over, at IPPF[1] standarderne var specifikt rettet mod intern revision.

Denne undren blev mit specialets omdrejningspunkt. Jeg ville forsøge at undersøge, i hvilke rammer der bliver foretaget intern revision i Danmark – samt prøve at forstå, hvordan intern revision er endt med disse rammer. Den styrende problemformulering blev derfor: *Hvilke standarder og risikostyringsmodeller baserer danske interne revisionsafdelinger deres arbejde på og hvorfor*. Der var derfor to elementer i mit speciale: Et eksplorativt element, hvor jeg skulle ud og undersøge, hvilke standarder interne revisorer anvender, og så et forklarende element, hvor jeg forsøgte at undersøge, hvorfor intern revision er endt, hvor de er.

Undersøgelsens design

Til at besvare min problemstilling anvendte jeg en kvalitativ metode – interviews. Interviews er velegnet til at få en mere dybdegående viden om et emne, hvilket er nødvendigt for at afdække det mere forklarende element i problemformuleringen. Der blev udvalgt en række repræsentative respondenter ud fra et ønske om at kunne generalisere undersøgelsens resultat mest muligt. Jeg valgte derefter at basere mine interviews på de ledende medarbejdere – revisionscheferne. Dermed sikrede jeg mig også adgang til respondenter, der typisk har en del erfaring og viden omkring branchen og markedet.

Det teoretiske fundament

Den lette del af undersøgelsen var nu at gå ud og spørge respondenterne, hvilke standarder og risikostyringsmodeller de anvendte i deres afdelinger. Det svære var at finde en videnskabelig metode der kunne hjælpe med at forstå, hvorfor interne revisorer anvender præcist disse standarder og risikostyringsmodeller. Til at prøve at forstå respondenternes bevæggrunde anvendte jeg to forskellige teorier: professionsteori og institutionel teori.

Institutionel teori søger på forskellige måder at forklare de processer, der foregår i et organisatorisk felt. Den institutionelle teori er velegnet til at bidrage med forståelse for de processer, der foregår i intern revision, som organisatorisk felt, og pege på, hvilke kræfter der er formende for de tendenser, der er.

Professionsteori søger at forstå, hvordan en profession opstår, og hvordan en profession er positioneret i relation til andre professioner. I en analyse af dette er fokus på, hvem der giver retten til, og hvem der har retten til at udføre et stykke arbejde. Professionsteori er passende at bruge, da intern og ekstern revisions forhold til hinanden er så definerende for, hvordan intern revision i Danmark udføres. Professionsteori arbejder med begrebet jurisdiktion. Jurisdiktion dækker over en professions ret til et givent arbejdsområde.

Virksomhedscases	
Virksomhed	**Forkortelse**
Mindre pensionsselskab finansielt)	PEN
Forsikringsselskab(finansielt)	FORSIK
Servicevirksomhed	SERV
Stor bank(finansielt)	BANK
Passagertransport	TRAN
Stor offentlig tjeneste	OFT
Søtransport af gods	TRAN2

[1] International Professional Practices Framework, IPPF. Udgivet af IIA - https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx

Denne ret til et arbejdsområde kan være formet på forskellige måder alt efter professionens sammenspil med andre professioner. Dermed opstår der forskellige typer jurisdiktionsordninger mellem professioner. Arena & Jeppesens (2006) undersøgelse viste, at intern revision dengang på grund af den fremtrædende fokus på finansiel revision, var intellektuelt underlagt ekstern revision.

I en ordning efter intellektuel jurisdiktion er det ekstern revision, der sidder på vidensbasen. Vidensbasen er her den base, som giver de nødvendige arbejdsteknikker til at udføre intern revision. Intern revision er således i nogen grad afhængig af den vidensbase, som ekstern revision sidder på. En del af specialets arbejde gik derfor på at prøve at forstå, hvilket forhold der nu er mellem intern og ekstern revision, da dette kan have udslag i brugen af standarder og risikostyringsmodeller.

Resultater

Resultaterne af interviewene er videregivet i tabellen "Data" herunder. Dataene viser en generel tendens i retning af anvendelse af IPPF og COSO. Men når man dykker ned i de enkelte cases, er anvendelsen ikke nødvendigvis ens.

Den mest direkte implementering findes hos BANK og FORSIK. For revisionschefen i BANK er der ingen tvivl om, at man helt klart anvender IPPF og desuden anvendes standarder udarbejdet af ISACA ved IT revisioner. Men BANKs revisionschef pointerer også, at BANK i de lokale lande er nødt til at efterleve den lokale lovgivning. Derfor tegner der sig også et mere komplekst billede af, hvordan standarderne implementeres i det enkelte land. I FORSIK forklarer revisionschefen, at de kun anvender IPPF til revisionshandlinger og COSO til risiko, samt COBIT til IT-relateret revision.

Det interessante i FORSIK er, at det er moderselskabet i udlandet, der dikterer, at den interne revision skal være IPPF baseret. Dette resulterer i, at den danske del af FORSIK bliver underlagt IPPF. SERV har også en forholdsvis direkte implementering af IPPF's framework. Det interessante ved SERV er, at de ikke er en finansiel virksomhed, og som revisionschefen siger: *"Altså, vi har en lidt pragmatisk tilgang til det. Vi siger, vi tilstræber at efterleve IIA's standarder, men da de ressourcer vi har i en industrivirksomheds interne revision ikke er den sammen, som du ser i den finansielle sektor, så er der nok nogle ting, hvor vi siger: Hvis vi skal vælge, så er vi nok nødt til at vælge noget fra engang imellem."* SERV har derfor deres egen adoptering af IPPF, hvor de bruger de elementer, der giver mening for dem.

TRAN befinder sig i en overgangsfase. Hvor revisionschefen og hans interne revisionsafdeling før i tiden lavede finansiel revision efter ISA'erne, er TRAN nu i gang med at skifte fokus til operationel revision. I OFT fortæller revisionschefen, at de kører efter Rigsrevisionens standarder – GoR, og derigennem kommer der indirekte efterfølgelse af IPPF standarderne.

Data			
Forkortelse	**Standarder**	**Risikostyringsmodeller**	
PEN	Egne standarder og ISA	Efter bekendtgørelsen	
FORSIK	IIA	COSO	
SERV	IIA	Egne modeller	
BANK	IIA og ISACA	(COSO)	
TRAN	IIA og (ISA)	Egne modeller og (COSO)	
OFT	GoR – INTOSAI	Egne modeller og COSO	
TRAN2	IIA	COSO	
Forkortelse	**Revisionschefens tilknytning til professionel organisation**	**Revisionschefens uddannelsesbaggrund**	**Revisionschefens Erfaring**
PEN	IIA og FSR passiv	Stat.aut.	Ekstern Revision
FORSIK	IIA, meget aktiv	Cand.merc.aud, CIA	Intern Revision
SERV	IIA, aktiv	PhD Økonomistyring, CIA	Intern Revision
BANK	IIA, meget aktiv	Stat.aut., CIA	Ekstern Revision
TRAN	IIA, aktiv og FSR passiv	Stat.aut. CIA, CRA	Ekstern Revision
OFT	IIA, aktiv	Cand.merc.	Ekstern Revision
TRAN2	IIA, passiv	Cand.Econ	Intern

Revisionschefen i den interne revisionsenhed i TRAN2 fortæller, at de er placeret i den finansielle enhed i TRAN2, hvor de opererer med intern revision, med primært fokus på risikobaseret revision og "risk and control compliance" med COSO som risikomodel. Revisionschefen fra PEN forklarer, at han som den eneste person i den interne revision har en meget stor fokus på at være compliance ifht. bekendtgørelsen (for finansielle virksomheder). Derfor er det også her grundlaget til at foretage intern revision skal findes, og dette gøres konkret ved brug af egne modeller, som oftest tager udgangspunkt i ISA'erne.

Institutionel teori peger på begrebet dekoblingsstrategi som centralt i relation til de interne revisionsafdelingers valg af standard og risikostyringsmodel. Dekoblingsstrategi er, når virksomheder "siger" en ting udadtil, men i praksis gør noget andet. Her er valget af standarder og risikostyringsmodeller primært styret af virksomhedernes opfattelse af, hvad samfundet mener, er den mest legitime standard og risikostyringsmodel - en forklaring som interviewene understøtter. Der er nemlig tegn på, at intern revision er en del af virksomheders dekoblingsstrategi, og intern revision vil derfor vælge de standarder og risikostyringsmodeller, der udadtil giver virksomheden den højeste ceremonielle værdi. Dette virker til at være en forklaring, der generelt set er beskrivende for intern revisions valg af standarder og risikostyringsmodeller.

Det viser, at den dominerende IPPF og risikostyringsmodellen COSO er dem, som samfundet mener har den højeste ceremonielle værdi, og derfor vælger virksomheder, at interne revisioner bør bruge dem. Teorien om dekoblingsstrategi er også med til at forklare, hvorfor alle respondenterne giver udtryk for, at de foretager lokale tilpasninger af standarderne og risikostyringsmodellerne, da der nødvendigvis ikke er sammenhæng mellem, hvad samfundet mener, er den rigtige måde at arbejde på, og hvad virksomheden mener er den rigtige måde at arbejde på. Derfor vil virksomheder adoptere standarden udadtil, og indadtil bero på, at medarbejderne er fleksible og implementerer den effektivt - lokale adopteringer.

En anden interessant faktor er regulativ isomorfisme – dette er den formende kraft, som organisationer, underlagt samme regelsæt fra samfundet, er udsat for. Her vil reglerne typisk trække det organisatoriske felt over mod et ensartet svar, og dermed kommer virksomheder, der er underlagt samme pres, til at ligne hinanden. For finansielle virksomheder underlagt bekendtgørelsen og offentlige institutioner underlagt Rigsrevisionen, er regulativ isomorfisme sandsynligvis en formende kraft for feltet. Lige nu er det en proces, som for finansielle virksomheder peger mod en samling omkring IPPF og COSO.
Hvis man kigger på tabellen med data, ses det, at størstedelen af respondenterne har en baggrund og uddannelse inden for ekstern revision. Det siger noget om, at ekstern revision sider på vidensgrundlaget til finansiel revision. Et videnssystem, der kunne være medvirkende til at give intern revision som profession, kontrol over de instruktioner hvormed viden rationaliseres til arbejdshandlinger.

Intern revision tager dog noget af ejerskabet tilbage gennem IIA's CIA uddannelse. Men grundlæggende er der en begrænset adgang til de teknikker, der anvendes i praksis. Den tekniske kunnen, og legitimitet kommer derfor som udgangspunkt fra ekstern revision. Udslaget kan ses i anvendelsen af standarder og risikostyringsmodeller, hvor nogle af respondenterne stadig anvender ISA'er, og når der anvendes IPPF, udarbejder man lokale tilpasninger.

Det er dog på ingen måde entydigt, da mange af respondenterne i langt højere grad identificerer sig med IIA DK som professionel organisation end med FSR. Hvilket viser, at på trods af at de interne revisorer kommer fra ekstern revision, sker der en omskoling til intern revision, der involverer et skift til et videnssystem, som er mere styret af intern revision. Interne revisorers ret til at udøve jurisdiktion over et arbejdsområde, synes at være delt med ekstern revision, hvor graden af jurisdiktion er styret efter hvilke arenaer der kigges på. Jurisdiktionen til arbejdsområdet gennem retssystemet er i høj grad styret af ekstern revision, hvor jurisdiktionen til arbejdsområdet gennem arbejdspladsen er styret af intern revision.

Professionsteori påpeger, at en stærk professionel organisation er med til at styrke en jurisdiktion position: Foreningen af Interne Revisorer (IIA DK) er de interne revisorers brancheorganisation og dataene viser, at der er

stor forskel på det udbytte, de interne revisorer får af IIA DK, og hvor tilknyttet og aktive respondenterne er i IIA DK. Det giver et billede af en brancheorganisation med en vis gennemslagskraft og autoritet i den finansielle verden, men lille effekt for interne revisorer i ikke-finansielle virksomheder.

Professionsteori beskriver en situation, hvor niveauet af kompleksitet kan blive så højt, at selv om professionen har fuld jurisdiktion til arbejdsområdet, er den nødt til at inddrage andre professioner for at løse området. Et interessant perspektiv i denne forbindelse kommer fra revisionschefen i TRAN, der blev spurgt til om cand.merc.aud. er den typiske rekrutteringsbaggrund, hvortil svares: *"Ja det har hidtil været den traditionelle vej, men det bliver det ikke fremadrettet. Fordi vi netop nu favner meget bredere, så i dag er det ikke en betingelse. Det kan være lige så vigtigt, at du har noget procesviden, så din baggrund kunne godt være en eller form for økonom, ingeniør eller et eller andet, hvis vi er ude i et eller andet område, hvor vi siger, det er vigtigt, at vi har den her type af kompetencer. Jeg tror i vores afdeling, er vi måske lige lovligt små til, at vi kunne arbejde reelt med ingeniører som sådan."* Dette peger på, at operationel revision i en stor virksomhed har en så høj kompleksitet, at der er brug for andre kompetencer end dem som cand.merc.aud. besidder.

Ét der synes at være klart er, at intern revision ikke har fuld jurisdiktion over hele deres arbejdsområde, men omvendt deler de heller ikke det hele med ekstern revision. Noget kunne tyde på, at relationen mellem intern og ekstern revision er præget af, at ekstern revision har ejerskabet over vidensbasen til finansiel revision. Samtidig giver den eksterne revision plads til, at interne revisorer anvender deres teknikker til udøvelsen af intern revision. Dette tyder på, at forholdet er baseret på en intellektuel ordning – hvor ekstern revision tillader intern revision at anvende ekstern revisions vidensbase.

Men en sådan ordning vil logisk betyde, at brugen af eksterne teknikker er lig med anvendelsen af eksterne revisorers standarder og risikostyringsmodeller ved udførelsen af intern revision. Dette stemmer dog ikke overens med empirien fra casene, hvor IPPF er mest udbredt. Respondenter giver også udtryk for, at de har efteruddannet sig til intern revision og føler en større tilknytning til IIA DK end til FSR. Dermed genvinder de vidensbasen og kontrollen over denne og nærmer sig en fuld jurisdiktion over intern revision.

Konklusion

De indsamlede data har vist, at de interne revisorer primært benytter IPPF som standard til udførelse af intern revision. Fem ud af de syv respondenter anvender IPPF. En anvender ISA og en af de fem, der anvender IPPF, anvender stadig en smule ISA. Respondenten, som repræsenterer en offentlige institution, baserer deres revision på ISSAI. Alle respondenterne anvender i større eller mindre grad COSO som risikostyringsmodel, og alle respondenterne laver egne tilpasninger af standarderne og risikostyringsmodellerne.

Hvorfor?

Mit speciale har peget på en række forklaringer, der samlet kan bruges til at forstå, hvorfor interne revisioner i Danmark anvender de standarder og risikostyringsmodeller, som de gør. Det kan konkluderes, at interne revisionsafdelinger er en del af organisationers dekoblingsstrategi.

Deres valg af standarder og risikostyringsmodeller er derfor styret af graden af accept af standarden og risikostyringsmodellen i de institutionaliserede omgivelser. Det regulative isomorfiske pres påvirker i høj grad finansielle og offentlige interne revisionsafdelinger.

Dette resulterer i, at interne revisioner vil vælge de standarder og risikostyringsmodeller, som de trendsættende og dominerende organisationer anvender, og feltet vil derfor blive mere homogent over tid. En tendens, der peger på, at finansielle virksomheders interne revisionsafdelinger i højere og højere grad vælger IPPF og COSO som risikostyringsmodel.

I offentlige interne revisioner har det regulativ isomorfiske pres fra Rigsrevisionen ført til en høj grad af homogenitet og samling omkring ISSAI. Det er blevet vist, at intern revision befinder sig i en gråzone mellem at være underlagt en intellektuel jurisdiktion under ekstern revision og at være på vej til at have fuld jurisdiktion over deres arbejdsområde. Dette kan være udslagsgivende i den udbredte brug af IPPF i stedet for ISA.

Perspektiver

Af de udvalgte cases er tre i den finansielle sektor og repræsenterer tre typer setup. Den store finansielle virksomhed, den lille revision efter IPPF og den lille revision efter ISA. Jeg mener, at de udvalgte cases repræsenterer et meget bredt udsnit af de typiske interne revisionsafdelinger, der kan findes i den finansielle sektor. Den offentlige sektor er repræsenteret af en enkelt virksomhed.

Casen peger på, at den offentlige sektor i et vist omfang er udsat for regulativ isomorfisme, og som følge af dette må man forvente nogen grad af homogenitet de offentlige virksomheder imellem. Den industrielle sektor er repræsenteret af SERV, TRAN og TRAN2 og her findes tilsvaren-

de brug af IPPF, men da der findes rigtig mange forskellige brancher inden for den industrielle sektor, vil det være nødvendigt at se på flere cases i denne sektor, for at kunne sige noget mere generelt om den industrielle sektor.

Et uventet perspektiv, der blev fundet, var en indikation på, at den interne revisions arbejdsområde er ved at nå en kompleksitet, hvor en klassisk intern revisor ikke længere er kompetent nok til at revidere det givne område.

Dette er en tendens, der i forvejen har ramt den eksterne revision, hvor der i højere og højere grad er brug for at involvere andre professioner. For at kunne løfte revisioner, vil man se eksempler, hvor advokater og IT eksperter bliver inddraget i revisionsprocessen. At intern revision har rykket sig, siden Arena & Jeppesen lavede deres undersøgelse for mere end 10 år siden, synes klart.

Dengang var det finansiel revision og ISA'erne, der dominerede billedet, nu er det vendt, og operationel revision og IPPF vinder frem. For nyligt har Danske Bank skiftet fokus til operationel revision, og dette vil yderligere drive processen i den finansielle verden mod operationel revision efter IPPF. Det bliver spændende at se om dette vil påvirke de ikke-finansielle virksomheders interne revisioner.

Bibliografi

Arena, M. & Jeppesen, K.K. (2006), "Intern revision i danske virksomheder: Karakteristika og konsekvenser", INFO Foreningen af Interne Revisorer, no. 34, s. 12-16

Abbot, A. (1988). The System of Professions: AN ESSAY ON THE DIVISION OF EXPERT LABOR. University of Chicago Press.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational field. American Sociological Review, 48, s. 147-160.

Meyer, J. W., & Rowan, B. (September 1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. American Journal of Sociology, Vol. 83, No. 2, s. s. 340-363.

Nye medlemmer

Nye medlemmer i IIA fra 1.12.2016 – 28.03.2017

Arbejdernes Landsbank
Carina Enggaard

ATP
Anette Ganesalingam

EY
Christian Reimar
Emil Christian Rishøj Jensen
Anh Nguyen

Danske Bank
Klaus Kandborg
Thomas Corvinius Andersen
Deniz Demir
Peter Christian Lintrup
Michael Rasch

ISS
Pernille Wolf
Morten N. W. Heding

Novo Nordisk
Mikkel Skou Larsen
Faissoil Mbae

Nykredit
Anders Meincke
Christine Mønsted

PwC
Prit Singh
Tue Jagtfelt

Sydbank
Lars Hansen

Uddannelsesaktiviteter

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

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

Kurser og gå-hjem møder

Kursus for pengeinstitut- og realkreditrevisorer, 27.4.2017. Afholdes på Quality Hotel, Høje Taastrup.

Kursus for forsikringsrevisorer, 2.5.2017. Afholdes på Forsikringsakademiet, Rungsted Kyst.

IIA Årsmøde 2017, 31.5.2017-01.06.2017. Afholdes på Comwell Hotel, Aarhus.

IIA Learning Webinars

18. april 2017: Members-only Webinar: Auditing Security Monitoring (aka Watching the Watchers)

16. maj 2017: Members-only Webinar: A Blueprint: Strategizing Your Anti-fraud Approach

Tilgås via følgende link. Gå til "Sign in" i øverste højre hjørne. Tryk derefter på "Upcoming IIA Webinars" og "Register now". Kan du ikke huske dit kodeord til IIA Global/USA kan du klikke her.

"Bagsmækken"

Foreningens adresse

Foreningen af Interne Revisorer (IIA)
Att.: Vicerevisionschef Kim Stormly Hansen
Intern revision
Nykredit
Anker Heegaards Gade 4-6
1560 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.

Certificeringer

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

Heino Hansen, Internal Audit Manager, CIA, Nordea
☎ 31 18 38 01 ✉ heino.hansen@nordea.com

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

Foreningen af Interne Revisorers bestyrelse har følgende sammensætning:

Formand
Vicerevisionschef
Kim Stormly Hansen
Nykredit
☎ 44 55 93 17 ✉ ksh@nykredit.dk

Næstformand
Senior Vice President
Jesper Siddique Olsen
Danske Bank
☎ 45 12 76 58 ✉ jol@danskebank.dk

Kasserer
Koncernrevisionschef , CIA
Morten Bendtsen
PFA Pension
☎ 39 17 60 12 ✉ mob@pfa.dk

Sekretær
Senior Audit Manager, CIA, Afdelingsdirektør
Anette Kauffmann Laursen
Nordea
☎ 55 47 33 19 ✉ anette.laursen@nordea.com

Bestyrelsesmedlemmer
Regional Chief Auditor, CIA, CISA
Neil Jensen
RSA Scandinavia
☎ 40 42 64 26 ✉ njz@codan.dk

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

Koncernrevisionschef
Poul-Erik Winther,
Alm. Brand
☎ 45 47 78 97 ✉ abrpwe@almbrand.dk

Revisionschef, CIA, CISA
Birgitte Rousing Svenningsen
Europæiske Rejseforsikring
☎ 33 27 84 82 ✉ brs@europaeiske.dk

Executive Director, CIA, CRMA, CFE
Jesper Jæger Granstrøm
Ernst & Young P/S
☎ 25 29 48 45 ✉ jesper.j.granstrom@dk.ey.com

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