

INFO

Foreningen af Interne Revisorer

Nummer 64 | December 2016 | 21. årgang

Minitema:

- ***IIA udviklingsværktøjer***
- ***Korruption***

Intern Audit funktion

Er det det samme som intern revision?

Ny revisionsbekendtgørelse

Hvilke ændringer kommer der i år?

Think Outside the Box - Part 2 • IIA Global Conference

INFOs redaktion

Ansvarshavende redaktør

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

Øvrig redaktion

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

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

Revisionschef
Michael Ravbjerg Lundgaard
DSB
✉ 24 68 06 01 ✉ mrl@dsb.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 65 udkommer i april 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

Leder	3
Nyt fra bestyrelsen	4
Nyt fra redaktionen	5

Minitema: IIA udviklingsværktøjer

Internal Audit Ambition Model	7
Talent Management for a viable Internal Audit function	13
Webinars - En introduktion.....	17
Ekstern kvalitetssikring af intern revision.....	19
IIA Global Conference 2016	24
Global Council 2016 og ECIIA General Assembly 2016..	26

Minitema: Korruption

Korruption - moralsk fordærv, en omkostning for andre	29
Anti-korruptionslovgivning, tendenser og praksis	34
Sådan undgår du, at korruption bliver et problem	39
Hvorfor er fokus på korruption vigtig for Intern Revision?	42

Ny revisionsbekendtgørelse.....	46
IIA's standardpåtegning på årsregnskaber for finansielle virksomheder	48
Intern audit	49
Think Outside the Box! - How Creative & Unconventional Audit Analytics Can help you take your Audits to the "Next Level" (Part II)	54

Nye medlemmer	63
Uddannelsesaktiviteter	63
Bagsmækken	64

Besøg foreningens hjemmeside:

www.ii.dk

Leder



Morten Bendtsen, Koncernrevisionschef, CIA, PFA Pension

Kravene til os som interne revisorer er i stadig udvikling og forandring. Vi mødes med konkurrence fra andre "assurance" funktioner i de virksomheder vi reviderer og det bliver mere afgørende for vores rolle og berettigelse at vi er bevidste om vores evne til at skabe værdi og evne til at kommunikere hvordan vi passer ind sammen med Compliance, Risikostyring, Aktuarfunktion m.fl.

Det er væsentligt at bestyrelsen og direktionen forstår de forskellige roller og ikke oplever at det er et det samme og at alle løber efter den samme bold og på samme måde.

I dette nummer af Info bringer vi en artikel om den Interne Auditfunktion som er indført via Solvens II og reguleres gennem ledelsesbekendtgørelsen for forsikringsselskaber. Forvirringen er nu total. Vi har en ny funktion med et navn der er så tæt på Intern Revision man kan komme, men er det det samme? Det giver Lars Maagaard svaret på og han kommer også ind på hvorledes vi kan gøre brug af andre funktioners arbejde.

Netop emnet værdi og kommunikation af mål og ambition med Intern Revision giver Micheal Ravbjerg Lundgaard os et meget spændende input til. I hans artikel beskrives "Internal Audit Ambition Model". Modellen er et hjælpeværktøj og I har alle mulighed for at få adgang til modellen ved at sende en mail til IIA i Holland.

I forhold til vores daglige arbejde skal jeg meget opfordre jer alle til at støtte op om de to arbejdsgrupper bestyrelsen har nedsat for at styrke vores viden om virksomhedens samlede risikobilled og risici knyttet til it-anvendelsen. Formålet er at skabe en fælles platform og hjælpeværktøjer og dermed skabe en mere effektiv revision af disse områder.

Netop risici knyttet til it-anvendelsen er et væsentligt emne når vi som revisorer skal forholde os til virksomhedernes forretningsmodel og risici forbundet hermed. Vi skal ikke være blinde for at tidens agenda går mod øget anvendelse af teknologi både i forhold til distribution af produkter til kunder men også i forhold til processeer. I back-office funktioner vil manuelle processer og kontroller blive overtaget af fx robotter og meget af det vi reviderer i dag vil forsvinde og i stedet optræde i et digitalt univers. Det er afgørende vi alle sammen kommer med på det "tog".

Sidst men ikke mindst skal vi altid overveje om vi ser alle de væsentlige risici, som kan ryste vores virksomheder. Atea sagen har vist at korruption også findes i Danmark og kan have stor effekt på både medarbejdere, kunder og virksomheder. I dette nummer har vi korruption som miniteam. Dette nummer af INFO kommer godt omkring en række centrale forhold både strategiske og på det praktiske plan.

God læselyst og en god jul og et godt nytår til jer alle.



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".

Nyt fra bestyrelsen - årets strategi



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

Bestyrelsen afholdt strategidag i august. Strategien for året vil blive en kombination af nye tiltag og videreførelse af tidligere fokusområder. Overordnet er strategien at **"IIA DK vil styrke den uddannelsesmæssige, etiske og faglige udvikling inden for intern revision"**. Dette vil vi gøre gennem følgende fire områder:

- Center for uddannelse og certificering
- Forum for erfaringsudveksling
- Talerør over for IIA's interesserter
- Formidling og promovering af IIA-standarder.

Helt konkret vil vi sætte en række tiltag i gang og vi glæder os meget til at arbejde hermed og håber, at vores medlemmer vil finde tiltagene værdifulde, men også at vores medlemmer vil bidrage til, at vi i fællesskab sikrer, at intern revision bliver styrket.

Center for uddannelse og certificering

Baseret på de mange input vi har fået fra vores medlemmer og erfa-grupper vedrørende vores uddannelsesstilbud, vil vi lave en ny uddannelsesstrategi. Planen er, at uddannelsesudvalget vil afholde en strategidag, blandt andet med henblik på at vurdere en diversificering af uddannelsesudbudet og brug af medier. Vi vil i den forbindelse også anvende de mange tilbud, som IIA Global har.

Forum for erfaringsudveksling

Væsentlige elementer i erfaringsudvekslingen er dette blad og vores mange erfa-grupper. Vi synes dog, at der er områder, som ikke er dækket heraf. Det er vores indtryk, at der er flere interne revisorer, som sidder med de samme udfordringer, men hvor INFO og vores erfa-grupper ikke på tilstrækkelig vis giver hjælp til at løse udfordringerne. Det er for eksempel spørgsmålet om, hvorledes revision af teknologi hænger sammen med den øvrige revision. Udfordringen her bliver ikke mindre af, at IT revisionen i flere virksomheder udføres af ekstern revision og ikke af den interne revision. Et andet spørgsmål er, hvordan intern revision hænger sammen med virksomhedens generelle risikostyring. For at hjælpe vores

medlemmer med disse udfordringer, har vi besluttet at nedsætte to arbejdsgrupper:

- [Virksomhedens samlede risikobillede](#)
- [Risici knyttet til it-anvendelsen.](#)

Formålet med arbejdsgrupperne er at øge informationen om området og at skabe nogle hjælpeværktøjer, således at vi ikke hver især sidder med de samme udfordringer og ikke ved, hvorledes vi skal gibe dem an. I denne forbindelse har vi dog brug for hjælp fra nogle medlemmer, som har interesse for området og for at styrke foreningens tilbud. Så har du særlig interesse for enten "Virksomhedens samlede risikobillede" eller "Risici knyttet til it-anvendelsen" og har du lyst til at bruge lidt tid på at skabe noget til gavn for både dig selv og andre interne revisorer, vil vi meget gerne have, at du kontakter foreningens formand Kim Stormly Hansen på mail (ksh@nykredit.dk) og melder dig til arbejdet i arbejdsgrupperne. Planen er, at arbejdsgrupperne selv kommer med et oplæg til, hvad målet skal være. Planen er også, at arbejdsgrupperne nedlægges igen, når målet er nået. Så det er ikke en livstidsaktivitet. Vi vil oprette flere arbejdsgrupper hen over årene i takt med at nye behov og forslag opstår.

Talerør over for IIA's interesserter

Vi vil fortsætte vores gode samarbejde med Finanstilsynet og arbejdet i det rådgivende revisionsudvalg, samt komme med høringsvar, når dette er relevant. Vi vil blandt andet prøve at påvirke, at der fra Finanstilsynets side kommer en klar udmelding på snitfladen mellem 2. og 3. forsvarslinje og forventninger og krav til eksempelvis Compliances virkefelt og arbejde. I denne bredere sammenhæng og ikke udelukkende i relation til den finansielle sektor, vil vi arbejde på at arrangere informations-/uddannelsesdage for vores stakeholders. Endelig har vi besluttet at genindføre en prisopgave for cand.merc.aud.'ere, som skriver hovedopgave om intern revision.

Formidling og promovering af IIA-standarder

IIA-standarderne ligger os meget på sinde. Vi vil fortsætte med at bringe artikler i INFO om IIA-standarderne, og vi vil i den forbindelse prøve at gøre dem mere nærværende. Et eksempel herpå er artiklen i dette nummer af INFO om talentudvikling, og hvorledes Nordeas nye revisionschef Jamie Graham selv har praktiseret dette i sine tidlige funktioner. Vi vil også arbejde med IIA-standarderne i relation til vores hjemmeside og gå-hjem møder.

Alt i alt ser vi fra bestyrelsen frem til et fanstatisk år, hvor du som medlem forhåbentlig vil synes, at vi tilfører

dig værdi. Men hvor vi også kommer til at opleve, at mange medlemmer engagerer sig i foreningens arbejde med henblik på i fællesskab at styrke den uddannelsesmæssige, etiske og faglige udvikling inden for intern revision.

Nyt fra redaktionen



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

Det er med stor glæde, at jeg kan skrive, at vi har fået et nyt redaktionsmedlem. Monica Vestergaard Rasmussen fra Skatteministeriets koncernrevision har indvilget i at deltage i redaktionsarbejdet. Ud over at Monica repræsenterer den offentlige sektor, så sidder hun til daglig i Silkeborg. Som førstegenerationsindvander til Københavnsområdet er jeg meget stolt af, at det er lykkes at få et redaktionsmedlem fra Jylland. Monica har en baggrund som henholdsvis revisor og controller i forskellige selskaber. Jeg ser meget frem til samarbejdet med Monica.



December 31 is almost here.

Have you earned all the CPE credits you need to fulfill your certification requirements?

Don't wait! Earn Continuing Professional Education (CPE) credits by participating in The IIA's:

- Events • *Internal Auditor Magazine Quizzes*
- Conferences • And More

Ready to report?

Visit www.theiia.org/goto/CPE to report or for more information on CPE qualifying activities.

CPE reporting fees vary globally based upon membership status.

Individuals from IIA Institutes should contact their local representatives for their CPE reporting process and fees.



CCSA®

CFSA®

CGAP®

CRMA®



141728_81

Minitema: IIA udviklingsværktøjer



Hvilke produkter og værktøjer stiller IIA til rådighed?

Svarene er mange. I de næste fire artikler bliver der sat lys på nogle af IIAs nyttige udviklingsværktøjer. Internal Audit Ambition Model er en self-assessment model, som giver overblik over ambitioner, og hvor langt fra målet den interne revision er. Talent Management tager udgangspunkt i IIAs standard herom, men bringer også Nordeas nye revisionschefs praktiske erfaringer hermed. Webinars tilbydes online og er en nem måde at få viden om aktuelle emner og tendenser. Ekstern kvalitetssikring af intern revision beskriver en certificering, hvor en intern revisionsafdeling vurderes i forhold til IIA standarder.

God fornøjelse.

Internal Audit Ambition Model



Michael Ravbjerg Lundgaard, Revisionschef, DSB

Hvor ambitiøse er dine mål for den interne revisionsfunktion? Er målene defineret og afstemt med Revisionsudvalget eller den ledelse der refereres til? Er den interne revision compliant med kravene i IPPF (International Professional Practices Framework), og kan ekstern revision base sig på dit arbejde (ISA 610)?

Den hollandske søsterorganisation af IIA har udviklet en self-assessment model, som kan hjælpe dig på vej til at få overblik over og fastlægge, hvad dine og Revisionsudvalgets ambitioner er med intern revision, og hvor langt fra målet du er i dag.

Baggrund

I den hollandske udgave af "Anbefalinger om god selskabsledelse" er den interne revisionsfunktion tildelt en mere prominent position end tidligere. Desuden ses en bredere anerkendelse af den interne revisionsfunktion reflekteret mere eksplisit i lovgivningen om Solvens II og Basel III. Som konsekvens heraf, så IIA Holland et voksende behov for etablering af professionelle interne revisionsfunktioner og udviklingen af en Ambition model, som giver indsigt i, hvordan en intern revisionsfunktion gradvist kan vokse sig til at være compliant med IPPF standarderne og de eksterne revisorers ISA standarder.

Sammenligner vi med Danmark, så nyder den finansielle sektor qua revisionsbekendtgørelsen, Solvens II og Basel III reglerne, samme opbakning fra lovgivers side. Ser man på de seneste anbefalinger om "God selskabsledelse", synes opbakningen til etableringen af interne revisionsfunktioner i Danmark og den rolle de tiltænkes, mindre udtalt end i Holland. I de danske anbefalinger for God selskabsledelse 2013 anbefales det, at der nedsættes et revisionsudvalg, som årligt skal vurdere behovet for en intern revision. Som kommentar anføres, at alternativet til at etablere egen intern revision kan være at outsource

opgaven til en ekstern revisor. Det kan næppe være en tilsvarende anbefaling, som i den hollandske version giver IIA anledning til at udtale, at den interne revisionsfunktion er tildelt en mere "prominent position" end tidligere.

Så meget desto mere er der vel god grund til at se nærmere på den hollandske Ambition model, da den kan anvendes til at formulere den interne revisionsfunktions rolle, scope og ambitionsniveau i konsultation med Revisionsudvalget. Tillige kan modellen anvendes som et værktøj til at opbygge de ønskede kapaciteter i den interne revisionsfunktion, og øge opmærksomheden hos relevante stakeholdere omkring den interne revisionsfunktion og den interne revision som profession.

The Ambition Model kan således anvendes som instrument til både kommunikation og benchmarking for at øge kendskabet til og anerkendelsen af den interne revision som profession. Modellen kan tilgås fra to perspektiver:

- Som støtte til revisionschefens formulering af funktions opgaver og ønskede ambitionsniveau, herunder guide til evaluering af funktionen og opnåelsen af de med ledelsen aftalte udviklingsmål.
- Som informationskilde for Revisionsudvalget, og et brugbart hjælpeværktøj til at promovere den interne revisionsfunktions uafhængighed og præstationer og forøge det ønskede ambitionsniveau.

Modellens tilblivelse

IIA Holland har taget udgangspunkt i Internal Audit Capabilities Model udarbejdet for den offentlige sektor. Baggrunden herfor var, at denne model var internationalt valideret og afprøvet. Desuden var de udarbejdede guidelines tilstrækkeligt generelle til, at kunne anvendes i både den private og offentlige sektor. Endelig var modenhedsniveauerne i modellen i overensstemmelse med generelt accepterede modeller såsom the Capability Maturity Model Integration.

Dernæst udviklede arbejdsgruppen et modelbaseret spørgeskema, som kunne anvendes som et self-assessment værktøj, og valideres af en ekstern part eller Revisionsudvalget. Afslutningsvis blev der indarbejdet et link mellem modellen, IPPF standarderne og ISA 610.

Hvad er Internal Audit Ambition Model (IA AM) ?

IA AM er et self-assessment værktøj, som tilvejebringer ambitionsniveauer og best practice, der kan fungere som vejledning til den revisionsansvarlige, som vil mere end blot at overholde professionelle standarder. IA AM hjælper den revisionsansvarlige til at formulere strategiske mål, evaluere den nuværende revisionsfunktion og defi-

nere vej og retning for at opnå de fastlagte mål. Modellen kan tillige hjælpe Revisionsudvalget med at beslutte, hvilke aspekter der skal tages i betragtning, når de skal vurdere den interne revisionsfunktions mandat og ambitionsniveau. Således kan IA AM anvise de skridt, der skal tages for at udvikle den interne revisionsfunktion fra den mindre etablerede enhed til den stærke, effektive funktion med de kapaciteter, som man typisk ser hos en mere moden og kompleks organisation.

IA AM er med andre ord:

- **Et kommunikationsværktøj** – et grundlag for at kommunikere hvad der menes med en effektiv intern revision, og hvordan den kan betjene en organisation og dens stakeholdere, og til overfor beslutningstagere, at advokere for vigtigheden af en intern revision.
- **Et framework til vurdering** – et framework til, som en self-assessment, at vurdere den interne revisions kapacitet holdt op imod de krav der stilles i internationale standarder og best practice.

- **En køreplan til forbedringer** – en køreplan til at opnå yderligere forbedringer og professionalisering af den interne revisionsfunktion.

IA AM er et værktøj, som organisationen kan anvende til at:

- Beslutte hvad kravene til intern revision skal være i forhold til organisationens beskaffenhed, kompleksitet og associerede risici i forhold til dens aktiviteter.
- Vurdere den nuværende interne revisions kapaciteter i forhold til behov og krav.
- Identificere signifikante gab mellem behov/krav og eksisterende kapaciteter og arbejde hen imod at udvikle et passende niveau for intern revisions kapacitet.

Strukturen i IA AM

Modellen (se uddrag i **Tabel 1**) er opbygget efter et byggeklodssystem bestående af:

1. **Temaer:** Seks temaer som definerer den interne revisionsfunktion.

Tabel 1: Uddrag af strukturen i byggeklodsmodellen

Theme	Sub theme	Topic
Services and Role of Internal Auditing	Assurance services	Role and authority Governance and Risk Management Strategy Soft Controls
	Advisory services	Scope
Professional Practices	Audit plan	Audit universe and scope Periodicity of evaluating the plan Prioritization and approval of the plan Resource planning Follow up monitoring
	Quality Assurance	Compliance with IPPF Audit procedures Performing the audit – Planning Performing the audit – Fieldwork Communicating audit results Performing the audit: Data analysis Quality Management reviews Advisory Services
Performance Management and Accountability	Internal Audit Business Plan	Scope Resourcing Budget Approval
	Reporting	Measures Audience Process

2. **Ambitionsniveauer:** Modellen illustrerer de moden-hedssstadier som revisionsfunktionen kan udvikle sig igennem, mens den definerer, implementerer, måler, kontrollerer og forbedrer sine processer og praksis.
3. **Undertemaer og emner:** For yderligere at detaljere og tydeliggøre de specifikke skridt som revisionsfunktionen kan tage for at komme til næste stadie, er de seks temaer opdelt i 11 undertemaer og 39 emner (topics).
4. **Essentielle aktiviteter:** De aktiviteter der er påkrævet at udføre er defineret for hver af de 39 emner, og kaldes essentielle aktiviteter.

Seks temaer

Services and Role of Internal Auditing

Intern revisions rolle og opgaver kan afhænge af organisationens behov, funktionens autoritet, scope og kapacitet. Revisionens fokus kan således variere.

I det meget smalle niveau, omfattes test af individuelle transaktioner, compliance testing i forhold til kontrakter, politikker, lovgivning. I det bredeste niveau er der fokus på organisationens governance aktiviteter for at under-

støtte, at organisationen når sine overordnede målsætninger og prioriterede mål, overholder etiske kodeks mm.

Professional Practices

Afspejler politikker, processer og den praksis, som sætter revisionsfunktionen i stand til at fungere effektivt og professionelt. Det inkluderer udviklingen og vedligeholdelsen af kvalitetssikring og programmer for forbedringer, som omfatter alle dele af intern revisions aktiviteter.

Performance Management and Accountability

Refererer til de informationer der er nødvendige for at lede, udføre og kontrollere den interne revisionsfunktions aktiviteter og stå til ansvar for funktionens præstationer og resultater.

People Management

Processen med at skabe et arbejdsmiljø som gør personerne i stand til at præstere bedst muligt. Omfatter tillige aktiviteter med at opbygge effektive teams for at tilvejebringe forbedringer og fremskridt via træning og udvikling.

Tabel 2: Uddrag af modellen (lodret: temaer og undertemaer) (vandret: skalaen for ambitionsniveau)

Theme	Subtheme	1 - Initial	2 - Infrastructure	3 - Integrated	4 - Managed	5 - Optimizing
Services and Role of Internal Auditing	Assurance services	Ad hoc services Isolated single audits or reviews of documents and transactions for accuracy and compliance.	Compliance auditing Carry out an audit of conformity and adherence of a particular area, process, or system to policies, plans, procedures, laws, regulations, contracts, or other requirements that govern the conduct of the area, process, or system subject to audit.	Performance auditing Assess and report on the effectiveness of activities or programs; or conduct engagements on governance, risk management, and control. Performance auditing covers the full spectrum of operating and business processes, the associated management controls, and the results achieved.	Performance auditing on a continuous basis Perform audit-related activities, such as control and risk assessments, on a continuous basis. Continuous auditing and reporting refers to the real-time or near real-time capability for (financial) information to be checked and shared. Technology plays a key role in continuous audit activities such as the use of process mining. Performance auditing on efficiency Assess and report on the efficiency and economy of operations of activities or programs; or conduct engagements on governance, risk management, and control.	Overall assurance on governance, risk management, and control Conduct sufficient work to provide an opinion on the overall adequacy and effectiveness of the organization's governance, risk management, and control processes. The IA activity has coordinated its audit services to be sufficiently comprehensive that it can provide reasonable assurance at a corporate level that these processes are adequate and functioning as intended to meet the organization's objectives.
Professional Practices	Audit plan	Ad hoc planning Internal audit activities are performed on an ad hoc basis.	Audit plan based on management/stakeholder priorities Develop periodic (annual or multiyear) plans for which audits and/or other services will be provided, based on consultations with management and/or other stakeholders.	Risk-based audit plans Systematically assess risks and focus the priorities of the IA activity's periodic audit and services plan on risk exposures throughout the organization.	Audit plan leverages organization's management of risk Link the IA activity's periodic audit and services plan with the organization's enterprise risk management strategies and practices. Enterprise risk management strategies and practices refers to formal and documented processes put in place by the organization to identify risks, and manage those risks within its risk appetite, thus providing reasonable assurance that the organization's objectives will be achieved.	Strategic Internal audit planning Understand the organization's strategic directions and emerging issues and risks. Anticipate future needs by changing the IA activity's skill sets and audit services.

Organizational Relationships and Culture

Refererer til organisationsstrukturer både internt i revisionsfunktionen som eksternt i den organisation, som revisionsfunktionen er en del af. Herunder revisionschefens relationer til ledelsen og mulighederne for at rådgive og influere på topniveau.

Governance Structures

Refererer til politikker og processer der er etableret for at sikre den nødvendige autoritet, støtte og ressourcer til den interne revisionsfunktion, for at den kan udføre sine pligter og bidrage til dens effektivitet og uafhængighed.

Fem ambitionsniveauer

Hvert af de stadier man skal igennem i modningen af revisionsfunktionen danner basis for at løfte sig til næste ambitionsniveau. Modellen arbejder ud fra en præmis om, at processen skal være stabil, før den kan forbedres. Hvert niveau beskriver karakteristika og kapaciteter, der skal være til stede i revisionsfunktionen på det pågældende ambitionsniveau. I takt med at størrelsen eller kompleksiteten af organisationen øges, eller risiciene associeret til dens aktiviteter øges, så øges kravene ligeledes til den interne revisions kapacitet. Modellen er en køreplan til at skabe kontinuerlige forbedringer. Afhængig af organisationen og ambitionerne kan man vælge at forblive på et givet ambitionsniveau og stadig repræsentere best practice på dette niveau - se **Tabel 2** på foregående side.

De fem ambitionsniveauer er:

1. **Initial** – intern revision udføres ad hoc eller ustyrket, der er få definerede processer og de udføres inkonsistent. Revisionshandlingerne er formentlig begrænset til test af transaktioner og basis compliance testing. Der er ikke etableret en professionel praksis, udover den som stilles til rådighed af anerkendte fagorganisationer.
2. **Infrastructure** – det primære mål er, at revisionsfunktionen arbejder efter en basisproces og praksis. Der er udarbejdet en funktionsbeskrivelse, der omfatter formål, autoritet og ansvar. Der udføres primært traditionel compliancerevision, men handlingerne kan tillige omfatte finansiel revision og system-, samt procesrevisioner. Der rekrutteres revisorer med de nødvendige kompetencer til at udføre arbejdet, men man baserer sig fortsat på, at den enkelte selv tager ansvar for sin professionelle udvikling. Der er udviklet et framework, som inkluderer politikker, processer og procedurer for at sikre konsistens i arbejdets udførelse, men der er ikke udarbejdet et fuldstændigt kvalitetssikringsprogram.
3. **Integrated** – på dette niveau er de relevante interne politikker, processer og procedurer defineret, doku-

menteret og integreret i hinanden og i organisationens infrastruktur. Der fokuseres på enhedens kapacitet, organisatorisk uafhængighed og personlig objektivitet. Funktionen udvikler sig fra at udføre traditionel intern revision til at være en integreret team spiller. Funktionen udvikler værdiskabende aktiviteter, som hjælper organisationen med at håndtere sine risici og drage fordel af revisors anførte muligheder for forbedringer. Revisionsfunktionen er opmærksom overfor andre emner såsom strategi og soft controls (tone at the top, leadership, ethical climate m.m.) og kan i varierende omfang supportere ledelsens behov. Ligeledes udfører funktionen rådgivning i form af guidance og forslag til ledelsen. Der er iværksat trænings- og udviklingsplaner for funktionens ansatte, ligesom de opfordres til at deltage i faglige foraer. På dette niveau overholder revisionsfunktionen de internationale kvalitetsstandarder (IPPF) og ekstern revision bør kunne basere deres arbejde herpå jf. ISA 610.

4. **Managed** – Revisionsfunktionen er en integreret og kritisk del af organisationens governancestruktur. Revisionschefen er positioneret, så han både formelt og uformelt rådgiver om strategiske forhold og kan influere bestyrelsen og eventuelle udvalg. Revisionschefen opretholder og udvikler effektive relationer til ledelsen og nøgle-stakeholdere for at sikre, at deres behov og forventninger er på linje med de ydelser, som revisionsfunktionen udfører. Bestyrelsens og ledelsens ord og handlinger demonstrerer fuld accept og støtte til revisionsfunktionen. Den periodisk fastlagte revisionsplan inddrager organisationens håndtering af risici. Organisationen og revisionsfunktionen forfølger en fælles strategi om at integrere lederudviklingen, så den omfatter træning og erfaring opnået hos revisionsfunktionen og omvendt. Revisionsfunktionen udfører nu også eksempelvis dataanalyse og proces mining i forbindelse med arbejdet med at vurdere effektiviteten i processer. Specifikke strategiske risici revideres ligesom effektiviteten af soft controls.
5. **Optimizing** – En revisionsfunktion på niveau 5 er karakteriseret som en lærende organisation med kontinuerlige procesforbedringer og innovation. Forandringerne i det eksterne miljø monitoreres, og informationer inde- og udefra organisationen anvendes til at raffinere fremgangsmåder og til at vurdere governance, risk management og kontroller. Funktionen rådgiver om nye trends, og bidrager til organisationens læring og forbedringer samt fremmer udviklingen af innovative forretningsprocedurer og processer med sigte på, at organisationen når sine strategiske målsætninger. Revisionsfunktionen forstår organisationens strategiske retning og de spirende risici og udforandringer. Funktionen udvikler sine kvalifikationer og forretningsbehov, herunder arbejdsstyrkens kapacitet

og færdigheder, risikovurderinger, og processen som sikrer, at de kan møde organisationens potentielle fremtidige behov.

I **Tabel 3** ses et udklip fra modellen med et eksempel på spørgsmålene i self-assessment skemaet. Det vedrører kvaliteten i udførelsen af revisionsarbejdet (Tema: Professional practices, Undertema: Quality assurance, Topic: Performing the audit Fieldwork). De enkelte niveauer er udtryk for modenheden/ambitionen. I Niveau 1 udføres revisionen med støtte i specifikke procedurer, og arbejdet dokumenteres. I næste niveau (2) udføres specifikke tests eller en metodisk revision for at opnå bevis for revisionsmålet. Der udarbejdes specifikke konklusioner og anbefalinger, og der opnås en overordnet revisionsoverbevisning og konklusion på revisionen. I niveau 3 er revisionen udført på baggrund af en risikobaseret revisionsplan.

Der er foretaget gennemgang af governancestruktur, risikostyring og kontroller i et tilstrækkeligt omfang til, at revisionen kan afgive en konklusion/erklæring. Som det tillige ses, er det først i niveau 3, at der er referencer til relevante IPPF-standarder.

Dashboard

Efter udfyldelsen af samtlige spørgsmål i Ambition modellen får man i et dashboard grafisk illustreret (se **Figur 1** på næste side), hvad besvarelserne har resulteret i. Målepunkterne er de 6 temaer, og det illustreres, hvilket niveau afdelingen aktuelt befinner sig på, og hvad ambitionsniveauet er.

Tillige er niveau 3 ambitionsniveauet markeret, da dette tilsvarer, at funktionen opfylder kravene i IPPF-

standarderne og ISA 610. Illustrationen giver et hurtigt og visuelt effektivt overblik over, hvor stort gabet er imellem det aktuelle niveau og ambitionsniveauet.

Praktisk anvendelse af IA AM

Vær opmærksom på følgende når du arbejder med modellen:

- Det kræver professionel dømmekraft at anvende og fortolke modellen.
- Det er grundtanken, at en proces eller praksis ikke kan forbedres, før den fungerer som en stabil proces.
- IA AM er en ambitionsmodel. Hvis revisionschefen i samarbejde med Revisionsudvalget fastsætter ambitionsniveauet til niveau 3, så har man aktivt valgt ikke at gå efter et højere niveau, men kan i stedet gå efter best practise på niveau 3.
- Modellen er primært tænkt som en self-assessment øvelse, der kan anvendes til at skabe kontinuerlige forbedringer.

Jeg har i forbindelse med udarbejdelsen af denne artikel gennemgået og besvaret spørgeskemaet og fået resultatet ud på et dashboard. Det er min oplevelse, at Ambition modellen i al væsentlighed kan anvendes på danske forhold, og derfor vil være en relevant øvelse at gennemgå for IIA Danmarks revisionschefer og ledende medarbejdere. Der er meget inspiration at hente i modellens enkelte spørgsmål, og byggeklodsmodellen fungerer godt. Man får både et overblik og et ganske nuanceret inblik i, hvor ens egen revisionsfunktion befinder sig, hvor man gerne vil flytte den hen, hvor lang vejen er dertil, og hvilke udviklingsstadier man skal igennem for at nå ambitionen.

Modellen synes at være et godt værktøj til både at understøtte revisionschefen i at tilrettelægge planen for den

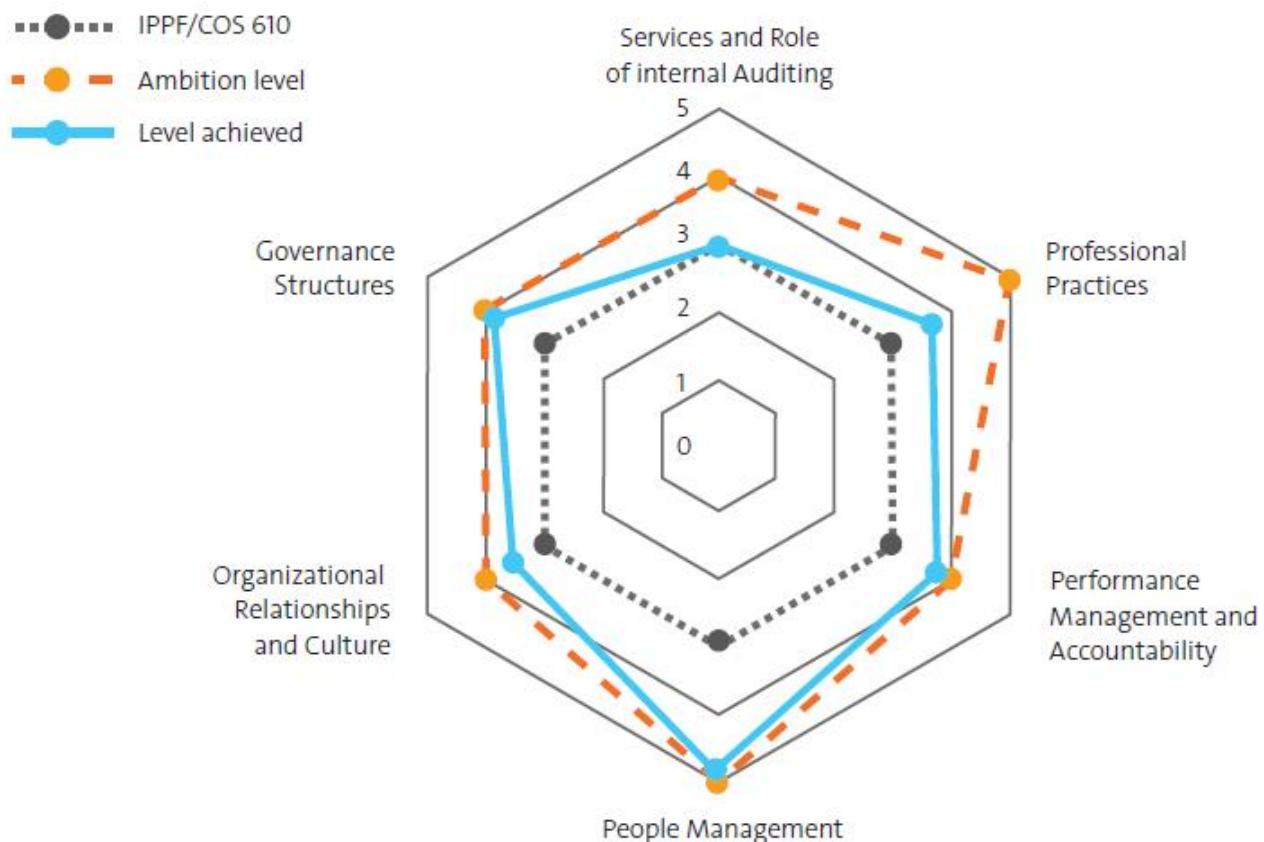
Tabel 3: Eksempel på spørgsmålene i self-assessment skemaet

		Theme	Subtheme	Topic	1 - Initial	IPPF	2 - Infrastructure	IPPF	3 - Integrated	IPPF	4 - Managed	IPPF	5 - Optimized	Dashboard	IPPF / ISA 610	
Professional practices	Quality assurance	Performing the audit - Fieldwork		<ul style="list-style-type: none"> • Perform the audit engagement: - Apply specific audit procedures. - Document the procedures performed and their results. - Evaluate the information obtained. - Draw specific conclusions and develop recommendations. - Review 	N	<ul style="list-style-type: none"> • Perform the audit engagement: - Conduct specific audit tests or methodologies that are relevant to achieve the audit objectives. - Draw specific conclusions and develop recommendations. - Provide overall assurance and/or conclusions on the results of the audit engagement. 	N	<ul style="list-style-type: none"> • In accordance with its risk-based audit plan, review sufficient elements of the governance, risk management, and control processes to express an opinion on the whole scope. 	2300 2310 2320 2330 2240 2340 2330 A1	<ul style="list-style-type: none"> • Perform and document thorough root cause analyses (process, system, people) of any deviations • Perform trend analyses of any deviations from previous/similar audits to identify 	N	No additional essential activities defined yet	N	3	4	2300 2310 2320 2330 2240 2340 2330 A1 A.11

interne revision, tage drøftelsen med Revisionsudvalget om, hvilket ambitionsniveau der skal arbejdes hen imod, samt hvilke fordele dette kan tilføre for organisationen. Desuden kan værktøjet bruges til bedre at kommunikere med stakeholderne om, hvad Intern revision kan bidrage med og dermed, hvilken værdi det kan tilføre virksomhederne at etablere og fastholde interne revisionsfunktioner. Du kan modtage et link til download af modellen ved at sende en mail til ambition@iai.nl.

Ovenstående artikel er skrevet med udgangspunkt i en publikation fra IIA Holland, som kan downloades fra https://www.nba.nl/Documents/voor-leden/LIO/Leeswijzer_Internal_Audit_Ambition_Model.pdf

Figur 1: Eksempel på Dashboard



Talent Management for a viable Internal Audit function



Vanita Shukla Hork, CIA, Senior Internal Auditor, Nordea

Talent management (TM) is probably not a term most people associate with an Internal Audit function. However, TM is key in enabling the Internal Audit function (IA) to live up to the IPPF's Standards on *Proficiency and Due Professional Care*, while also ensuring a viable IA capable of continuously delivering value to the business. In addition, lack of TM can lead to running significant audit risk, both at the audit plan and audit engagement levels.

The IIA have published a Practice Guide (PG) or Supplemental Guidance on Talent Management¹ that describes what TM entails. The intention of this article is to share some of the important and also more unusual points in the PG. In order to give the reader some insights on using TM in practice, Nordea's new CAE, Jamie Graham has shared some of his views on TM and also his ideas for TM in Nordea Group Internal Audit going forward.

Why Talent Management?

The PG defines TM as "recruiting, developing, motivating, and retaining competent team members".

TM is important for IA's ability to address high-priority risks and drive business value, and is not just a matter of having the right staff size but also the right talent mix. The IA needs to attract and retain team members who not only understand but are also able to *anticipate* the rapidly changing business (and regulatory) environment.

Professional development also plays an important role in TM, and internal auditors should share responsibility for their professional development with IA.

So what has TM to do with audit risk? With inadequate TM the IA runs a risk of having insufficient resources to deliver on the audit plan agreed to by the board, insufficient skills to perform the audit engagement with the necessary level of proficiency and due professional care and, finally, inability to conform with relevant IPPF Standards.

Relevant IPPF Standards

TM is primarily related to the 1200-series of the Standards:

1200 – Proficiency and Due Professional Care

Engagements must be performed with proficiency and due professional care.

1210 – Proficiency

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

1220 – Due Professional Care

Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility.

1230 – Continuing Professional Development

Internal auditors must enhance their knowledge, skills, and other competencies through continuing professional development.

These Attribute Standards are supplemented by Implementation Standards specific to assurance and consulting engagements, respectively. In addition, the following Standards are relevant, underscoring the key role that the CAE plays for TM:

1300 – Quality Assurance and Improvement Program

The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

2030 – Resource Management

The chief audit executive must ensure that internal audit resources are appropriate, sufficient, and effectively deployed to achieve the approved plan.

Understanding stakeholders' needs and expectations – the starting point

As indicated above, the CAE is responsible for a successful TM program, and he or she needs to first understand stakeholder needs and expectations before recruiting tal-

¹ Talent Management - Recruiting, Developing, Motivating, and Retaining Great Team Members, The Institute of Internal Auditors, Inc. (IIA), Dec. 2015

ent. (Note that the term *talent* in this context applies to all team members and not just potential leaders).

Stakeholder needs and expectations of IA are changing, and this requires IA to focus not only on traditional compliance and controls evaluation, but to take on a more strategic role in the organization. Recall that the UK Code recommends that IA challenges Executive Management to improve the effectiveness of governance, risk management and internal controls. For this to happen, internal auditors need to demonstrate competencies such as analytical or critical thinking as well as communication skills. IA needs people who can operate at all levels and impact the risk culture and control environment of the organization.

This, in turn, will require recruiting from a wider and more diverse base than previously.

TM is not a one-off exercise, but should be a structured and systematic process involving the following steps:

1. Assess stakeholder needs and expectations
2. Develop an audit plan to meet stakeholder needs and expectations, with consideration for organizational objectives, strategies and risks
3. Leverage the Global Internal Audit Competency Framework (Competency Framework)² to identify competencies required to execute the audit plan
4. Perform a competency gap analysis
5. Develop a talent management strategy
6. Periodically reassess internal audit's collective competencies and address key gaps.

There are several important points to note here. Firstly, assessing the needs and expectations of primary stakeholders is critical in defining IA's organizational structure, deliverables, working practices, communication protocols, and resourcing model. Secondly, the audit plan drives the need for talent and competencies, and not the other way around. That is, the audit plan includes what *should* be audited and not what can be audited. In determining the need for talent, the CAE needs to take the long view, both by considering the organization's strategic plans and assessing IA's future role in it. Finally, TM requires the CAE to develop a *strategy* to cover the competency gaps identified. To best serve IA's long term interests, core competencies should be acquired through hiring and pro-

fessional development. Ad hoc competencies for specific engagements could be acquired through alternative strategies such as rotational or guest auditor programs or co-sourcing.

Recruiting talent – consider new and alternative approaches

Recruiting talent involves both internal and external recruitment, and each resourcing option involves pros and cons to consider carefully. Recruitment involves not only the CAE but also IA managers, and recruiting should be carefully coordinated with the organization's HR function.

There are several ways to recruit *internally* in the organization:

Full-time permanent recruitment: This is the more common approach. It should be noted that while internal recruits bring a high level of organizational awareness and strong business knowledge to IA, they need to be trained in core audit skills. Also, impaired objectivity is a potential concern to be mitigated.

Rotational recruitment: This is less traditional and includes both outbound and inbound rotational programs (rotation, as the name implies, is not permanent but time-limited).

Outbound rotation rotates internal auditors out into the business, thereby enhancing their business knowledge of functional areas. *Inbound* rotation rotates talent from other business units into IA, giving them the opportunity to learn about governance, risk management and internal controls.

Rotation facilitates sharing of best practices, and potentially increases awareness of internal controls and the IA function among business staff. However, inbound rotation requires careful planning from IA, including selection of suitable candidates, addressing potential impairment of individual objectivity, providing audit skills training and securing commitment from the business to avoid possible disruption of career development paths.

Guest auditor program: Perhaps yet another less common approach, to fill competency gaps in specific audit engagements. Since this is a short-term commitment, it might be a more attractive option for sourcing subject matter expertise for a unique IA assignment, and it also facilitates knowledge sharing within the organization.

The PG also elaborates on the other main options for recruitment: External recruitment, co-sourcing and outsourcing. These options also require careful planning and

² The IIA's Global Internal Audit Competency Framework, The Institute of Internal Auditors, Inc. (IIA), 2013.

consideration from the IA function. For example, external recruitment requires clearly defined job descriptions and baseline criteria in order to attract and select the right candidates. It is important that potential hires not only have the requisite competencies but are also aligned with the values of the new organization. Finally, external recruits must be properly onboarded and trained to become familiar with the new organization's culture, processes, regulatory requirements and dynamics.

Developing, motivating and retaining talent - acknowledge the individual

Developing and motivating IA staff will ultimately also contribute to retaining high-performing team members, and both the CAE and IA managers play an important role here. The key is to remember that one size does not fit all. There are different ways in which IA can develop its staff:

Professional development plans: These should be individual plans, and require IA staff members to take ownership for their own professional development. A plan may support quite different career paths, such as career internal auditor, business operations (e.g. becoming line managers), or a rotation through IA may be a part of the organization's executive leadership development program.

The PG recommends that individual development plans include a path toward certification so that collectively, IA staff certifications form a base level of qualifications for the IA department.

Development practices should be customized based on generational differences, professional goals, position, experience and seniority. Professional development plans should be reviewed and updated as necessary.

Training and continuing education: There are several options available, such as on-the-job training, classroom training, e-learning and reading or writing articles for professional publications. IA managers should consider the needs of the individual as well as the IA function, and the best results are generally achieved through a combination of activities.

Mentoring: A mentoring program can be key to developing talent and should be considered not only for new hires but also for more experienced staff. A mentoring program should be informal, and it is best if the mentor is not the mentee's supervisor.

Succession plan: Succession planning should start well in advance of any potential succession event. Succession

plans should identify potential candidates for existing positions, taking into consideration the needs of the organization and the candidates' career goals, competencies and potential for development.

Just like professional development plans, potential motivators are also individual in nature. However, challenging work, career opportunities, quality of the work environment and recognition, rather than compensation, are considered leading drivers of staff retention.

In addition, rewards, flexible working practices and work-life balance can potentially help in retaining talent. The PG describes these options in some detail. It is worth noting that the PG points towards helping staff members find *meaning* in their work and establishing a connection to it, and effort should be made to ensure that the work is aligned with employees' expectations and needs.

Talent Management in Nordea

Jamie Graham joined Nordea as the new CAE in August 2016. Jamie comes from Barclays, where he was Regional Head of Audit, Asia. Here are some of his views on TM as the CAE.

Jamie Graham, what is the role of TM in a modern IA function?

- I am a firm believer that an IA department is nothing without its people. Recruiting and retaining the best people should always be the top priority of any CAE. If you have the right people, who understand the business, have great interpersonal skills and can deliver a quality audit output, then you will have an effective and impactful audit department. As such, I think it's impossible to over-state the importance of having an effective TM program. While it's up to an individual to actively consider their own development, too often we don't spend enough time discussing with our staff how they want to progress in their career and opening up the doors to help them get there.

How do you view the role of the CAE in TM?

- The CAE sets the tone of the department. It is important that the CAE prioritizes TM above other activities, ensuring staff have the time and the tools to focus on their personal development. In Nordea's Group Internal Audit (GIA), for example, we are introducing personalized development plans for all staff. These are designed to structure learning and development to help everyone reach their full potential, and to provoke more thought from our staff on what their future career goals might be, whether that's in or outside of the audit department.

IA managers also play an important role in motivating and retaining talent. What leadership and management qualities do you look for as the CAE?

- Authentic leadership. The most important leadership quality, in my view, is the ability to be open and honest, both with yourself and others. The best leaders are those that feel comfortable with themselves and know their own limits. In the context of TM, those with an authentic leadership style are likely to connect best, on a personal level, with their team, and have the most meaningful developmental conversations with their staff. The ability to connect and empathize with your team is, for me, a critical skill in managing talent.

What role do staff auditors play, and how do IA team members contribute to the success of TM?

- Everybody has a role in TM and everyone has a role in encouraging learning and development. It's important to take a proactive approach to your own development, whether you are a staff auditor or the CAE. It's also important to recognize that in many cases we learn from our peers. Although you may be at a more 'junior' corporate grade in an organization, that doesn't mean you do not have valuable skills and experiences to share with your colleagues. In this way, peer-to-peer learning is also a great way to help everyone develop.

What is your experience with less traditional recruitment practices such as rotational and guest auditor programs?

- I am a huge fan of rotations, secondments and guest auditor programs. These provide not only great development opportunities for staff, but also can fill important skills gaps across the company. Having experts from the business provide advice on our audits (assuming there are no immediate independence-related conflicts), can help ensure that the audit has the right focus, and at the same time it allows business staff to more fully understand the audit process. Conversely, a secondment into the business for an auditor can be a great opportunity to gain some real commercial exposure and to help the business become more control-focused.

Flexible work practices and work-life balance are acknowledged as important motivators. How do you see this as being compatible with a career in IA?

- One of the great benefits of working in IA is flexibility. We are fortunate enough to have roles with a high degree of freedom as to how and where we spend our time. As a consequence, adopting more flexible work practices (including working from home), are practices that we can easily adopt in IA. I think a very im-

portant aspect of TM is recognizing that people may have different priorities at different stages of their lives. There will be times when people are very keen for new challenges and more responsibility, and other points in their lives (perhaps as a new parent or while caring for a sick relative), where continuing to perform effectively in their current role will be enough. Providing a framework which allows people to grow and develop at a more personal pace, is an important aspect of TM.

What are your current ideas for TM in Nordea Group Internal Audit?

- All of the things I've mentioned! At the heart of TM is a strong focus on individual development. Understanding where people want to get to in their careers, what experiences matter to them most, and how Nordea can help them to get there.

What is the key to successful TM in practice, and what advice would you give other CAEs embarking on a TM program?

- Know Your People (KYP)! Take the time to know everyone in your team. Too often we assume we know what people want from their careers - if we take the time to really ask them, we may find the reality is quite different. So, ask them, now, before it's too late...



Webinars - En introduktion



Kim Nehls, Intern Revisor, DSB

Indledning

Intern Revisions virke har de senere år undergået markante forandringer. Eksempelvis er omfanget af den operationelle revision blevet udvidet i en lang række virksomheder. Derudover tilstræber flere Interne Revisionsafdelinger, såvel nationalt som internationalt, at positionere sig som rådgivere og "trusted advisors", og derved distancere sig fra den klassiske perception af Intern Revision som en kontrol- og "politi"-funktion. Endelig plæderes der fra flere sider for, at "blødere" fokusområder, såsom virksomhedskultur, "business ethics" og værdier, i endnu højere grad bør indarbejdes i den fremadrettede udarbejdelse og operationalisering af revisionsplaner.

Udviklingen i branchen går således stærkt i disse år, og stiller nye krav til den Interne Revisors kompetencer, viden, adfærd og forretningskendskab. En succesfuld og kontinuerlig udvikling af den Interne Revisionsfunktion fordrer derfor, at vi konstant søger ny indsigt, og lader os inspirere af andre til at blive endnu dygtigere. Denne artikels sigte er at henlede opmærksomheden på et nyt medium, som kan bidrage til, at den Interne Revisor på simpel og overskuelig vis, kan holde sig skarp på forandringer og tendenser i branchen og omverdenen.

Udbredelsen af webinars

De senere år har de såkaldte "webinars", vundet stadigt større indpas i eksempelvis undervisning, foredrag og præsentationer. "Webinar" er en sammenfletning af ordene **web-based seminar**. Som navnet antyder, er der tale om et internet-baseret medium, som muliggør en direkte formidling og udveksling af informationer mellem afsender og modtager. Til forskel fra "webcasts", som er baseret på envejs kommunikation, er webinars kendtegnet ved muligheden for real-time interaktion mellem afsender og modtager. Deltagere i et live webinar får derved adgang til en platform med mulighed for at udveksle informationer og synspunkter, debattere, stille/besvare spørgsmål samt etablere netværk.

Webinars udgør en simpel måde hvorpå man kan målrette og tilpasse sin søgning efter relevant og opdateret viden og information. Fordelen ved dette medium er således, at man på forhånd kan udvælge og tilmelde sig netop de webinars, som man vurderer er relevante og væsentlige for ens interessefelt. En anden fordel er, at man ikke fysisk behøver at frekventere bekostelige kurser eller konferencer i f.eks. USA. I stedet kan man følge, og aktivt deltage i, seancerne hjemmefra via mobil, tablet eller PC. Endelig er en tredje fordel fleksibiliteten. Er man forhindret i at deltage i den direkte transmission, kan allerede afholdte webinars ofte downloades og efterfølgende overværes.

Webinars for IIA medlemmer

Først fornyeligt blev undertegnede ved et tilfælde gjort bekendt med, at IIA tilbyder sine medlemmer gratis deltagelse i webinars via IIA North America. På IIA USA's hjemmeside findes således en oversigt over de webinars, som IIA aktuelt udbyder samt tidspunkter herfor. Deltagelse i IIA's webinars forudsætter blot en forudgående tilmelding på hjemmesiden med angivelse af sit IIA medlemsnummer samt et system-setup, som understøtter webinar formatet. Når tidspunktet for webinaret indtræffer, logger man sig på via et adgangs-link, som typisk modtages via e-mail dagen forinden. Herefter har man adgang til webinaret, hvor en eller flere speakers afholder en præsentation, oftest med afsæt i PowerPoint slides. På webinar-sitet har deltagere desuden mulighed for, via en tekstboks på skærmen, skriftligt at stille spørgsmål eller bidrage med kommentarer under præsentationen.

Er man forhindret i at deltage i et live transmitteret webinar, hvilket ikke er et unrealistisk scenarie med tanke på tidsforskellen til USA, er der, som omtalt ovenfor, mulighed for efterfølgende at downloade præsentationen med tilhørende slides. IIA USA opbevarer alle afholdte webinars i et online arkiv på hjemmesiden, som er tilgængeligt for alle IIA's medlemmer. Der afholdes cirka 12-15 webinars årligt i IIA USA's regi.

Jeg har haft fornøjelsen af at følge 8 IIA webinars i indeværende år. Speakerne udgøres typisk af Interne Revisorer fra offentlige eller private virksomheder. Derudover har jeg overværet webinars afholdt af konsulenter, Eksterne Revisorer samt af repræsentanter fra IIA. Præsidenten for IIA, Richard F. Chambers, leverede eksempelvis et indlæg på et webinar tidligere i år, hvor han delte sine refleksioner om Intern Revisions fremtidige rolle, udfordringer og prioriteringer.

Andre temae som IIA's webinars har adresseret i 2016, omfatter bl.a. indlæg om cyber-sikkerhed, personfølsomme oplysninger og dataanalyse, samt konkrete forslag til

hvordan udfordringerne forbundet hermed kan tilgås. Derudover har flere webinars fremhævet virksomhedskultur som et yderst relevant fokusområde for Intern Revision. Et fokus, som bl.a. kan tilskrives, at der i nogle kredse i USA er en udbredt opfattelse af, at netop en usund virksomhedskultur har været en stærkt medvirkende faktor til at flere store amerikanske virksomheder er kollapsede senere år, herunder Enron og World.com.

Et tredje omdrejningspunkt for flere af IIA's webinars i 2016 har desuden været, at kravene til Intern Revisions kompetencer er under forandring som følge af voksende diversitet i revisionernes formål, karakter og fokus. Det entydige budskab fra disse webinars er, at Intern Revision bør sikre den nødvendige mangfoldighed i medarbejderstabben, samt prioritere en kontinuerlig opgradering af afdelingens kompetencer for at undgå, at et kompetencegap opstår. Endelig er der flere eksempler på at speakers har præsenteret og diskuteret resultater af en række surveys, som bl.a. har adresseret Intern Revisions anvendelse af analyseværktøjer, revisionssystemer, co-sourcing m.v. I Figur 1 nedenfor er indsat en oversigt over de webinars, som er afholdt i 2016.

Temaerne i de udbudte webinars dækker med andre ord et bredt spektrum i relation til fokus, vægtning og dybde. Dertil kommer betydelige variationer i tilgangen til teori og praksis, om kvantitative eller kvalitative metoder lægges til grund, og om budskaberne er af overvejende subjektiv og/eller objektiv karakter. Endelig afhænger omfanget af publikums involvering af hvor meget speakeren prioritiserer, at invitere til spørgsmål og kommentarer.

Figur 1: IIA's arkiv over webinars afholdt i 2016 (theiia.org)

Original Air Date	Event Title
October 18, 2016	Leveraging Data to Manage Your Fraud Risk Playback Presentation Slides
October 12, 2016	Guidance Webinar: What You Need to Know Now About the Revised Standards Playback Presentation Slides
September 20, 2016	Technology Champions: Key Enablers for Internal Auditors Playback Presentation Slides
August 16, 2016	Data Analytics – Maximizing Value for Internal Audit Playback Presentation Slides
August 3, 2016	Guidance Webinar: Coping With Ethical Pressures Playback Presentation Slides
July 12, 2016	Maximizing the Value of the "Three Lines of Defense" Playback Presentation Slides
June 21, 2016	The Uncharted Territory of an Organization's Audit Culture Playback Presentation Slides
April 19, 2016	The Evolution of Internal Auditing: Assure, Advise, Anticipate Playback Presentation Slides
March 15, 2016	Auditing Cybersecurity in an Unsecure World Playback Presentation Slides
February 16, 2016	Filling the Void: Addressing Today's Skill Gaps in Internal Audit Playback Presentation Slides
February 11, 2016	Getting to Know the Proposed Changes to the Standards Playback Presentation Slides
January 20, 2016	2016 Outlook for Internal Audit Playback Presentation Slides

IIA's medlemmer har dog mulighed for at foretage en kritisk forhåndsvurdering af om de udbudte webinars er relevante for den enkeltes interessefelt før tilmelding foretages. På hjemmesiden er de forestående og afholdte webinars tema og speaker kort beskrevet. Ønskes et større eller bredere udbud af webinars kan man via links på IIA USA's hjemmeside tilgå andre IIA godkendte webinars fra eksterne udbydere.

CPE point

For de af IIA's medlemmer, som er i besiddelse af en IIA certificering, som kræver en årlig optjening af CPE point, er der yderligere en grund til at overveje at tilmelde sig et webinar. Deltagelse i et IIA webinar berettiger således typisk til 1 CPE point forudsat at det følges live, at man er forbundet til webinar-sitet i minimum 50 af de planlagte 60 minutter, samt at man besvarer en række "polling questions" under afviklingen af webinaret. I forlængelse heraf skal det understreges, at download og overværelse af allerede afholdte webinars fra IIA's arkiv ikke berettiger til CPE point.

Deltagelse på de af IIA godkendte eksternt udbudte webinars medfører ligeledes en optjening af CPE point, såfremt de gældende regler for deltagelse efterleves.

Baseret på min hidtidige erfaring med IIA og andre udbydere af webinars, er det min vurdering at disse udgør et kvalificeret alternativ, eller supplement, til de mere gængse informations- og undervisningskilder, som tilbydes Interne Revisorer. Kvalitet, relevans og væsentlighed i disse webinars varierer, men må selvagt bero på en individuel vurdering afhængig af hvilke forventninger og interesser, som man tilgår webinaret med. Min oplevelse er dog, at kvaliteten har været relativt høj i flertallet af de afholdte webinar-seancer, og at der i flere tilfælde har været viden, inspiration og ideer, som vi har taget til kritisk efterretning i vores Interne Revisionsafdeling. Fremfor alt er webinarene dog efter min mening en kærgommen og fleksibel kilde, som bidrager til indsigt i aktualiteter og strømninger indenfor, og relateret til, Intern Revision. De leverer derfor en platform for kritisk refleksion, og dermed et afsæt for yderligere fordybelse i temaer og tendenser, som kan have relevans for den enkelte Interne Revisor og afdeling.

Ekstern kvalitetssikring af intern revision



Søren Larsen, Senior kon-
sulent, Deloitte



Thomas Nygaard, Director,
Deloitte

Indledning

En intern revisionsafdeling kan være værdiskabende for de fleste virksomheder, da intern revision kan bidrage til en effektiv governancestruktur, et mere klart risikobillede samt optimerede interne kontroller. Men hvordan og hvornår er en intern revisionsafdeling værdiskabende? Og hvordan formår en intern revisionsafdeling at levere resultater i forhold til de forventninger der påhviler afdelingen fra ledelsen og den øvrige forretning? En af måderne, hvorpå intern revision kan sikre, at de både nu og i fremtiden leverer værdi for organisationen, er ved at vurdere om intern revision i forhold til IIA's standarder har et stærkt fundament for dets arbejde, herunder f.eks. er placeret rigtigt i organisationen, er uafhængige og har relevante værktøjer og metoder på plads. Ved at gennemføre en ekstern kvalitetssikring af intern revision kan man på den måde bekræfte, at intern revision efterlever IIA's standarder, og derved at de udførte revisioner har et fagligt højt niveau.

Baggrund for certificering

For at efterleve IIA standarderne, og derved erklære at de interne revisioner er udført i overensstemmelse med IIA's standarder, er det nødvendigt at intern revision får lavet en kvalitetsvurdering mindst hvert femte år. Kvalitetsvurderingen skal i henhold til IIA udføres af eksterne personer (udenfor virksomheden / organisationen) med kompetencer indenfor IIA's Professional Practice Framework og certificeringsprocessen. Dette kan være "IIA quality assurance reviewers, regulatory reviewers, consultants, external auditors, other professional service providers and internal auditors from outside the organization". I praksis vælges oftest mellem et anerkendt revisionsfirma, "peer to peer review" hvor andre interne revisorer foretager reviewet eller via IIA. En alternativ fremgangsmåde kan være at foretage en selvevaluering, hvor en uafhængig ekstern part efterfølgende validerer selv-

evalueringen. I samråd med den pågældende virksomheds bestyrelse, er det typisk revisionskomiteen der vælger evalueringstyperne og hyppigheden heraf, især hvis denne ønskes foretaget oftere end hver femte år, samt vurderer om der ved kvalitetsvurderingen kan opstå potentielle interessekonflikter.

Generelt er flere ledelser og revisionskomiteer begyndt at have større fokus på intern revisions rolle og værdiskabelse, hvilket har ført til et større behov for uvildige vurderinger af intern revisions arbejde. Tilsvarende er flere interne revisionschefer også begyndt at anvende den eksterne kvalitetsvurdering som et værktøj til at få uvildig feedback som et vigtigt element i den løbende forbedring af intern revision.

I det hele taget er der i de senere år opnået en større anerkendelse af, at en ekstern kvalitetssikring er mere end blot en bekræftelse af, at intern revision følger IIA's standarder, men at en certificering faktisk kan anvendes til at forbedre intern revisions position i organisationen og bidrage til en øget værdiskabelse.

For den interne revision i dag, er det altså forhåbende for afdelingen, at have øget fokus på at skabe værdi for den øvrige forretning og være mere end blot organisationens politibetjente. Den moderne ledelse forventer i dag, at intern revision indgår i en række rådgivningsopgaver og hjælper organisationen med at forbedre og optimere deres governance og styring. Samtidig forventer de, at intern revision råder over moderne teknologi og de nyeste metoder, således at en effektiv, relevant og nutidig intern revision bliver foretaget. Nutidens krav til intern revision kræver langt mere end blot forståelse af regnskab og interne kontroller. Der er behov for en dyb indsigt i virksomhedens strategi, værdikæder og aktiviteter. Der er behov for en intern revision som kan udfordre og rådgive virksomhedens ledelse og tilføre indsigt i organisationen.



For at skabe den størst mulige værdi for forretningen, er det dog vigtigt, at intern revision først kigger indad og vurderer sin egen forretning. Er der de nødvendige kompetencer, den rigtige teknologi og de bedste metoder? Følger intern revision almindelige revisionsprincipper? Er intern revision placeret rigtigt i organisationen? Har intern revision adgang til de rette beslutningstagere? Har intern revision et retvisende risikobillede – og ligger det til grund for de opgaver, som faktisk løses? Er intern revision i tilstrækkelig grad uafhængige? Og hvordan er samarbejdet med den øvrige organisation. Er alle disse forudsætninger ikke på plads, kan det være meget vanskeligt for intern revision at løfte den meget krævende opgave, som de har i moderne virksomheder.

Hvis alt dette er på plads kan intern revision i samarbejde med revisionskomiteen og øvrige interesser begynde at vurdere, hvorvidt de tilfører relevant værdi til resten af organisationen. Men udgangspunktet for disse drøftelser bør altid være, at have den bedst mulige afdeling med de ressourcer og værkøjer der er til rådighed.

En ekstern kvalitetsvurdering tager udgangspunkt i IIAs standarder og benchmarker de faktiske forhold i intern revision op imod disse. Hertil kan man med fordel samtidig foretage yderligere analyser i forhold til andre revisionsafdelinger med henblik på at vurdere afdelingens generelle effektivitet og efficiens.

Det primære formål med gennemgangen er at vurdere compliance med standarderne, men gennemgangen vil typisk samtidig vise en række områder, hvor intern revisions performance kan forbedres. På den måde vil den eksterne kvalitetsvurdering medvirke til at pointere og fremhæve forbedringsmuligheder for den interne revision. Optimalt bør dette endvidere udmønte sig i konkrete handlingsplaner for intern revision.

Anbefaling til forbedringer foretages med henblik på gøre en proces mere simpel eller at tilføre afdelingen anden værdi, der kan afledes direkte eller indirekte af denne forbedring. Et af formålene ved at give disse anbefalinger er, at kommunikere tydeligt og klart når der rejses en observation. Det skal gerne være forståeligt hvordan en observation i forbindelse med en ekstern kvalitetsvurdering bør tolkes som en forbedringsmulighed. Det er ikke altid en let opgave, hvorfor det også er vigtigt, at vælge en ekstern part, der har den nødvendige erfaring med at

foretage ekstern kvalitetsvurdering, så kvalitetsvurderingen tilfører den nødvendige værdi. Vi er ikke i tvivl om, at når intern revision vælger at implementere forbedringer i umiddelbar tilknytning til en ekstern kvalitetsvurdering afspejles dette og resulterer i øget værdi.

Generelt oplever de organisationer, hvor intern revision gennemgår en ekstern kvalitetsvurdering, og som efterfølgende arbejder med anbefalingerne, at kvaliteten af intern revisions arbejde forbedres væsentligt, og at interne revisionsrapporter og anbefalinger bliver mere relevante.

Organisationens modenhed

Før en certificeringsproces igangsættes, er det vigtigt for intern revision, at både medarbejdere i intern revision samt væsentlige interesser i organisationen er informerede om processen, forløbet, og ikke mindst formålet med gennemgangen.

For den optimale kvalitetsgennemgang er det væsentligt, at de der foretager gennemgangen ligeledes har adgang til interesser for at vurdere, hvordan intern revisions arbejde og metoder opleves fra "den anden side". Ligeledes er det afgørende, at intern revision har gjort sig klare tanker om hvordan man vil anvende certificeringen. Er det alene en compliance opgave, eller skal det anvendes til at løfte afdelingen?

“ Forinden intern revision overhovedet indleder sig på en ekstern kvalitetsvurdering bør de vurdere, om de er klar til at gennemgå en ekstern kvalitetssikring, herunder om de har den nødvendige modenhed.

Forinden intern revision overhovedet indleder sig på en ekstern kvalitetsvurdering bør de vurdere, om de er klar til at gennemgå en ekstern kvalitetssikring, herunder om de har den nødvendige modenhed.

Det er langt fra alle interne revisionsafdelinger, der har forudsætningerne for en positiv certificering. Det kan skyldes mange faktorer, men grundlæggende ser vi ofte, at afdelinger, der i mange år har været statiske og ikke fulgt udviklingen i forhold til den internationale udvikling indenfor intern revision, har svært ved at efterleve kravene til en position certificering. Det kan både skyldes manglende generel forståelse af IIAs standarder, men er i mange tilfælde i højere grad et udtryk for en eller flere af følgende faktorer:

- Intern revision er placeret for lavt i organisationen, hvilket kan have indflydelse på uafhængigheden
- Fokus på de enkelte opgaver i højere grad end fokus på det samlede risikobillede for organisationen hvorved væsentlige risikoområder ikke afdækkes

- Revisionsmetoder er ikke tidssvarende eller lever ikke op til de generelle kvalitetskrav.

Ovenstående er forhindringer for et positivt udfald af kvalitetsgennemgangen som bør overvejes forinden gennemgangen igangsættes. Dette kan gøres ved en forundersøgelse, som foretages på et væsentligt mere overordnet niveau end selve kvalitetsgennemgangen. Typisk ved intern revision godt selv, hvor der kan være problemer, og derfor anbefaler vi altid, at intern revision i første omgang fokuserer på at udbedre kendte svagheder inden kvalitetsvurderingen foretages. Equity Partner i Deloitte, Morten Egelund, udtales:

"Når vi i Deloitte foretager en certificering af vores kunder, så anbefaler vi altid, at en IIA certificering forestås som et led i en forbedring og udvikling af intern revision. Det bør derfor altid foregå i et tæt samarbejde mellem kunden og os både inden, under og efter selve gennemgangen for at sikre dels en god forståelse af afdelingen, dels hvordan de mest optimalt kan arbejde og øge værdiskabelsen for organisationen, herunder den bedste måde at implementere eventuelle forbedringsforslag."

En certificering bør altid være en proces, hvor den eksterne assessor, intern revision og organisationen samarbejder mod et og samme mål, nemlig at forbedre den interne revisionsafdeling og metoder med henblik på at bidrage mest muligt til organisationen samlede opnåelse af strategiske og operationelle mål fremfor udelukkende at fokusere på at opnå den egentlige certificering.

Udførelsel af kvalitetsgennemgangen

Når man har vurderet at en intern revisionsafdeling er klar til at gennemgå selve certificeringsprocessen, er det vigtigt, at selve processen for kvalitetsgennemgangen planlægges. Eventuel deadline skal fastsættes, og væsentlige milepæle defineres. Hvilket materiale er nødvendigt at analysere for at komme i mål? Hvad kræves der fra parterne hver især – og hvilke opgaver er fælles? Det er vigtigt, at få lavet en aftale på forhånd, hvor forventningerne til processen afstemmes.

En ekstern kvalitetsvurdering sigter mod at foretage en grundig diagnostisk gennemgang af intern revision som funktion. Selve gennemgangen kan opdeles i en række forskellige metodeafsnit, der alle skal gennemføres for at nå i mål:

- Planlægning af gennemgangen
- Forstå intern revisions formål og organisering
- Gennemgang af intern revisions styringsprocesser og metoder
- Vurdering af den overordnede planlægningsproces

- Gennemgang af intern revisions arbejdsmetoder, herunder planlægning, udførelse og rapportering af de enkelte revisioner og opfølgning på observationer
- Opsummering af observationer og udarbejdelse af handlingsplaner til mitigering af bemærkninger fra gennemgangen
- Endelig vurdering af intern revisions arbejde er i overensstemmelse med IIAs standarder.

I planlægningsfasen kan man med fordel indlægge en til flere workshops med intern revision med det formål at foretage en overordnet selvevaluering af hvorvidt de efterlever IIAs retningslinier. Typisk ved medarbejdere og ledelse allerede, hvilke områder som kræver en ekstra indsats, og denne viden kan bruges til at identificere svagheder og fastlægge fokusområder i gennemgangen.

Selve gennemgangen omfatter blandt andet en række interviews af interesserter, medarbejdere og andre relevante personer, der skal give et indblik i hvordan intern revision fungerer og opfattes, både internt i intern revision og eksternt i organisationen.

Møder med de eksterne interesserter kan ligeledes medvirke til at forstå hvor organisationen er på vej hen og i hvilket omfang intern revision i samme grad følger denne retning. Ligeledes giver møderne en dybere forståelse af organisationens sammensætning og værdisæt.

Herudover indeholder en ekstern kvalitetsgennemgang en detaljeret gennemgang af en række centrale informatorer i intern revision såsom:

- Intern revisions funktionsbeskrivelse
- Placering af intern revision i organisationen og rapporteringslinier
- Medarbejdernes erfaring
- Styringsværktøjer, f.eks. tidsregistrering og opfølging herpå
- Revisionsplanen og grundlaget for denne
- Værktøjer, der anvendes til udførelse af revisionerne (Analytics, software etc.)
- Procesbeskrivelser
- Dokumentation fra udvalgte revisionsprojekter

Et ofte overset element i i forbindelse med en kvalitetsgennemgang er hele styringen af intern revision. Fravær af tilstrækkelig tidsregistrering medfører, at det ikke er muligt at holde øje med tidsanvendelsen på de enkelte projekter, og dermed kan det være vanskeligt at optimere ressourceanvendelsen. Det kan med rette rejse et spørgsmål om, hvor mange revisioner intern revision bør foretage i løbet af et år, hvor meget skal medtages i revisionsplanen og hvor lang tid har revisorerne til de enkelte

projekter. Det er derfor vigtigt at inkludere dette område i en gennemgang.

I forbindelse med gennemgangen af de udvalgte revisionsprojekter foretages en vurdering af indhold og struktur fra planlægning af opgaven over dokumentation af det udførte arbejde til observationer og den endelige rapport. Det er vigtigt for gennemgangen, at der findes en klar rød tråd hele vejen fra planlægning til endelig rapport, så det sikres, at arbejdet udføres i en tilfredsstillende kvalitet. Ligeledes er det vigtigt for kvaliteten af arbejdet, at der sker en dokumenteret og synlig kvalitetssikring af det udførte arbejde. Man kan med fordel i denne forbindelse også vurdere den kommunikation, der har været mellem de reviderede og intern revision for at sikre, at organisationen involveres tilstrækkelig i revisionen og i planlægningen.

Selve denne gennemgang bør holdes sammen med intern revisions egne processer for at sikre, at disse følges og at revisionerne foretages ensartet og i overensstemmelse med standarder for intern revision.

Med udgangspunkt i de foretagne interviews, analyser m.v. kan den samlede overensstemmelse med IIAs standarder vurderes per standard og samlet, ligesom eventuelle observationer og anbefalinger kan opsummeres.

IIA standarderne

Der findes ikke to interne revisionsafdelinger, der er ens. Det bør heller ikke være tilfældet idet intern revision bør være individuel fokuseret med udgangspunkt i forretningsens forventninger og krav. Fælles for intern revision er dog, at de bør operere i overensstemmelse med IIAs standarder. Det er disse standarder, der lægges til grund for den eksterne kvalitetsgennemgang.

I forbindelse med den eksterne kvalitetsvurdering vurderes det, hvordan intern revision opererer i forhold til den enkelte standard. For hver standard scores ud fra hvorvidt de faktiske forhold i intern revision er i overensstemmelse (conformance) med den enkelte standard hvor følgende kriterier anvendes:

- "Conformance" (overensstemmelse)
- "Partial conformance" (delvis overensstemmelse)
- "non-conformance" (ikke overensstemmelse).

Det er muligt at have "Partial Conformance" med nogle standarder og stadig opnå "Conformance" som overordnet score. I tilfælde hvor der er store afvigelser mellem standarderne og de faktiske forhold bør assessor dog vurdere, om der er tilstrækkeligt grundlag til et overordnet positivt resultat af gennemgangen.

For en intern revisionsafdeling er det et kvalitetsstempel når en kvalitetsvurdering er vel overstået. Det er vigtigt, at dette resultat bliver kommunikeret til ledelse og revisionskomite med det formål at sikre, at de er opmærksomme på, at kvaliteten af intern revisions rapporter, og det bagvedliggende arbejde, er høj. Det bør enhver intern revision promovere.

Der er fra vores side ingen tvivl om, at alle interne revisionsafdelinger kan have meget stor nytte af at gennemføre en ekstern kvalitetsvurdering. Den kan bidrage til i højere grad at fremme udvikling af intern revision, ligesom den kan skabe mere fokus på intern revision i organisationen. Intern revision bør gøre chancen og udnytte denne oplagte mulighed for både at operere i overensstemmelse med IIAs standarder, og samtidig få fokus på eventuelle forbedringspotentiale, som de med fordel kan udnytte.



Meld dig til en af foreningens nye arbejdsgrupper

ARBEJDSGRUPPE:
VIRKSOMHEDENS
SAMLEDE RISIKO-
BILLEDE

ARBEJDSGRUPPE:
RISICI KNYTTET TIL
IT-ANVENDELSEN

JEG VIL GERNE VIDE
MERE OM ARBEJDS-
GRUPPERNE



IIA Global Conference 2016



Thomas Nordestgaard Sørensen,
Lead Audit Specialist, Internal Audit -
DONG Energy

Der var lagt op til en stor (faglig) fest, da dørene blev åbnet for den internationale konference, som samtidigt kunne fejre IIA's 75 års jubilæum. Konferencen blev afholdt i New York City (NYC) i juli måned med over 2.400 deltagere fra mere end 100 lande, hvilket gjorde denne konference til den mest velbesøgt nogensinde.



Årsagen til det store fremmøde skal sandsynligvis findes i jubilæet, samt at NYC har en stor tiltrækningskraft. Inden de officielle speakers gik på, var der en musikalisk introduktion fremført af et gospelkor. Koret sluttede naturligvis af med Frank Sinatras evergreen "New York, New York", således at ingen glemte hvor de befandt sig.



Velkomsten var herefter præget af taler med temaet "Inspire the future and celebrate 75 years", som inkludeerde en video med velkomster fra flere IIA landeansvarlige. Den første hovedtaler var Ian Bremmer, som er specialist i globale politiske risici og ansvarlig for udenrigsanliggender for 'Time' Magasin. Han tog os igennem de forskellige politiske risici i verdensregionerne, som virksomheder og Internal Audit funktioner bør være opmærksomme på. En super god introduktion til at sætte scenen for de efterfølgende dages kurser og seminarer.

Over de næste par dage var der en god blanding af hovedtaler og specifikke emner, som blev behandlet mere uddybende.

Konferencen var vanen tro delt op i en række undertemaer:

1. The Significant Impact of Financial Services Auditors
2. Fraud, Bribery and Corruption
3. Emerging Global Issues
4. Governance, Risk, and Controls
5. The future of Internal Auditors
6. Take Your Team to the Top
7. Elevating Corporate Culture
8. Public Sector and Not-for-Profit.

Samlet set var der ca. 70 forskelligartede indlæg, som det var muligt at deltage i, hvilket gjorde det vanskeligt at vælge imellem dem. Vi var to deltagere fra DONG Energy's Internal Audit funktion, og vi valgte en strategi om ikke at deltage på de samme indlæg for at sikre maksimalt udbytte til afdelingen.

Baseret på de indlæg og foredrag, som vi deltog i, så var de overordnede områdefordelte take-aways – for mig – følgende:

- **Fremadskuende revisioner:** og derved begrænse tiden, som bruges på at kigge på historiske tal:
 - Fokuser på hvorledes Internal Audit kan være med til at understøtte, at virksomheden opnår dens langsigtede mål
 - At Internal Audit er omstillingsparate og dermed har en dynamisk plan, hvor projekter kan tages ud og erstattes med andre projekter.
- **Data Analytics:** Hvorledes kan Internal Audit bedst inkorporere dataanalyser for at udføre revisioner og konsulentprojekter på den mest effektive og værdiskabende måde:
 - At lave kontinuerlig monitorering og revision
 - Identificere mulighederne for at optimere projekter og hverdagen gennem brugen af data, og få dataanalyse inkluderet så tidligt som muligt i projekterne

- Få kommunikeret og vist værdien af dataanalyse til ledelsen kontinuerligt – success breeds success...
- Det er en iterativ proces, og tager tid og penge at bygge et brugbart værktøj.
- **Kulturrevisioner:** Hvordan kan Internal Audit være med til at opdage og forebygge, at der opstår eller udvikles en uhensigtsmæssig kultur i organisationen:
 - Benyt trafiklys til at fremhæve kulturen i et givent område. Der kan bl.a. måles på tonen, værdierne, roller og rettigheder, governancestruktur, håndtering af risici, risikotransparens, aflønning og tælenthåndtering
 - Ledelsesopbakning er essentielt
 - Være transparent og have en kontinuerlig samt klar kommunikation. Hertil er det vigtigt at være konsistente
 - Kan være en svær 'hød' at knække.
- **Enterprise Risk Management:** Hvorledes kan Internal Audit bedst være med til at understøtte den tværgående risikostyring, f.eks. indenfor top 20 risici, outsourcing, underleverandører samt it-løsninger. Der blev fra foredragsholderne lagt op til:
 - At der tænkes strategisk
 - At der i øget grad laves integreret rapportering og 'combined assurance' ift. risikorapportering til ledelsesorganer
 - At der ved implementering af ERM overvejes følgende – buy in, regular quality assurance, keep it simple and clarity on the concept of three lines of defence
 - At implementeringen af ERM er en iterativ proces – så sæt realistiske måål.
- **Lean auditing:** Overvejelser omkring, hvad kunden er villig til at betale for:
 - Hvis der er konstateret en svaghed – er der så et behov for at grave dybere?
 - Får man identificeret årsagen til, at fejl sker – eller behandler man 'symptomerne'?
 - Dele opgaven i flere faser for at sikre en hurtigere afrapportering
 - Benyt scopebegrænsninger, det er ikke altid nødvendigt at revidere hele området
 - Identificer og afhjælp stopklodser for opgaven for at sikre, at tid og budgetter overholdes.

Det overordnede indtryk af konferencen er, at den var velplanlagt, præget af nogle gode, relevante og interessante indlæg og det var spændende at høre fra revisionsafdelinger, som havde 1 ansat til City Group's Internal Audit funktion som beskæftigede 2.500. Yderligere var

konferencen en godt sted at skabe nye kontakter, ikke mindst blandt de danske deltagere, og der var arrangeret flere sociale arrangementer i løbet af dagene. Næste års internationale IIA konference bliver afholdt i Sydney, Australien i perioden 23.7–26.7.2017.



Global Council 2016 og ECIIA General Assembly 2016



Kim Stormly Hansen, Formand, IIA Danmark

Global Council 2016

Global Council er en mulighed for de enkelte landes institutledere til at drøfte og udveksle erfaringer om aktuelle emner. Global Council 2016 blev afholdt i New York i weekenden op til den globale konference.

Måske netop derfor og fordi, at IIA, Global i år fejrede 75års jubilæum var antallet af deltagere meget højt. 108 lande var repræsenteret.

De 2 dage var et mix af indlæg og breakout discussions. Der blev drøftet og givet input til eksempelvis følgende:

- **Standards: Aspirational or a minimum requirement**, hvor der var bred enighed om, at IIA Standarder skal være et minimumskrav.
- **The need for Advocacy.** Konklusionen var, at IIA generelt bør have skarpere fokus herpå.
- **Stakeholder Expectations.** Vi bør i højere grad indbrage vores stakeholdere. Fsva. CFO'ere og revisionsudvalgsmedlemmer bør vi måske gå så langt, som til at "uddanne" dem.
- **A Truly Global Exam.** Deltagere uden for USA kunne ikke genkendende til, at den nuværende eksamensform og ikke mindst de spørgsmål der stilles er meget amerikanske. Det budskab tog IIA, Global til sig, men lad være med at glæde jer for tidligt.
- **Millennials.** Den yngre generation medarbejdere har en helt anden tilgang til læring. Det skal være her og nu, hvilket stiller øgede krav til diversifikationen af institutternes uddannelsesudbud.



ECIIA General Assembly 2016

Stort set alle europæiske institutter er medlem af ECIIA. Det primære fokus for ECIIA er, at påvirke lovgivere og regulatorer i EU, hvorfor deres primære targets er EU-parlamentet, EU-kommissionen, EBA, ECB, EIOPA og ESMA. Det vigtigste punkt på agendaen var ændringer til ECIIA visionen:

Furthering the development of good Corporate Governance and Internal Audit at the European level through knowledge sharing, Developing key relationships and impacting the regulatory environment.

og ikke mindst ændringer til medlemsstrukturen, membership fees og voting rights. Dette gik ikke stille af. I den nye struktur vil UK, Frankrig, Tyskland, Spanien og Italien betale 55% af de totale fees, udgøre 53% af medlemmerne og have 45% af stemmerettighederne. Strukturen blev stemt hjem med mindst mulig margin. Især Israel og Tyrkiet, som er associerede institutter, vil komme til at være uden stemme, og forsøgte at samle stem-

mer til en nedstemning. For IIA, Danmark bør den nye struktur betyde en væsentlig reduktion af vores betaling til ECIIA.

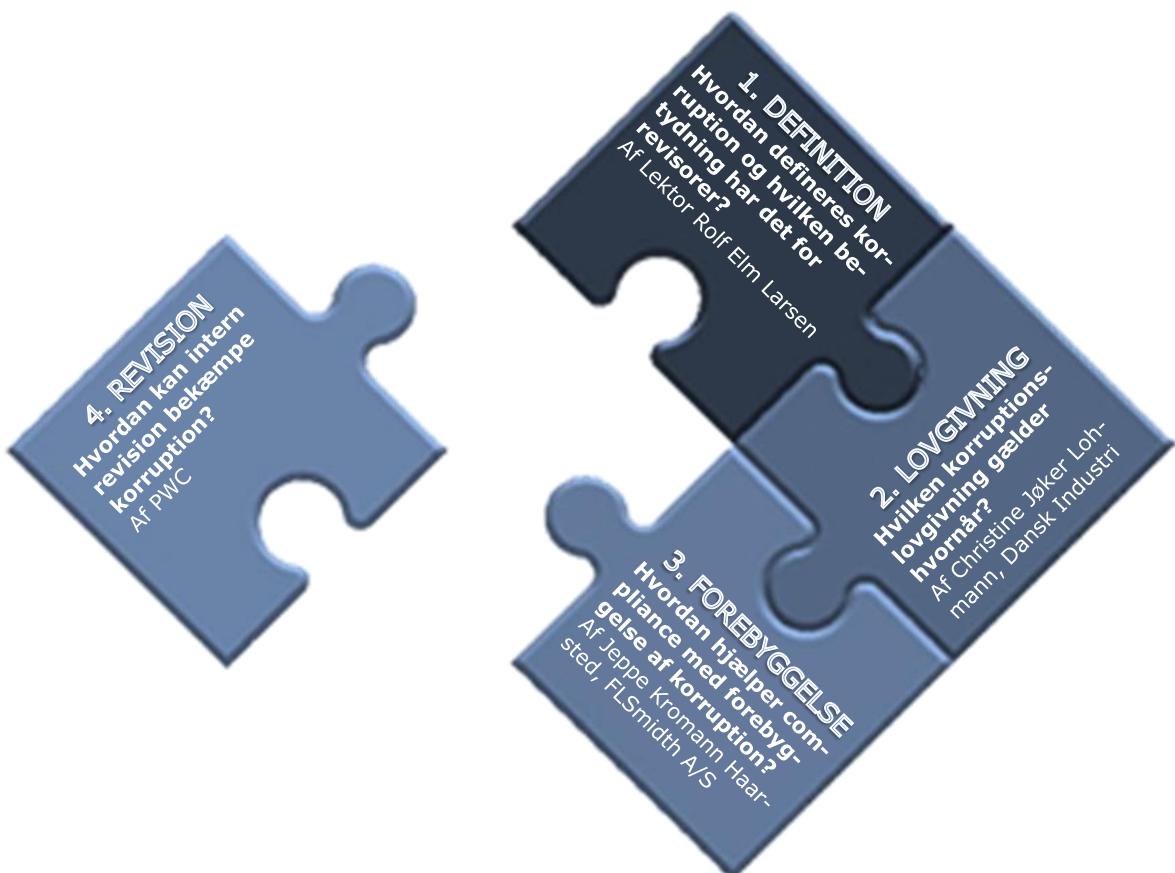
General Assembly blev afholdt i umiddelbar forlængelse af den årlige ECIIA konference i Stockholm, hvor specielt de sociale rammer var helt i orden.



Minitema: Korruption



Er korruption noget som interne revisorer skal overveje? Med de næste fire artikler har vi samlet et puslespil, som kaster lys på dette spørgsmål.



God fornøjelse.

Korruption - moralsk fordærv, en omkostning for andre



Rolf-Elm Larsen, Ekstern lektor,
CBS

Indledning

Denne artikel har til formål at give nogle grundlæggende elementer til forståelsen af korruption som fænomen samt et overblik over, hvorledes forskellige samfund har sat regelsæt og normer op for at bekæmpe korruption. Videre vil jeg se på korruptionens økonomi i et samfundsøkonomisk perspektiv samt, hvorledes revisorer kan identificere eksistensen af korruption i et regnskab.

Korruption i filmens fiktive univers

Det er "movie-night" med fransk sort-hvid gangsterfilm: "Scene 1: Gennem et overvågningskamera ser vi den hårdtslående ærlige politibetjent, som åbner døren til sit stålskab i garderoben, og ud falder en 500 € seddel. Den var sat i klemme i døren. Han samler den op og stikker den i lommen. Scene 2: Operatøren i overvågningscentret downloader optagelsen på et USB-stik. Scene 3: Gangsteren betaler videoovervåningsoperatøren for optagelsen."

På et splitsekund har vi tre korrupte individer og dramaet kan starte.... Men i den virkelige verden er korruption ikke underholdning, men en alvorlig moralsk fordærvelse, der dybt mærker de enkelte mennesker og samfundet.

Danske virksomheder har også været involveret i korruptionssager. Således overfakturerede en dansk medico-virksomhed, der gennem sin russiske distributør leverede udstyr til russiske offentlige hospitaler. Den danske virksomhed fordelte det overfakturerede beløb til ukendte personer, formodentlig russiske læger. Regnskabsteknisk blev det gennemført ved brug af fiktive fakturaer og interimskonti. Da den danske virksomhed var dattervirksomhed af en amerikansk børsnoteret virksomhed, blev sagen undersøgt af både det amerikanske justitsministerium og det amerikanske børstilsyn. Sagen blev afgjort uden retssag ved, at virksomheden medvirkede til opklaring af sagen og accepterede en bøde.¹

Denne sag er ikke enkeltstående selv i et af verdens mindst korrupte lande.

Hvad er korruption?

Ordet korruption har latinsk oprindelse og betyder moralsk fordærvelse. Der er ikke en præcis juridisk definition af ordet, selvom det er i den betydning, der i daglig tale anvendes. I videnskabelige værker forstår korruption i den brede betydning. Historikeren Mette Frisk Jensen anvender ordet korruption til også at dække bedrageri og underslæb blandt kongerigets embedsmænd i 1800-tallet.² I daglig tale er korruption ikke en specifik handling men noget moralsk forkasteligt. Det betyder, at for at få et operationelt begreb, er det nødvendigt med en håndfast definition fra juraen og samfundsviden.

Definition af korruption

Juridisk defineres korruption som en persons misbrug af sin magt i en organisation ved at tage imod bestikkelse fra anden person, som ønsker at opnå en fordel. Det er den aktive handling at yde bestikkelse og den passive handling at modtage bestikkelse, der efter den danske straffelov er strafbart med en strafferamme op til 6 års fængsel.³ Straffeloven kender ikke termen "korruption", og bestemmelsen sigter ikke kun på bestikkelse af offentlig ansatte men også personer, der varetager offentlige hverv, såsom medlemmer af Folketinget, kommunalbestyrelser mv.

Fordærvelsen "korruption" kendes også i private virksomheder og organisationer, ofte i form af returkommission, gaver mv.⁴ Her straffes den, der yder, lover eller tilbyder en fordel (aktiv bestikkelse), og den, som kræver eller modtager fordelen, med fængsel indtil 4 år.

En nominel sociologisk definition er, at korruption er misbrug af offentlig position eller ressource til privat vinding eller fordel.⁵ Verdensbanken, som gennem adskillige årtier har arbejdet med bekæmpelsen af korruption, definerer det således:

"Korruption er misbrug af offentlig magt til personlig vinding eller til fordel for en gruppe, som man skylder troskab".⁶

Denne definition har den ulempe, at den er meget bred og i denne artikel vil jeg derfor primært koncentrere mig om en forståelse af korruption som det forhold, at personer eller organisationer bliver "köbt" til at give "betaleren" en fordel. Andre former for "fordærv" så som nepotisme, bedrageri, misbrug af aktiver og regnskabsmanipulation vil ikke blive behandlet i artiklen.

Der er således to måder at definere korruption på. På den ene side en juridisk definition, der skal indeholde de præcise elementer, som er nødvendige for at få korrupte individer dømt ved domstolene under de nødvendige garantier for en fair rettergang. På den anden side har vi korruptionsdefinitioner, som er nødvendige for at foretage samfundsgrundvidenskabelige undersøgelser af fænomenet korruption og dets konsekvenser, hvor kravet til definitionen er dens evne til at skabe ny viden og en samfundsdebatt om, hvordan korruption bekæmpes. De to måder at beskrive fænomenet korruption er komplementære.

For at forstå fænomenet korruption og de elementer, der skaber betingelserne for korruption, kan det sættes på følgende formel:

$$C = (M + D) - A$$

⁷

Hvor

C = korruption

M = Graden af magt koncentration eller monopol på magten

D = Graden af mulighed for vilkårlig (diskretionær) magtudøvelse

A = Ansvarlighed

Korruption fremkommer således, når en person eller gruppe opnår monopol på udøvelsen af magt, ofte i offentlige organisationer, men et sådan magtmonopol kan også forekomme i store private erhvervsdrivende virksomheder, non-profit organisationer m.fl. Jo mere lederne kan udøve sin magt diskretionært eller efter for godt befindende, jo større er sandsynligheden for, at magten misbruges til egen fordel/vinding, og korruption forekommer.

For revisorer er det væsentlig at have fokus på, hvorledes revisionsrisikoen minimeres, eller hvordan den reviderede organisations hæderlighedsniveau ($H = Honest$) hæves. Hvordan skabes, gennem revision, et mindre korrupt samfund eller organisation? Det gøres ved at påvirke de enkelte elementer i følgende ligning.

$$H = A - (M + D)$$

Ansvarligheden kan øges ved bedre selskabsledelse eller regeringsførelse. Graden af magtkoncentration bestemmes af mulighederne for at udfordre de siddende magthavere. Er der nogle i organisationen eller samfundet, der tør sige ledelsen imod og bremse magtmisbrug af den vej? Findes der i organisationen regelsæt, der forhindrer, at magten bruges vilkårligt til egen vinding og ikke til glæde for organisationen som helhed? Disse elementer fungerer som inspiration, når revisor skal gennemføre sin risikoanalyse. En virksomhed er eksponeret for korruption, når den mangler at tage stilling til sin "governance" struktur (M, D) og processer (A), har koncentreret sin

magt på en eller få personer eller mangler et regelsæt, der præciserer udøvelsen af ledelsesfunktionen.

International regulering

Internationale organisationer har anerkendt, at korruption er et uvæsen, der både ødelægger den internationale økonomi og gør lande til fejlslagne stater. De har af den grund vedtaget standarder, der medvirker til at bekæmpe korruption.

FN

I september 2015 fastsatte FN "The 2030 Agenda for Sustainable Development". Blandt målene er Goal 16: Promote peace, justice and strong institutions. Det mål opnås gennem target 16.5: Substantially reduce corruption and bribery in all their forms.⁸



Med andre ord er et korrupt samfund et uretfærdigt samfund, fordi nogle bliver mere lige end andre på samme måde som i Orwells bog om "Kammerat Napoleon". Dem, som bruger korruption, køber sig til en fordel, de ikke er berettiget til. De skader deres medmennesker ved ikke at understøtte en bæredygtig udvikling.

I FN's Global Compacts er der ti principper for ansvarlig virksomheds drift.⁹ Det tiende princip fastslår, at virksomheder bør modarbejde alle former for korruption, herunder afpresning og bestikkelse. I dag har 237 dansk virksomheder tilsluttet sig dette princip.

OECD

I OECD regi har de vestligt orienterede medlemsstater udarbejdet en konvention for, hvordan korruption kan bekæmpes og Danmark har tilsluttet sig konventionen. Den ser korruption som et alvorligt moralsk og politisk problem, der undergraver god regeringsførelse, den økonomske vækst og forvrider den internationale handel. Ud fra den betragtning opfordrer konventionen alle erhvervsorganisationer, fagforeninger, virksomheder, regeringer til at samarbejde både nationalt og internationalt i korruptionsbekæmpelsen. Medlemsstaterne har påtaget sig at fastsætte straffebestemmelser for korruption i den nationale retsorden.¹⁰

EU

Medlemskab af EU forudsætter et retssamfund. Det omfatter bl.a. en anti-korruptionslovgivning og institutioner, der bekæmper korruption. EU's retsorden omfatter ikke regler, der forbryder korruption, men den forudsætter, at medlemsstaterne har det. Der stilles krav til medlemsstaterne lovgivning om, at der lever op til FN's Konvention



Group of States against Corruption

Groupe d'États contre la corruption

til bekæmpelse af korruption samt til Europa Rådets (en europæisk mellemstatslig organisation med 47 medlemsstater der arbejder med menneskerettigheder, demokrati og "rule of law" og deltager i GRECO (Group of States against Corruption)) to konventioner om bekæmpelse af korruption: en konvention om strafferet og korruption samt en konvention om den borgerlig ret og korruption.¹¹ Disse traktater skal EU's medlemsstater opfylde for at opnå medlemskab. EU har ikke selv nogen lovgivning på området.

USA

Flere amerikanske olie- og våbenfirmaer bestak i 70'erne udenlandske politikere og embedsmand. Som reaktion



herpå kriminaliseredes brugen af bestikkelse i den internationale handel for børsnoterede selskaber. Det skete i Foreign Corrupt Practice Act fra 1977, som et tillæg til den amerikanske børslovgivning. Loven stiller to krav til virksomhederne. For det første skal børsnoterede virksomheder have bogførings- og registreringssystemer, der afspejler de økonomske dispositioner. For det andet skal de have de nødvendige interne kontrolsystemer.

Loven gør det ulovligt at bestikke politikere og embedsmand med det formål, at den børsnoterede virksomhed opnår eller bibeholder forretning ved, at modtageren misbruger sin position. Imidlertid er det efter loven ikke ulovligt at betale "smørelse" (facilitation fee), der er normal praksis for at drive virksomhed i det pågældende land. Undersøgelser af lovens virkninger viser, at den ikke har gjort det vanskeligt for amerikanske virksomheder at gøre forretninger i andre lande.¹²

Man kan efter denne gennemgang af en række af de væsentligste legale tekster tænke som den romerske historiker Tacitus, der sagde, at jo mere korrupt et samfund er, jo flere love har samfundet.¹³ Der er selvfølgelig et gran af sandhed i den betragtning, men selve produktionen af reglerne skaber en debat internationalt og nationalt, der skaber en forståelse af korruptionens skadelige virkninger og nødvendigheden af at have straffebestemmelser, der afskrækker fra at begå korruption.

Korruptionens økonomi

Korruption er en økonomisk transaktion, hvor en person betaler den korrumperede for en fordel, som den korrumperede ikke er berettiget til. Den korrumperende anvender sine økonomiske ressourcer til at opnå en fordel, som andre personer ikke kan komme i besiddelse af. Med andre ord forsøger den korrumperende at privatisere godt for sig selv og udelukke andre fra det ved at betale.

Den korrumperede udnytter sin position til at opnå en ekstra økonomisk fordel, udover det den pågældende retmæssigt har krav på. I økonomiske termér forsøger den pågældende at maksimere sit økonomiske udbytte af sin position.

I økonomien arbejdes med forudsætning om, at individerne maksimerer deres eget økonomisk udbytte, handler rationelt og strategisk. Det at den enkelte handler økonomisk rationelt, er ikke nødvendigvis ensbetydende med, at samfundet som helhed optimerer sin velfærd. Selvfølgelig kan korruptionen begrænses ved stærke strafferetlige sanktioner, men det er ikke nødvendigvis et virkemiddel i længden.

Det er mere hensigtsmæssigt at søge til mere sociologisk orienterede modeller for en anti-korruptions strategi.

Samfundet er organiseret i sub-grupper med hver deres kultur og samarbejdsmønstre. Først når hovedparten af medlemmerne af en gruppe i fællesskab erkender, at de enkeltvis kommer bedre ud af det økonomisk, er der basis for en kollektivhandel, der kan eliminere den sub-optimale situation: Korruption. Det forudsætter, at det medlem, der bruger bestikkelse sanktioneres så hårdt, at han ikke kan se nogen fordel i at være "free-rider".¹⁴

Kollektivhandel indebærer, at virksomhederne instituerer en norm om, at brugen af korruption ikke er acceptabelt, og sanktionerer overtrædelser af denne norm. Ingen virksomhed må kunne udnytte en situation som "free-rider" og bruge bestikkelse for at opnå en egen fordel. Dette forudsætter naturligvis en gennemsigtighed, som regnskabs- og revisionslovgivningen medvirker til at sikre. Kollektive foranstaltninger er et effektivt redskab til at hjælpe virksomhederne til at bremse bestikkelse. Det kan være særlig nyttigt i miljøer, hvor korruption er forsankset, opfordring til bestikkelse er fremherskende og retshåndhævelsen svag.

Fjernes den usikkerhed, som bestikkelse og korruption skaber, hjælper det med at fremme et effektivt og konkurrenceydigt marked, samtidig med at virksomheder kan spare betydelige summer til bestikkelse. Et anstændigt samfund har lavere transaktionskostninger for styring, kontrakter og kontrol.

Revision og korruption

Revisionens funktion er at skabe troværdighed til regnskaber og virksomheders forvaltning af de betroede midler. Gennem revisionsprocessen opnår revisor en indsigt i virksomheden og hvorledes dens aktiver forvaltes. Derfor er revision et omkostningseffektivt middel til at fremme gennemsigtighed og åbenhed i både private og offentlige virksomheder samtidig med, at det er revisionens pligt at rapportere om brud på lovgivningen, når virksomhedens ledelse kan ifalde et ansvar. Regnskabs- og revisionslovgivningen er derfor effektive midler til bekämpelse af korruption.

Både OECD's konvention om bekämpelse af bestikkelse (artikel 8) og FN's konvention mod korruption (Artikel 12.3) kræver at lande forbyder og effektivt straffer manglende overholdelse af, hvad der her i landet normalt falder indenfor begrebet god bogføringsskik.¹⁵

Derfor kan manglende overholdelse af bogføringsloven være en indikation på, at virksomheden anvender bestikkelse som en forretningspraksis.

Indikation på risiko for korruption	Synonymer for bestikkelse
<ul style="list-style-type: none"> konti udenfor virksomhedens normale bogholderi system utilstrækkeligt identificerede transaktioner registrering af ikke-eksisterende udgifter passiver med forkert identifikation brug af forfalskede dokumenter. 	<ul style="list-style-type: none"> Kommision eller royalty Konsulent honorar Salgs og marketingsudgifter Tilskud til videnskabelige undersøgelser Rabatter og prisnedslag Efter salgsservice honorar Diverse udgifter Frynssegoder Afskrivninger Kundeloyalitetsprogrammer

Nogle typer udgifter påkalder sig umiddelbart revisors opmærksomhed. Det vil typisk være betalinger med betegnelsen "Facilitation fee", der i dag er en eupemisme for "smørelse" til embedsmænd m.fl. En type udgifter af korrumperende karakter er dyre arrangementer for og gaver til forretningsforbindelser.¹⁶

Væsentlighedsgrænsen for transaktioner, der dækker over korruption, er ikke kvantitativ men kvalitativ. Derfor har revisorerne en rapporteringspligt, når ledelsen vil kunne ifalde et straffeansvar, eller når det er af betydning for regnskabslæserens forståelse og brug af regnskabet. Hertil kommer, at virksomheder, der betjener sig af korruption, har snydt sig til en konkurrencefordel, så revisor har heller ikke sikkerhed for, at virksomheden vil kunne klare sig eller være "going concern", når korruptionens "konkurrencefordel" ikke længere virker.

Afsluttende bemærkninger

Artiklen beskriver og analyserer fænomenet korruption. Anti-korruptionslovgivningen gennemgås og det påpeges at kollektivhandel er det virkningsfulde middel til korruptionsbekämpelse. Revisionen har også en rolle at spille i enhver anti-korruptionsstrategi.

Hovedpointerne i artiklen er følgende:

- Korruption er misbrug af magt, der tager forskellige og hele tiden nye former
- Korruption betyder, at det økonomiske system fungerer både ineffektivt og uretfærdigt
- Både lovgiver og retsvæsenet arbejder med regelværk og straffeprocessen for at mindske de skadelige virkninger af korruption

- Revisorer, både eksterne og interne, har en forpligtelse og værktøjerne til at medvirke til korruptionsbekæmpelse
- Virksomheder, der betjener sig af korruption, er på sigt selvdestruktive og øger risikoen for, at det destruktive virus indfiltrer revisors egen virksomhed.

Samlet set er korruption enkeltindividers moralske forær, som skaber en samfundsstruktur med henblik på at opretholde en sub-optimal social orden. Under et korrupt regime betaler alle en merpris, der er uøkonomisk og uretfærdig. Korruptionsbekæmpelse bidrager til at gøre økonomien mere effektiv og retfærdig. Revision er en betingelse for dette.

Noter

¹ US Department of Justice, June 6 2016, <https://www.justice.gov/opa/file/868771/download> og UNITED STATES OF AMERICA: Before The SECURITIES AND EXCHANGE COMMISSION. SECURITIES EXCHANGE ACT OF 1934 Release No. 78113 / June 21, 2016. ACCOUNTING AND AUDITING ENFORCEMENT, Release No. 3784 / June 21, 2016. <https://www.sec.gov/litigation/admin/2016/34-78113.pdf>

² Jensen, Mette Frisk: *Korruption og embedsmændsetik*. Danske embedsmænd i perioden 1800-1866. Syddansk Universitetsforlag 2013 og hendes bog: *Korruption*. Aarhus Universitets Forlag 2015.

³ Justitsministeriet: *Undgår korruption*. Februar 2015.

⁴ Se Rådets rammeafgørelse 2003/568/RIA af 22 juli 2003 om bekæmpelse af bestikkelse i den private sektor. Denne afgørelse er sket efter dansk initiativ.

⁵ Johnstone, Michael: *Corruption Contention and Reform. The Power of Deep Democratization*. Cambridge University Press 2014, p. 9.

⁶ World Bank: *World Development Report 1997*, Oxford University Press 1997, p. 102. Stapenhurst, Rick and Shahrzad Sedigh: *An Overview of the Costsof Corruption and Strategies to Deal with It*, i World Bank: *Curbing corruption: toward a model for building national integrity*,1999, p. 1.

⁷ Klitgaard, R.: *Controlling Corruption*. University of California Press 1988, p. 75

⁸ UN: *The 2030 Agenda for Sustainable Development*

⁹ UN: *Power of Principles. The Ten Principles of the UN Global Compact*. <https://www.unglobalcompact.org/what-is-gc/mission/principles>

¹⁰ OECD: *Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents*. 2011

¹¹ Europa Rådet: *Convention pénale sur la corruption og Convention civile sur la corruption*. http://www.coe.int/t/dghl/monitoring/greco/general/1.%20The%20Fight%20against%20Corruption%20-%20A%20Priority%20for%20the%20CoE_en.asp

¹² Romaneski, Mark: *The Foreign Corrupt Practice Act of 1977: An Analysis of Its Impact and Uncertain Future*. Boston College International and Comparative Law Review Vol 5. Issue 2. 1982 p. 429

¹³ Citeret efter Holmes, Leslie: *Corruption. A Very Short Introduction*. Oxford University Press 2015, p. 94

¹⁴ Olson, Mancur: *The Logic of Collective Action: Public Goods and Theory of Groups*. Havard University Press 1965

¹⁵ African Development Bank Group & OECD: *Anti Bribery Policy and Compliance for African Companies*, 2016, p. 20

¹⁶ US Departement of Justice and US Security and Exchange Commission: *FCPA. A resource Guide to the US Foreign Corrupt Practices Act*. November 2012, p. 39



Anti-korruptionslovgivning, tendenser og praksis



Christine Jøker Lohmann, Chefkonsulent, Dansk Industri

Indledning

To spørgsmål går igen, når jeg taler med virksomheder om anti-korruption: "Er vi underlagt engelsk eller amerikansk anti-korruptionslovgivning, når vi opererer i for eksempel Afrika?" Og "Kan vores virksomhed risikere at blive udelukket fra offentlige udbud, hvis en ansat har brudt vores retningslinjer og brugt urent trav?" Til begge spørgsmål er svaret klart JA.

Spørgsmålene udspringer af stor uvidenhed omkring lovgivningen om korruption og bestikkelse, til trods for at reglerne overordnet er ret simple: Al brug af bestikkelse kan retsforfølges i for eksempel Danmark, England eller USA, såfremt virksomheden har en relation hertil, samt at det også er ulovligt i det land, forseelsen er foregået. Og til det andet spørgsmål: Det er virksomheden, der som juridisk enhed, står til ansvar for, at medarbejderne ikke anvender bestikkelse, hvormed det også er virksomheden, der pålægges sanktionen herved, som for eksempel udelukkelse fra offentlige udbud.

Men selv om disse to overordnede rettesnøre er forholdsvis enkle, ligger djævlen som altid i detaljen. Eftersom revisorloven pålægger revisorer rapporteringspligt, hvis der er begrundet formodning om økonomisk kriminalitet, er viden om lovgivning på anti-korruptionsområdet særlig relevant for netop revisorer. Nærværende artikel vil derfor se nærmere på disse detaljer, og søge at afdække de væsentligste forhold, som gør sig gældende inden for de retningslinjer og den lovgivning, som dækker korruptions- og bestikkelsesområdet. Der lægges særligt vægt på Danmark og de internationale tendenser, vi møder.

Virksomhederne driver agendaen fremad

Overordnet set er der ikke tvivl om, at lovgivningen sætter rammen for, hvad virksomheder må og ikke må, og hvordan de skal agere. Det understreges yderligere af de forholdsvis store økonomiske konsekvenser ved en korruptionssag, som for eksempel ramte Siemens AG i 2014

med henholdsvis 450 mio. dollars i bøde og 350 mio. dollars i konfiskation som følge af overtrædelse af den amerikanske korruptionslovgivning. I en nordisk kontekst kan nævnes Yara-sagen, som de norske myndigheder idømte bøde og konfiskation på NOK 295 mio. i 2014 for bestikkelse i Libyen, Indien og Rusland.

Når det er sagt, er der heller ingen tvivl om, at det ikke er myndighederne, som i dag driver anti-korruptionsagendaen, hverken i Danmark eller internationalt. Det er i høj grad virksomhederne, som gennem collective action, investering i interne procedurer og træning, udvikling af værktøjer og standarder, samt ved at indskrive krav om interne risikostyringsprocedurer i kontrakter med underleverandører kombineret med due diligence, fører anti-korruptionsagendaen fremad.

Desværre ser vi ikke samme iver og tendens hos myndighederne verden over. Det er således også klart, at mens nogle virksomheder og deres ansatte bryder lovgivningen og anvender bestikkelse for at opnå kontrakter, ser vi også mange tilfælde, hvor det er de lokale myndigheder, som er de aktive og presser virksomheder til at betale under bordet. Det kan være for at opnå en kontrakt eller bare et stempel, som de i forvejen har ret til.

Hvem der er skurkene, og hvem der er ofrene i korruptionsligningen er derfor ikke entydigt, om end det typisk er virksomhederne, som i sidste ende så godt som altid kommer til at stå til ansvar, når domstolene taler. Derfor er det essentielt, at virksomheder sørger for at have et godt implementeret anti-korruptionsprogram og beredskab på plads, som de kan dokumentere at medarbejderne kender og er grundig trænet i. Det kan nemlig lette sagsgangen for virksomheden, hvis en ansat har ageret på den forkerte side af loven i Danmark eller et sted ude i verden.

Dansk lovgivning rækker også ud over landets grænser

OECD-landene har generelt intensiveret opmærksomheden på udenlandske bestikkelsessager de seneste 10 år. Samtidig er en korruptionssag i mange lande lig med udelukkelse fra offentlige udbud i en periode, hvilket kan være dyrt for virksomheden. Antallet af individer og enheder, der er blevet sanktioneret som følge af korruption, er således steget markant fra én sag i 1999 til 78 sager i 2011. I 2013 blev 42 sager sanktionerede i OECD-regi. Det sker i kraft af OECD's anti-korruptionskonvention fra 1997.

Konventionen blev ratificeret i Danmark i november 2000 og senest ændret i 2013 hvor strafferammen blev sat op. I Danmark er antallet af udenlandske sager, hvor danske

virksomheder har være involveret, dog meget begrænset. Men også her gælder, at domfældelse for bestikkelse fører til, at virksomheden ikke kan deltagte i offentlige udbud. Det er endnu uklart, om en virksomhed i Danmark kan undgå straf eller opnå en reduceret straf, hvis det kan påvises, at der eksisterer et fornuftigt anti-korruptionsprogram. Årsagen til uklarheden ligger i, at der er ført meget få sager om bestikkelse i Danmark. Det må dog formodes, at eksistensen af et anti-korruptionsprogram vil spille ind på domstolenes strafudmåling og et eventuelt tilbud om bødeaftaler med henblik på afgørelse af sagen. Brugen heraf er dog langt fra de amerikanske og engelske regulerede forhold herfor.

Til trods for, at udfordringer med korruption særligt er forbeholdt det internationale marked, og her i høj grad vækstmarkederne, er det dog vigtigt som virksomhed at have dansk ret for øje.

Mens de fleste dele af straffeloven dækker strafbare forhold, der finder sted i Danmark, dækker de danske korruptionsparagraffer også over forhold, der finder sted uden for landets grænser. Det drejer sig især om:

- § 122 vedrørende aktiv bestikkelse af personer i offentlig tjeneste eller hverv; og
- § 299, nr. 2 vedrørende bestikkelse i den private sektor.

Ifølge straffelovens § 122 gør

"den, som uberettiget yder, lover eller tilbyder nogen, der virker i dansk, udenlandsk eller international tjeneste eller hverv, gave eller anden fordel for at formå den pågældende til at gøre eller undlade noget i tjenesten"

sig skyldig i aktiv bestikkelse af personer i offentlig tjene-
ste eller hverv, hvilket kan straffes med bøde eller fæng-
sel i op til seks år. Også i virksomheder, der udover
"funktioner på det offentliges vegne", men er organiseret
som erhvervsdrivende selskaber (f.eks. forsyningssirk-
somheder), kan de ansatte betegnes som udøvere af et
"offentlig hverv".

Det skal tilføjes, at "gaver eller anden fordel" omfatter såvel økonomiske som andre fordele, f.eks. tilsvarende om personlige ikke-økonomiske gentjenester. Yderligere er det værd at bemærke, at det er uden betydning, om fordele komme andre til gode, så som ægtefælle, børn eller andre hvis fordel pågældende har interesse i.

Ovenstående ligger til grund for, at det klart anbefales, at virksomheder afholder sig fra at give gaver til offentlig

tjenestemænd, også selv om det er mindre gaver, som er givet i god tro. For mens ovenstående dækker aktiv bestikkelse af offentlig tjenestemand, dækker straffelovens § 144 offentlige tjenestemænds passive uberettiget modtagelse af en gave eller anden fordel, selv om gaven eller fordele ikke er givet med henblik på at få tjenestemannen til at foretage eller undlade at foretage en handling, men f.eks. alene er givet som belønning for en allerede udført handling uden forudgående tilsvarende.

Også bestikkelse af ansatte i den private sektor er forbudt i henhold til den danske straffelov. Ifølge § 299, nr. 2 kan den som

*"ved varetagelse af en andens formueanliggen-
der for sig selv eller andre på pligtstridig måde
modtager, fordrer eller lader sig tilslige gave eller
anden fordel, såvel som den, der yder, lover
eller tilbyder en sådan gave eller anden fordel"*

straffes med bøde eller fængsel i op til fire år. Som det er tilfældet med bestikkelse af offentlige tjenestemænd, vil man kunne straffes i Danmark, hvis man for eksempel vælger at bestikke sig til en kontrakt hos en privat køber i udlandet. Modsat § 122 vil f.eks. beværtning sjældent anses som en gave eller anden fordel, ligesom markedsførings- og reklamekampagner almindeligvis ikke falder ind under loven. Der er således en bredere ramme for gaver og repræsentation overfor private aktører end offentlige, såfremt disse er givet i åbenhed i forhold til arbejdspladsen, og ikke kan betegnes som ekstravagante og dermed falder ind under skattelovgivningen.

Grundet de forskelligartede regler for gaver og anden fordel har mange virksomheder i dag klare politikker for hvad medarbejderne må give og modtage, og hvordan det skal foregå. Overordnet er der dog sket en kraftig reduktion af gavegivning i den private sektor, som med nogen ret kan tilskrives den store opmærksomhed nogle gavesager har haft i medierne, sammen med større formalisering af gavepolitikker og anti-korruptionsprogrammer de seneste år blandt danske virksomheder.

Ud over den danske lovgivning, og lovgivningen i de lande man som virksomhed har filialer eller datterselskaber i, skal man være bevidst om nationale regler i de lande, man i øvrigt gør forretning eller opererer i. Det er snarere reglen end undtagelsen i dag, at lovgivning på området er eksterritorial. Dækker virksomheden flere jurisdiktioner, kan lovgivningen meget vel variere fra land til land, hvilket fører til at kompleksiteten stiger. Det leder typisk til, at virksomheder sigter mod et strengere compliance-niveau, der dækker bredt, for at mindske risikoen for nationale forskelle og fortolkninger.

Amerikansk lovgivning

USA var i mere en 20 år det eneste land, der i kraft af The Foreign Corrupt Practices Act (FCPA) fra 1977 havde mulighed for at retsforfølge virksomheder for bestikkelse af offentlige embedsmænd i udlandet. Den amerikanske korruptionslovgivning er gældende for danske virksomheder, der er registreret i USA.

Det betyder også, at danske virksomheder, der er registreret på amerikanske fondsbørser, er berørt af the Sarbanes-Oxley Act fra 2002. Sarbanes-Oxley kræver blandt meget andet, at virksomheder etablerer en fortrolig kanal til brug for ansatte, der ønsker at rapportere om ulovligheder – de såkaldte whistleblower-ordninger. Samtidig lægges der i United States Sentencing Commission vægt på, at bøder kan reduceres væsentligt, såfremt virksomheden kan dokumentere samarbejde med myndighederne, at forseelsen var et enkeltstående tilfælde uden link til topledelsen og at der er implementeret et anti-korruptionsprogram i virksomheden. Disse elementer er også tydelige pejlemærker i den britiske lovgivning.

Blandt OECD-landene er USA den jurisdiktion med den mest aktive håndhævelse af anti-korruptionslovgivningen. Ud af 427 sager er de 128 ført af de amerikanske myndigheder, efterfulgt af Tyskland med 26 sager, mens England findes længere nede på listen. Noget tyder dog på, at det kommer til at ændre sig i fremtiden som følge af opprioritering af emnet i England.

Britisk lovgivning

Den britiske anti-korruptionslov, UK Bribery Act, trådte i kraft den 1. juli 2011. Alle virksomheder med aktiviteter i Storbritannien er omfattet af loven, som også gælder for virksomhedernes aktiviteter uden for Storbritannien. Lozen kan have vidtrækende konsekvenser for danske virksomheder, der har en filial, datterselskab, salgskontor eller lignende i England, da de vil være underlagt den britiske anti-korruptionslovgivning.

Virksomheder er også ansvarlige for handlinger begået af agenter og andre repræsentanter for virksomheden, såfremt det kan påvises, at virksomheden har fået en uberettiget fordel som følge af handlingen eller burde have vidst gennem sin risikostyring, at der var en risiko for bestikkelse.

De britiske guidelines i tillæg til lovgivningen anbefaler derfor, at der foretages due diligence, hvor det undersøges, hvem man ansætter, og om agenter, leverandører og samarbejdspartnere har været involveret i korruptionssager, eller er i risiko for at anvende bestikkelse. Hvis en af virksomhedens ansatte eller en agent, der repræsenterer virksomheden, begår bestikkelse, kan det give

høje bøder, offentlig udhængning og udelukkelse fra offentlige udbud.

Dog er den britiske lovgivning indrettet således, at myndighederne i deres vurdering af hvorvidt der skal rejses tiltale, eller ved tilbud om at indgå en deferred prosecution agreement¹, vurderer om virksomheden kan påvise, at den har tilstrækkelige procedurer sat op internt, og at hændelsen var en enlig svale, initieret af medarbejderen eller agenten selv. Herved kan virksomheden muligvis klare frisag. Det vil dog altid være en individuel vurdering fra sag til sag hvorvidt virksomheden har gjort nok for at forebygge.

Faciliteringspenge: Go eller no-go?

Brugen af faciliteringspenge, eller smørelse som det også kaldes herhjemme, er et evigt omstridt emne. I praksis såvel som lovgivningsmæssigt. For mens brugen af faciliteringspenge er indskrevet i den britiske lov som direkte ulovlig, er det undtaget af både den danske og amerikanske lovgivning, såfremt der er tale om en almindelig praksis i det land, hvor det finder sted, hvorved betalingen ikke er uberettiget.²

Hvis man for eksempel skal krydse grænsen til Ukraine, og her skal betale € 10 for at få sine varer gennem tollen, til trods for at alle papirer og licenser er på plads, vil det ikke være ulovligt efter dansk og amerikansk lov, fordi det desværre er helt almindelig praksis, mens det derimod er ulovligt ifølge den britiske lovgivning. Det er dog vigtigt at bemærke, at lovligheden altid skal bero på en konkret vurdering i det enkelte tilfælde. En systematisk accept af faciliteringspenge er således ikke i overensstemmelse med lovgivningen i Danmark. Det tilrådes derfor, at virksomheder har en politik om generelt ikke at gøre brug af faciliteringspenge, men at det i særlige tilfælde, hvor ingen anden mulighed er tilgængelig, undtagelsesvist accepterer betalingen.

¹ Deferred Prosecution Agreements er aftaler med myndighederne om samarbejde mod at tiltale ved domstolene udelades dog med mulighed for bøder, konfiskation m.v. Denne fremgangsmåde leder typisk til hurtigere afgørelser.

² Se i øvrigt Justitsministeriets pjece "Undgå korruption" fra 2015.

Det pointeres, at mens ligningslovens § 8 D siden 2013 omfatter forbud mod fradrag af bestikkelsesomkostninger, som i Danmark ville være strafbare, men ikke ville være det i udlandet, så er det ikke direkte klart, "hvorvidt ligningslovens § 8 D udelukker fradrag for small facilitation payments foretaget i udlandet, hvis betalingerne bedømt efter dansk ret anses for straffri.³ Det medfører en umiddelbar usikkerhed om fradrag for faciliteringspenge. En usikkerhed som flere og flere virksomheder dog forholder sig til ved at indføre interne rapporteringsprocedurer, således at virksomheden kan opgøre betalingerne og få overblik over, hvor de finder sted. Baggrunden herfor er dels at komme problemet til livs, ved at adressere myndighederne som forlanger disse betalinger, og dels at undgå en uagtet kambulering med skattelovgivningen.

Ny anti-korruptionsstandard giver et fælles sprog

Et nyt værktøj målrettet virksomheder og organisationer til styrkelse af de interne processer for anti-korruption blev publiceret i oktober 2016. Det går under det knap så mundrette navn ISO 37001 Ledelsessystemer vedrørende anti-korruption, og er, som navnet siger, en standard på, hvad ledelsessystemet bør indeholde for at øge resisten- sen mod korruption. Standarden er således også kompatibel med andre ledelsesstandarder såsom ISO 9001.

Det ser på stående fod ikke ud til, at mange danske virksomheder vælger at lade sig certificere. Men standarden vil i stedet blive brugt som et benchmarking værktøj, hvor virksomheder kan vurdere, om de har de nødvendige interne procedurer, politikker og kontroller på plads, i forhold til hvad der er international praksis. Og her skaber standarden en global konsensus om, hvad der udgør et anti-korruptionsprogram.

Når vi ser på den britiske og amerikanske anti-korruptionslovgivning, er der ingen tvivl om, at ISO 37001 standarden bliver en rettesnor for, hvad der anses for tilstrækkelige procedurer i en virksomheds anti-korruptionsprogram. Samtidig forventes det også, at virksomheder vil komme til at indskrive i sine kontrakter, at leverandører skal leve op til standarden for på den måde at sikre sig mod at blive associeret med samarbejdspartners mulige korrupte handlinger, hvilket selvført vil styrke udbredelsen af standarden. Det forventes dog næppe at blive et krav, at man er direkte certificeret i standarden,

blot at man følger dens anbefalinger. Allerede i 2012 udgav det internationale handelskammer dog en anti-korruptionsklausul, som virksomheder kan anvende i deres kontrakter internationalt.⁴ Det er en tydelig trend, at anvendelse af kontraktretlig regulering af korruption og bestikkelse vil vinde mere og mere frem de kommende år.

Et interessant træk ved standarden er, at der eksplisit står nævnt, at bestyrelsen skal vise lederskab og tage det overordnede ansvar for virksomhedens procedurer og politikker. Tillige skal ledelsen opbygge en tillidskultur, "culture of integrity". Overordnet er netop organisationskulturen et gennemgående træk i standarden, som også bliver bærende for, hvorvidt virksomheden reelt lever op til sine ord, på samme måde som netop den britiske anti-korruptionslovgivning lægger op til.

Men også i dansk lovgivning nævner såvel selskabsloven § 115 som årsregnskabsloven § 107b, at bestyrelsen skal sikre, at virksomheden har de fornødne procedurer for risikostyring og interne kontroller, samt at disse er beskrevne og formaliserede. Den nye standards fokus på bestyrelsen og øverste ledelse er derfor ikke ukendt i eksisterende lovgivning, om end det ikke er nævnt eksplisit i den danske anti-korruptionslovgivning. Den danske revisorlov § 31 pointerer dog også, at revisionsudvalget i børsnoterede virksomheder skal påse, at den interne revision og risikostyringssystemer er tilstrækkelige og effektive.

Flere faktorer til grund for anti-korruptionsprogrammer

Anti-korruption og compliance området er i stigende grad i vækst blandt danske virksomheder. Det skyldes som nævnt ovenfor den styrkede internationale lovgivning og regulering, men også en række andre faktorer. Af medvirkende faktorer kan nævnes, den øgede internationalisering af danske virksomheder på markeder som ikke tidligere var i kikkerten, men hvor virksomheder nu møder eller hører om udfordringer med korruption og bestikkelse, som medarbejderne skal klædes på til at kunne håndtere. Men den øgede internationalisering betyder også, at danske virksomheder i højere grad ansætter medarbejdere med forskellige kulturelle baggrunde. Denne øgede diversitet på arbejdsplassen kalder ofte også på et større behov for at ensrette praksis og regler, således

³ "Korruption og bestikkelse i forretningsforhold" i *Erhvervs strafferet*, Karnov Group, 2015.

⁴ ICC Anti-Corruption Clause, 2012.

at virksomheden får opbygget en stærk og solid virksomhedskultur med høj integritet, hvor alle trækker i samme retning med samme værdier.

Vigtigheden heraf skal også ses i lyset af den lette adgang til information og viden om samarbejdspartnere i dag. Bliver en virksomhed indblandet i en korruptionssag, spredes informationen hurtigt via internettet, sociale medier og virksomheder der udbyder due diligence services. Branding af virksomheden som anti-korrupt og med høj integritet som kunder, leverandører, investorer og andre kan have tillid til, er derfor sårbare over for medarbejdere, som ikke følger virksomhedens regler og politikker. Denne goodwill og renomme er ikke let at opbygge med en korruptionssag i bagagen, og kan koste virksomheden dyrt.

Det er i dette lys anti-korruptionsprogrammer drives fremad og gennem de seneste år har udviklet sig til at være mere omfattende i deres scope, således at de ikke

blot er et fordyrende add-on. Compliance og anti-korruption indgår derimod i stigende grad i de strategiske forretningsmæssige overvejelser og virksomhedens risikoappetit, og bidrager positivt til værdiskabelsen internt. Det betyder også, at ledelsens fokus herpå kommer til udtryk i ikke blot virksomhedens politikker, men også at træning af ansatte og konsekvenserne ved overtrædelser af politikkerne foregår mere konsekvent, ligesom der er set en stor stigning i antallet af whistleblowing systemer i Danmark.

Samlet investeres der meget tid og mange ressourcer i anti-korruptionsprogrammer blandt danske virksomheder, og der er ikke længere behov for at forklare virksomheden hvorfor. I stedet drejer spørgsmålene sig nu mere om hvordan. Det lægger samtidig pres på regeringer for at højne deres standarder og mindske både mulighederne, men også den mange steder accepterede praksis, at kontrakter, licenser og tilladelser "koster lidt ekstra".



Sådan undgår du, at korruption bliver et problem



Jeppe Kromann Haarsted, Group
Compliance Manager, FLSmidth A/S

Indledning

Et hurtigt blik på et par internationale korruptionssager vil formodentlig få de fleste beslutningstagere i virksomheder til at sikre sig, at de gør et eller anden ved det emne. I denne artikel forsøger jeg at opnå grundprincipperne for det praktiske arbejde med at bekæmpe korruption i en virksomhed. Dette arbejde kalder vi normalt blot "compliance" eller "legal compliance", og de ansvarlige har typisk titler som "compliance manager", "compliance officer" eller lignende. Det er en disciplin og titel, der er ganske ny i Danmark men også en, der udvikler sig meget hurtigt i disse år. Måske er det derfor, at vi bruger mange engelske ord og ofte slet ikke kan finde passende danske udtryk for ord som "compliance" eller "due diligence". Så tilgiv din compliance manager, hvis han eller hun lyder en smule fjllet.

De fleste store danske virksomheder har i dag en compliance-afdeling, og mange mellemstore virksomheder opretter i disse år compliance-funktioner i en eller anden udstrækning. Væksten i compliance-afdelinger og deres ansvarsområder har været organisk og lidt rodet. For en del virksomheder startede det med, at de skulle have et adfærdskodeks (Code of Conduct), for det havde kunderne og de andre store danske virksomheder. Så kom mange i tanke om, at de hellere måtte lave en udgave, der var til at forstå, og træne medarbejdere i reglerne. Og oprette en whistleblower hotline. Og sørge for, at også samarbejdspartnere såsom distributører og agenter forstod reglerne. Og hvad med internationale sanktioner og persondata? På den måde voksede compliance til at blive et selvstændigt fagområde.

Grundprincipper

I dag findes der heldigvis et par standarder og dokumenter, man kan støtte sig til, når man prøver at opbygge et compliance-program. Tendensen i disse år går mod større standardisering og det er positivt, da det kan være med

til at gøre nogle af de meget ressourcekrævende opgaver lidt lettere.

To vigtige dokumenter er det såkaldte "Guidance Document", som er et bilag til UK Bribery Act, Storbritanniens anti-korruptionslov, og den tilsvarende "Ressource Guide" til den amerikanske lov Foreign Corrupt Practices Act (FCPA). Begge dokumenter opnås, hvad myndighederne i de to lande mener, at et solidt compliance-program bør indeholde. I november 2016 lancerede ISO en ny international standard for compliance – ISO 37001. Denne standard er certificérbar og kan underkastes revision. ISO 37001 har potentiale til at blive den vigtigste internationale standard, men det er stadig for tidligt at sige, hvor mange virksomheder, der vil gøre brug af den. I gennemgangen nedenfor tager jeg udgangspunkt i UK Bribery Acts seks grundpiller for et compliance-program.

UK Bribery Act – de seks grundpiller

1. Risikovurdering
2. Opbakning fra ledelsen
3. Regler og organisation
4. Træning og kommunikation
5. Due diligence
6. Kontrol og monitorering.

Risikovurdering

Den første og absolut en af de vigtigste opgaver er at lave en grundig risikovurdering. Ingen virksomhed kan sikre sig 100% imod, at en medarbejder eller samarbejdspartner gør noget ulovligt. Derfor må man fokusere på det, der udgør den største risiko. Compliance er blevet en ganske ressourceret opgave, så en risikovurdering er også vigtig i forhold til at prioritere ressourcer og undgå, at compliance manageren går ned med stress efter seks måneder i jobbet.

En risikovurdering bør indeholde en række dimensioner og emner. Typisk vil man vælge at undersøge risikoen for forskellige typer af overtrædelser (bestikkelse, brud på gaveregler, konkurrenceret etc.), i forskellige lande/geografiske regioner, og i forhold til forskellige typer af kunder, samarbejdspartnere og kontraktformer. Nogle virksomheder vælger at sende et survey ud til en repræsentativ gruppe af medarbejdere, nogle foretrækker dybdegående interviews med nøglemedarbejdere, mens andre primært baserer analysen på eksterne kilder. Korruption er et ømtåligt emne, så uanset hvordan data indsamles, er det meget vigtigt at gøre klart, om der er tale om en anonym undersøgelse, og hvad den skal bruges til.

Opbakning fra ledelsen

Det siger næsten sig selv, at et adfærdskodeks uden ledelsens fulde opbakning vil have en meget lille effekt. Det er derfor helt essentielt, at den enkelte medarbejder er klar over, at ledelsen virkelig mener det, når de får at vide, at de skal sige nej til en forretningsmulighed, hvis det involverer et brud på lovgivning eller adfærdskodekset. Den besked går formodentligt først helt klart ind, når medarbejderne ser den øverste ledelse eksplisit nævne adfærdskodekset og gøre det helt klart, at de støtter op om det. Medarbejderne tager det ikke for givet, at ledelse mener det alvorligt. De tror først på det, når de ser deres administrerende direktør eller egen chef fortælle det – gerne i egen person, eller på video el. lign.

Desuden er det vigtigt, at den øverste ledelse konsekvent tager den rigtige beslutning, når virksomheden står over for svære beslutninger, der kan involvere brud på lovgivning. Ligesom alle er lige for loven bør alle medarbejdere behandles ens, hvis de har brutt reglerne. Den største fare er nok, hvis ledelsen giver køb på principperne, når der er en stor ordre på spil, eller hvis en nøglemedarbejder i en høj position går fri efter et alvorligt brud på reglerne, mens den menige medarbejder bliver afskediget. I sådanne tilfælde er der en stor risiko for, at medarbejderne opfatter compliance-arbejdet som ren pynt, og der kan hurtigt danne sig en kynisk holdning blandt medarbejderne.

Regler og organisation

Virksomheden skal klart definere, hvilke regler der gælder for medarbejdere og evt. samarbejdspartnere. Dette gøres som oftest i et adfærdskodeks (Code of Conduct).



I dag ligner de fleste adfærdskodekser hinanden. De indeholder typisk forbud mod bestikkelse, smørepenge og svindel, samt regler for interessekonflikter, gaver, middage, underholdning, donationer, interaktion med embedsmænd og konkurrenceret. Nogle adfærdskodekser dækker også emner som diskrimination, hvidvask af penge, IP-rettigheder eller regler om god opførsel på arbejdspladsen. Der kan dog stadig være forskelle i tilgangen til visse emner, særligt angående reglerne for smørepenge, som nogle virksomheder tillader i særlige situationer, eller i forhold til gaveregler, hvor standarderne kan variere meget. Den største forskel på adfærdskodekser i dag

er nok i virkeligheden, hvilke emner man har valgt at inkludere, hvor præcis man har valgt at være, og hvordan man har valgt at kommunikere det.

Derudover skal virksomheden kunne redegøre for, at den har oprettet en organisation til at håndtere compliance. Én løsning er at oprette en central afdeling, som implementerer compliance globalt. En anden populær model blandt danske virksomheder er en mindre central organisation, som udstikker retningslinjer og værktøjer, og hjælper forretningsenheder eller underselskaber med at implementere dem. Nogle virksomheder har udpeget regionalt ansvarlige chefer eller advokater, der fungerer som en forlænget arm for compliance i den pågældende region. Virksomheden bør vælge det setup, der passer bedst til den, men det er vigtigt, at den kan redegøre for, hvorfor det er en effektiv løsning.

Træning og kommunikation

Adfærdskodekser skal ofte bruges til kontrakter o. lign. og er derfor ikke nødvendigvis specielt læsevenlige. Desuden vil der altid være et vist rum for fortolkning. Det er derfor vigtigt, at virksomheder løbende kommunikerer omkring adfærdskodekset og underviser medarbejderne. Mange virksomheder vælger en kombination af klasseværelsestræning og e-læring. Klasseværelsestræning har den fordel, at det giver rum til debat og mulighed for, at medarbejderne selv kan tage stilling til dilemmasituitioner, hvilket øger chancen for, at de kan huske reglerne. Det er dog også meget tidskrævende, så en del virksomheder fokuserer derfor på e-læring, eller de bruger små animationer, video eller online spil til at minde medarbejderne om reglerne med jævn mellemrum. Uanset træningsmetoden er det helt essentielt, at virksomheden registrerer, hvem der er blevet trænet hvornår.

Et succesfuldt compliance-program er også afhængigt af, at reglerne bliver kommunikeret klart og jævnligt bliver gentaget i et nemt og forståeligt sprog. Det kan være lidt af en balancegang mellem at forklare reglerne kort, præcist og gerne med lidt humor, og samtidig understrege alvoren i emnet og de konsekvenser, det kan have for implicerede medarbejdere og virksomheden. For virksomheder, som arbejder globalt er det her også vigtigt at tænke på, hvordan man kommunikerer til forskellige kulturer og på forskellige sprog. For eksempel indikerer et ord som "bestikkelse" på visse sprog en helt specifik udveksling af penge og tjenester, mens det på andre sprog indikerer en bredere vifte af situationer, fx udveksling af gaver, visse former for drikkepenge etc. Nogle kulturer vil sætte pris på en vis portion humor i kommunikationen, mens det for andre kulturer kan være bedre at holde sig til den mere alvorlige tone.

Due diligence

Den største arbejdsbyrde for mange compliance managers i dag er due diligence af agenter, distributører, konsulenter, leverandører og kunder. Due diligence betyder kort sagt, at virksomheder ser grundigt på sine samarbejdspartnere og vurderer, hvilke compliance-relatede risici, der måtte være. Det kunne for eksempel være, at samarbejdspartneren ikke er ordentligt registreret i virksomhedsregistre, at den har kontor i et skattely, at den er dømt for bestikkelse eller brud på sanktionsregler, at den har været genstand for negativ presseomtale, og meget andet. Typisk laver man også en lignende analyse af enkeltpersoner tilknyttet samarbejdspartneren. Endelig bør en due diligence-rapport indeholde en analyse af en række kommercielle aspekter, herunder betaling og betalingsformer, business casen for at indgå et samarbejde, kontraktuelle forhold etc. Ud fra sådan en analyse må virksomheden så afgøre, om den kan leve med de risici, der måtte være, om den kan hjælpe samarbejdspartneren med at forbedre sig, eller om den vil afbryde samarbejdet.

Due diligence-arbejdet er for mange virksomheder relevant både i forbindelse med introduktion af nye samarbejdspartnere og løbende i forhold til eksisterende samarbejdspartnere. En særlig grundig form for due diligence bruges typisk i forbindelse med fusioner (mergers and acquisitions).

Due diligence-arbejdet kan være meget tidskrævende og indebærer ofte store mængder data. Som udgangspunkt bør virksomheden underkaste samtlige samarbejdspartnere en eller anden form for analyse, men det er normalt umuligt at foretage en dybdegående analyse af hver eneste. Et vigtigt første skridt er derfor typisk at definere, hvilke samarbejdspartnere, man vil undersøge grundigt og hvilke, man kan lade gå gennem et mere overfladisk tjek. Der findes i dag mange forskellige muligheder for at købe sådanne analyser – alt fra helt basale tjek af firma-navn på sanktionslister til meget grundige analyser, der nærmer sig detektivrapporter. Nogle virksomheder prøver også at udvikle kompetencer og procedurer, så de selv kan lave nogle af analyserne internt.

Kontrol og monitorering

Det sidste element i et compliance-program er kontrol og monitorering. Kontrol indebærer mange ting, som ofte ligger uden for eller på grænsen af compliance-funktionens ansvarsområde, herunder intern og ekstern revision, interne finansielle kontroller, kontrol med ekssterne betalinger, interne udbudsprocedurer etc. Et i Danmark ret nyt emne er dataanalyse, hvor virksomheden analyserer store mængder data, herunder typisk betalinger og fakturaer, for at finde anomalier og dermed mulige

eksempler på svindel eller andre brud på adfærdskodekset. Desuden laver en del compliance managers intern revision af datterselskaber, landekontorer eller enkeltafdelinger, fx for at tjekke, om de har implementeret adfærdskodekset korrekt og om den lokale ledelse tager emnet alvorligt.

Et andet vigtigt element er brugen af whistleblower hotlines – altså en kanal, som medarbejdere kan bruge til at rapportere uregelmæssigheder. En virksomhed kan introducere mange interne kontroller, men i sidste ende vil der nok altid være et vist spillerum for svindel, hvis noget i en betroet stilling eller beslutningskompetence virkelig vil det. Ofte vil der dog være andre medarbejdere, som ser med på siden, som bliver bedt om at hjælpe på en eller anden måde, eller som bare har en fornemmelse af, at noget ikke er, som det skal være. Det kan også være, at en samarbejdspartner eller konkurrent har viden om eller indtryk af, at der er sket brud på reglerne. For mennesker i den situation vil det være helt essentielt, at de har mulighed for at rapportere på en fortrolig måde, og i mange tilfælde vil de også ønske at være helt anonyme. Der findes i dag forskellige whistleblower hotline-systemer, som gør det muligt at rapportere anonymt samtidig med, at man kan kommunikere med vedkommende, også anonymt. Det er i denne sammenhæng vigtigt at have etableret særlige procedurer for at foretage en intern efterforskning af indrapporterede sager. Sådanne procedurer bør bl.a. beskrive, hvem der modtager rapporterne, hvem der undersøger hvad, hvem der tager beslutningen om eventuelle sanktioner, hvordan man foretager et interview, og hvor man opbevarer dokumentation og hvor længe.

Intern revisions rolle

Intern revision spiller en central rolle i forhold til compliance-arbejdet, særligt i forbindelse med kontrol og monitorering. Det er derfor vigtigt, at de to funktioner har tæt kontakt og forstår, hvad der er relevant for den anden funktion og hvordan den arbejder. Desuden er intern revision bedre klædt på til at undersøge svindelsager, som typisk kræver en grundig forståelse af finansielle procedurer og kontroller, samt nem og direkte adgang til den relevante information internt i virksomheden. Enkelte danske virksomheder har valgt at slå legal compliance-funktionen sammen med finansiel compliance-funktionen, hvilket formodentlig er en genvej til et samarbejde med mange fælles udfordringer og ensartede arbejdsmetoder.

Hvorfor er fokus på korruption vigtig for Intern Revision?



Johan Bogen-toft, Partner,
PwC



Rasmus Grejs
Beyer, Senior
Manager, PwC



Martin Schantz
Pickardt, Senior
Consultant, PwC

Indledning

Danmark oplever et lavt niveau af korruption, relativt set, i sammenligning med resten af verden.¹ Ikke desto mindre har der også været danske korruptionssager, og i takt med, at danske virksomheder etablerer sig i udlandet, eller indgår samarbejde med udenlandske selskaber, eksponeres danske virksomheder over for risikobilledet i de pågældende lande. Samtidig har mange lande indført skærpede lokale lovgivninger på området, og flere af lovene er ydermere eksteritoriale, hvilket kan ramme et dansk moderselskab.

I takt med det øgede fokus, og de strammere lovgivninger, har de seneste år vist et stort antal sager, som har haft store konsekvenser for virksomhederne. Korruptionssagerne har ikke blot medført store økonomiske tab og bøder for de involverede virksomheder, der har også været tilfælde af fængselsstraffe for de ansvarlige forretningsledere.² Virksomhederne lider ikke blot det umiddelbare tab ved en retssag, men ofte også et stort tab i omødmme samt i forholdet til kunder og interesser, som risikerer at gå tabt.

Derfor er det vigtigt, at Intern Revision til stadighed har fokus på at sikre, at virksomheden har et nødvendigt

¹ Danmark var i 2015 det land, med mindst korruption i den offentlige sektor, af i alt 168 lande/territorier i følge Transparency International – Corruption perceptions index 2015.

² Flere sager kan nævnes, men eksempelvis blev flere af de ansvarlige i virksomheden Smith and Ouzman Ltd blev idømt fængselsstraffe i 2015 i en sag om bestikkelse. Læs mere om sagen [her](#).

³ Appendix til World Economic Forum's 2005-2006 Global Competitiveness Report (link), side 97. En analyse fortaget af en forhenværende direktør i Verdensbanken med ansvar for at lede arbejdet på omkring bekämpelse af korruption.

niveau af kontroller på plads til at minimere risikoen for korruption til et acceptabelt niveau. Flere virksomheder har indført en nultolerance i forhold til korruption, da én enkelt hændelse kan have vidtrækkende negative konsekvenser for virksomheden. Andre virksomheder kan principielt have accepteret en lidt højere risikoappetit, hvis de eksempelvis opererer i markeder hvor smørelse (facilitation payments) er uundgåeligt.

Hvad er korruption?

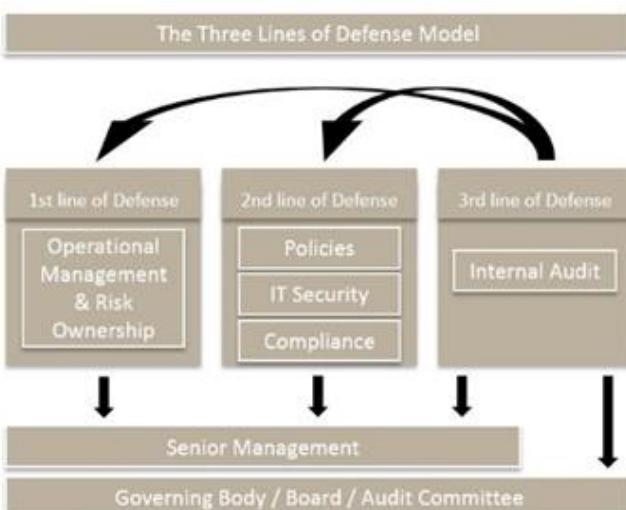
Korruption findes i mange former. Velkendte eksempler herpå kan være bestikkelse, bedrageri, underslæb, mandatsvig, embedsmisbrug og nepotisme, men det findes også i form af pengehvidvask, priskarteller, eller korruption i relation til eksportkontroller. De forskellige typer af korruption kan endvidere foregå mere eller mindre koordineret, og med ledelsens direkte eller indirekte involvering, eller for medarbejderens egen vindings skyld. Korruption kan samtidig være enkeltstående eller gentagne handlinger som er systematiseret over en længere periode.

Ud af de forskellige typer korruption er bestikkelse et af de mest aktuelle emner. Verdensbanken anslår således, at omkring 1 Billion USD bliver betalt som bestikkelse hvert år.³ Samtidig viser den seneste tids store korruptionssager, samt den skærpede lovgivning og senest den nye ISO 37001 standard, at bestikkelse bør være et risikoområde som Intern Revision har fokus på. Derfor har vi i artiklen fokus på netop bestikkelse.

Intern Revisions tilgang til korruption (Bestikkelse)

Korruption og bestikkelse vil ikke altid efterlade tydelige spor i de finansielle regnskaber. Sporerne skal derimod

Figur 1. The Three Lines of Defense Model



findes i medarbejderens eller ledelsens handlingsmønster, eller ændringen heraf, hos de ansatte i virksomheden, som besidder en autorisation/mandat til at fx at bruge af virksomhedens penge, indgå aftaler med partnere og leverandører, give rabatter og/eller personer, som er provisionslønnet eller på anden måde får en performancerelateret løn. Samtidig skal Intern Revision forholde sig til, at skellet mellem korruption og lokalt anerkendt handelspraksis kan fremstå udvasket. Bestikkelse er udbredt i mange kulturer og områder af verdenen, da man oplever det at modtage og udveksle gaver som normal praksis for handel. Men ikke mindst fordi det kræver erfaring og specialiseret viden for at kunne identificere risikoen for korruption og bestikkelse.

Intern Revision kan bidrage til kampen mod korruption ved at give deres uafhængige assurance, og udfordre integriteten og effektiviteten i risikostyringsrammeværket samt dets implementering på tværs af hele koncernen. Herunder kan Intern Revision udføre revision af 1st line & 2nd line jævnfør "The Three Lines of Defense" modellen (se **Figur 1** på foregående side).

Revision af kontrolmiljøet i virksomheden

Når Intern Revision har lavet en risikovurdering af den organisation, som skal revideres, er der et godt udgangspunkt for at kigge på fordelingen af roller og ansvar mellem 1. & 2. Line of Defense vedrørende risikoen for korruption, og vurdere om den er hensigtsmæssig.

Intern Revision kan dernæst se på designet af kontrolapparatet som 2. line of Defense har sat op. Her kan med fordel revideres op mod lovgivning, eller benchmarke mod best practice.

Inden for bestikkelse er der flere lovgivninger man kan revidere op mod. Hvis man udelukkende opererer i Danmark, kan man tage udgangspunkt i straffelovens regler om bestikkelse (som Justitsministeriet har redegjort for i pjecen "Undgå korruption").⁴

Er man derimod en mere internationalt agerende virksomhed, kan det være mere fordelagtigt at revidere op mod den eksterritoriale lovgivning, så som den Amerikanske FCPA (Foreign Corrupt Practices Act) eller den britiske UK Bribery Act. En af de skrappestes lovgivninger er UK Bribery Act.

⁴Ifølge Justitsministeriet "Pjecen har først og fremmest til formål at højne kendskabet til korruption og bestikkelse. I pjecen redegøres for straffelovens regler om bestikkelse, og der gives gode råd om, hvordan den enkelte kan gøre sit til at modvirke korruption og bestikkelse". Pjecen kan tilgås her.

Figur 2. UK Bribery Act vs. FCPA

UK Bribery Act	vs.	FCPA
Bribe payer, company and receiver	Target	Bribe payer
Public and private sector	Applicability	Public sector
Extra-territorial	Reach	Extra-territorial
Active and passive	Type of bribery punished	Active
Yes	Third party exposure	Yes
Criminal	Facilitation payments	Allowed

I forhold til FCPA rammer UK Bribery Act både den offentlige og private sektor samt både "giver og modtager" af bestikkelse og anser i principippet smørelse som en kriminel handling.

Udover at være et godt benchmark, er UK Bribery Act relevant for de fleste danske virksomheder med internationale aktiviteter, idet den er eksterritorial og danske virksomheder kan derfor rammes af den overalt i verdenen, såfremt de har en tilknytning til UK. Forskellen på UK Bribery Act og FCPA fremgår nærmere af **Figur 2**.

Vejledende principper

UK Bribery Act giver en guidance på seks vejledende principper som en virksomhed kan tilstræbe at have på plads for at undgå risikoen for korruption - se **Figur 3**. Af guiden fremgår det, at en virksomhed skal have en risikobassert tilgang, og at principperne ikke er præskriptive. Ikke desto mindre giver principperne en god inspiration til Intern Revision i deres gennemgang af kontrolmiljøet.

Ifølge UK Bribery Act kan virksomheder eller personer ifaldes strafansvar, hvis den ikke forhindrer bestikkelse, eller kan bevise at den har tilstrækkelige foranstaltninger på plads. Der findes ikke en "one size fits all" men det er vigtigt at virksomheden har tilstrækkelige foranstaltninger på plads.

1. Proportional procedures

Har til hensigt at sikre, at virksomheden har et omfang af politikker og procedurer på plads, som modsvarer det

Figur 3. Guidance UK Bribery Act vs. FCPA

1	Proportionate procedures	4	Due diligence
2	Top-level commitment	5	Communication (including training)
3	Risk assessment	6	Monitoring and review

risikoniveau som virksomheden er eksponeret imod. Som inspiration kan Intern Revision således give deres uafhængige vurdering af, om virksomheden har et acceptabelt niveau af politikker på plads såsom adfærdskodekser, anti-korruptionspolitik, disciplinære processer, rejse - og gavepolitik, performance management-rammer m.v.

2. Top level commitment

Handler om, at bestyrelsen og den øverste ledelse tydeligt demonstrerer, at de er med til at bekæmpe korruption. Det er helt afgørende, at topledelsen udviser den rette holdning til korruption, og at medarbejderne ikke er i tvivl om ledelsens holdning.

Hvis Topledelsen ikke har den rette adfærd er det svært for medarbejderne at handle anderledes. Den interne revisor kan i den henseende evaluere the "tone at the top" og se om den er understøttet af kommunikationen fra den øverste ledelse om god etik.

Ifølge PwC's Global Economic Crime Survey fra 2016 er det således også opfattelsen, at medarbejdernes moral er det første og vigtigste værn mod korruption. Intern Revision kan eksempelvis se på, om ledelsen demonstrerer de rette værdier når de kommunikerer og om det det er dokumenteret.

Intern Revision kan også tale med medarbejdere, som vurderes at være særlig risikoeksponerede, og spørge ind til medarbejdernes opfattelse af, om ledelsen udviser en nultolerance over for korruption eller ej.

3. Risk assessment

Skal tilsiere at virksomheden har foretaget en vurdering af risikoen for bestikkelse i virksomheden. Det vil sige, har man fra virksomhedens side foretaget en vurdering af hvorledes/hvor man er mest eksponeret over for risikoen for bestikkelse.

Denne risikovurdering er helt afgørende for, om man som virksomhed kan prioritere sine ressourcer og kontrolaktiviteter optimalt. Logikken er således, at når først man har overblikket over sin risikoeksponering, kan man vurdere om man også har et effektivt design af kontroller og politikker, som kan mitigere hvert enkelt område.

Intern Revision vil kunne se på, om virksomheden har gennemført en risiko assessment og vurderet om relevante faktorer er belyst, så som landerisici, transaktionsrisici, brancherisici etc. Samtidig kan Intern Revision se videre på, om det eksisterende kontrolapparat er designet til, at mitigere de identificerede risikoområder hvor man eksempelvis kan foretage en fit/gap-analyse.

Her kunne det også være relevant for Intern Revision at se på om der er en klar ansvarsfordeling og ejerskab af processen, og om risikovurderingen foretages periodisk og bliver dokumenteret.

4. Due diligence

Et væsentligt element i UK Bribery Act er, at man som virksomhed kan blive stillet til ansvar for de gerninger som en tredjepart foretager på ens vegne. Tredjeparter er bredt defineret da det kan inkludere alle som bidrager til din virksomheds værdikæde, herunder leverandørsiden men også salgssiden (inklusiv distributører, agenter m.fl.) samt andre tredjeparter så som konsulenter m. fl.

Det vejledende princip vedrørende due diligence anbefaler, at virksomheder tager en risikobasseret tilgang til tredjeparter. Første skridt er at få et overblik over tredjeparterne, og dernæst foretage en risikovurdering af dem inden man foretager det relevante niveau af due diligence.

Intern Revision kan bidrage med, at se på om der er taget en risikobasseret tilgang, og se om alle relevante tredjeparter er inkluderet (erfaring viser, at det ofte er svært for en virksomhed at danne sig et fuldt overblik over tredjeparterne). Intern Revision kan se på om der er klare procedurer på plads vedrørende tredjeparter, og om der er en klar proces for, hvordan en tredjepart risikoklassificeres og på hvilket niveau en due diligence skal gennemføres.

Ydermere kan Intern Revision se på om den udførte due diligence er dokumenteret, og om den er udført af interne medarbejdere, som har den nødvendige erfaring og ekspertise. Ved due diligence på højrisiko-tredjeparter vælger nogle organisationer således at benytte sig af eksterne eksperter, der besidder værkøjer og metoder inden for områder som korruption og bestikkelse.

5. Kommunikation (inklusiv træning)

Det femte princip anbefaler, at virksomheden sikrer sig at deres politikker vedrørende bestikkelse er implementerede og forstået af hele organisationen, og at der er gennemført træning som er proportional med den risiko som findes.

Intern Revision kan se på om kommunikationen er kommet ud til alle, og undersøge om virksomheden har foretaget en relevant vurdering af hvilke medarbejdergrupper, som er mest eksponeret for korruptionsrisici, samt om organisationen har gennemført en tilpasset face to face undervisning og/eller e-learning, inklusiv tests der demonstrerer og dokumenterer træningen af virksomhedens medarbejdere.

6. Monitorering og gennemgang

Det sidste princip anbefaler, at virksomheden løbende monitorerer og gennemgår deres procedurer, samt tilpasser dem efter behov. Intern Revision kan se på, om virksomheden har mekanismer til at sikre, at de kan identificere hændelser, hvor anti-bestikkelsesmekanismer ikke fungerer efter hensigten, og om der bliver fulgt op derpå.

Test af operationelt effektive kontroller

I forlængelse af, at det er blevet vurderet om designet af kontrolmiljøet er hensigtsmæssigt, skal Intern Revision som vanligt efterprøve, om kontrollerne er operationelt effektive. Her giver det god mening at begynde med analytiske tests for at ramme en større population, og komplettere med klassiske stikprøver. Denne test kan gøres ved at teste kontrollerne og transaktionerne, som vurderes at være særligt utsatte for bestikkelse.

Områder som den interne revisor bl.a. kan kigge på her kunne eksempelvis være: "petty cash" register, kreditkorttransaktioner og expense/rejseafregninger.

Det vil også være interessant at se på high risk-betalinger, som eksempelvis kunne være betalinger til offentlige myndigheder i udlandet, ikke-standardbetalinger eller ekstraordinære rabatter, som kunne være en indikation på "indirekte" bestikkelse. Den interne revisor kunne også kigge på kontrakter, for at se om de indeholder signifikante kommissioner, eller kigge på områder i forretningen hvor manglende funktionsadskillelse (SoD) kunne have bevirket en øget korruptionsrisiko.

Konklusion

Meget tyder på, at korruption og bestikkelse er svært helt at komme til livs, men en effektiv Intern Revision kan spille en vigtig rolle i bekæmpelsen ved at give deres uafhængige assurance, samt udfordre integriteten og effektiviteten i risikostyringsrammeværket.

NB. Artiklens indhold skal udelukkende ses som inspiration, og ikke som udtømmende anbefalinger, rådgivning eller fyldestgørende arbejdsprogrammer.



Ny revisionsbekendtgørelse



Peer Højlund, Chefspecialist, Nykredit

Indledning

Finanstilsynet har i december 2016 udstedt ny revisionsbekendtgørelse.

Den nye bekendtgørelse træder i kraft den **1. januar 2017** og har virkning for revisionsprotokollater eller anden tilsvarende rapportering, der vedrører regnskabsår påbegyndt den **1. januar 2016** eller senere.

Hvor de senere års bekendtgørelser har indeholdt mere materielle ændringer, er der i årets bekendtgørelse kun foretaget ganske få justeringer, primært som følge af tilpasning til ændringer i anden lovgivning.

Nedenfor er årets tilføjelser og ændringer nærmere gen nemgået og kommenteret.

Årets ændringsforslag

Krav om at føre en revisionsprotokol

I juni 2016 blev der udsendt ny revisorlov, hvor det tidligere krav om at føre en revisionsprotokol opnåedes **for andre virksomheder end virksomheder af interesse for offentligheden**. Definitionen af "virksomheder af interesse for offentligheden" (såkaldte PIE-virksomheder) begrænses ifølge revisorloven til:

- Pengeinstitutter
- Realkreditinstitutter
- Forsikringsselskaber
- Virksomheder, der har kapitalandele, gældsinstrumenter eller andre værdipapirer optaget til handel på et reguleret marked i et EU-land eller et EØS-land.

For alle øvrige selskaber stiller **revisorloven** således **IK-KE** længere krav om revisionsprotokol, uanset om virksomheden er underlagt tilsyn eller ej.

I den ny Revisionsbekendtgørelse lægges der op til, at de nye krav i revisorloven også skal gælde vedrørende udarbejdelse af protokollater i finansielle institutter.

Det skal dog bemærkes, at Finanstilsynet endnu ikke har taget stilling til, om ændringerne skal gælde for både intern og ekstern revision. **Det er derfor vigtigt at understrege**, at ændringen i den nye bekendtgørelse er foretaget således, at det kun er de bestemmelser, der vedrører **den eksterne revisions protokol og afgivelse af konklusioner**, der er berørt, men at kravene til udarbejdelse af protokol og afgivelse af konklusioner er **uændrede for intern revision**. På et gå-hjem møde for IIA's medlemmer den 6. december 2016 har Finanstilsynet oplyst, at der arbejdes på en praktisk løsning, men at der indtil videre må tages udgangspunkt i, at kravene til intern revision **er de samme som tidligere år**.

For **ekstern revision** er revisionsbekendtgørelsen ændret således, at det i definitionen i § 5, stk. 1, nr. 1 er præciseret hvilke virksomheder (PIE-virksomheder), hvor ekstern revision har pligt til at føre revisionsprotokol. For virksomheder, der ikke er omfattet af denne definition, men som fortsat er underlagt tilsyn, er der dog fortsat krav til afgivelse af konklusioner (jf. bilag 1). Denne konklusionsafgivelse behøver altså ikke længere ske i form af et protokollat, men kan i stedet ske i form af "anden tilsvarende rapportering", hvilket er præciseret i alle relevante bestemmelser om den eksterne revisions protokollat.

Den nye definition ledsages af nye bestemmelser i § 5, stk. 5-9, hvor det fremgår, at såfremt ekstern revision vælger at udarbejde protokollat for en virksomhed, der efter de nye bestemmelser ikke er krav herom, så skal protokollatet udarbejdes efter de bestemmelser, der er relevante for PIE-virksomheder.

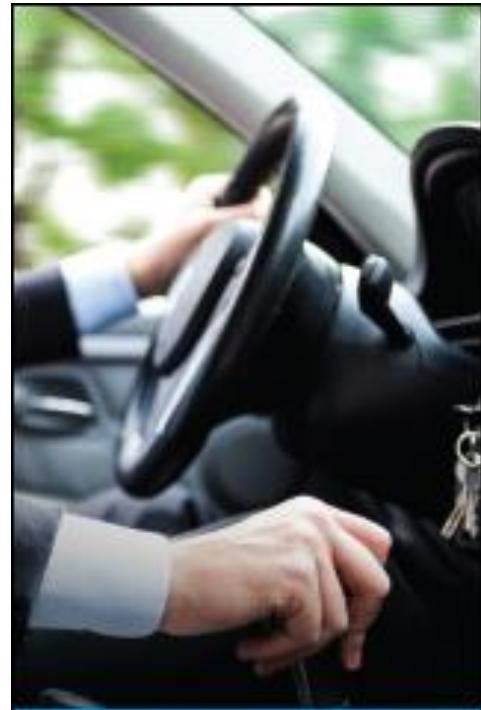
Langt hovedparten af de justeringer, der herefter forekommer i årets bekendtgørelse, vedrører konsekvensrettelser i revisionsbekendtgørelse og bilag i relation til ændringen af kravet om udarbejdelse af protokol. Justeringen er foretaget således, at der i tilknytning til begrebet "protokollat" foreslås tilføjet "eller anden tilsvarende rapportering". Endvidere bortfalder krav om indsendelse af protokollat til Finanstilsynet vedrørende ikke-finansielle dattervirksomheder (tidl. § 5, stk. 4).

For intern revision er kravene uændrede. Ændringen af krav til udarbejdelse af protokollater har som sagt ikke fundet vej til bekendtgørelsens § 26 om den interne revisions protokol, hvorfaf det således følger, at den interne revision, som hidtil, skal føre en protokol til bestyrelsen i alle virksomheder med hjemsted i Danmark.

Øvrige ændringer

Ud over ovennævnte ændring, er der tale om yderst beskedne justeringer, der primært har redaktionel karakter.

Dog skal nævnes, at der er der som følge af ændringer i bekendtgørelsen om ledelse og styring af forsikringsselskaber er der foretaget tilpasninger i revisionsbekendtgørelsen og berørte handlinger i bilag 2, så det fremgår, at indberetninger af kapitalforhold og risici (trafiklysindberetninger) fremadrettet alene gælder "gruppe-2 forsikringsselskaber".



Drive
Your
Career
Forward

IIA Certifications
and Qualifications

Invest In Your
Tomorrow, Today.

 The Institute of
Internal Auditors

IIA's standardpåtegning på årsregnskaber for finansielle virksomheder



Lars Geisler, Afdelingsdirektør,
Nykredit

Foreningen har i november 2016 opdateret IIA's standardpåtegning for de interne revisorer, som påtægner årsregnskaber for finansielle virksomheder. Faktisk har medlemmerne mulighed for at vælge imellem 2 påtegninger, som er [tilgængelige via foreningens hjemmeside](#) (man skal først være logget på hjemmesiden).

Hvorfor lige det?

Ændringerne i standardpåtegningen skyldes væsentlige ændringer til ekstern revisions påtegning, hvor bl.a. rækkefølgen af de enkelte afsnit er ændret. Læs mere om ændringer til påtegningen her:

http://www.fsr.dk/Faglige_informationer/Om_revisor/Lovgivning%20og%20bekendtgørelser/Ny%20revisorlov_De%20centrale%20forhold%20for%20alle%20revisorer_190516

For PIE-selskaber er der endvidere krav om at gengive centrale forhold ved revisionen (Key Audit Matters - KAM) i påtegningen.

Med ændringerne til ekstern revisionspåtegning stod IIA ved en skillevej: Skulle IIA følge de eksterne revisorer eller gå egne veje. Valget er faldet på det sidste. Der er valgt en kort og overskuelig påtegning, som har samme rækkefølge som de eksterne revisorers påtegning. Endvidere er det valgt ikke at gengive KAM for PIE-selskaber.

Tidligere adskilte IIA's standardpåtegning sig ved følgende udtalelse:

"Det er vores opfattelse, at de etablerede forretningsgange og interne kontroller, herunder den af ledelsen tilrettelagte risikostyring, der er rettet mod koncernens og selskabets rapporteringsprocesser og væsentlige forretningsmæssige risici, fungerer tilfredsstillende."

For at synliggøre de krav interne revisorer efter regnskabsbekendtgørelsen skal efterleve, har forslaget været fremover at inkludere intern revisions konklusion fra revisionsprotokollatet om § 27 i revisionsbekendtgørelsen i påtegningen.

§ 27 i revisionsbekendtgørelsen:

"Den interne revision skal i årsprotokollatet konkludere, hvorvidt virksomhedens risikostyring, compliancefunktion, forretningsgange og interne kontroller på alle væsentlige og riskofyldte områder er tilrettelagt og fungerer på betryggende vis, jf. bilag 4."

For nogle interne revisorer kan dette imidlertid indebære en udfordring i de tilfælde, hvor Finanstilsynet har afgivet påbud eller påtale om eksempelvis mangler i compliancefunktionens arbejde.

På IIA's temadag den 10. november 2016 blev dette forhold drøftet. Som forening er det vigtigt, at der så vidt muligt anvendes samme intern revisionspåtegning. På temadagen var der enighed om at udarbejde en undersøgelse af forventninger til den afgivne påtegning for 2016 blandt revisionschefer for finansielle virksomheder. Der er modtaget 26 svar, som viser følgende:

Ingen erklæring	6
Blank inkl. § 27	7
Blank ekskl. § 27	7
Modificeret	3
Eksisterende	3
Anden	0
I alt	26

På den baggrund er det besluttet at udarbejde to versioner af standardpåtegningerne: En med og en uden omtale af § 27.

Intern audit



Lars Maagaard, Director, Deloitte

Indledning

Implementeringen af Solvens II har medført et krav om, at alle forsikringsselskaber skal have 4 nøglefunktioner – en aktuar-, risikostyrings-, compliance- og intern auditfunktion. Dette har for nogen betydet en yderligere administrativ byrde og for andre har opgaverne allerede været udført, bare under andre former og betegnelser. I denne artikel vil jeg fokusere på, hvorledes indførelsen af funktionerne påvirker den interne audit/interne revision. Reglerne om organisering af indholdet af de 4 funktioner fremgår af Ledelsesbekendtgørelsen for forsikringsselskaber og Solvens II-forordningen. Der er heri præciseret en række opgaver, der skal udføres, men som så ofte før med denne type lovgivning, er der efterladt et rum for fortolkning. Det kan derfor være forbundet med udforandringer, hvordan du som revisor skal forholde dig til disse krav, særligt hvis du er ny intern audit, eller hvis det er nyt i forhold til den virksomhed, du reviderer.

Den interne audit funktion skal udtale sig om hvorvidt virksomhedens interne kontrolsystem er tilstrækkeligt og effektivt. De 4 funktioner, herunder aktuar-, risikostyrings- og compliance-funktionerne er væsentlige elementer i virksomhedens interne kontrolsystem, og revisionen af disse funktioner bør derfor være at finde i Intern Audits strategiske revisionsplan. Dette underbygges endvidere af, at den interne revision jf. bekendtgørelsen for gennemførelse af revision i en finansiel virksomhed, er påkrævet i årsprotokollatet at konkludere, hvorvidt virksomhedens risikostyring, compliancefunktion, forretningsgang og interne kontroller på alle væsentlige og risikofyldte områder er tilrettelagt og fungerer på betryggende vis. (Revisionsbekendtgørelsen gælder for revision af alle finansielle virksomheder, hvorfor aktuar funktionen ikke er særskilt nævnt.)

Jeg vil i denne artikel fokusere på, hvorledes Intern audit funktionen vil være væsentligt influeret af samarbejdet

med de øvrige funktioner, særligt compliance funktionen og revision af de øvrige funktioner vil være en væsentlig del af intern audits strategiske revisionsplan.

Intern audit er ikke det samme som intern revision.

Intern audit er et krav i alle forsikringsselskaber. Intern revision er kun et krav i selskaber med mere end 125 ansatte.

Intern audit nøglepersonen kan referere til direktionen. Intern revision refererer til bestyrelsen.

Intern audit funktion reguleres af ledelsesbekendtgørelsen og direktivet. Intern revision reguleres af revisionsbekendtgørelsen.

Trots forskellene i bl.a. formaliseringen af arbejdet giver det god mening at drage erfaringerne fra udførelsen af intern revision over på intern audit. Trods forskellige navne for revision (intern audit, interne revision, ekstern revision, compliance audit mv.) er revisionsprocessen den samme og formålet er at udtale sig til nogen om et emnes funktionalitet. Formålet med arbejdet er, at en given proces (eller samling af processer) fungerer efter hensigten. Det være sig efter lovgivningen eller ud fra ledelsens muligheder for at opnå dets målsætning. For at kunne opnå tilstrækkelig overbevisning til at kunne udtale sig om det reviderede, skal revisionen planlægges, de planlagte handlinger udføres og der skal konkluderes på opgaven.

Såfremt der i forsikringsselskabet allerede er en intern revision, kan denne udgøre den interne audit. Den interne revision skal i de situationer sørge for, at den strategiske revisionsplan inkluderer forhold der sikrer, at kravene til den interne audit ligeledes afdækkes.

Min umiddelbare opfattelse er, at hvis den interne revision overholder kravene i revisionsbekendtgørelsen og derned kravene i henhold til bilag 4, vil den interne revision ligeledes opfylde kravene til den interne audit.

Organisering af de 4 funktioner

Der er følgende krav mht. organisering af de 4 funktioner:

- Udover den interne auditfunktion skal der som nævnt som minimum oprettes en compliance-, aktuar-, og risikostyringsfunktion.
- For hver af disse fire nøglefunktioner udpeges en nøgleperson, der er den øverste ansvarlige i funktionen.

- Direktionen skal udarbejde funktionsbeskrivelser for nøglefunktionerne. Heraf fremgår det hvorledes arbejdsopgaver og ansvar fordeles, adskilles og koordineres i overensstemmelse med bestyrelsens politikker. Funktionsbeskrivelserne skal forhindre unødig sammenfald imellem funktionerne og sikre effektivt samarbejde i virksomheden.
- Virksomheden skal underrette Finanstilsynet om dens nøglepersoner. Virksomheden skal sikre, at alle medarbejdere i nøglefunktionerne er egnede og hæderlige, mens Finanstilsynet vurderer nøglepersonernes egnethed og hæderlighed.
- En person eller organizatorisk enhed kan udføre mere end én nøglefunktion, hvor det er forsvarligt under hensyntagen til bl.a. omfanget og kompleksiteten af virksomhedens risici og aktiviteter. Der skal dog altid sikres fornøden funktionsadskillelse, herunder at medarbejdere ikke er involveret i både udførelse og kontrol af en opgave. Den ansvarlige for intern audit funktionen kan dog ikke varetage ansvaret for en af de andre nøglefunktioner.
- Udpeges en overordnet medarbejder som nøgleperson, der også har ansvar for andre opgaver end funktionens, skal direktionen sikre, at mulige interessekonflikter mellem nøglepersonens funktionsopgaver og øvrige opgaver håndteres, samt at nøglepersonen er uafhængig.
- Et medlem af direktionen kan ikke udpeges som en af de nævnte nøglepersoner, med mindre følgende betingelser er opfyldt:
 - 1) Udpegningen sker under hensyntagen til arten, omfanget og kompleksiteten af virksomhedens risici og aktiviteter.
 - 2) Det kan dokumenteres, at den pågældende er tilstrækkelig uafhængig.
 - 3) Det sikres at mulige interessekonflikter håndteres betryggende.
 - 4) Udpegningen besluttes af bestyrelsen.
- Direktionen kan vælge, at en nøglefunktions opgaver placeres i organisatoriske enheder udenfor nøglefunktionen. Hvis direktionen vælger at placere en nøglefunktion i organisatoriske enheder, som har andre opgaver, skal direktionen sikre, at placeringen af nøglefunktionen er betryggende, herunder at eventuelle interessekonflikter i forhold til varetagelsen af funktionens opgaver og øvrige opgaver håndteres betryggende.
- Såfremt virksomheden har outsourceret en eller flere nøglefunktioner, skal virksomheden udpege en ansvarlig internt i virksomheden, der har ansvaret for den pågældende funktion. Virksomheden skal underrette Finanstilsynet om denne person, hvis egnethed og hæderlighed skal vurderes af Finanstilsynet.

Jeg vil i øvrigt henvise til Ledelsesbekendtgørelsen for forsikringsselskaber og Solvens II-direktivet, hvoraf der for hver nøglefunktion er specificeret en række krav, som skal være opfyldt.

Den interne audit funktion

I lighed med de regler vi kender fra den interne og eksterne revision, skal intern audit være objektiv og uafhængig af virksomhedens operationelle funktioner. Det betyder, at intern audit ved dets vurdering og rapportering af resultatet af arbejdet ikke må være under påvirkning fra direktionen eller bestyrelsen, som kan bringe intern audits uafhængighed og upartiskhed i fare. Intern audit må ikke vurdere aktiviteter eller funktioner, som den selv har udført i perioden.

Den interne auditfunktions overordnede formål er at give ledelsen dets vurdering af, hvorvidt det interne kontrolsystem er tilstrækkeligt og effektivt. Det interne kontrolsystem omfatter som minimum administrative procedurer, en intern kontrolstruktur, passende rapporteringsrutiner på alle niveauer i virksomheden, og en compliance funktion. Dette inkluderer bl.a. en test af, at de interne kontroller fungerer effektivt.

Intern audit rapporterer som nævnt til direktionen med mindre ansvaret for interne audit funktion varetages af intern revision. I så fald rapporterer intern audit til bestyrelsen jf. revisionsbekendtgørelsen. Det er pålagt bestyrelsen at udarbejde en politik for intern audit, der, i det omfang det er relevant, beskriver:

- a. vilkår og betingelser for, hvornår den interne auditfunktion kan blive opfordret til at udtales sig eller yde bistand eller udføre andre særlige opgaver,
- b. interne regler for, hvilke procedurer den ansvarlige for den interne auditfunktion skal følge, når Finanstilsynet skal underrettes om intern audits resultater,
- c. kriterierne for rotation af medarbejderopgaver.

Auditplan

Intern audit udarbejder en årlig revisionsplan, der som minimum skal foreligges for direktionen. Jeg vil anbefale, at den interne audit funktion ligeledes forelægger revisionsplanen og resultatet af arbejdet for bestyrelsen. Det vil være nyttigt for både den interne audit og bestyrelsen, at de planlagte arbejder og resultatet heraf drøftes med bestyrelsen. I især mindre forsikringsselskaber, kan direktøren være en meget dominerende person, hvorfor det er god idé at involvere bestyrelsen. Varetager intern revision intern audit funktionen skal revisionsplanen forelægges bestyrelsen til godkendelse, idet det så er revisionsbekendtgørelsens bestemmelser, der er gældende.

Planen skal omfatte alle væsentlige planlagte aktiviteter og udarbejdes baseret på en metodisk analyse af risici og inddrager tidligere, nuværende og fremtidige aktiviteter fra ledelsen og styringen af virksomheden. Alle væsentlige områder skal revideres inden for rimelig tid. Revisonen kan derfor foregå på rotationsbasis. Såfremt der ikke er nogen særlige forhold gældende, kan rotationsperioden være 3 år. Jeg vil anbefale at medtage rotationsplanen i den årlige revisionsplan.

Ved planlægningen af opgaverne fokuserer intern audit bl.a. på at understøtte ledelsen i at opnå virksomhedens strategiske mål og revisionsplanen vil indeholde en gennemgang/overvågning af risikostyrings-, compliance- og aktuarfunktionen.

Direktionen skal ikke godkende planen, da det er nøglepersonen for intern audits ansvar. Men direktionen kan anmode den interne auditfunktion om at inddrage specifikke emner i den interne audit, uden at dette strider imod funktionens uafhængighed.

Den interne auditfunktions arbejde skal dokumenteres med henblik på at vurdere funktionens effektivitet og muliggøre en gennemgang af den foretagne interne audit og dens resultater. Intern audit vil drage egne konklusioner på vurderingen af det interne kontrolsystem, men vil i videst muligt omfang basere sig på gennemgang/tests foretaget af de øvrige nøglefunktioner.

Den interne auditfunktion rapporterer resultat af det udførte revisionsarbejde til direktionen og/eller bestyrelsen. Situationer kan som sagt opstå, hvor den interne auditfunktion vurderer, at der er behov for rapportering direkte til bestyrelsen. Afrapporteringen skal indeholde en frist til at afhjælpe eventuelle mangler, angive hvem der er ansvarlige for at afhjælpe disse, samt oplyse om status på tidligere rapporterede anbefalinger.

Særlige forhold

Kompetencer og ressourcer

En værdiskabende intern auditfunktion planlægger og udfører sit arbejde, for at kunne udtale sig om det interne kontrolsystem, der sikrer overholdelse af loven og understøtter ledelsen i at nå deres strategiske mål. Den interne auditfunktion organiserer arbejdet på en måde, der sikrer identifikation af de relevante risici, for at det interne kontrolsystem ikke fungerer effektivt og de implementerede kontroller til imødegåelse af disse risici.

Den strategiske revisionsplan skal bl.a. indeholde en redegørelse for, hvorledes man påtænker at revidere disse interne kontroller for at opnå tilstrækkeligt revisionsbevis til at kunne udtale sig om det samlede interne kontrolsy-

stem. For at kunne gennemføre denne opgave, kræves der kompetencer inden for bl.a. følgende områder: Markedsrisiko, Aktuar, Risikostyring/solvens, Regnskabsprocesser og Forsikringsydelses.

Det er en udfordring af finde en nøgleperson/intern audit, der besidder alle disse forskelligartede kompetencer, hvorfor det bør overvejes, at der indgås en out- eller co-sourcing aftale med en ekstern leverandør, som revisionsarbejdet kan udføres i samarbejde med. Samarbejdspartneren besidder de krævede kompetencer og vil kunne supplere den interne auditfunktion. Kompetencerne er nødvendige dels for at kunne gennemføre den krævede interne audit, men i lige så høj grad at kunne levere en høj værdi til direktionen/bestyrelsen.

Det er ikke tilladt at outsource nøglepersonen, men selve arbejdet som funktionen udfører kan outsources eller gennemføres ved en co-sourcing aftale. Hvad der er mest relevant afhænger af flere faktorer, herunder virksomhedens størrelse, om der allerede er en intern revision osv.

Der er ikke så stor forskel mellem outsourcing og co-sourcing, da det ofte er områder hvor den interne auditfunktion ikke har tilstrækkelig med kompetencer, der udføres af co-sourcing samarbejdspartneren. F.eks. revision af aktuarfunktionen gennemføres af en samarbejdspartner, der kan kombinere revisions- og aktuarkompetencer. Dermed får den interne auditfunktion de kompetencer tilført, der gør, at den kan udfordre de beslutninger og arbejder som aktuarfunktionen foretager.

Ved indgåelse af en outsourcing eller co-sourcing aftale er det relevant at diskutere uafhængighed. Det grundlæggende krav i lovgivningen er at direktionen skal træffe passende foranstaltninger, for at mindske risikoen for interessekonflikter for den interne auditfunktion. Direktionen skal endvidere sikre, at medarbejdere i og den ansvarlige for den interne auditfunktion ikke udfører audit af aktiviteter eller funktioner, som de selv har udført eller udarbejdet grundlaget for i den periode, som den interne audit omfatter. Herfra er det så op til bestyrelse, direktion, intern audit og outsourcing partner at fortolke derfra.

Mht. til outsourcing/co-sourcing aftaler er der set flere forskellige løsninger. Fra den mere 'rene' hvor outsourcing/co-sourcing partner ikke også udfører nogen af de andre funktioner, til en situation hvor alle 4 funktioner er outsourcet til samme samarbejdspartner. Sammenholdt med intern revision i traditionel forstand er intern audits uafhængighed anderledes, ved at der rapporteres til direktionen. Intern revision rapporterer til bestyrelsen. Der er derfor ikke helt samme rigide regler for uafhængighed. Er det en intern revision, der er udpeget til at være den

interne auditfunktion, skal uafhængighed fortolkes i forhold til revisionsbekendtgørelsen.

Der er forskellige holdninger til om den sidste model er holdbar, såfremt intern audit skal kunne opfattes som værende uafhængig. Min holdning er, at outsources intern audit, kan de øvrige 3 funktioner ikke outsources til samme samarbejdspartner. Jeg ser ingen problemer i at samme samarbejdspartner udfører compliance-, risikostyring og aktuarfunktionen.

Modenhed

Hos mange forsikringsselskaber er implementeringen/formaliseringen af nøglefunktionerne nyt. Det vil derfor være meget nærliggende for intern audit at vurdere, hvorvidt den enkelte funktion er moden til en revision eller ej. Intern audit bør initiere et opstartsmøde med den enkelte funktion, hvor status for funktionens opbygning mv. drøftes. Derudover bør intern audit forklare hvad en revision indeholder, herunder formålet med revisionen og hvad der er i fokus. Baseret på disse risikovurderings-handlinger beslutes det, om funktionen er moden til revision eller ej. Konkluderes det, at en egentlig revision udskydes bør forholdet drøftes med bestyrelsen/direktionen ved gennemgang af den strategiske revisionsplan og rapporteringen.

Brug af de andre funktioners arbejde

Som tidligere omtalt vil intern audit være tæt forbundet med de øvrige nøglefunktioner. Intern audit reviderer funktionerne og deres funktion, men det arbejde der foretages i funktionerne vil ligeledes kunne afdække en række af de forhold, der skal revideres, for at intern audit kan udtales sig om det interne kontrolsystem. Som f.eks. hvis compliance foretager test af nøglekontroller i et bestemt område, for at sikre at interne procedurer overholderes, er det meget sandsynligt at intern audit ligeledes vil

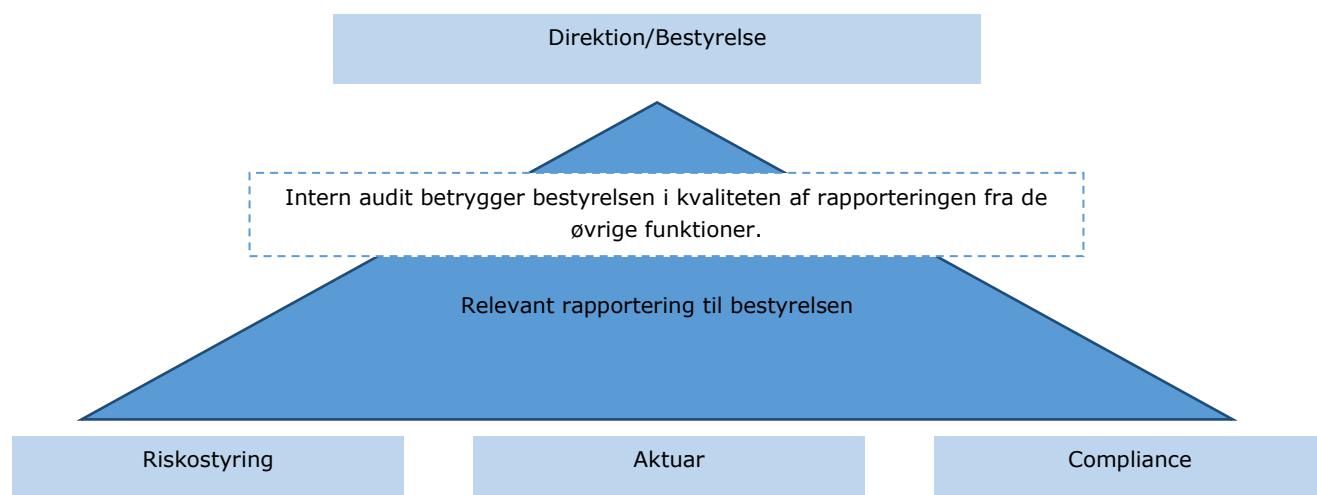
inkludere disse kontroller ved en forestående revision. For at mindske de administrative byrder bør intern audit i videst muligt omfang gøre brug af det arbejde de øvrige funktioner udøver.

Ved planlægning af revision af et specifikt område, skal revisor derfor indhente informationer om hvorvidt f.eks. compliance funktionen har foretaget noget arbejde/testet relevante kontroller på dette område. I så fald skal revisor foretage en gennemgang af dette arbejde, hvilket inkluderer:

- En gennemgang af planlægningen af opgaven: Er de relevante risici identificeret, er der identificeret relevante interne kontroller der imødegår disse risici, er der fastsat en passende stikprøve til test af kontrollerenes design og implementering og evt. effektivitet.
- En gennemgang af det udførte arbejde: Er det planlagte arbejde udført, er arbejdet udført af personer med rette kompetencer til at kunne udføre arbejdet, er arbejdet tilstrækkeligt dokumenteret, intern audit foretager re-performance (genudfører de tests mv. der er foretaget for at vurdere om intern audit ville være kommet frem til samme konklusion) af en stikrøve af det udførte arbejde, afspejler konklusionerne det udførte arbejde herunder om mangler er oplistet.
- En gennemgang af rapporteringen: Afspejler konklusionerne i rapporteringen til området (ansvarlige for det reviderede), direktionen (og bestyrelsen) på korrekt vis det planlagte og udførte arbejde.

Baseret på denne gennemgang vurderer revisor hvorvidt det udførte arbejde er tilstrækkeligt til at opfylde intern audits krav eller der er behov for at foretage yderligere handlinger. Ved gennemgangen af compliancefunktionens arbejde tager revisor højde for compliancefunktionens

Figur 1: Intern audit



uafhængighed eller mangel på samme. Compliance funktionen vil umiddelbart ikke have samme uafhængighed som revisionen, men det betyder ikke at intern audit ikke kan gøre brug af arbejdet. Det vil blot øge behovet for genvurdering af de identificerede kontroller, den udvalgte stikprøve, øget omfang af re-performance samt evt. udvidelse af det arbejde, der vurderes nødvendigt.

Som illustreret er der et stort potentiale i at koordinere indsatsen i de 4 nøglefunktioner for at undgå overlap af opgaver og sikring af at forventede opgaver falder ned mellem 2 funktioner og dermed ikke udføres. Særlig fokus bør rettes mod fælles terminologi samt koordineret planlægning og rapportering.

I de selskaber der allerede har en intern revision, er en væsentlig del af bestyrelsens betryggelse i hvorvidt det interne kontrolsystem fungerer, kommet fra den interne revision. Den øgede investering og fokusering på compliance-, risikostyring- og aktuarfunktionen medfører at der kommer flere rapporteringskilder til bestyrelsen. Det har jeg forsøgt illustreret i figur 1 på foregående side. Fremadrettet vil en del af intern revision/intern audits rapportering til direktionen/bestyrelsen være en betryggelse af, at de øvrige funktioners rapportering til bestyrelsen er pålidelig. Altså, at rapporteringen afspejler resultaterne af det udførte arbejde og at arbejdet er planlagt og udført på en måde, der muliggør en konklusion af det omfang der frembringes.

Revision af en nøglefunktion - de specifikke handlinger

Jeg har i nedenstående skitseret de handlinger, der gennemføres ved revisionen af en nøglefunktion. Som tidligere beskrevet er de andre nøglefunktioner en væsentlig del af virksomhedens interne kontrolmiljø, hvorfor disse funktioner bør revideres. Der er flere formål med revisionen: Direktionen/bestyrelsen har krav på at få en vurderingen af funktionens virke, intern audit bør overvåge, at der er et tæt og effektivt samarbejde og intern audit skal vurdere om arbejdet i funktionen fungerer på en måde, der muliggør at intern audit kan gøre brug af det udførte arbejde.

Ud over nedenstående handlinger, vil intern audit også foretage konkrete vurderinger af resultatet af funktionens arbejde, når intern audit ønsker at gøre brug af arbejdet og dermed gennemgår den konkrete planlægning, de udførte tests og konklusionen/rapporteringen.

Handlinger til inspiration ved revision af en nøglefunktion (vil ikke afvige meget ved revision af de øvrige funktioner):

- Gennemgang af governance strukturen, herunder rollenfordeling, rapporteringsrutiner mv.
- Påse, at de formelle krav til funktionens organisering er overholdt. Kravene fremgår af ledelsesbekendtgørelsen for forsikringsselskaber og Solvens II-forordningen (er ligeledes tidligere omtalt under "organisering").
- Påse at der foreligger en politik for funktionen og vurder indholdet i forhold til formålet med funktionen jf. ledelsesbekendtgørelsen for forsikringsselskaber og Solvens II-forordningen.
- Påse at der er udarbejdet relevante forretningsgange for funktionen i overensstemmelse med politikken.
- Påse at forretningsgangene er overholdt.
- Gennemgå processen for identificering af risici og planlægning af opgaverne (årshjul) set i forhold til de forventede formål med funktionen. - Er identificerede risici fuldstændige, er de dokumenteret, er de koordineret med de øvrige funktioner og organisationen om helhed.
- Påse at der er planlagt og gennemført handlinger til afdækning af risici.
- Påse at planen er præsenteret for og godkendt af direktionen/bestyrelsen og at planen er gennemført, eller at afvigelser fra planen er behørigt kommunikeret til direktionen/bestyrelsen.
- Påse at det udførte arbejde er dokumenteret tilstrækkeligt. – Der er ikke samme dokumentationskrav som til en intern audit, men der bør dog være dokumenteret i en sådanne omfang, at det er muligt at foretage en vurdering af det arbejde, der er udført.
- Kontroller at der er sammenhæng mellem rapportering til ledelsen og resultatet af de underliggende arbejder/dokumentation. – Kan funktionen efter intern audits vurdering rapportere som den gør, baseret på det udførte arbejde.



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



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

Introduction

Welcome back to the outer side of the box!

This article is **Part II** of a three-part series, which was created with the hope of providing new ideas and inspiring auditors to approach projects a bit differently, look at problems under a new angles, and ask new questions.

These articles aim at helping you find solutions where none seem possible, and showing you what to do in such situations where you have just stepped into the unknown and do not know where to start, or what tools to use, or whom to go to for help.

In **Part I** (featured in the previous issue), we discussed how “*out-of-the-box analytics*” can open up whole new areas of value in auditing and introduced a theoretical (yet practical) framework to apply to such situations.

The objective of **Part II** today is to delve deeper into this approach, by applying it to real-life, practical examples.

Building a Test from Scratch

In **Part I**, we concluded by introducing the main concept behind “building on innovation”: **“Start Small, then Go Big!”**



In other words:

- Don't try to boil the ocean.
- Start with the basic ideas, then add to it gradually.
- Break down big problems into smaller parts.
- Expand your universe by asking three basic questions:
 1. *Why not? (...do something new)*
 2. *What other data exists?*
 3. *What else should I know?*

This is a good start, but we will need more than that to tackle the most demanding problems that life can send our way (for me, it was challenges such as password sharing, contractors overbilling or anti-money laundering that really pushed my skills to the edge – what will your big test be?)

So let us dive into the comprehensive seven-step method to guide our steps from creativity to reality. I will start with the theory behind each step, and then put it in practice, using one concrete and compex case (password sharing).

The Seven Steps to Innovation

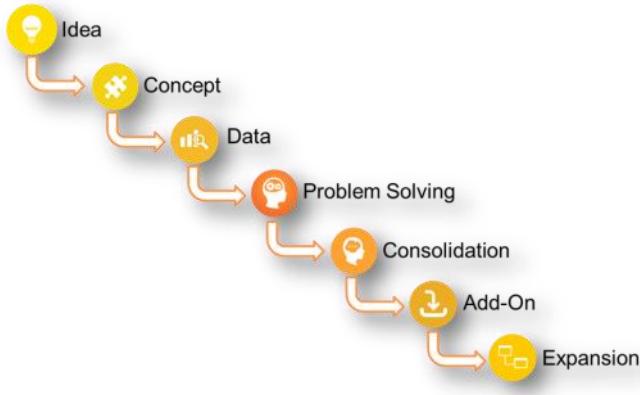
So here is the full picture, the framework that we will go through in details: **Idea, Concept, Data, Problem Solving, Consolidation, Add-On, and Expansion ... (see Figure 1 on the next page)**

Let me preface this section by stating again that mapping out this process has been one of the toughest things to do for me. I spent years doing this without realizing that I was following a consistent pattern... until I had to speak and write about it. Essentially, how do you explain Innovation? How do you put a frame around creativity? In other words, how do you take “outside-the-box thinking”... ...and put it in a box?

Looking back at my prior experience now, this approach has led me to conduct many successful projects and guided me through difficult phases when I was on the verge of giving up, and I hope that this can help you too.

Each one of these steps is extremely important, and as you can see from the picture, each one has been assigned a specific color, representing the degree of difficulty. The ‘lighter yellow’ steps are usually the easier, more creative, I would even dare to say “more fun” parts of the process. They tend to rely on your imagination, your artistic brain. On the other hand, the darker, red/orange parts represent the steps that are more challenging, and can be the most frustrating and discouraging.

So as you may have established from the picture: in this

Figure 1: The Seven Steps to Innovation

type of project, it usually starts well, but then it tends to get worse before it gets better.

Don't panic though! We will go through each step, one by one... and don't worry if you do not grasp the theoretical principles right away, it will all make sense when we put it in practice, in the second half of this article.

Let's get started then!

1. Idea

First stop on our journey: the basic Idea!

- This is where we plant the seed. It is the "Why Not" step. This is where we just jot down ideas on a piece of paper with no consideration for reality. On this step, it is critical that there be no room for negative thoughts, no time for counter arguments, no considerations of why this could not work or how things could go wrong.

In everything we do, it is usually natural for us to see the weaknesses in our ideas, the logical flaws in our reasoning... this is in our DNA, it is how our auditor brain is naturally wired, and it is usually a very useful trait to have in our line of work.

In this step however, you will need to go against your own nature, and NOT look at the issues, not think about them, not even consider they may exist. There will be time for that in the later steps (specifically in steps 4 & 5).

For this step, we just need to be 100% constructive, hang onto one positive thread and pull on it. Basically, all we need for now is to find a way, just one way – no matter

how far-fetched – to get some type of result, some hits, some "true positives" that can get our process started (even if, in the back of our mind, we could think of 101 types of false-positives that our method could bring into our results – just leave those to the side, at least temporarily).

So how do we know when we are successful with this step? When we have found a basic idea... a high-level test outline that "could probably" show us something interesting (along with some unwanted garbage of course), even if we remain clueless as to whether the systems or data required would even exist! Consider this "mission accomplished". That is really all we need at this stage.

2. Concept

Most auditors I know usually have no problem going through the first step – it is common sense to start at such a high-level, and quite often a part of regular planning even. Now after that stage is completed however, most of us would jump straight into the data collection (step 3), since it seems logical to set the plan to motion after all, now that we have the basic idea laid out.

Well.... Let's not!

In this step, we need to remain positive a little while longer. Why?

Because plunging into the "harsh reality" too soon is the most common mistake. This is where most "unconventional" projects fail, and where the innovation dies. If you are trying something new and special, the time to execute your plan has not come yet, and you must force yourself to take one extra, counter-intuitive step: the "Concept" stage.



I think that **Ernest Hemingway** said it best, in his famous advice to aspiring writers: "**Write drunk; edit sober**".

Now please, drop that glass! ...this advice does not really work that well when taken literally (trust me) – However, the idea behind it can be extremely valuable!

The core of the message is really an encouragement to cast off our inhibitions. It prompts us to let ourselves go, and allow our unrestricted creativity to take over.

This is important, because when we formalize things and bring in structure too soon, we allow our logical brain to

take control and constrain our choices, and freeze our innovative thinking before all alternatives have been considered.

So for this step, we want to stay in "dream-wonderland" a while longer. Just imagine you had a magic wand and you could obtain any data you need, and make everybody cooperate on request... what would you do in such a perfect world (at least from an auditor's perspective)? Then just build your test plan accordingly, with the end in mind, giving again no consideration for real-life challenges and setbacks.

How is this different from the idea stage?

Well this time you need to describe a specific plan as to how the test would work, a real model and not just a vague notion. You need to identify what specific data point you would match with what other data table (regardless of whether such data exists, or is accessible, we are not there yet).

I usually like to draw a process flow and insert "tentative" systems and data fields, along with test description and expected results. The main benefit of this approach is that we now have a solid documented plan that we can bring to our IT team or our clients, and it will be more difficult for them to reject our requests. Now that we have a credible plan (not just an idea), it will also make it easier to bring our manager on board with us, and escalate the issue through the hierarchy if we do not get what we need.

Now that we have built a solid foundation, we are ready to face the music.



3. Data

Welcome to the real world!

You now have a nice test concept, ready to be executed. You have laid out every detail of what files and data are needed, and how they should be processed or matched with one another. You are excited, everything looks rosy, until you realize... it simply doesn't work!

So you tried to use common sense in the concept stage, but now you recognize that your plan simply could not foresee that "Table A" does not exist... and that those other two files do not have a common key to match them... and the dates are not in the same format, and this last data point? Stored on legacy mainframe that nobody can extract for you.

Don't worry, this is quite common. This 'Data step' is really where the rubber hits the road for the first time, and where all the nice plans in place come crashing down to the altar of bitter reality. Honestly, this is where most projects fail. This is where most people give up. ...and this is where I will try very hard to convince you not to!

For starters, just take what you have for now. Use the data that exists. When data does not exist, seek for alternatives. Update your plan accordingly. More importantly, keep your head cool and jump into the problem solving phase:



4. Problem Solving

If the 'concept' stage was all about "writing drunk", this is really the "edit sober" part (and I guess the data step must have been the painful hungover awakening in-between).

Now is an important moment to remember the earlier key advice in such situation: **Break down each big problem into smaller parts and address them separately.**

First, you need to realize that you are not empty-handed. The data phase probably provided you with a large part of what you needed already.

Next thing playing in your favor: you have a concrete plan of what is missing. You can take this outline to go one item at a time, (possibly with the clients) and see if other options are available. Oftentimes, a missing link can be replaced by a combination of two or more interlinked files. Sometimes you just need an index table to translate one key into another to make the connection work.

You should probably realize by now why the Concept stage was so important. Imagine if you went in front of the client armed only with a vague idea... Your process would be interrupted right away and your project would probably fail before it even started.

Little by little, you need to fill in the gaps, even if it means adding on to the possibility of inaccurate results and false-positives. All you need is one logical path to finding exceptions.

Once you have reached that stage, you can consider that the hardest part has probably been done and now you just need to crystalize it into something solid and reliable: onto the consolidation.



5. Consolidation

We are almost there! "Consolidate" here is really just a fancy way of saying 'clean-up'.

You were finally able to pull something out of your data. Your main task now is to filter your early results to try and remove all the false-positives (or false-negatives). Chances are that because of the way your test was designed, and the tricks you had to do to see it through, your data has now also collected a lot of garbage along the way.

Keep in mind that nothing kills your credibility more than handful of false-positives, even when distilled among a full list of real issues. These little dark cloud will just cast a shadow over all of your results and make the stakeholders doubt the validity of your whole test. We do not want that!

The **bad news** is that in order to filter our file to the level required for a clean, consolidated result, we will probably filter out a significant amount of good results as well. We will miss out on several exceptions, most of which could be serious violations, which will thus remain undetected.

The **good news** though, is that **we are auditors**... which means that we are the third line of defense! This comes with one key advantage, which makes this whole method valid: we do not need to find 100% of issues!

We do **not** own the controls, we own the **assurance** over the controls, and that is a crucial difference. In other words, we are here to verify that the process is reliable (i.e. the controls work), and as such, we only need to find a number of exceptions to "feed the issues". We only need to prove that "something went wrong" – not to show everything.

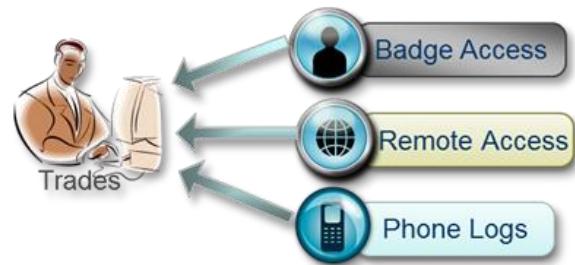
Which is why in such a case, it is better to have a few valid issues that are reliable, rather than a long list that could contain false-positives, so do not shy away from filtering and cleaning up as much as possible. Now let's take our "concentrated" list and improve it in the next stage.



6. Add-On

At this stage, the project usually starts becoming exciting again. We have basically solved most of our problems, and we are just now finding ways to make it work better. This "Add-On" step is when we start asking one of the key question mentioned at the beginning of this article "What other data exists?"

In **Part I**, we had a case-study where we looked at a trader who seemingly processed transactions while he was not even logged in. What did we do next? We had to reinforce our test to prove that this was actually happening, so we asked the very specific question "*What other data exists?*" – and we started to gradually **add onto** our original test.



We eventually came up with badge, phone and remote-access logs – thus widely increasing our confidence over our claim.

We didn't really add anything new to the matter itself, but we made sure the issue was really an issue, beyond any possible doubts.

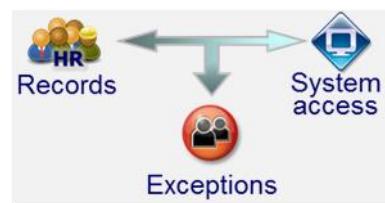
This is what this step is all about. Take the findings that you have, and see if you can find ways to make it stick, by adding whatever is needed to make it fool-proof.



7. Expansion

The final step is probably the most interesting of the lot. This is where we go the extra mile to look into the implications and the magnitude of the issues we have just uncovered. This can be done by asking ourselves the other key question: "*What else should we know?*"...

For instance, you may still remember another case-study in **Part I**, which was about terminated employees who



still had their user account active in the system (a very common type of test for every IT auditor).

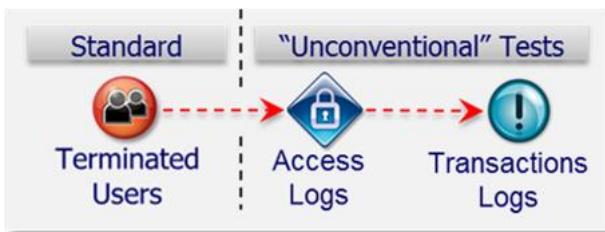
Upon finding exceptions, we were able to expand upon that test by pushing the boundaries of what we had originally set out to analyze.

After we found terminated employees with active accounts, we asked ourselves "what else we should know", and determined that it was time to start digging deeper,

and looked at the access logs to check if such accounts had actually been used.

This gave a whole new dimension to our test, as it showed us that we had some potentially disgruntled ex-employees who were still logging onto our systems regularly **after** they had left the company. This was actually even serious for us keep asking the same key question over again, "what else should we know?"...

Well, going one level deeper, we even checked the comprehensive transactions log, in order to find out what they did while they were connected, what types of transactions they processed, etc...



This approach really changes the perspective of a test, from a rather benign "housekeeping" matter into a serious criminal issue, possibly fraught with hacking, embezzlement or fraud.

Of course, some could consider this as crossing over from auditing into the investigative world, and thus overstepping our mandate... and they wouldn't be wrong.

I would argue however, that we would not be fulfilling our duties as a third line of defense, if we failed to report on such major issues, simply because it was not in our original test design.

From Theory to Practice: Password Sharing

Congratulations, we have concluded the theory on the seven steps. I hope that this process made sense to you so far, but do not worry if some parts are still unclear, it will all come to light as we put it all in practice!

So let us try to apply what we have just learned into a concrete, real-life example, which was a really demanding yet stimulating and thought-provoking challenge for me. When my manager stepped into my office on that fateful Friday night and charged me with an unexpected complex task, it was about finding out who, in our company, were sharing their passwords (from top executives to assistants). You can bet that it had never been done before, and nobody had any clue where to start, what to use, or whom to involve. There wasn't any literature on

the topic on the Internet either, so I was really on my own...

So welcome to my world, imagine the problem is yours now: what would you do to tackle it?

Let's get right on it... So how do we start?

As you know by now, the first step is to start with basic **idea (1)**. So let's think about it for one second... what idea of a test could show us – for instance – that "John" shared his password with "Jane"?... in other words, how can we see that Jane used John's password (whether it was willingly or not).

Well how about checking if John's password has ever been used to logon from Jane's computer?



Now I know what you are thinking: this is too simple, and this test is really not fool proof. What is John borrowed the PC once? What if the recorded PC number is incorrectly attributed to Jane? What if they are using "pooled" laptops when traveling? What if...?

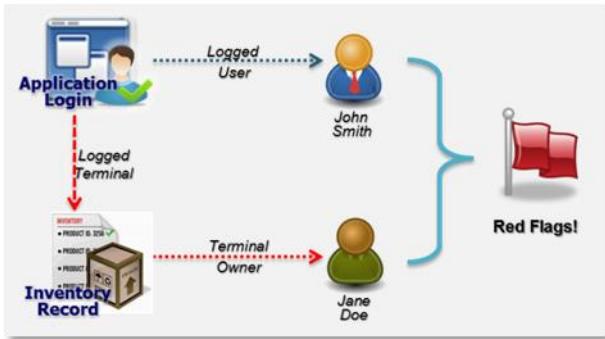
Stop! Remember the first rule of this stage: there is no room for negative thoughts at this point. There may be 101 reasons why this test is weak and for it to yield false results, but we should not focus on that for now. As long as we have one idea, one path that could yield the right result, we will just stick to it and start building upon it.

What's next?

Next we will do just that, build on the idea and make it more concrete: onto the **Concept (2)** phase!

We will describe the whole test realistically, but acting as if we had a magic wand and any and all possible data tables and files were readily available to us, and in a perfect format, ready to be linked with one another effortlessly.

This is how it would look like: We will need the application logs, to capture the login entries from John. The logs will conveniently tell us what terminal this logon came from. We will match that imaginary "terminal key" with our Inventory records, which will indicate that this asset actually belongs to Jane, not John...



-> So John equals not Jane... ergo: **Red Flag!**

Great! We have just defined a straightforward and systemic way to get a list of all passwords that were used on different computers than their rightful owners', that has to be worth something right?

Well we have reasons to feel excited at this stage, so let's carry on to make it become real.

Now we need to collect the **Data (3)**! Time to go to the client, check the systems, and try to see what results could come out our test...

...and as expected, reality shatters our hopes and dreams of any easy resolution for this problem!

- First, the application login does not recognize "John" by his official ID.
- Next, John's computer is identified in the application logs by its 'network name', which does not correspond to the number that was assigned to that machine in the Inventory.
- Finally, the inventory entries are not assigned to the official user IDs either...

So we are caught in a three-way mismatch! This happens all the time when matching data sources from different universes: they were named by different people for different reasons. We had system or network administrators on the one side, and controllers/accountants on the other. One side sees "a terminal", a logical entity that needs connectivity in a logical Domain, and therefore uses a logical name for that Domain – while the other sees this as "an asset" and wants to classify it in the right asset class to ensure that it is reflected in the proper books and follows the correct depreciation schedules.

Two different worlds that never collided, until you came around trying to reconcile the two. As discouraging as it could be, let's not panic, and let's not give up. You are on the right track, and by doing what no one has done

before, you will likely be rewarded by finding things that nobody had found before.

Remember the general advice for this stage: take the data you can find, and when you cannot find it, seek for alternatives. In this case, we have logs from the application and inventory records. We could also obtain HR records, to help with the identification part. That is already a decent start, so let's carry this into the next section.

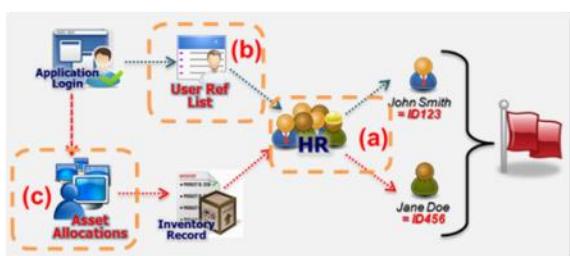
Next, we jump headfirst into the difficult **Problem-Solving (4)** stage.

We now need to follow the common wisdom for this step, which is to break down the problem into smaller parts, and address each of them separately!

First, we need to solve the problem of user identification. We will therefore use the corporate user-ID (from HR data) as the key identifier of a person, regardless of the platform (a). This means that we will potentially need to build an "ID translation table", i.e. a list of what the users' accounts are named in different systems (thus allowing to track a single user across different platforms). There will likely be slightly different conventions in each system; sometimes it will be based on the individual's name (eg, "jdoe" for "Jane Doe"), in others, a variant of the user ID (eg, "00123" instead of "ID123"); but such a table can be built rather fast, using very simple Excel formulas (and even if you get just 90% of it, you are fine).

In most cases though, you do not even need to build such a table! You should be able to obtain a "**User Reference List**" (b) from the application administrator, which is used for user maintenance (such as knowing what system accounts to revoke when someone leaves). Actually if they don't have one, you can write an audit issue right away because they should (how else do they maintain their system?)...

Finally you need a way to translate the machine's network ID into its corresponding asset number. Luckily, most ERP systems will have an "**Asset Allocation Table**" (c) readily available, you just need to do some digging and asking around (SAP most definitely has one such aptly named table).



If you cannot find it, you will have to build it yourself, as we did with the user table. Although these are “two different worlds”, it could be quite easy: I would start by looking for a common key field that should be used by both sides: the machine’s serial number (controllers and administrators will both need this for different reasons).

Now that we have all the pieces we need, we just have to “assemble our puzzle”. As you can see from the picture, our test has grown more complex, but now for the first time at least we have something that works, and we should start getting some results already!

Keep in mind though: Red flags are not issues! Not yet at least. Our early results will very likely contain an unpleasant amount of false-positives, which is why we will jump right into the **Consolidation (5)** step!

This will be quick: we want to clean up our ‘red flags’ to keep only the ‘high probability’ exceptions. Luckily, we do not need to catch 100% of exceptions, but only enough to show that the control is deficient. This means that there is no need to be “surgical” in our filtering: we can comfortably remove large populations, even if they may contain valid exceptions.

We already have an idea of what needs to be filtered out by now. Some common sense and a little brain storming should tell you what could generate a false-positive hit, for instance:

- What if John used Jane’s PC only once (with her permission)?
- What if the computers were recently reassigned?
- What happens when using RAS (Remote Access Services)?



There can be several others and they are usually easy to find, but it can also help to start by sampling some of the early results to see what the most common errors are. So let’s just focus on those three for now, and remove all red flags where: **(1)** we have only a single occurrence of the violation (we’ll only take repeat-offenders); **(2)** the computers were reassigned in the last six months; and **(3)** all logins through remote access.

We now have a list of highly probable exceptions. Can we **add-on (6)** to our test to improve it and get closer to 100% confidence?

Of course, and we will do so by asking ourselves “*What other data exist?*”

In other words: What data could show us that people were not actually present when their passwords were used?

We can start of course with their badge access logs. Then what about their leave and travel records? You can probably think of others, but let us use those three:



Great! We have now almost completely removed the likelihood of false-positives, so our test is already extremely successful.

Can we the **Expand (7)** on our test to make it even better? Sure, let us ask the final question: “*What else should I know?*”

You are probably ahead of me on this one: We know that those people used somebody else’s credentials, so what we really want to know now is “What have they used it for?” Here is a list:



We will of course want to start with approvals (have they approved their own leave, travel, expenses, etc...?)

Then the other transaction types will fall under general common sense for auditors, for instance: Did they use an admin password to elevate their privileges? Did they commit and conceal fraud by creating fictitious G/L accounts? Any fake AP Entries? Any fishy operational transactions? Have fun with this section, there is much to look into!

So this is it! Congratulations for sticking through the seven steps! Let us take on step back and admire the work done (see **Figure 2** below): this is what our test has become, from idea to reality.

When we conducted this test the first time, the findings were so unbelievable in scope and magnitude that they shook the highest levels of hierarchy and generated profound, multi-year changes and far-reaching remediation actions. This really illustrates the power of adhering to a clear step-by-step approach, as we would have never been able to do this as a block, without breaking it down into smaller, easier parts.

Conclusion

This concludes **Part II** of this series. I hope that this provided you with enough insights, without overwhelming you with details.

Taking your audits to the **next level** is not always easy, but it is not that difficult either when sticking to a tried and true **methodology**, and it is always extremely rewarding to **succeed** where others cannot, by trying new ways and getting outside of our comfort zone.

Part III will revisit this model by exploring what to do when things do not work as expected, and look at the big picture by addressing the planning and governance aspects over such projects. In the interim, feel free to contact me at YSF.data@gmail.com with any questions or comments you may have.

Till next time - Thank you!

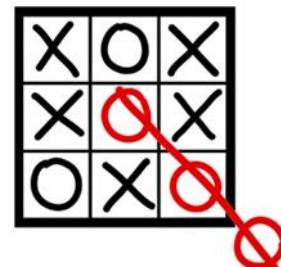
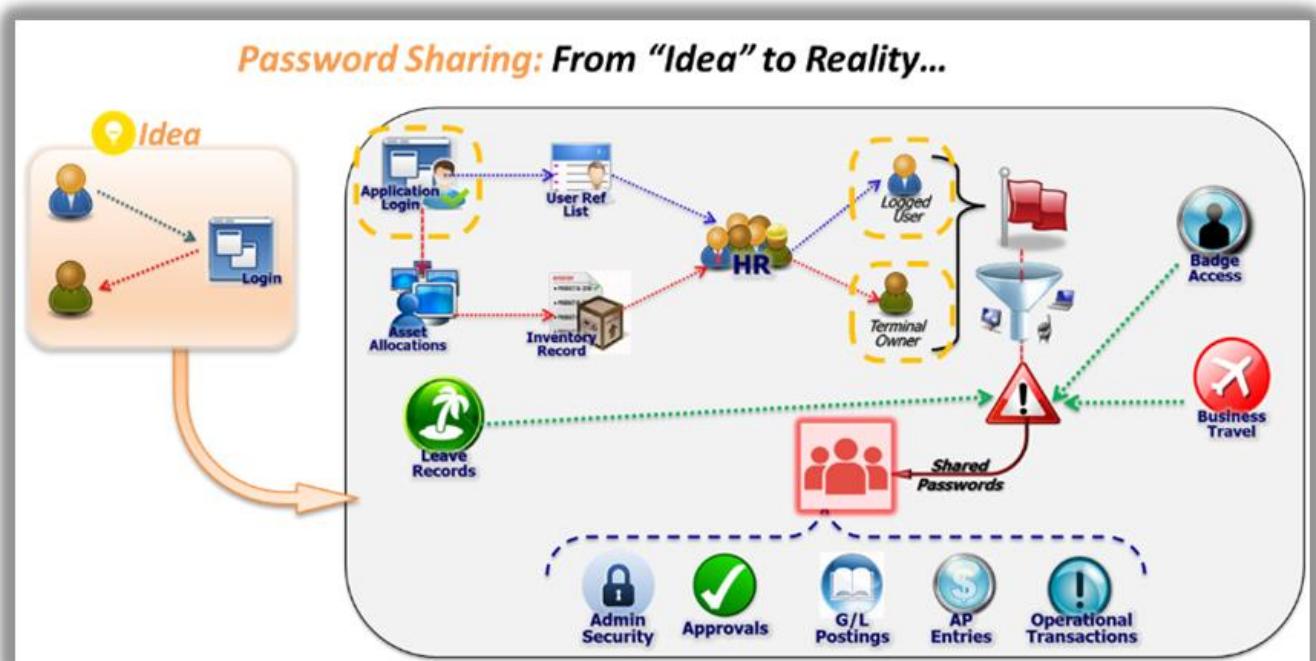


Figure 2: From "Idea" to Reality



PREPARE TO PASS THE CIA® EXAM

NEW for 2016! **StudyPLUS**



When you're in the home stretch and want a final confidence boost for the CIA exam, The IIA's StudyPLUS is your competitive edge. The IIA's CIA Learning System® provides everything you need to prepare for the Certified Internal Auditor® (CIA) exam, PLUS, with these exciting new tools and tips you will feel even more in control on exam day.

Take your exam day confidence over-the-top with The IIA's CIA Learning System.

Easily access StudyPLUS on your computer, tablet, or mobile device wherever you are, day or night:

NEW! ✓ CIA Exam Tips & Techniques Video

NEW! ✓ Guide to CIA Exam Scoring

NEW! ✓ Bonus Printable Practice Questions

NEW! ✓ CIA Question Analysis Grid

NEW! ✓ Guide to Knowing When You're Prepared

NEW! ✓ Study Tips from Successful Candidates

For more information or to create your free study plan, visit www.LearnCIA.com/plus.



The Institute of
Internal Auditors

Nye medlemmer

Nye medlemmer i IIA fra 1.9.2016 – 30.11.2016

Arbejdernes Landsbank

Bastian Martin Pedersen
Michelle Rohde Pedersen

Deloitte

Bjørn Philip Rosendal

Eik Banki

Høgni Hansen

Ernst & Young P/S

Thomas Bruun Kofoed

Københavns Kommune

Ann-Bjørg Karbech Niclassen
Linda Claudia K. Nkundabanyanka
Jim Sørensen

Lån og Spar Bank

Lasse Sonne
Yimin H. Nielsen

Nordea

John Kitchener
Nidhi Gandhoke

Saxo Bank

Andreas Ramsing

Spar Nord

Britta Skærup Nielsen
Nille Rinder

Sparekassen Vendsyssel

Malene Rask Trudslev

Uddannelsesaktiviteter

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

**Gå-hjem møde om AML (Anti Money Laundering),
14.3.2017.** Afholdes hos PwC.

**Kursus for penge- og kreditinstitutrevisorer,
27.4.2017.** Afholdes på Quality Hotel, Høje Taastrup.

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

IIA Learning Webinars

20. December 2016: Members-only Webinar: The Election's Over, Now What? Understanding Washington's Agenda for Public Policy Change in 2017

7. februar 2017: EHS Webinar: Risk Proofing Your Organization And Probably Your Career

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.iiak.dk eller til:

Chefsekretær Dorte Dreie
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.globaliiak.org eller ved kontakt til:

Director
Lars Maagaard
Deloitte
☎ 61 62 18 90 ☐ l.maagaard@deloitte.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 Svensnungsen
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



European Space Agency

The European Space Agency (ESA) is seeking an

Internal Auditor (m/f)

in the Internal Audit and Evaluation Service,
Director General's Services

to be based at the ESA Headquarters in Paris, France or ESTEC,
Noordwijk, Netherlands, with some travel required within Europe

The European Space Agency (ESA) is an intergovernmental organisation whose mission is to shape the development of Europe's space capability and ensure that investment in space continues to deliver benefits to the citizens of Europe. ESA employs about 2200 staff members over Europe and has a budget of 5.2 billion euros.

Within the Internal Audit and Evaluation Service, the postholder will conduct audits of the Agency's activities and carry out management consultancy assignments. The main duties and responsibilities, conducted in accordance with international professional standards will be :

- auditing the governance mechanisms in place to ensure effective performance management, accountability and appropriate ethics and values within ESA;
- assessing the adequacy and effectiveness of the Agency's internal control and risk management framework to achieve the Agency's strategic objectives;
- auditing compliance of the Agency's activities with applicable regulations, policies and procedures;
- analysing potential weaknesses and improvement opportunities in corporate governance, risk management and control processes;
- conducting investigations into suspected malpractice.

Applicants for this post should have a Master's degree in internal audit, engineering, business administration, or other relevant discipline, with a minimum of three years' experience of internal auditing in an international environment. Candidates should be Certified Internal Auditors or the equivalent. Certified competence in auditing Information Systems will be considered a strong asset.

Excellent analytical, organisational and coordination skills and the ability to provide quality summary output against tight deadlines are prerequisites for this post as well as good communication and interpersonal skills.

The working languages of the ESA are English and French. A good knowledge of one of these is required together with a working knowledge of the other.

For a complete job description click [here](#) or visit the "Careers at ESA" webpage. If you wish to apply, please complete the online application form obtained by clicking on the link within the vacancy notice, reference ESA/VN-HO(2016)019.

Closing date is: 4th January 2017

ESA is an equal opportunity employer, committed to achieving diversity within the workforce and creating an inclusive working environment. Applications from women are encouraged.

Please note that applications are only considered from nationals of one of the following States: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the United Kingdom and Canada.