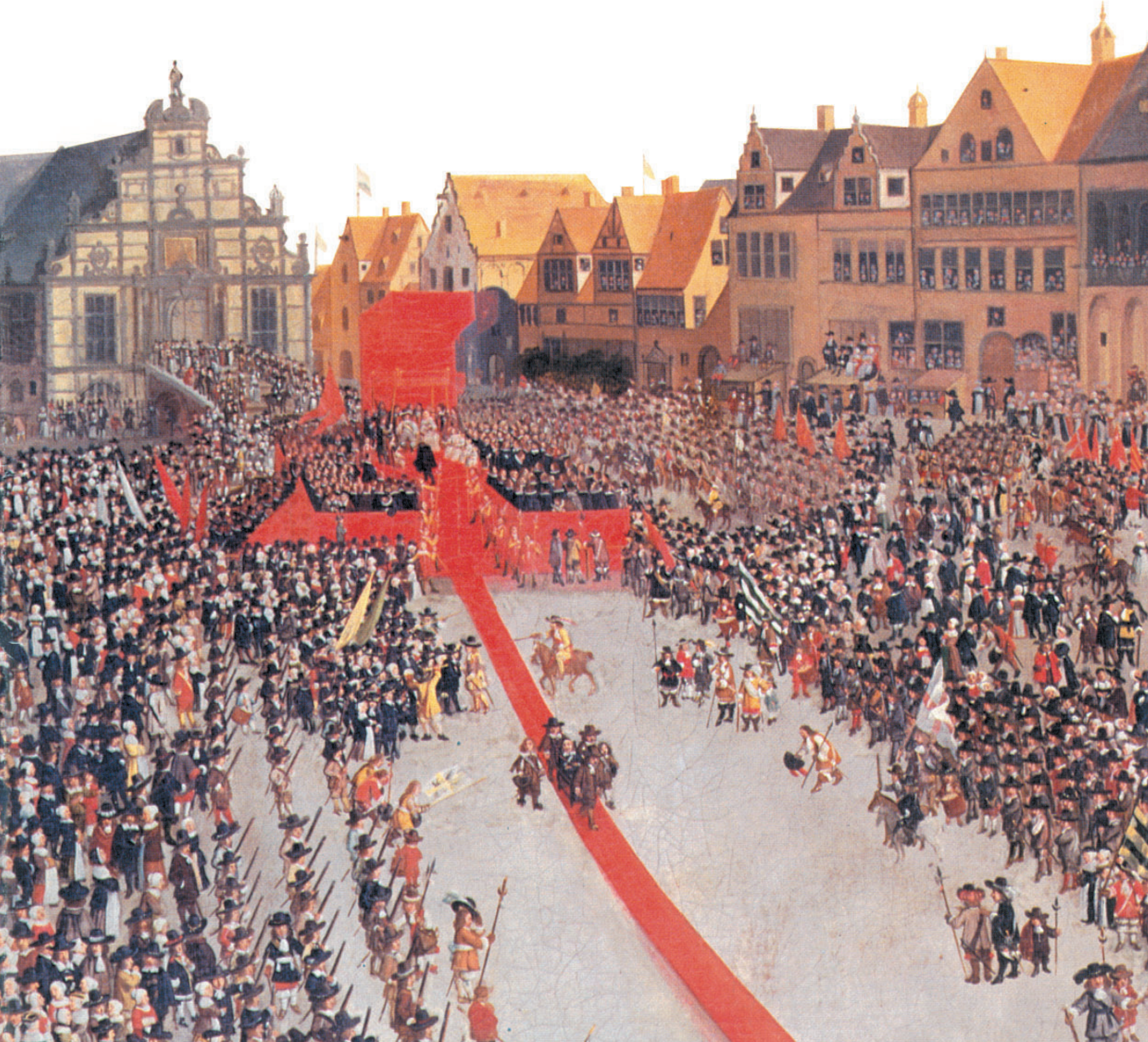
The Institute of Internal Auditors

Foreningen af Interne Revisorer

Nummer 29 April 2005 10. årgang

INFO



INFOs redaktion:

Ansvarshavende redaktør:
Chief Internal Auditor, Ane Marie Christensen
☎ 33 33 10 75
E-mail: ane.marie.christensen@nordea.com
Nordea

Øvrig redaktion:

Senior Manager Vibeke Aggerholm
☎ 35 87 26 68
E-mail: vibeke.aggerholm@dk.ey.com
Ernst & Young

Revisor Bente Hallberg
☎ 33 75 64 08
E-mail: beh@post.dk
Post Danmark

Revisor Brian Hansen
☎ 33 63 66 03
E-mail: brh@nationalbanken.dk
Danmarks Nationalbank

Revisor Henning Jørgensen
☎ 44 20 30 82
E-mail: henning.joergensen@tryg.dk
Tryg

Revisor Louise Claudi Nørregaard
☎ 33 41 82 24
E-mail: lono02@handelsbanken.dk
Handelsbanken

Revisor Henning Funck Nielsen
☎ 77 33 14 66
E-mail: hfn@sampension.dk
SAMPENSION

Revisor Birgitte R. Svenningsen
☎ 39 77 41 30
E-mail: bsv@saxobank.com
Saxo Bank

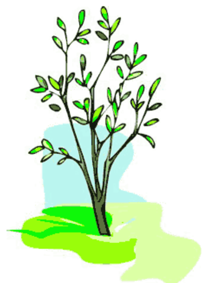
Revisor Pui Fong Yau
☎ 44 42 11 49
E-mail: pfy@novonordisk.com
Novo Nordisk

Redaktionens adresse:

Koncernrevisionschef Søren Kongsbo
Post Danmark
Intern Revision (IIA)
Tietgensgade 37
1566 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
v/ Jens Peter Thomassen

IIA's formål er som bekendt at varetage den uddannelsesmæssige, etiske og faglige udvikling for intern revision. Bestyrelsen har for at dække det uddannelsesmæssige området nedsat et uddannelsesudvalg, som skal varetage medlemmernes interesser indenfor revisionsteknik og metode for finansiel og operationel herunder revision af compliance ved udbud af kurser med afsæt i IIA standarder og ISA standarder, IT-standarder, COSO-rapporter mv. Branchespecifikke kurser udbydes i samarbejde med nedsatte sektorudvalg, der som bekendt varetager de mere branchespecifikke uddannelsesaktiviteter.

Ambitionerne er mange, ligesom de hastigt ændrede krav til intern revision stiller meget store krav til intern revisions kompetencer.

Vi i bestyrelsen, uddannelsesudvalget samt de branchespecifikke udvalg, vil gøre vort bedste for at identificere relevante emner for kurser, men det er vigtig, at I – brugerne af kurserne - kommer med forslag til emner og kurser, som I synes kunne være relevante. Det er et fælles ansvar. Send en mail til et af medlemmerne af uddannelsesudvalget, så vil vi vurdere muligheden for udbud af netop det kursus, som du måtte ønske.

Udbuddet af kurser er meget stort – det vi ønsker er, at sikre et relevant kursusudbud til en konkurrencedygtig pris. Dette sidste kræver, at I støtter op om kurserne, dvs. at I tilmelder jer - det reducerer enhedsprisen. Kurser vil løbende blive udbudt via hjemmesiden, og der vil, når IIA's hjemmeside er fuldt oppe at køre, være en opdateret kursuskalender. Alle kurser vil blive udbudt direkte til det enkelte medlem via e-mail, og al kursustilmelding vil ske via hjemmesiden.

Uddannelsesudvalget vil fra efteråret 2005 også have ansvaret for at tilrettelægge og gennemføre medlemsmøder, herunder kontakt til foredragsholdere og kursussteder. Vi vil bestræbe os på, at datoer for det kommende års medlemsmøder fastlægges i november. Temaer for medlemsmøder fastlægges i samarbejde med IIA's bestyrelse.

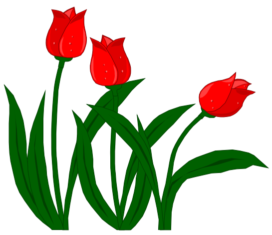
Kompetence er et begreb, der bør ligge langt fremme på pandelappen hos såvel ledelse som medarbejdere i intern revision. Forudsætningen for, at intern revision kan levere i det virkelige liv er, at intern revision har den rette kompetence og en opdateret viden, der matcher kundernes behov. Forudsætningen for at medarbejdere synes, at intern revision er en attraktiv karrierevej er, at medarbejdernes muligheder bibeholdes via målrettet undervisning, der sikrer, at vi kan levere de ydelser vore kunder efterspørger. Der er endvidere også krav om et minimum antal timer uddannelse, som den enkelte skal modtage inden for en tre årig periode. Udfordringen er derfor at sikre, at vore medarbejdere får disse uddannelsestilbud.

Det pointeres, at det er den enkelte og dennes leders ansvar, at kompetencerne vedligeholdes og udbygges, således at markedsværdien for den enkelte opretholdes og gerne øges. Herigennem sikres intern revisions mulighed for at tiltrække kompetente medarbejdere på såvel kort som lang sigt.

Skal der satses på at udvikle kompetencerne indenfor operationel og/eller finansiel revision? Det er min klarer opfattelse, at der skal satses på begge kompetencer, idet kravene fra USA og EU trækker i retning af øget fokus på den finansielle revision. Dette blev også bekræftet af **Prof. T. Flemming Ruud** på månedsmøde marts.

Også i dette info er der mange gode tilbud på uddannelse, men også mange gode artikler, som kan give inspiration til områder, hvor kompetencerne med fordel kan udvikles for at sikre, at intern revision kan levere de ydelser vore primære kunder efterspørger.

God læselyst.



Aktivitetskalender

I den kommende periode er der planlagt følgende aktiviteter:

<u>Medlemsmøde den 14. april 2005</u>
Emne: Besvigelser – aktuelle tendenser med fokus på regnskabsmanipulation.
Foredragsholder: Partner og statsautoriseret revisor Torben Lange, KPMG.

\- - - - - - - - -

Foreningen sender indbydelser ud til medlemsmøderne ca. 2 - 3 uger før møderne afholdes.

Tilmelding til medlemsmøder skal foretages til:

Anne Nordberg, SAMPENSION
☎ 7733 1465 eller
FAX nr. 7733 1477 eller
E-mail: ***ano@sampension.dk***

senest mandagen før afholdelse af medlemsmødet.

IIAs årskonference 2005 – præsenteret af revisionschef Claus Okholm, Nykredit

Den 8. – 10. juni 2005 afholder IIA årskonference på Hotel Marienlyst i Helsingør med mange spændende faglige emner og mulighed for godt socialt samvær med kolleger.

Der er tale om "årets" konference for alle, der er ansat i den interne revisorbranche.

Hurtig tilmelding tilrådes på IIAs hjemmeside: **www.iia.dk/konference**, da tilmelding registreres efter "først til mølle" princippet. **<u>Tilmeldingsfrist er 2. maj 2005</u>**. På IIAs hjemmeside fremgår detaljeret program, som ligeledes udsendes separat til alle IIA medlemmer.

Årskonferencen løber over 3 dage. De to første dage den 8.- 9. juni er tiltænkt alle medlemmer af IIA, mens fredag den 10. juni er tiltænkt ledelsen af intern revision. Deltagelse i 2 dage inklusive overnatning mv. koster 4.500 kr. og 3 dage koster 6.900 kr.

Årskonferencen er tilrettelagt med en række fælles indlæg i plenum for alle deltagere suppleret med streams, hvor der holdes indlæg specifikt for sektorerne finansielle, industri og offentlige.

Det sociale program omfatter udflugt og middag på Kronborg Slot onsdag den 8. juni. For deltagere alle 3 dage er der fælles middag mv. på Hotel Marienlyst torsdag den 9. juni.

Det faglige program omfatter følgende:

Generelle emner
- Præsentation af IIA v/ formand Søren Kongsbo, Post Danmark
- Den europæiske organisation ECIIA v/ Yves Chandelon, President ECIIA
- Etablering af revisionskomiteer v/ koncerndirektør Lise Kingo, Novo
- ERM and the opportunities for Internal Audit v/ Terry Cunnington, the immediate past president of the IIA UK and Ireland, Director, Group Risk Management for Euronext.
- Legal Risk Management v/ professor Mads Bryde Andersen
- Revisors uafhængighed og erklæringer v/ statsaut. revisor Per Gunslev, KPMG
- Eksempler på funktionsbeskrivelser/revisionsaftaler v/ statsaut. revisor Lars Holtug, PwC og koncernrevisionschef Anne Jæger, Codan
- Udviklingen i revisorbranchen v/ FSRs nye formand
- Udvikling af medarbejdere v/ psykolog Arne Schumann, eget konsulentfirma
- Styring og kompetenceudvikling af medarbejdere v/ uddannelseschef Marianne Svenningsen, PwC
- Gode råd om kommunikation v/ underdirektør Lisbeth Vedel, Danske Bank

Stream A: Den finansielle sektor
- Nyt fra Finanstilsynet v/ kontorchef Lars Østergaard og specialkonsulent Anne Charlotte Helskov
- Udvalgte emner vedrørende IFRS v/ statsaut. revisor Jesper Edelbo, PwC
- Kvalitetssikring af intern revisions arbejde v/ spesialrådgiverne Morten Thorbjørnsen

og May-Brit Riksheim, Det Norske Kredittilsyn
- Udvalgte forhold i revisionsbekendtgørelsen v/ statsaut. revisor Jesper Dan Jespersen, KPMG

Stream B: Industri sektoren
- Forventninger til Intern revision v/ chefkonsulent Jens Valdemar Krenchel, Industrirådet
- Sarbanes-Oxley v/ Vice President Kim Bundegaard, Corporate Governance & Risk, Novo
- Udvalgte emner vedrørende IFRS v/ statsaut. revisor Mogens Mogensen, PwC
- Entreprise Risk Management v/ statsaut. revisor Henrik Holmmark, E&Y
- Transfer Pricing v/ statsaut. revisor Michael Sørensen, KPMG

Stream C: Den offentlige sektor
- Intern revisions relationer v/ revisionschef Hans Kr. Møller, Direktoratet for FødevareErhverv
- Intern revisions rolle i forbindelse med "Public Governance" v/ kontorchef Rolf Elm-Larsen, Rigsrevisionen
- Udvalgte emner v/ Rigsrevisor Henrik Otbo, Rigsrevisionen
- Risikostyring i det offentlige v/ repræsentant fra Handelshøjskolen i København
- Risikostyring og intern kontrol v/ afdelingsdirektør Torun Reite

Vel mødt til IIAs årskonference i Helsingør.

- - - - - - - - -

Kursuskalender

Kursuskalenderen for 2005 ser således ud:

Kursus for Forsikringsrevisorer	**26. april 2005**
Revision af overholdelse af lovgivning (compliance) Jylland	**10. maj 2005**

Tilmelding kan foretages via foreningens hjemmeside: **www.iia.dk**

Eksamen
CIA, CCAP, CCSA og CFSA eksamen gennemføres i maj og november måned hvert år. Eksamen foregår i Danmark og er på engelsk. Tilmelding til eksamen skal foretages til IIA i USA.

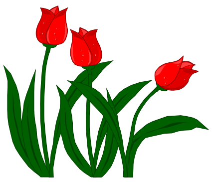
De næstkommende eksamener afholdes på følgende datoer:

	Eksamensdato	**Tilmeldingsfrist**
CIA		
Foråret 2005		
Part I & II	18. maj	31. marts
Part III & IV	19. maj	31. marts
Efteråret 2005		
Part I & II	16. november	30. september
Part III & IV	17. november	30. september
CGAP		
Foråret 2005	19. maj	31. marts
Efteråret 2005	17. november	30. september
CCSA		
Foråret 2005	19. maj	31. marts
Efteråret 2005	17. november	30. september
CFSA		
Foråret 2005	19. maj	31. marts
Efteråret 2005	17. november	30. september

Bestået CIA – eksamen

Redaktionen ønsker **TILLYKKE** til

Thomas Borch Nygaard, ATP
Karen Skakke Jørgensen, SAXO Bank
Nina Belcaid, Nordea



Bestået CFSA – eksamen

Redaktionen ønsker **TILLYKKE** til

Claus Tormod Nielsen, Nordea

Medlemsmøder m.v. i IIA

Medlemsmøde den 1. marts 2005

IIA Standarder, konsekvenser for Intern Revisions arbejde

Af Jan Bjarne Hansen, Senior Audit Manager, Nordea

Medens Kong Vinter iklædte København sin smukke hvide vinterkåbe, bød foreningen på foredrag af høj international kvalitet ved Prof. T. Flemming Ruud, PhD, CPA (Norway) fra Universität, Zürich, Institut für Rectnungswesen und Controlling.

Foruden IIA Standarderne og konsekvenserne for risk management, intern kontrol og governance processerne bød foredraget også på særdeles inspirerende vinkler på den seneste udvikling for eksempel Sarbanes Oxley og forholdet mellem intern og ekstern revision.

I en verden, hvor begreber anvendes i flæng, gav foredraget en befriende klar definition på forskellen mellem assurance og consulting, ligesom de tre kategorier af IIA guidelines indenfor the Professional Practices Framework (mandatory, authoritative og non-authoritative) blev gennemgået i detaljer.

Når man siger risk management, intern kontrol og governance, siger man jo samtidig nutildags Enterprise Risk Management (ERM). Medens hidtidige præsentationer som regel har behandlet dette emne ved en gennemgang af de 8 komponenter og de 4 målsætninger i ERM kuben, udmærkede dette foredrag sig ved at gå skridtet videre ved at præsentere nogle praktiske metodikker, som kunne anvendes inden for de enkelte komponenter.

Gennemgangen af the Sarbanes Oxley Act og dens indflydelse på især ekstern revisions ansvar og arbejdsopgaver var vel efterhånden kendt. Imidlertid var Flemming Ruud's betragtninger om den internationale trend om arbejdsfordelingen mellem intern og ekstern revision blandt andet som følge af Sarbanes Oxley interessante, idet trenden bærer i retning af at Intern Revision i højere grad (igen) bør fokusere på kvaliteten af den finansielle rapportering.

Et helt igennem gennemført arrangement som fuldt ud retfærdiggjorde den store tilmelding.

Prof. T. Flemming Ruud, PhD, CPA (Norway) fra Universität, Zürich, Institut für Rectnungswesen und Controlling.

Åbning af Center for Corporate Governance på Copenhagen Business School, Frederiksberg

Af Jan Bjarne Hansen, Senior Audit Manager, Nordea

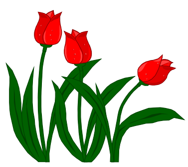
Foreningen havde fået en aftale med direktør Steen Thomsen, som er hovedarkitekten bag det ny center for Corporate Governance på Copenhagen Business School, om at deltage i åbningen af det ny center. Åbningen indeholdt så prominente talere som professor Igor Filatotchev, King's College, London og Lars Nørby Johansen, CEO for Group4 Securicor.

Igor Filatotchev er en af de førende eksperter inden for international corporate governance, medens Lars Nørby Johansen er velkendt herhjemme for sit arbejde over de sidste 5-6 år med Corporate Governance. Lars Nørby Johansen vil være formand for Centerets Advisory Board.

Centeret har været undervejs et stykke tid og det var en stolt Steen Thomsen, som nu kunne åbne centeret. Det var væsentligt for Steen Thomsen at understrege, at centeret har til formål at samarbejde med de øvrige centre på skolen og ikke være en konkurrent. Skolen havde dog fundet at med den stærke udvikling inden for Corporate Governance, var det betimeligt også at have et center som dækkede præcis dette område.

Da intern revision jo både er en del af virksomhedens governance samt, efter alle international pejlemærker, også har til at opgave at revidere corporate governance processen, er det med stor interesse at interne revisorer vil følge centerets udvikling og arbejde.

IIA ønsker Center for Corporate Governance held og lykke med sit fremtidige virke.



Information fra IIA i Orlando

Financial Services Conference

In Philadelphia, Pennsylvania, USA
May 23-25, 2005

Where can you find out what's affecting internal auditing within the financial services industry? Attend The IIA's Financial Services Conference to learn best practices in managing regulations, as well as addressing fraud, privacy, governance, and more. Hear keynote speaker Kayla J. Gillan, PCAOB member, provide an update on the group's activities and address lessons learned in 2004.

Attend sessions addressing:

- Sarbanes-Oxley
- Fraud detection
- Current issues in insurance and mutual fund
- COSO ERM
- Accounting derivatives
- And much more

Take advantage of this year's opportunity to participate in a CFSA Prep Course Workshop, attend the conference, and sit for the CFSA Exam – all in one week and at one location.

Fraud and Ethics Conference

In Litchfield Park (Phoenix), AZ
June 6-8, 2005

Enhance your organization's fraud prevention controls. Uncover the latest techniques for preventing, detecting, and investigating fraud at The IIA's 2005 Fraud & Ethics Conference. Explore the role of an organization's ethics culture in the prevention of fraud during this two-and-a-half day, three-track conference.

International Conference 2005

Illinois, Chicago, USA
July 10-13

You'll find this conference is conveniently presented in the heart of downtown Chicago, where the Magnificent Mile meets Wacker Drive at the Hyatt Regency Chicago Hotel on the Riverwalk.

ECIIA Pan-European Internal Audit Conference

In Larnaca - Cyprus
October 13-14, 2005

For more information, please contact IIA Cyprus by e-mail: ikoumera@eac.com.cy, or ECIIA at enquiries@eciia.org, or visit the ECIIA Web site.

Yderligere information kan ses på IIA´s hjemmeside: **www.theiia.org**

Entreprise Risk Management i praksis

Af Thomas Christensen, Ernst & Young

COSO's rapport fra 1992 om intern kontrol havde til formål at fremsætte fælles standarder for intern kontrol, herunder især definitionen, vurderingen og rapporteringen af interne kontroller. COSO's rapport om Enterprise Risk Management (ERM), som udkom i september 2004, har som hovedformål at skabe en fælles referenceramme eller standard, som virksomheder, store som små – offentlige som privat – vil kunne referere til for at kunne vurdere virksomhedens risikostyring, og så vidt muligt tage skridt til at forbedre denne.

Hvorfor er der så meget fokus på ERM?

Hvor COSO's 1992-rammebetingelser for intern kontrol fokuserede snævert på virksomheders interne kontrolmiljø, er ERM tiltænkt at være væsentligt bredere funderet på virksomhedens interne miljø, dvs. virksomhedens kultur, etiske værdier og politikker. Det interne miljø er grundlaget for de 7 øvrige komponenter i ERM, og er dermed afgørende for virksomhedens strategiudvikling, planlægning samt risikostyringprocedurer. ERM giver således ledelsen et strategisk risikostyringsværktøj, der sikrer, at virksomheden ikke udsættes for unødige risici, samt at indbyrdes relaterede risici er kontrolleret.

Figur 1. COSO's rammer fra 1992 og 2004 for hhv. intern kontrol, og Enterprise Risk Management.

Kilde: COSO´s Enterprise Risk Management – Integrated Framework, Executive Summary side 7, © september 2004, forfatter: PWC.

Baggrunden for denne udvikling er, at øget globalisering, teknologisk udvikling og ændrede organisationsformer medfører nye forretningsmuligheder for virksomheder og organisationer. Men samtidig medfører ændringerne også nye og øgede risici. Sammen med den større fokus på regulering, lovgivning og retningslinier for corporate governance og intern kontrol betyder dette, at virksomheder i dag er tvunget til at have et mere formelt fokus på risk management som et element i god corporate governance og som et middel til at fastholde og øge virksomhedens værdi.

Hvad kendetegner et effektivt ERM-system?

Et effektivt ERM-system kræver, at håndteringen af risici understøttes af en effektiv risk management struktur i organisationen. Dette indbefatter:

1. *Risikostrategi* - at ledelsen implementerer et overordnet framework, der sikrer en effektiv risikohåndtering med stakeholder value og virksomhedens strategi som omdrejningspunkt.

2. *Ledelse/governance* - at ledelsen tager ansvaret for, at virksomheden styres med udgangspunkt i interessenternes krav, samt identificerer og uddelegerer ansvaret for væsentlige risici.

3. *Risk management proces* - at virksomhedens risikohåndtering er integreret og velfungerende i samtlige væsentlige forretningsprocesser.

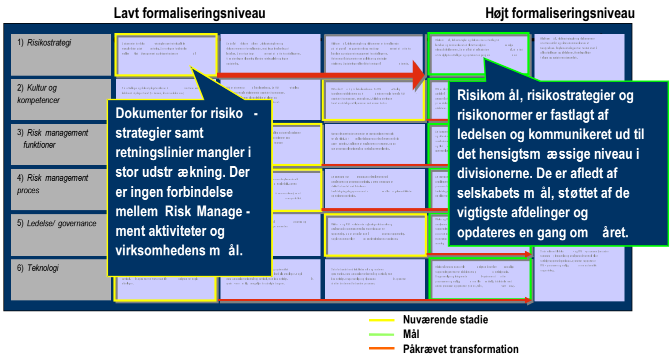
4. *Teknologi* - at virksomheden har en velfungerende infrastruktur, der sikrer en effektiv informationsudveksling og udnyttelse af den forhåndenværende information.

5. *Risk management funktioner* - at beslutningsprocessen effektivt understøttes gennem en løbende koordinering mellem virksomhedens risikostyringsfunktioner.

6. Kultur og kompetencer - at de nødvendige kompetencer for en tilfredsstillende risikohåndtering er til stede, samt at der eksisterer en risikobevidst kultur, som sikrer, at medarbejderne kan træffe velunderbyggede beslutninger.

Først når disse overordnede strukturer er på plads og integreret i organisationen har virksomheden skabt et fundament for en velfungerende risk management funktion.

Figur 2. Eksempel på ERM-modenhedsmodel.



Hvordan kommer jeg videre i min organisation?

Der er flere indgange til Enterprise Risk Management. Man kan tage udgangspunkt i konkrete risici, rammebetingelser for risikostyring eller virksomhedens/organisationens strategiske mål. At kombinere alle disse tre parametre er en meget tidskrævende, kompleks og omkostningstung proces. Ofte har man derfor behov for at skabe sig et overblik, hvilket i sig selv er særdeles værdifuldt som styreværktøj. Samtidigt kan dette overblik fungere som første skridt på vejen mod et fuldt funktionsdygtigt og integreret ERM-system.

For at kunne tage det første skridt mod ERM kræves det, at man har sikret sig en generisk referenceramme, ud fra hvilket man kan arbejde. Hermed menes, at der er opstillet modeller til informationsindsamling og analyse, der sikrer fuldstændigheden i det udførte arbejde. Ofte er det jo netop en silobaseret indgang til risikostyring, der gør, at man ikke får afdækket alle hjørner og risici i organisationen. Man sikrer sig mod dette ved at definere et risikounivers, som efterfølgende skal fungere som omdrejningspunktet for al informationsindsamling og analyse.

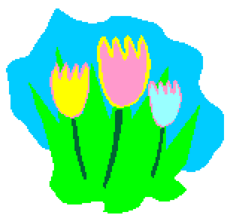
Dernæst er det væsentligt, at man forholder sig kvalitativt til den information man får indsamlet om risici i organisationen. En kvalitativ vurdering i forhold til sandsynlighed og effekt foretages som hovedregel mest effektivt gennem et workshopforløb. Derfor er det meget væsentligt, at man som organisation sikrer sig adgang til specialister, der qua brancheindsigt og viden om risikostyring og kontrolmiljøer formår at facilitere en sådan proces effektivt. Samtidigt vil et workshopforløb kunne skabe en "awareness", der vil være meget værdifuld i et senere ERM-forløb.

Værktøjer er en tredje væsentlig forudsætning for at kunne få succes med at kortlægge og analysere virksomhedens risici. I første omgang behøver disse værktøjer ikke at være særligt avancerede. Et krav er det dog, at man skal være i stand til at koble identificerede "what can go wrong" til virksomhedens forretningsprocesser. På denne måde bliver man i stand til at tilpasse virksomhedens kontrolmiljø i linie med ledelsens risikoappetit.

Har man disse ting på plads, vil man med en relativt begrænset ressourceindsats kunne lave den første risikoprofil indeholdende:

- En kortlægning af virksomhedens væsentligste risici.
- Risici koblet til virksomhedens forretningsprocesser.
- En GAP-analyse, der identificerer afvigelser mellem ledelsens ønsker og den opstillede risikoprofil.

Dermed har man et optimalt udgangspunkt for at vurdere hvorvidt man ønsker at gå hele vejen mod en systematisk identifikation, vurdering og styret håndtering af væsentlige forretningsmæssige risici, nemlig Enterprise Risk Management.



Intern revisions rolle i en Sarbanes-Oxley kontekst

Intern revisions rolle i en Sarbanes-Oxley kontekst.
- ***fokus på Sarbanes Oxley, intern kontrol og risikostyring.***

Af cand. merc. aud. Per Kristensen, Global Risk Management Solution, PricewaterhouseCoopers.

Nærværende artikel[1] er hovedsageligt baseret med afsæt i konklusionerne, som er gjort i kandidatafhandlingen ”Intern revisions rolle i et Corporate Governance perspektiv i finansielle virksomheder”, samt de erfaringer, som er erhvervet ved udførelsen af Sarbanes-Oxley 404 projekter i forbindelse med udstationering i Los Angeles, USA.

Nærværende artikel vil være opdelt i en teoretisk behandling af de interne revisorers rolle i en Sarbanes-Oxley kontekst samt en beskrivelse af de erfaringer, jeg har gjort i forbindelse med mit arbejde i USA som intern revisor / IT revisor på flere Sarbanes-Oxley projekter.

Indledning

Vedtagelsen af “the Sarbanes-Oxley Act of 2002 (herefter SOX)” var en kulmination af de største konkurser i amerikansk historie, revisionsvirksomheden Arthur Andersens fald samt en generel mistillid i samfundet til selskabernes ledelse samt korrektheden af de offentliggjorte årsregnskaber. Formålet med SOX har bl.a. været at genvinde tilliden til det amerikanske kapitalmarked samt medvirke til at gøre selskabernes ledelse ansvarlig for deres handlinger ved at implementere standarder, der udstikker omfattende krav til selskabernes ledelse, for så vidt angår bl.a. etablering af revisionskomité, øgede fokus på ledelsens ansvar for aflæggelsen af det finansielle årsregnskab samt ledelsens ansvar for implementering, vedligehold og vurdering af virksomhedens interne kontrol.

Sarbanes-Oxley Act of 2002

SOX indfører nye og mere restriktive regler på 11 punkter herunder bl.a. øget ansvar for revisionskomiteer, skærpet straf for økonomisk kriminalitet og skærpelse af ledelsens ansvar. Det er det amerikanske børstilsyn, som skal udstede detaljerede krav og retningslinjer.[2]

I tilknytning til nærværende artikel er især bestemmelserne i medfør af paragraf 302 og 404 i SOX centrale og omhandler i væsentlig omfang nedenstående faktorer:

A. Ledelsen skal ved afgivelse af kvartalsvis erklæring bekræfte, at oplysninger er nøjagtige, fuldstændige og giver et retvisende billede, herunder deres ansvar for selskabets procedurer for afgivelse af information, benævnt ”Disclosure controls og procedures”. (SOX §302)
B. Ledelsens ansvar for, at virksomhedens interne kontrolsystem fungerer effektivt. Endvidere er ledelsen pålagt at etablere procedurer for regnskabsaflæggelse, krav om årlig vurdering af og erklæring om effektiviteten af de etablerede interne kontroller. (SOX §404)
C. Det er virksomhedens eksterne revisor, som har ansvaret for at gennemgå ledelsens vurdering og erklæring om effektiviteten af de etablerede interne kontroller. Den eksterne revisor skal erklære sig om den udførte gennemgang. (SOX §404)

Hvad der forekommer interessant i en europæisk og dansk sammenhæng er, at regelsættet foruden amerikanske selskaber også omfatter udenlandske selskaber, der er noteret på børser i USA, samt selskaber uden for USA, som indgår i en koncern, hvor moderselskabet er børsnoteret på en børs i USA.[3] Der er for nærværende 4 selskaber i Danmark, som

[1] ***Per Kristensens artikel er en fortsættelse af en artikel i INFO nr. 28 med samme overskrift. Der vil derfor forekomme enkelte gentagelser, men redaktionen har fundet dette hensigtsmæssigt dels for at sikre en samlet forståelse, dels for at tilgodese nye læsere af bladet.***

2 Kilde: PricewaterhouseCoopers: ”Det børsnoterede selskab 2004 – nyheder og udviklingstendenser for ledelsen”, 2003, side 27.

3 Kilde: PricewaterhouseCoopers: ”Det børsnoterede selskab 2004 – nyheder og udviklingstendenser for ledelsen”, 2003, side 27.

er noteret på børser i USA og dermed direkte omfattet af SOX, samt et ikke uvæsentligt antal datterselskaber som følge af tilhørsforhold til en amerikansk koncern er berørt af SOX regelsættet.

Intern revisions rolle i en Sarbanes-Oxley sammenhæng

I en undersøgelse foretaget i et samarbejde mellem PricewaterhouseCoopers og ”The Institute of Internal Auditors' Global Auditing Information Network (GAIN)”[4], som havde til formål at klarlægge den rolle, de interne revisorer i Fortune 1000 virksomheder i USA indtog i selskabernes implementering af kravene jf. SOX § 404, blev det bl.a. konstateret, at de interne revisorer indtager en central rolle i forbindelse med rådgivning om begrebsapparaterne intern kontrol og risikostyring, udarbejdelse af dokumentation og gennemgang og test af effektiviteten af virksomhedens interne kontrol.

Baseret på bl.a. ovennævnte analyse kan det indledningsvis postuleres, at netop de interne revisorer besidder en kompetence og hermed mulighed for at assistere virksomhedens ledelse i arbejdet med at effektuere og implementere bestemmelserne jvf. SOX 404. Med postulatet in mente kan spørgsmålet stilles, om de interne revisorer i danske virksomheder allerede i dag helt eller delvis udfylder denne rolle, og hvorvidt fremtidens interne revisorer er forberedte på en forøget fokusering på begrebsapparaterne intern kontrol og risikostyring? Det er af flere årsager ikke muligt at besvare dette spørgsmål i nærværende artikel. Det blev imidlertid konkluderet i min kandidatafhandling ”Intern revisions rolle i et Corporate Governance perspektiv i finansielle virksomheder”, at netop de interne revisorer i Danmark besidder en særlig grund til og mulighed for at imødekomme virksomhedernes eksterne interessenters informationsbehov ved eksempelvis at afgive særskilt erklæring om effektiviteten af virksomhedens væsentlige forretningsgange, effektiviteten af de interne kontrolprocedurer, hvorvidt virksomheden har betryggende kontrol- og sikringsforanstaltninger på it-området og om virksomhedens økonomiske fremtidsudsigter.

Det blev endvidere konkluderet, at der eksisterer åbenbare forskelle mellem den danske og de internationale tilgange til begrebet intern revision. Det blev bl.a. udledt af den foretagne behandling af begrebet intern revision, at formålet med intern revision i en international kontekst sædvanligt relateres til en 'add value' funktion med fokus på gennemgang af virksomhedens risikostyring, interne kontrol samt governance processer, og hvor kendetegn som ‘evaluate and improve the effectiveness of risk management, control, and governance processes' tilknyttes de interne revisorer. Herimod mangler tilgangen til begrebet i en dansk sammenhæng en entydig definition og stillingtagen og diskussion af de interne revisorers arbejdsfelt.

Sarbanes-Oxley Act of 2002 og fremtidsperspektiverne

I The Institute of Internal Auditors "Internal Auditor" udgave fra april 2004 understreges den Sarbanes-Oxley regelsættes relationer og mulige betydning for europæiske selskaber således,

> If Europe doesn't embark on a program to establish something similar to Sarbanes-Oxley, with a culture and approach that is specific to European member states, then we run the risk of having Sarbanes-Oxley becoming the reference through the back door".[5]

Citatet vidner i stor grad om, at den fremtidige europæiske corporate governance agenda i nogen udstrækning vil bære præg af bestemmelserne fra Sarbanes-Oxley regelsættet og i nogen udstrækning direkte eller indirekte vil øve indflydelse på de interne revisorers hverdag.

The Public Company Accounting Oversight Board (PCAOB), hvis opdrag er at udstede standarder til understøttelse af bestemmelserne i Sarbanes-Oxley loven, udsendte i marts 2004 standarden "Auditing Standard No. 2 - "An Audit of Internal Control Over Financial Reporting Performed In Conjuction With An Audit Of Financial Statements" (herefter A-S 2) som referencestandard for SOX paragraf 404.

Den europæiske pendant til SOX skal i nogen grad søges i den af Europa-kommissionen udsendte handlingsplan. Handlingsplanen skal medvirke til at styrke aktionærernes rettigheder og på én gang tilgodese øvrige interessenters interesser.[6] I hand-

4Kilde: PricewaterhouseCoopers: ”GLOBAL BEST PRACTICES, Beyond Compliance: How Internal Audit. Reaps Value from SarbaneSOXxley Section 404”.Side 3

5 Kilde: The Institute of Internal Auditors, Internal Auditor: "The European reform agenda", april 2004, s. 55.

6 Kilde: COMMISSION OF THE EUROPEAN COMMUNITIES: “COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN

lingsplanen lægges op til, at ledelsen i børsnoterede virksomheder ved afgivelse af erklæring i årsrapporten bl.a. skal redegøre for effektiviteten af virksomhedens interne kontroller.[7] Sammenholdelse ovenstående med den af Europa-kommissionens udarbejdede handlingsplan for samt Basel Komiteens forslag til nye kapitaldækningsregler synes de interne revisorers fremtidige arbejdsfelt i stort omfang at relateres til gennemgang og vurdering af effektiviteten af virksomhedernes interne kontroller og risikostyring.

Baseret på ovenstående konklusioner kan det postuleres, at de internationale udviklingstendenser ikke har haft en afgørende afsmittede effekt på de interne revisorers virkefelt i en dansk kontekst. Der må nødvendigvis udestå et arbejde for de interne revisorer i Danmark og de interne revisorers faglige organisation, såfremt professionen også i fremtiden skal indtage en central rolle som virksomhedens primære interne rådgiver i henseender som virksomhedens interne kontrol, risikostyring og corporate governance i en bred kontekst.

Det forekommer som en logisk konsekvens af ovenstående skildring af de international udviklingstendenser, at de interne revisorer i Danmark medvirker til at udarbejde en standard for udarbejdelse af dokumentation, test af kontroller og samarbejde med eksterne parter herunder den eksterne revision i sikringen af en ensartet tilgang til området.

SOX i praksis sammenhæng

Erfaringer gjort i forbindelse med deltagelse på SOX projekter i USA

Gennem mit virke som intern revisor / IT revisor på SOX projekter i USA har jeg opnået et førstehåndskendskab til udførelsen af SOX projekter fra planlægningsstadiet til det afsluttende samarbejde med ekstern revision. Beskrivelserne og teserne i nedenstående afsnit vil således være baseret med afsæt i de erfaringer, jeg har gjort i forbindelse med dette arbejde.

Planlægning af projektet

Planlægningsfasen er grundstenen i et SOX projekt og bør som minimum omfatte forhold som ressourceplanlægning, fastlæggelse af kriterier for projektets gennemførelse, tidsfrister for udførelse og afrapportering af de enkelte delfaser af projektet fastlæggelse af metoder for ensartet dokumentation af såvel narrative, kontrolmatricer og flowcharts samt dokumentation af identificeret ”control gaps”. Herudover bør der afsættes tilstrækkelige ressourcer og tid til at afholde periodiske møder i teamet med det formål at diskutere væsentlige problemstillinger samt etablere videns deling blandt teamdeltagerne.

Det er min erfaring, at denne fase af projektet typisk indeholder faldgruber såsom manglende/ utilstrækkelig PMO (project management), utilstrækkelig kommunikation mellem projektets interessenter samt manglende etablering af paradigmet (”Framework”) for projektets gennemførelse.

Udarbejdelse af dokumentation

Der er ikke et ”one size fits all” svar på omfanget, og graden af ledelsens dokumentation af virksomhedens interne kontrol. A-S 2 giver imidlertid visse rettesnor jf. paragrafferne 42,43 og 44, som ledelsen og den intern revision kan (skal) iagttage i forbindelse med udarbejdelsen af ledelsens dokumentation.

A-S 2 paragraf 42 lister en række forhold vedrørende ledelsens dokumentation, som ekstern revisor skal påse foreligger. Herunder bl.a., at dokumentation indeholder:

1. The design of controls over all relevant assertions related to all significant accounts and disclosures in the financial statements.
2. Information about how significant transactions are initiated, authorized, recorded, processed and reported;
3. Sufficient information about the flow of transactions to identify the points at which material misstatements due to error or fraud could occur;
4. Controls designed to prevent or detect fraud, including who performs the controls and the related segregation of duties;
5. Controls over the period-end financial reporting process;
6. Controls over safeguarding of assets; and
7. The results of management's testing and evaluation.

Dokumentations omfanget for SOX 404 projekter kan umiddelbart fastlægges jf. punkt 1, 2 og 3 . Ledelsens dokumentation skal således omfatte alle ”significant” regnskabsposter” og processer og skal

PARLIAMENT - Modernising Company Law and Enhancing Corporate Governance in the European Union - A Plan to Move Forward”, Brussels, 21.5.2003.

7 Initiativet er betydeligt præget af den amerikanske SarbaneSOXxley lov som er beskrevet i afhandlingens kapitel 2.

være dokumenteret i en sådan grad, at det i tilstrækkeligt omfang giver ekstern revision de nødvendige informationer om bl.a. processflowet, eksisterende kontroller, identificeret manglende kontroller samt regnskabsafslutningsprocessen.

Herudover skal ledelsens dokumentation jf. punkt 5 og 6 indeholde beskrivelse af forhold vedrørende processen for regnskabsafslutning samt kontroller vedrørende " safeguarding of assets". Endelig skal ledelsens dokumentation indeholde resultatet af den foretagne test af virksomhedens interne kontrol.

A-S 2 fastsætter ikke måden, hvormed ledelsen skal dokumentere dens gennemgang. Omfanget af ledelsens dokumentation afhænger bl.a. af kompleksiteten af virksomhedens processer samt virksomhedens størrelse samt andre virksomheds specifikke forhold og kan således omfatte forskellige former herunder bl.a. papirform eller elektronisk medie. Dokumentationen kan således bestå af informationer såsom forretningsgange, procesmodeller, flowcharts og jobbeskrivelser osv.

Det er min erfaring, at denne fase af projektet kan indeholde endog adskillige faldgruber, der som oftest kan relateres til mangel på tilstrækkelig instruktion og undervisning af de, som udarbejder dokumentationen, mangel på følelse af "ejerskab" hos centrale personer "processowner", mangel på fælles dokument paradigmer samt mangel på tilstrækkelig kendskab til virksomhedens processer samt oprettelse af et fælles opbevaringssted for dokumentation, som er tilgængelig for såvel ledelse som teamdeltager ("on-site" såvel som "remotely").

Walkthrough samt test af effektiviteten af virksomhedens interne kontrol

A-S 2 angiver ikke, i hvilket omfang ledelsen bør udføre *walkthroughs* samt test. Det er imidlertid min erfaring fra de SOX projekter, jeg har deltaget i, at ledelsen har valgt at foretage walkthroughs af alle væsentligste processer samt test af alle nøglekontroller som identificeret i forbindelse med udarbejdelsen af projektets "*scope*". Formålet med walkthroughs er at verificere den udarbejdede dokumentation og identificere en eventuel mangelfuld beskrivelse eller kontrolaktiviteter, som er beskrevet men ikke udføres i praksis.

Efter færdiggørelse af dokumentation og walkthrough skal testprogrammet udarbejdes. Testprogrammet skal som udgangspunkt medtage alle *"nøgle"* kontroller. Omfanget af de enkelte test afhænger af frekvensen (daglig, ugentlig, månedlig osv.) samt typen af kontrollen (manuel eller automatisk).

Det er her væsentligt at gøre sig bevidst, at der i projektplanen bør være indarbejdet tilstrækkelig med tid mellem indledende testfase til gentestfasen, således at der for kontrolaktiviteter med identificeret mangler kan implementeres en "afhjælpningsplan" i tilstrækkelig lang tid til at dokumentere, at afhjælpningen er effektiv.

Det er min erfaring, at faldgruberne i denne del af projektet normalt omfatter problemstillinger vedrørende planlægning af ressourcer, mangel på en fælles database til registrering af identificeret fejl og mangler i forbindelse med udførelsen af test, utilstrækkelig undervisning af teamdeltager i testmetodikker samt prioritering af afhjælpningerne.

Perspektivering

SOX 404 projekter indeholder endog mange faldgruber såsom manglende Project Management, manglende "commitment" fra projektets interessenter, manglende eller utilstrækkelig undervisning af projektets teamdeltager osv. Størsteparten af føromtalte problemstillinger kan løses eller undgås ved tilstrækkelig planlægning fra projektets start samt sikre en acceptabel "commitment" fra projektets deltagere allerede fra projektets første fase.

Med afsæt i konklusionerne ovenfor samt førnævnte kandidatafhandling "Intern revisions rolle i et Corporate Governance perspektiv i finansielle virksomheder" kan det postuleres, at ressourcekrævende og specialist orienterede projekter såsom SOX projekter kan (vil) medføre, at interne revisorer i mindre virksomheder ikke i tilstrækkelig grad besidder kompetencen, eller ikke i alle tilfælde har ressourcerne eller den specielle kompetence, der er nødvendig for at løfte opgaven effektivt, hvorfor en co-outsourcing af opgaven er en nærliggende mulighed. Gennem mit arbejde på flere SOX projekter i USA erfarede jeg, at et stigende antal virksomheder vælger at co-outsource den interne revision på områder / projekter, som er ressource- og kompetencekrævende. Der var ikke kun tale om mindre virksomheder men i stigende grad også store virksomheder med en omsætning på mere end 5 milliarder US Dollars. Det må således forventes som en naturlig konsekvens af de internationale udviklingstendenser, at ledelsen i danske virksomheder i fremtiden i større grad vil vælge at fremtiden i større grad vil vælge at co-outsource sådanne projekter med det formål at sikre den mest optimale sammensætning af kompetence, ressourcer og specialist viden i forbindelse med større projekter, der involverer intern revision.

COBIT- set fra en praktisk synsvinkel

Af IS Audit Manager & CISA Claus Rosenquist, TrygVesta

Indledning

Formålet med denne artikel er at give en praktisk indgangsvinkel til anvendelsen af COBIT med afsæt i, at TrygVesta Intern Revision nu i over et halvt år har arbejdet med COBIT.

Jeg vil i denne artikel redegøre for, hvad COBIT er, hvorfor vi valgte den, TrygVesta's anvendelse af COBIT, samt vores erfaringer med den.

Hvad er COBIT?

Baggrunden for COBIT (Control OBjectives for Information and related Technology) var at forme en model for IT Governance.

Ved udarbejdelsen blev der taget udgangspunkt i flere anerkendte referencerammer, såsom ISO 17799, COSO, Professional Standards in Auditing mv., men også med udgangspunkt i Risk Assessment.

COBIT er udarbejdet af ISACA – Information Systems Audit and Control Association, og blev første gang publiceret i 1996 og den nuværende third edition i juli 2000. ISACA er på nuværende tidspunkt i gang med at gennemgå den igen – fourth edition.

Modellen skal dække de control objectives, som er afledt af den stigende brug af IT i forretningsprocesserne.

COBIT skal forbedre kommunikationen mellem ledelse, brugere og revisorer. Derfor er modellen også anvendelig som både ledelsesmodel og revisionsmodel.

> ***The COBIT Mission***
> *To research, develop and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.*

COBIT tager udgangspunkt i business objectives, hvor kriterierne (Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance & Reliability) afdækkes af IT-ressourcerne (Data, Application systems, Technology, Facilities & People).

Dette gøres ved at fokusere på 4 hovedtemaer (domains) i COBIT:

PO Plan and Organise
AI Acquisition and Implementation
DS Delivery and Support
M Monitor and evaluate

COBIT er grundlæggende opbygget efter følgende struktur/hierarki:

Domain
↕
Process
↕
Control Objectives
↕
Control Practices

"**Control Practices** are key control mechanisms that support the achievement of control objectives as well as the prevention, detection and correction of undesired events through responsible use of resources, appropriate management of risk, and alignment of IT with business".

Indenfor de 4 domains findes der

- 34 high-level IT-processer
- 318 detaljerede control objectives
- 1.550 control practices (nøglekontroller).

Antallet af processer, control objectives og control practices er på nuværende tidspunkt under revision i forbindelse med den kommende fourth edition af COBIT.

COBIT giver et flow og indblik i de kritiske IT-processer, som er gældende indenfor IT - en naturlig struktur for IT-projekternes og IT-processernes livsforløb

Man skal dog være opmærksom på, at ikke alle processer kan være lige væsentlige for den enkelte virksomhed og dens IT-anvendelse – en risikovurdering skal afgøre dette.

Hvorfor COBIT?

I sommeren 2004 stod vi ved en skillevej. Vi vidste, at FSR's vejledning 14 for generelle IT-kontroller ville forsvinde primo 2005. Vi skulle derfor finde en "anden måde" at se verden på – en ny metodik.

Denne metodik skulle samtidigt understøtte os og vores nordiske integration, procestankegang og revision. TrygVesta opererer på flere forskellige markeder, og er underlagt flere landes tilsyn. Det var derfor vigtigt at kunne vælge en IT-revisionsmodel, som vil kunne dække de krav som stilles i den enkelte lande, herunder disse landes eksterne revision - en international anerkendt model.

En del arbejde og research blev foretaget for at afstemme vores mål og behov til COBIT. Dette var en yderst konstruktiv og lærerig proces.

Denne læringsproces lærte os, at

1. COBIT er en international anerkendt og mangeårigt bearbejdet model.
2. Den er procesorienteret, hvilket for os er en fordel, da TrygVesta er en procesorienteret organisation.
3. Den giver en naturlig struktur for IT-projekternes og IT-processernes livsforløb - sikre bl.a. overblik og fuldstændighed.
4. Den har i modsætning til andre modeller og standarder fokus på IT og kontroller.
5. Den kan mappes op mod relevante nationale og internationale standarder og modeller. For at opnå en grundlæggende indsigt i COBIT's opbygning undersøgte vi først sammenhængene til COSO og ISO 17799. Vi foretog derefter en mapping op mod FSR vejledning 14, Finanstilsynets §71 IT-vejledning samt erklæring fra tredje part i forbindelse med outsourcing af IT. Vi har efterfølgende foretaget en mapping op mod de kommende RS 3411 (udkast) og RS 315 (udkast) – med fokus på generelle IT-kontroller. Sammenfattende viste kortlægningerne, at der er fuld dækning af de nævnte standarder og modeller i COBIT.
6. Den understøttes af internationale og bearbejdede arbejdsprogrammer – sikrer bl.a. kvalitet og konsistens.

> ***"Public Company Accounting Oversight Board*** *requires the adoption of an established internal control framework to foster quality and consistency in the process of building and implementation the organisations internal controls. COSO may not contain sufficient detail to provide appropriate to CIO's as they look to identify and assess the adequacy of their IT controls".*

Efter vores vurdering er COBIT at betragte som best practices for kontrol og governance af IT.

TrygVesta's anvendelse af COBIT - revision

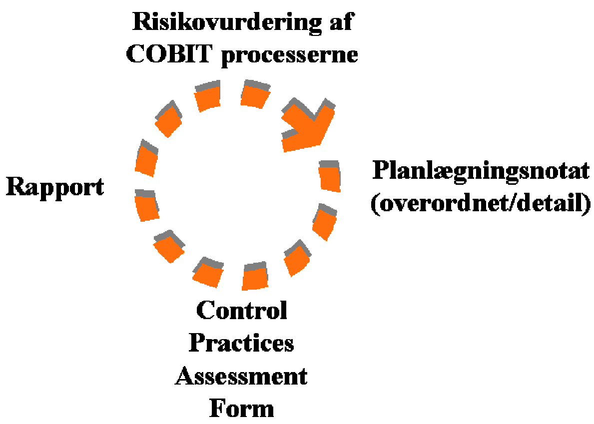
I forbindelse med vores valg af COBIT fandt vi det hensigtsmæssigt at re-tænke vores overordnet procesflow vedrørende IT-revisionen.

Vi ville sikre os, at COBIT blev en integreret del af faserne risikovurdering, planlægning, udførelse og rapportering.

Risikovurdering/planlægning faldt "naturligt" for COBIT, da modellen oprindeligt blev udarbejdet med udgangspunkt i risikovurdering. Vores største udfordringer var derfor at skabe et link mellem udførelse og rapportering. Et link som skulle sikre en rød tråd igennem alle fire faser.

Det var faktisk først sent i processen, at vi fik skabt dette link i form af Control Practices Assessment Forms (omtales senere i artiklen). Med denne kunne vi operationalisere vores udførelse og samtidigt sikrer den røde tråd i faserne – og dermed i revisionen.

Vores arbejde med at skabe sammenhængene blev senere til vores overordnet procesflow for IT-revisionen. Denne kan illustreres på følgende måde:



En nærmere beskrivelse af faserne følger nedenfor.

Risikovurdering:
De 34 high-level IT-processer i COBIT vil løbende blive vurderet ud fra risiko og væsentlighed i forbindelse med processernes påvirkning på Tryg-Vesta's IT-anvendelse.

Risikovurderingen skal være objektiv og dokumenteret. Den skal kunne verificeres af tredje part.

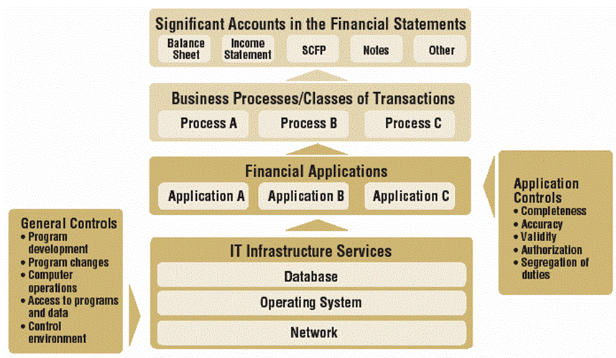
En 'trafiklys' ordning skal sikre at kritiske processer (rød) f.eks. revideres hvert år indtil de ændres til gul eller grøn. Et rotationsprincip skal ydermere sikre, at alle COBIT's 34 processer revideres over f.eks. en 3-årig periode.

Risikovurderingen vil løbende blive sammenholdt med TrygVesta's egen IT-risikoanalyse, som er udarbejdet af vores Koncernsikkerheds- og Risk Management funktion. Dette skal ske for at sikre konsistens og samme univers.

Planlægning:
En væsentlig del af risikovurderingen er koblingen til intern revisions samlede Audit Universe. Det kan betragtes som et stjernekort, der viser vejen for, hvor revisionen bør foretages - 'nogle stjerner lyser mere end andre'.

Det er en synliggørelse og risikoanalyse af forretningsprocesserne set ud fra et revisionsperspektiv. Dette skal bl.a. sikre en effektiv og nødvendig revision - '*a risk based audit approach*' - ligesom den synliggører de fravalg, der er foretaget.

I IT Governance Institute's paper vedrørende "*IT Control Objectives for Sarbanes-Oxley*" kan dette Audit Universe afspejles på følgende måde:



Figuren afspejler et krav om revisors forståelse af transaktionsflowet og interaktionen mellem teknologi, interne kontroller og regnskabet.

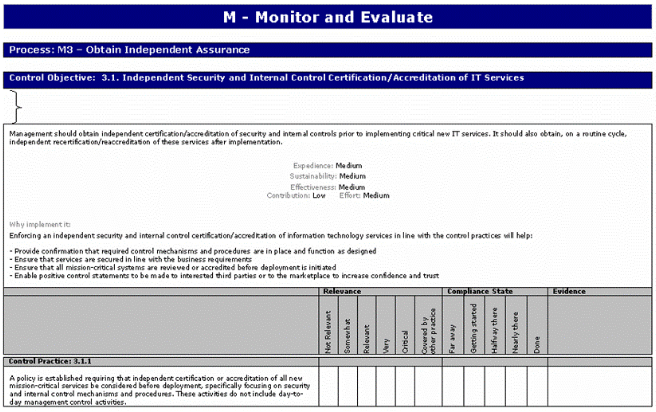
Den afspejler også en metode til at risikovurdere en regnskabspost, såfremt der er problemer i underliggende IT-infrastruktur – og omvendt.

Dette er bl.a. et af principperne i Public Company Accounting Oversight Board (PCAOB) Auditing Standard No 2. Figuren kan betragtes som en afgrænsning af IT-kontrollernes del af transaktionsflowet.

Audit Universe er også et værktøj, der i langt højere grad vil sikre en sammenhæng og interaktion mellem IT-revision og den finansielle revision.

Control Practices Assessment Forms – (udførelse):
En væsentlig del af vores procesflow og fremgangsmåde er anvendelsen af *Control Practices Assessment Forms.* Disse generes fra *COBIT Online* (isaca.org) ud fra brugerdefinerede kriterier.

Nedenstående er et eksempel på en Control Practices Assessment Form:



M - Monitor and Evaluate

Process: M3 – Obtain Independent Assurance

Control Objective: 3.1. Independent Security and Internal Control Certification/Accreditation of IT Services

Management should obtain independent certification/accreditation of security and internal controls prior to implementing critical new IT services. It should also obtain, on a routine cycle, independent recertification/reaccreditation of these services after implementation.

Expedience: Medium
Sustainability: Medium
Effectiveness: Medium
Contribution: Low Effort: Medium

Why implement it:
Enforcing an independent security and internal control certification/accreditation of information technology services in line with the control practices will help:

- Provide confirmation that required control mechanisms and procedures are in place and function as designed
- Ensure that services are secured in line with the business requirements
- Ensure that all mission-critical systems are reviewed or accredited before deployment is initiated
- Enable positive control statements to be made to interested third parties or to the marketplace to increase confidence and trust

	Relevance						Compliance State					Evidence
	Not Relevant	Somewhat	Relevant	Very	Critical	Covered by other practice	Far away	Getting started	Halfway there	Nearly there	Done	
Control Practice: 3.1.1												
A policy is established requiring that independent certification or accreditation of all new mission-critical services be considered before deployment, specifically focusing on security and internal control mechanisms and procedures. These activities do not include day-to-day management control activities.												

Figuren kan umiddelbart være svær at læse, men formålet er at vise det konceptuelle i designet.

Den afspejler COBIT's føromtalte struktur/ hierarki; *domain, process, control objectives og control practices*.

For hver control objective er noteret '*Why implement it*'. Dette beskriver de overordnede kontroltiltag, som skal gøres for at være i overensstemmelse med den pågældende control objective. Hermed beskriver det indirekte risikoen ved ikke at implementere kontroltiltagene. Dette giver efterfølgende hjælp til beskrivelsen af observation, risiko og anbefaling i den efterfølgende rapportering.

Styrken i Assessment Form er i dens muligheder som *Control Self Assessment* (CSA), idet organisationen selv kan vurdere '*Relevance*' og '*Compliance State*'. Efterfølgende skal revisionen foretage en vurdering og revision af svarene.

Self-assessment delen giver en unik mulighed for at få en dybdegående og konstruktiv dialog og vurdering af de enkelte control practices med organisationen. Denne del skal ikke undervurderes. Det er værdiskabende for begge parter, ligesom det sikrer åbenhed og gennemskuelighed igennem hele revisionsprocessen.

Såfremt Control Practices Assessment Forms (CPAF) ikke opfylder de specifikke behov, så kan man altid selv tilføje Control Practices. Dette har vi f.eks. gjort i forbindelse med en forestående implementering af SAP. Her var der behov for yderligere Control Practices end dem som COBIT som udgangspunkt tilbyder, f.eks. SAP specifikke eller lovgivningsmæssige forhold. Det er her vigtigt, at opbygge disse 'add-ons' på lige fod som de øvrige Control Practices.

CPAF danner et væsentligt grundlag for vores revisionsinstrukser.

CPAF skal suppleres med arbejdspapirer som opsummerer afgrænsning, konklusion og udført arbejde.

<u>Rapportering:</u>
Der skal være en rød tråd mellem Control Practices Assessment Forms (CPAF) og rapporteringen. Vores standardrapporter er opbygget så det sikres, at observationer fra CPAF bliver rapporteret videre til ledelsen.

Hele processen med CPAF vil endvidere sikre en åbenhed og gennemskuelighed i den samlede rapportering, da de interviewede har været aktiv deltagere – ingen overraskelser.

Prisen for at anvende *COBIT Online,* herunder CPAF, er USD 200 om året for medlemmer af ISACA.

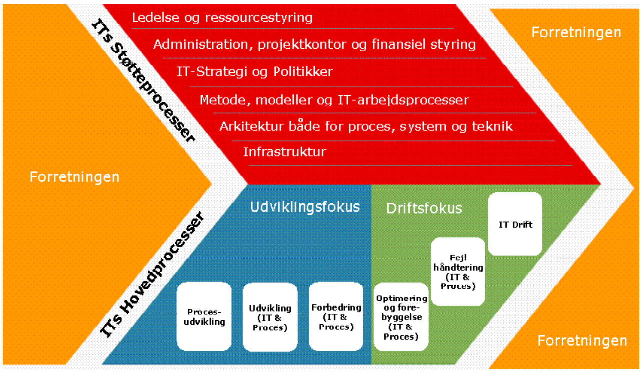
TrygVesta's anvendelse af COBIT – IT

I denne sammenhæng skal det for forståelsen oplyses, at <u>driften</u> af TrygVesta systemer er outsourcet til CSC. I den forbindelse modtages systemrevisorerklæringer for de generelle IT-kontroller, som CSC varetager for TrygVesta.

I forbindelse med TrygVesta IT's nordiske integration og strategi har det været nødvendigt at redefinere metoder, processer og procedurer.

I dette forløb har man defineret en værdikæde for IT-afdelingen, som er baseret på Michael E. Porter's værdikæde. IT-organisationen er således opbygget omkring værdikæden baseret på Porter's model, men omskrevet til en forretningsorienterede IT-organisation.

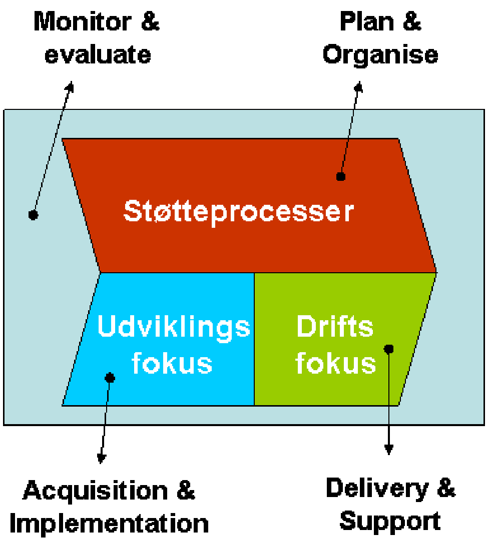
IT-afdelingens værdikæde kan illustreres på følgende måde:



Via vores løbende dialog med vores metodeafdeling i IT har vi faciliteret, at IT har anvendt COBIT som et værktøj (framework) til at årsag/virkning forklare en række væsentlige problemstillinger i IT.

I IT vil COBIT nu blive anvendt i forbindelse med den løbende metodeudvikling – som en form for ramme og checkliste.

Koblingen mellem COBIT og IT's værdikæde kan illustreres således:



'*Monitor & evaluate*' vil i denne forbindelse blive udført af vores Koncernsikkerhedsfunktion.

Dette giver os som revisorer en unik mulighed for bedre at kunne rapportere observationer, risici og anbefalinger direkte ind til IT's værdikæde – en værdiskabende proces for begge parter.

TrygVesta's erfaringer

I forbindelse med vores arbejde med COBIT har vi gjort os følgende væsentlige erfaringer:

1. Man skal igennem en erkendelsesproces før en implementering af COBIT kan ske – 'plejer' skal være gået på pension.
2. Man skal inddrage IT- og sikkerhedsorganisationen tidligt i processen – sikre deres løbende accept og forståelse. Koblingen af COBIT til IT-afdelingens værdikæde har været en bonus.
3. Man skal investere den nødvendige tid til møder, hvor COBIT og Control Practices Assessment Forms gennemgås med organisationen. På disse møder skal man forklare det grundlæggende indhold og formål med modellen. Man skal endvidere forklare, hvorfor man har valgt at arbejde ud fra denne model samt anvendelsen af dens værktøjer.
4. Man skal være tålmodig. Der er også behov for en stor grad af fleksibilitet. COBIT skal og kan ikke sluges på en omgang. Risikovurderingen af COBIT processerne vil hjælpe med at fastsætte omfanget.
5. Benyt COBIT Online (isaca.org) aktivt, da den tilbyder yderst brugbare og udbytterige værktøjer og fora, f.eks. generering af Control Practices Assessment Forms, benchmarking, Community (world wide chat).
6. 'Walk the talk'- de interne metoder, strukturer og rapportering skal afspejle viljen til at operere fuldt ud med COBIT.

Herudover skal man indgå i en proaktiv dialog og proces med den eksterne revision for at sikre, at de kan basere deres overbevisning på baggrund af revisionen foretaget ud fra COBIT. I vores tilfælde har dette været og er en yderst konstruktiv og åben proces for at sikre fælles univers og forståelse for anvendelsen af COBIT.

Afslutning

Efter vores vurdering og praktiske anvendelse af COBIT vil den give en større åbenhed og gennemskuelighed i revisionen og rapporteringen.

Vores proces med COBIT har været og er utrolig spændende, inspirerende og udviklende, da den bl.a. har medført, at organisationen nemmere kan se relevansen og væsentligheden i revisionens observationer, risici og anbefalinger. Denne åbenhed og gennemskuelighed vil bl.a. sikre en bedre dialog med organisationen. Der er en meget værdiskabende proces for begge parter.

Jeg mener, at COBIT er fremtiden for kontrol og governance af IT. Der er et behov for en større dialog og forståelse af COBIT's muligheder og anvendelsespotentiale både i relation til revision og IT.

Der bør derfor etableres ERFA-grupper. Dette arbejde/initiativ bør ske igennem IIA og DISIF (ISACA, DK).

Præsentation af den interne revisionstjeneste i Ministeriet for Fødevarer, Landbrug og Fiskeri, Direktoratet for FødevareErhverv

Af Hans Kristian Møller, Revisionschef og Vibeke Højmark, Chef for Intern Revision, Direktoratet for FødevareErhverv

Hans Kristian Møller

Vibeke Højmark

Indledning

Interne Revisioner i staten fungerer traditionelt som Rigsrevisionens forlængede arm i den organisation, hvor den interne revision er placeret. Den interne revisionstjeneste i Direktoratet for FødevareErhverv eksisterer således på baggrund af en såkaldt § 9-aftale mellem Fødevareministeren og Rigsrevisor.

Til forskel fra andre statsinstitutioner er Direktoratet for FødevareErhverv Danmarks udbetalende organ for EU's garantifond for landbrug. For at kunne løfte hvervet som udbetalende organ er der fra EU's side lovkrav om, at Direktoratet skal have en velfungerende og uafhængig revisionstjeneste, der reviderer efter internationale revisionsstandarder, samt at der skal være en særlig tjeneste, der har til opgave at koordinere den danske svigsbekæmpelse inden for garantifondsområdet[1]. Endvidere er der krav om, at det årsregnskab, der aflægges til Kommissionen, skal attesteres af en ekstern revision. Fødevareministeriet har p.t. valgt Ernst & Young til denne opgave[2].

[1] Den interne revisionstjeneste i DFFE er etableret og organiseret i overensstemmelse med EU krav fastlagt i Rådsforordningerne (RFO) 729/95 (senere ændret ved 1258/1999), 1257/99, 1259/99, 1260/99 og 4045/89.
[2] Hvervet som attesterende organ udliciteres p.t. for en periode af 3 år af gangen.

Direktoratet for FødevareErhverv er sammenlagt af flere direktorater og har rødder tilbage fra henholdsvis 1920 og 1973. Direktoratet har omkring 400 ansatte og beskæftiger sig hovedsageligt med tilskudsadministration i landbrugs- og fiskerisektoren. Direktoratet administrerer ca. 70 forskellige støtteordninger og udbetaler årligt ca. 10 mia. kroner i støtte. Til at understøtte tilskudsadministrationen har Direktoratet ca. 30 forskellige IT systemer af varierende størrelse, alder og kompleksitet. Direktoratet har en udmærket hjemmeside (www.dffe.dk), hvor man kan finde yderligere oplysninger om direktoratets opgaver.

Organisering

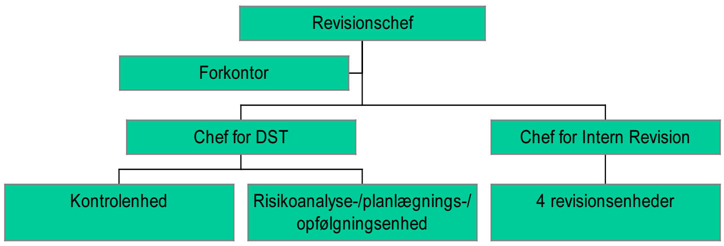
Intern Revisions uafhængighed er organisatorisk sikret ved, at afdelingen er placeret direkte under den administrerende direktør, samt at revisionschefen er ansat af Departementet og selv ansætter sine medarbejdere, hvorfor revisionschefen kun kan afskediges eller forflyttes af Departementet og afdelingens medarbejdere kun kan afskediges af revisionschefen.

Intern Revision er organisatorisk opdelt i to enheder med selvstændig faglig ledelse. De to enheder er Revisionsenheden og Den Særlige Tjeneste (DST).

- Revisionsenheden varetager i samarbejde med Det Attesterende Organ (Ernst & Young) og Rigsrevisionen alle nationale revisionsopgaver i Direktoratet for FødevareErhverv og overvåger sikkerheden og effektiviteten omkring forretningsmæssige transaktioner omfattende hele spektret af aktiviteter administreret af direktoratet, herunder støtteudbetalinger der finansieres/medfinansieres af Den Europæiske Udviklings- og Garantifond for Landbrug (EUGFL), Garanti- og Udviklingssektionen, nationale støtteordninger, EU finansierede/medfinansierede forskningsprojekter under Fødevareministeriet, Direktoratet for FødevareErhvervs og Fiskeridirektoratets drifts- og anlægsregnskab samt revisionsopgaver i kontrollerende og anvisningsberettigede organer (Plantedirektoratet, Skov & Naturstyrelsen, Fødevarestyrelsen, Økonomistyrelsen, Told & Skattestyrelsen, Amterne m.fl.) i henhold til skriftlige aftaler.
- DST varetager den efterfølgende regnskabskontrol (bekæmpelse af svig og uregelmæssigheder) iht. RFO 4045/89.

Intern Revision er p.t. normeret til i alt 20 medarbejdere bestående af 1 revisionschef, 1 chefkonsulent som faglig leder af Revisionsenheden, 1 chefkonsulent som faglig leder af DST, 1 sekretær, 12 revisorer på forskellige kompetenceniveauer (heraf minimum 5 på cand. merc. aud. – niveau), 1 4045-analytikker og 3 4045-inspektører, hvoraf den ene er chefkonsulent med ansvar for kvaliteten af de gennemførte 4045-inspektioner. Denne bemanding anses for tilstrækkelig til at varetage såvel nuværende arbejdsopgaver som de udviklings- og specialopgaver der er et must, såfremt kontoret også fremover skal kunne formå at tiltrække og fastholde kvalificerede medarbejdere.

Organiseringen af enheden kan skematiseres som følger:



Udviklingen af medarbejderressourcer samt medarbejdertilfredshed søges fremmet mest muligt ved organisering i en matrix orienteret projektorganisation, hvor hvert revisionsprojekt ledes af en projektleder. Funktionen som projektleder er ikke permanent. En erfaren medarbejder kan således i visse projekter være projektleder og i andre projekter være projektmedarbejder.

Formål

Revisionsenhedens overordnede formål er at sikre, at Direktoratet for FødevareErhverv's interne kontrol- og forvaltningssystem, herunder IT sikkerhed, fungerer effektivt i henhold til akkrediteringskravene.[3]

[3] i Rådsforordning (RFO) 1257/1999, RFO 1258/99 / Kommissionsforordning (KFO) 1663/95, RFO 1259/99, RFO 1260/99 / KFO 438/01 og § 9 aftalen mellem rigsrevisor og ministeren for fødevarer, landbrug og fiskeri (omfattende de krav, som Rigsrevisionen stiller til forvaltningen af offentlige midler, som kommer til udtryk ved begrebet god offentlig revisionsskik som forudsætninger og betingelser for revision af regnskaber, hvor staten har ydet tilskud m.m.) samt diverse guidelines og revisionsmanualer udstedt af Europa Kommissionen, revisionsstandarder fra IFAC - International Federation of Accountants, Statslig Revision, INTOSAI revisionsnormerne, og nationale revisionsstandarder (FSR's revisionsstandarder).

Såfremt en national revisionsenhed afdækker et svaghedsområde i forvaltnings- og kontrolsystemet har nationalstaten ca. 1 år til at få rettet op på svagheden. Såfremt svagheden derimod afdækkes af fællesskabets revisorer indebærer dette, at der straks indledes et tilbagebetalingskrav beregnet som en procentvis finansiel korrektion af det udbetalte beløb der er omfattet af svagheden 2 år tilbage i tid og frem til svagheden er elimineret. Sådanne finansielle korrektioner kan løbe op i flere hundrede millioner kroner.

Revisionstjenesten er underlagt en omfattende kvalitetskontrol der uafhængigt af hinanden udføres af både Europa Kommissionens tjenestegrene, Den Europæiske Revisionsret, Rigsrevisionen og Det Attesterende Organ. De to sidstnævnte udarbejder årlige evalueringsrapporter der fremsendes til henholdsvis statsrevisorerne og Europa Kommissionen, medens de to førstnævnte foretager aperiodiske kontrolbesøg med rapportering til Departementet og direktoratets direktør.

Revisionen tilrettelægges som rullende 5 års planer, hvor hver støtteordning skal revideres mindst en gang og væsentlige/risikobetonede støtteordninger flere gange inden for 5 år. Derudover foretages der en årlig akkrediteringsrevision af, om direktoratet opfylder de forordningsbestemte akkrediteringskrav, der er en betingelse for, at direktoratet kan bibeholde sin status som nationalt udbetalende organ. Revisionschefen indgår for 1 år af gangen en resultatlønskontrakt med direktøren for at sikre en optimal målopfyldelse.

Intern Revision i Direktoratet for FødevareErhverv er af Kommissionens tjenestegrene evalueret til at være mellem de bedst fungerende revisionsenheder indenfor medlemsstaterne i EU. Vi samarbejder med revisionsenheder i andre udbetalende organer i Europa for at fastholde et højt fagligt niveau.

Revisionsstrategi

Intern Revision anvender i lighed med visse andre statsinstitutioners interne revisionstjenester processtyringsværktøjet TeamMate. Herudover anvendes tidsregistrering pr medarbejder/ pr projekt/ pr aktivitet for at kunne foretage en optimal planlægning og opfølgning på revisionsprocessen.

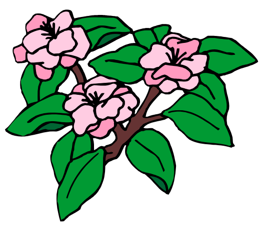
Revisionen tilrettelægges horisontalt så tilskudsordninger, der anvender samme sagsbehandlingssystem og/eller har mange fællestræk revideres under et. Så vidt det er muligt integreres applikationsrevisionen i revisionen af forretningsprocesserne. Alle henstillinger der afgives af diverse revisionsinstanser registreres løbende i en database og der følges løbende op på om henstillingerne implementeres.

Under revisionsprocessen tilstræbes det:

- at opgavedelingen mellem Revisionsenheden og Det Attesterende Organ løbende afgrænses på en rationel og hensigtsmæssig måde med forøget kvalitet og effektivitet for øje under hensyntagen til Kommissionens krav og internationale revisionsstandarder.
- at horisontale checkpunkter revideres under et, fx i form af ACL tests.
- at regnskabsanalyser søges anvendt i den udstrækning det er hensigtsmæssigt og muligt.
- at påse, at der løbende foretages opfølgning på gennemførelsen af kontrolplanerne og på fagkontorernes opfølgning på fejl, der afdækkes under kontrollerne.
- at påse, at der løbende sker implementering af de i afgivne revisionsrapporter givne henstillinger og anbefalinger

Afslutning

At være intern revisor i Direktoratet for FødevareErhverv, der er en politisk organisation bl.a. underlagt et omfattende europæisk regelsæt, er meget udfordrende og inspirerende. Der er ikke et år, der ligner det foregående. Regelsættet for støtteudbetalinger og kontrol ændrer sig hele tiden, ligesom kravene til anvendt revisionsmetodik er under konstant forandring. Dette kræver stor omstillingsparathed og krav til løbende ajourføring af faglige kompetencer. Herudover er det meget vigtigt at have et stærkt netværk med kolleger i andre europæiske lande, hvor faglige problemstillinger kan drøftes, og erfaringer kan udveksles på tværs af landegrænserne.



Revisionsbekendtgørelsen for finansielle virksomheder - igen

Af Chief Internal Auditor Søren Lund, Nordea

Samtidig med at det forrige INFO kom med posten udsendte Finanstilsynet en ny revisionsbekendtgørelse for finansielle virksomheder, der på væsentligere punkter afveg fra omtalen i min INFO-artikel, der var baseret på høringsudkastet.

Tilsynet modtog ved høringen en række indsigelser og forslag fra interesseorganisationerne, og en del har fundet vej til den foreliggende bekendtgørelse.

Jeg skal kort gennemgå de væsentligere ændringer.

Bestyrelsen i en finansiel virksomhed skal nu fastlægge, om den interne revisionschef skal forsyne årsrapporten med en revisionspåtegning. Det formelle krav (indført i slutningen af 80'erne) om en revisionspåtegning fra den interne revisionschef er hermed bortfaldet.

Vælger en bestyrelse, at revisionschefen fortsat skal påtegne årsregnskabet, skal der gives meddelelse herom til Finanstilsynet inden 1. juni 2005, og fremtidigt skal denne indberetning medsendes ved meddelelse om tiltrædelse af ny revisionschef. Ændrer bestyrelsen beslutning, skal dette ligeledes meddeles til tilsynet.

Den interne revision skal - såfremt revisionschefen påtegner årsrapporten - deltage i revisionen af væsentlige og risikofyldte områder, hvilket indebærer, at den interne revision selvstændigt skal udføre en del af revisionen og ikke blot kan bero på revision udført af den eksterne revision. I høringsudkastet var forudsat en deltagelse i "alle væsentlige og risikofyldte områder", men med baggrund i ønsker om en fortsat hensigtsmæssig arbejdsdeling mellem den eksterne og interne revision, herunder en mere effektiv udnyttelse af omkostninger til revision, bortfaldt "alle" kravet.

Såfremt den interne revisionschef ikke påtegner årsrapporten indeholder bekendtgørelsen - efter min opfattelse - ikke krav om, at den interne revision skal summere bemærkningerne til bestyrelsen, idet dette krav kun vedrører revisionsprotokollatet vedrørende årsrapporten.

På denne baggrund svæver enkelte andre bestemmelser, bl.a. om fremsendelse af den interne revisionschef protokollat til tilsynet, nu i det usikre. Det må derfor forventes, at tilsynet i løbet af 2005 finder behov for en klargøring af regler i de tilfælde, hvor den interne revisionschef ikke påtegner årsrapporten.

Nye krav til en revisionsmæssig gennemgang af god skik - fastlagt i et særskilt udvalg i tilsynet - kom ikke med i den endelige udgave. Den omkostningsmæssige byrde i forbindelse med en revisionsgennemgang var her et væsentligt element.

Begrebet "selvrevision", som såvel den eksterne som den interne revision efter udkastet til bekendtgørelse i ethvert revisionsprotokollat skulle erklære sig om ikke at have foretaget, er i den endelige udgave erstattet af en bestemmelse om, at en sådan erklæring som minimum skal fremgå af protokollatet i forbindelse med årsrapporten, hvilket jeg finder er væsentligt mere afbalanceret end kravet i udkastet.

I realkreditinstitutter er der, vedrørende intern revisions gennemgang af lån, blevet slækket på kravene til gennemgangen, idet nu også engagementer, der bevilges af bestyrelsen, kan omfattes af en stikprøvevis gennemgang. Tidligere var der krav om en fuldstændig gennemgang af disse engagementer. Ændringen er meget velkommen og har været drøftet mange gange, men først nu altså ændret. Som bekendt skal den interne revision sammenfatte sin gennemgang af udlån i revisionsprotokollatet vedrørende årsrapporten. Hvordan og om denne sammenfatning skal foretages, såfremt den interne revisionschef ikke påtegner årsrapporten, fremgår ikke, jf. min omtale af forholdet ovenfor.

Afslutningsvis skal det blot nævnes, at bl.a. omfanget af revisionserklæringer, der i vid udstrækning blev drøftet i tilsynets udvalgsarbejde også tydeligt blev kommenteret i høringssvarene, men som det kan konstateres må en reduktion vente til et senere tidspunkt.

Detecting financial fraud

By John Wallhoff (CISA, CISM, CISSP)

John Wallhoff, CISA, CISM, CISSP
is the founder and Managing Director of Scillani Information AB. Prior to this position, he worked both as an IT-auditor, IS-consultant and with Security management practices within enterprises like Ernst & Young and AddTrust. He has over thirteen years experience in the IT field as an IT/IS consultant and in IS audit.

Financial Fraud is not fiction, it is the reality. According to the 2004 FBI/CSI Computer Crime and Security Survey it reaches number five on the list over "Dollar amount losses by type". Over the years of the FBI/CSI survey financial fraud has remained to be an issue of this magnitude with a constant number of detected fraud cases that results in financial losses. The numbers are higher but many fraud cases are never detected or are handled internally. There is a business case of paying more attention to financial fraud than what has already been done and the driver is to reduce costs related to fraud.

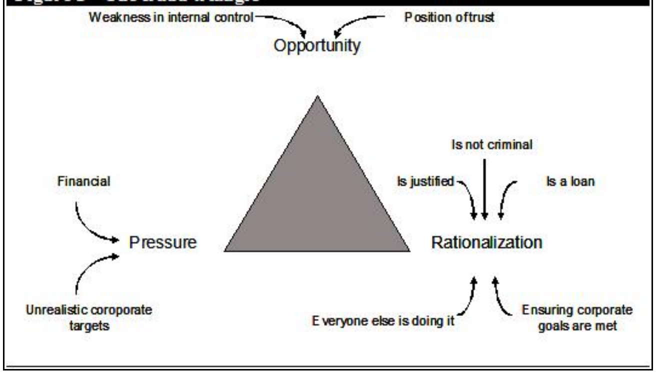
What is fraud

Fraud is defined by The Association of Certified Fraud Examiners (ACFE) as "The use of one's occupation for personal enrichment through the deliberate misuse or application of the employing organization's resources or assets". This means theft that does not have to be related to cash but most often that is the bottom line. From the organizations perspective fraud is a business risk that requires involvement from several parties within the organization.

Last but not least management has the ultimate responsibility to ensure that controls are in place to mitigate the risk of fraud. Today we have seen the effect of Sarbanes Oxley and all work that is done to mitigate the risk of fraud related to fraudulent statements. For fraud related to corruption and theft we still have not seen the same effort.

One basic question when you talk about fraud is why it takes place. Experts in the psychology of Fraud have described it in the fraud triangle (figure 1).

Figure 1 – The fraud triangle

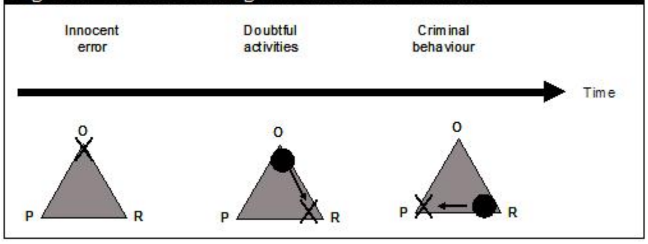


Each corner of the triangle has its own explanation:

- Opportunity: Weaknesses in internal control or a position of trust enables the opportunity to commit fraud.
- Rationalization: The individual has his or her own explanation of why fraud is committed. It cover believes such as it is justified, it is a loan, it is not criminal, everyone else is doing it or that it is done to meet corporate goals.
- Pressure: Often there are financial factors that trigger an individual to commit fraud but it may also be unrealistic targets that must be met.

With the fraud triangle in mind we have something to help us understand why it takes place. There are also studies that have shown that the behaviour changes from the first initial attempt of committing fraud changes until it is a criminal behaviour (figure 2). First an innocent error reveals the opportunity that may be used. If there are no controls a realization takes place to justify an individual to take advantage of the opportunity. Finally if there is a pressure on the individual, activities will evolve from doubtful to a criminal behaviour.

Figure 2 – The fraud triangle and behaviour over time



Who is responsible

As mentioned already fraud is a business risk and it is the responsibility of the management. Often fraud is assigned to be handled by the internal audit or security department. This responsibility involves assessment and evaluation of internal controls strategies, suggesting improvements of internal control strategies and to provide assurance that the organisation has implemented controls that are efficient and effective.

As well as assigning the responsibility, management has the responsibility to dictate what is accepted within the organization and how a suspected fraud is handled. The fraud policy together with a fraud awareness program is necessary to achieve this.

One instance of the responsibility is about how a tip of ongoing fraud within the organization, shall be handled, which is also called “whistle blowing”. It is highly recommended that this is handled in a separate policy, to ensure that the tips are handle with due care and that employees are encourage to “blow the whistle”.

Detecting fraud

Today most organizations are dependant on IT for its business. This means that a fraudster must learn how to use the technology to be able to commit fraud. That is why the work of detecting fraud involves IT-security. It is necessary that IT-systems and the IT-infrastructure is designed and implemented in a secure manner to mitigate fraud attempts and to enable detection of fraud. Some of the technical aspects include:

- Access control features must identify the individual that uses IT-systems
- User activity must be recorded in a log file
- Log files and financial data must be analysed to detect suspicious transactions.

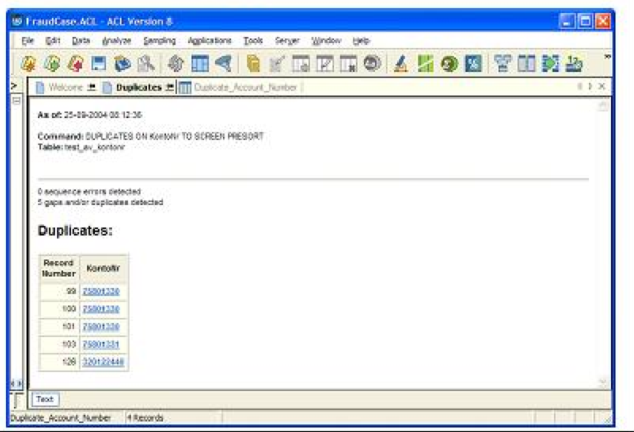
In most IT-systems there is a log file but the level of granularity is dependent on the design of the system. In some systems it is only possible to trace login and logout activities, while in others it is possible to trace each individual activity within the system. For financial transactions, like invoices from vendors, credit notes to customers and payment of salaries and expenses to employees, it is reasonable to expect a timestamp and signature but it is nothing you can take for granted.

One method of detecting financial fraud is the use of generalised audit software, such as ACL, where financial transactions are analysed and sometimes extracted to a separate IT-environment to enable data analysis. There are several tests that shall be utilized when assessing suspicious fraud attempts or high risk areas.

First of all we have the deletion of financial transactions after they have been committed and resulted in payments. A system shall use sequence number for these transactions which in turn enable a test on the integrity of number series. The test you can run is to identify if there are any gaps and if there are they must be analysed further. Gaps do also involve the log file where you must analyse the integrity of log file data. With a sequence number on all the transactions in the log file it is an easy test to run. Many times the IT-department is worried about the huge amount of data that needs to be analysed, but with the right tools it is no real problem.

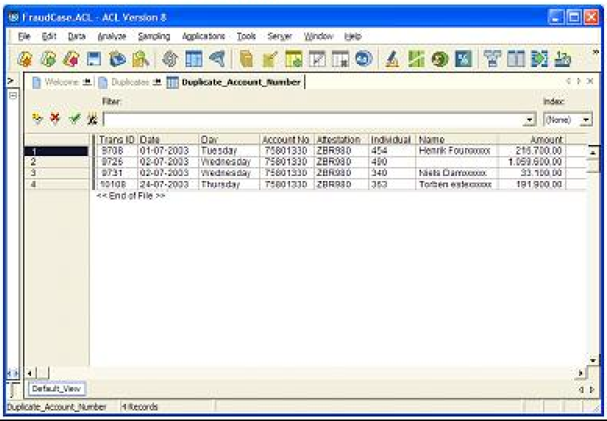
Another test is to identify duplicates of payments. This means that payments to different individuals, vendors or customers has been done to the same bank account or address on the payment check (figure 3).

Figure 3 – Finding Duplicates



Finding a duplicate does not meant that fraud is committed, as spouses may work within the same organisation and have set up joint account. There you must go into details to identify who has granted the payment and who has received the payment (figure 4).

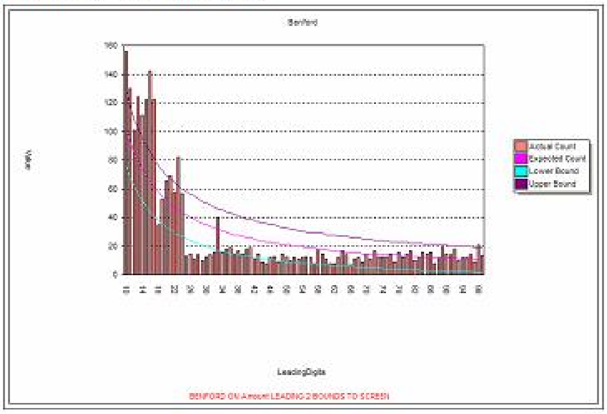
Figure 4 – Analysing Duplicates



Other tests you may use require you to join data from different sources. One of those tests is to verify segregation of duties to ensure that all employees have taken their vacation and that no financial transaction has been authorised by that employee when he or she was on leave. Another test is to verify the integrity of date in different tables within the database. In figure 4 above you can see that the name is missing in the second row of the table. The test here is to join the payment transaction file with the employee master data file, where we have chosen to display the name from the employee master data file. If the fraudster have registered a non-existing employee, committed a payment transaction and then deleted the non-existing employee from the master data file, this would provide you with evidence that something is not right. In this case you can also see that the attestation of the payment transaction has been committed by ZBR980.

When you talk about fraud, it is hard not to mention the Benford test, based on the Benford Law developed by Frank Benford in 1920s. This law identified that in large number of transactions (over 10 000) the number 1 is present more often than the number 2. The same goes for two digits where the number 12 is more present than the number 33 (figure 5).

Figure 5 – Benford test



To detect fraud there are many other tests to be run and it is important to identify weaknesses in controls, security measures that have been implemented in IT-systems and procedures to capture, analyze and report findings of suspected fraud attempts.

Case study – Perstorp Kommun

It is difficult learn from real cases of financial fraud, because it is often handled internally. Due to "offentlighetsprincipen" in Sweden we have a fraud case in Perstorp Kommun, a Swedish municipality, where the details of the fraud has been described in the media.

In the evening the 22nd May 2003 a 27 year old employee entered the main building of the municipality. For several years he had been working at the welfare department preparing payment to non-existent individuals, now it was time for the final fraud. At this time he was under investigation and had no key to their facilities. He therefore used a copy of the key to the front door that he had come across and he had also captured his manager's password to the financial system that handled payment transfers to the bank. The manager was authorized to commit payment transaction. At 10.40 p.m. he had transferred SEK 20 000 000 (aprox. USD 2 500 000) to different bank accounts. When the transfer was done, the voltage level was changes for all the computers within the welfare department and to complete his fraud he damaged a water pipe to create a water leakage. The last two activities were initiated to delay the time for the staff at the municipality to detect that money was transferred from their bank account.

Next morning staff returned to work and was met by the water leakage and then the computers at welfare department broke down one by one. The CFO got a feeling that something was wrong, even if he didn't know what, so he ran down to the bank to stop all payments transfers from their bank account. It saved the municipality 85% of the total amount that was transferred and at that point they had only lost SEK 3 000 000 (aprox. USD 375 000). The fraudster had vanished at the same time but was caught several days later and got convicted.

Figure 6 – The fraud at Perstorp Kommun

Sverige Skåne Danmark

Perstorpshärvan i domstol

Men den huvudmisstänkte 27-åringen är alltsedan kuppen spårlöst försvunnen.

Kuppen mot Perstorp välplanerad

Source: Sydsvenskan, Thuseday 1st July 2004

Several lessons can be learned from this case:

- Fraud can take place in any organization, even if you believe that you know all the employees. Therefore it is necessary to implement and assess internal controls on a regular basis.
- You must know how to act when you suspect a fraud attempt. A fraudster that understands that he or she is under investigation may commit the "final fraud" before disappearing.
- Data Analysis techniques would have enabled the detection of fraud and had revealed its impact earlier. For high risk transactions, a continuous monitoring approach is an efficient and effective way to achieve this.
- IT-security measures are necessary to implement and maintain to prevent and detect financial fraud. With proper procedures for access control, security awareness together with efficient procedures to analyse log files and financial data you will have a chance to act before it is too late.

Conclusion

No organisation, neither in the public or private sector, is excused from financial fraud. For a long time surveys like the CSI/FBI survey have identified and quantified its impact. It is therefore important for management to implement controls to detect financial fraud. One of these controls is the use of data analysis techniques and the implementation of continuous monitoring. For an efficient use of theses techniques it is necessary not only to be able to analyse data, you must also design the solution to enable you to obtain data from the source without involving the IT-department. For each and every step when investigating financial transactions the integrity of the data must not be tampered with, otherwise it can not be used as evidence against the fraudster.

References

- IS Auditing Guidelines, 060.020.070 Use of Computer Assisted Audit Techniques (CAATs), ISACA - Information Systems Audit and Control Association
- Fraud Detection, Using Analysis Techniques to Detect Fraud, Daved G.Coderre, 1999
- CSI/FBI Computer Crime and Security Survey 2004, CSI – Computer Security Institute, 2004
- CSI/FBI Computer Crime and Security Survey 2003, CSI – Computer Security Institute, 2003
- The Internal Auditors's role in the prevention of Fraud, Position Paper European Confederation of institutes of internal auditing, October 1999
- Sydsvenskan, Thuseday 1st July 2004
- ACL Version 8, ACL Services Ltd.

Præsentation af IIA-standarder

Af Birgitte Rousing Svenningsen, Revisor, Saxo Bank

Opbevaring og beskyttelse af dokumentation

Som intern revisor skal man dokumentere sin revision. Det foreskrives i IIA's standard 2300, som angiver, at den interne revisor skal identificere, analysere, vurdere og arkivere væsentlig information vedrørende revisionsopgaven. Dette uddybes i standard 2310, hvoraf det fremgår, at dokumentation skal være væsentlig, pålidelig, relevant og anvendelig set i forhold til formålet med revisionen.

Interne revisorer indsamler og udarbejder således dokumentation – somme tider i sådant omfang, at den interne revision har behov for det største antal hyldemetre eller den største lagerkapacitet i virksomheden. Meget af dokumentationen indeholder fortrolige oplysninger, og det er derfor vigtigt at være opmærksom på, hvorledes disse oplysninger opbevares og beskyttes.

IIA's standarder – som skal overholdes af alle Certified Internal Auditors og alle medlemmer af IIA – stiller en række krav hertil.

<u>Retningslinjer (standard 2230.A1, 2330.A2 og 2330.C1)</u>
IIA's standarder stiller således krav om udarbejdelse af retningslinjer for opbevaring af dokumentation, arkiveringsperiode og udlevering af arbejdspapirer til interne og eksterne parter. For så vidt angår revisionsopgaver fremgår det af standard 2330.A1 og 2330.A2, mens kravet for konsulentopgaver fremgår af standard 2330.C1[1]. Revisionschefen har ansvaret for udarbejdelse af retningslinjerne. I Practice Advisory (PA) 2330.A1-2 anbefales det indirekte, at retningslinjerne udformes skriftligt. Selvom det således ikke direkte er anført, må det formodes, at disse retningslinjer skal foreligge skriftligt.

PA 2330.A1-2 anbefaler endvidere, at det sikres, at alle medarbejdere i den interne revision er bekendt med retningslinjerne via jobbeskrivelser. Umiddelbart er det ikke særligt normalt i Danmark at indføje sådanne retningslinjer i jobbeskrivelserne, og det kan også være en smule problematisk i forbindelse med opdateringer. Derimod er det praksis at have en generel bestemmelse om tavshedspligt i ansættelseskontrakter.

<u>Ansvaret for arkivering (standard 2330.A1)</u>
Arbejdspapirerne ejes af virksomheden jf. PA 2330.A1-1. Ifølge standard 2330.A1 er det revisionschefen, som har ansvaret for at kontrollere adgangen til de arkiverede arbejdspapirer.

Dokumentationen kan opbevares som såvel fysiske dokumenter som elektroniske dokumenter. Dette betyder, at revisionschefen har ansvaret for sikring af såvel den fysiske adgang som den logiske adgang til dokumentationen. De skriftlige retningslinjer skal indeholde retningslinjer herfor.

Retningslinjerne bør, for så vidt angår den fysiske sikkerhed, for eksempel tage stilling til:

- Hvorledes den fysiske adgang til revisionslokalerne sikres
- Om arbejdspapirer skal opbevares i aflåste skabe/skuffer
- Om skrivebordene skal være ryddet for arbejdspapirer, når der ikke er revisorer tilstede i revisionslokalet
- Om dokumentation i fysisk form må fjernes fra revisionslokalerne og i givet fald, hvorledes adgangen dertil skal sikres.

[1] IIA's standarder indeholder to typer. Standarder benævnt med A omfatter standarder for revisionsopgaver og skal overholdes af personer med CIA samt medlemmer af IIA. Standarder benævnt med C omfatter konsulentopgaver og omfatter samme personkreds som A-standarderne. Herudover omtales Practices Advisory (PA) i denne artikel. Disse vejledninger, hvorfor overholdelse af dem er frivilligt.

For så vidt angår den logiske sikkerhed (adgangen til elektroniske dokumenter), bør der i de skriftlige retningslinjer bl.a. tages stilling til:

- Hvor den logiske arkivering skal foretages (skal det være på en fælles server med virksomhed, den interne revision egen server eller harddisken på Pc'en)
- Hvem skal administrere den logiske sikkerhed til dokumenterne
- Om der skal anvendes kryptering
- Hvorledes dokumenterne sikres, hvis der anvendes bærbare PC, som medbringes uden for revisionslokalerne.

Der er således en del forhold, som revisionschefen skal tage stilling til for at opfylde sit ansvar i forbindelse med sikring af adgangen til de arkiverede arbejdspapirer.

<u>Udlevering af arbejdspapirer til tredjemand</u>
Et af de forhold, som nævnes specifikt i standard 2330.A1, og som kan virke lidt underligt set med danske briller, er, at revisionschefen skal indhente godkendelse fra ledelsen og/eller den juridiske afdeling, inden arbejdspapirer udleveres til tredjemand.

I praksis ser man, at interne revisorer udleverer arbejdspapirer til eksterne revisorer, Finanstilsynet, andre offentlige myndigheder, domstole, advokater etc. For at opfylde standardens krav skal udleveringen godkendelse af ledelsen inden udleveringen. Det må antages, at det ikke er nødvendigt med godkendelse i hvert enkelt tilfælde, men at det er tilstrækkeligt med godkendelse af retningslinjer for udlevering af arbejdspapirer til tredjemand. Det vil derfor være hensigtsmæssigt at indarbejde retningslinjer herfor i funktionsbeskrivelsen (charter), som godkendes af bestyrelsen.

Der kan være lidt tvivl om kravet om godkendelse fra ledelsen omfatter udlevering af arbejdspapirer til eksterne revisorer, idet Practice Advisory 2330A1-1 anbefaler, at udlevering til eksterne revisorer godkendes af revisionschefen, mens udlevering til øvrige tredjeparter bør godkendes af ledelsen. Jeg vil dog anbefale, at man sikrer bestyrelsesgodkendelse af retningslinjer for udlevering af arbejdspapirer til såvel ekstern revision som øvrige tredjeparter.

Practice Advisory 2330A1-1 omtaler endvidere, at det i visse situationer kan være hensigtsmæssigt, at direktionen eller andre medarbejdere i virksomheden får adgang til den interne revisions arbejdspapirer. I sådanne situationer anbefales det, at der stilles krav om godkendelse fra revisionschefen før udlevering af arbejdspapirerne. I praksis kan man tænke sig flere situationer, hvor arbejdspapirer udleveres til virksomheden – referater, beskrivelser mv. udarbejdet af revisor samt kontrollerede regnskaber er eksempler på arbejdspapirer, som mange interne revisorer vil udlevere til virksomheden uden at tænke nærmere over det. For at sikre, at det praktiske arbejde kan udføres på en hensigtsmæssig måde og samtidig beskytte arbejdspapirerne i nødvendigt omfang, er det hensigtsmæssigt at udarbejde retningslinjer herfor.

<u>Arkiveringsperiode (standard 2330.A2)</u>
Revisionschefen har endvidere pligt til at fastlægge krav til arkiveringsperioden jf. standard 2330.A2. Kravene skal som minimum opfylde virksomhedens og lovgivningens krav.

Bogføringslovens bestemmelser har medvirket til, at de fysiske arbejdspapirer typisk i Danmark arkiveres i løbende år plus 5 år. Efterhånden som flere og flere virksomheder får relationer til udenlandske selskaber – som moderselskab eller datterselskab – dannes der anden praksis, fx er lovkravet til opbevaring løbende år plus 10 år i Sverige.

Dette er en praksis, som de fleste interne revisorer vil nikke genkendende til. Det er dog min erfaring, at arkiveringsperioden for elektronisk dokumentation er mere flydende. Teknologien har jo betydet, at de elektroniske arbejdspapirer fylder forsvindende lidt, hvorfor mangel på plads ikke længere er et argument for, at arbejdspapirerne skal makuleres efter udløb af den lovpligtige periode for arkivering. Dette betyder, at arbejdspapirerne i mange tilfælde opbevares i det uendelige, for den interne revisor vil jo gerne være på den sikre side. Mange gange kan opbevaringspladsen reduceres ved at anvende komprimeringsteknik for de elektroniske dokumenter, så har man dem, for det kunne jo være, at man en dag fik behov for at se et arbejdspapir fra 1995. Det er dog vigtigt også at have nogle retningslinjer for arkiveringsperioden uafhængig af, om dokumentationen er på fysisk eller elektronisk medie. Det er ligeledes vigtigt at overveje de ulemper, der er ved at opbevare arbejdspapirerne ud over den lovpligtige periode, såsom at arbejdspapirerne kan misforstås, fordi forholdene (virksomheden, lovgivning etc.) er ændret væsentligt siden udarbejdelsen af arbejdspapirerne.

Retningslinjerne for elektronisk dokumentation skal indeholde bestemmelser om arkiveringsperiode, oprydning mv. I nogle tilfælde ses det, at ældre arbejdspapirer lagres på eksternt medie, således at de ikke optager plads på den normale server. I sådanne tilfælde skal der også være retningslinjer for den fysiske beskyttelse heraf.

Sammenligning med revisionsstandard 230

Revisionsstandard 230, som vedrører dokumentation, er meget kort, når det gælder vejledning om opbevaring og beskyttelse af dokumentation. I RS 230 anføres det således overordnet, at der skal foreligge nogle retningslinjer, således at lovgivning og god skik opfyldes. IIA's standarder og vejledninger giver på dette område mere omfattende retningslinjer og vejledning og bør derfor anvendes af alle interne revisorer med henblik på at opnå den bedste sikring og beskyttelse af de interne revisorers arbejdspapirer.

Vejen til CFSA

Af Claus Tormod Nielsen, CIA, CFSA, Nordea

Efter at have bestået del 4 af CIA i maj 2004 blev jeg gennem vores Competence and Development Centre i Nordea IAA opmærksom på, at der var en stor mulighed for, at CFSA fra november 2004 ville blive gjort international og ikke kun forbeholdt USA.

Gennem THEIIA.ORG holdt jeg mig orienteret om udviklingen og så, at CFSA fra november ville blive gennemført på international basis.

Jeg tilmeldte mig i september, hvor der som bestået CIA blot krævedes attest for at have været beskæftiget i revision i et finansielt institut i minimum 2 år, hvilket ikke var noget problem, da jeg havde 20 års anciennitet i revision i et pengeinstitut.

I CFSA-eksamen er der udover den generelle del, som er fælles for alle, en speciel del, hvor der kan vælges mellem Banking, Insurance eller Securities. Jeg vaklede lidt mellem Banking eller Securities, da jeg har beskæftiget mig med revision af begge dele, men valgte i den sidste ende Banking.

Efter at tilmeldingen var på plads, var det et spørgsmål om at finde studiemateriale til testen i november. På IAA's hjemmeside er opgivet en del materiale, som kan anvendes. Jeg valgte A Study Guide to CFSA. IIA's hjemmeside gjorde opmærksom på, at Guiden ikke var opdateret efter at testen var blevet gjort international, og at den var outdated med hensyn til Standarderne, da den ikke var opdateret med de nyeste ændringer. De nyeste standarder kunne hentes på IIA's hjemmeside, så det ville være til at leve med.

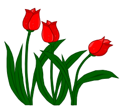
Jeg fik så Study Guiden på en CD, hvor udprintningen gav 312 A-4 sider. Indholdet var for Banking's vedkommende ikke overraskende meget amerikansk præget med en meget detaljeret gennemgang af Federal Reserve systemet med ansvarsdeling mellem de forskellige roller og meget om den amerikanske lovgivning i bank forhold. Afsnittene om Insurance og Securities var ikke helt så detaljerede med hensyn til US forhold.

Kort tid efter jeg havde modtaget CD'en modtog jeg fra IIA's boghandel en CD med den nyeste tekst til Standarder. Der havde man været så venlig, efter at have set at jeg gik op til CFSA, at sende mig en CD med det nyeste materiale uden beregning.

Læsningen af Study Guiden som forberedelse til testen viste, at denne forberedelse ville blive anderledes end forberedelsen til de enkelte dele af CIA. Study Guiden indeholdt 4 sektioner med hver 10 testspørgsmål for de 4 områder. Det er meget lidt, når man er blevet vant til de interaktive testspørgsmål til de enkelte dele af CIA. Nogle af kapitlerne i de to første bind af CIA dækker imidlertid de samme områder med Standarderne og revisionsprocessen, så der kunne jeg med fordel anvende disse testspørgsmål i forberedelsen af disse områder.

Selve testen med de 125 spørgsmål indeholdt spørgsmål vedrørende Standarderne, Revisionsprocessen, Banking, Insurance og Securities. Der skal man være opmærksom på, at der ikke kun vil blive testet i det specialområde, man har valgt, men i alle tre områder. Hovedvægten lå i specialområdet. Det skal lige for en god ordens skyld tilføjes, at der ikke var nogle US-specifikke spørgsmål.

Efter at have taget CFSA kan man i bagklogskabens klare lys se de fordele og den synergieffekt, der er i, at man har taget de første dele af CIA. Rent eksamensteknisk ville det være en fordel at tage del 1 og 2 af CIA samtidig med, at man gik op til CFSA. Standarderne og revisionsprocessen vil være kendte områder, og produkterne og processerne i CFSA vil være kendte fra det daglige arbejde.



Bevar din CIA certificering !

Annette K. Laursen, Senior Audit Manager, CIA, Nordea

En "Certified Internal Auditor" (CIA), der ønsker at beholde certificeringen, er selv ansvarlig for at vedligeholde viden og færdigheder indenfor intern revision og for at opdatere viden og færdigheder relateret til fornyelse og løbende udvikling i standarder, procedurer og teknikker indenfor intern revision. Dette skal ske gennem "Continuing Professional Education" (CPE).

Eget ansvar

Vedligeholdelse og opdatering af viden og færdigheder indenfor intern revision er den enkelte CIAs eget ansvar.

For at fremme forståelse for og overholdelse af standarderne fra the Institute of Internal Auditors (IIA) kræves, at man holder sig opdaterede om IIA standarderne som en del af deres CPE. Således skal CIAs gennemgå eller modtage uddannelse i IIA standarderne i løbet af en CPE rapporteringsperiode.

CIAs skal selv indberette overholdelse af CPE timer, ligesom man selv er ansvarlig for at sikre sig, at CPE timerne er i overensstemmelse med retningslinier fra IIAs Board of Regents. Opgørelse af CPE timer skal ske hvert andet år og tjener som signeret erklæring for at alle CPE krav er opfyldt.

Certificerede med lige certificerings nummer rapporterer i lige år og med ulige certificerings nummer i ulige år. CPE timer for den foregående 2 års periode skal været rapporteret inden 31. maj. Board of Regents kan på forespørgsel give hel eller delvis fratagelse fra CPE kravene for enkeltpersoner, hvis der er en god grund - defineret som f.eks. militærtjeneste eller personlige årsager.

CIAs skal sende en oversigt over opnåede CPE timer i perioden. En kopi af oversigten med relevant dokumentation for de seneste 3 år gemmes af CIA, bl.a. til brug for dokumentation overfor IIA, hvis de efterfølgende forlanger det.

Indberetningen af CPE timer, der kan ske via IIAs hjemmeside, fax eller e-mail, indeholder

- en erklæring, hvor CIA bekræfter at have modtaget undervisning/gennemgået IIA standarderne og have opnået en forståelse af standarderne der er tilstrækkelig til af udføre den løbende revision

  "I affirm that I have reviewed and/or received training on The IIA's Standards and achieved understanding of the Standards sufficient for me to carry out my current duties."

- en bekræftelse af at det krævede antal CPE timer er gennemført

  "This form constitutes my official submission of Continuing Professional Education hours. By submitting this form to the IIA, I signify that all information on this form is true and correct."

Som dokumentation for den fremsendte rapportering til IIA skal følgende information opbevares:

- Titel og indhold af kursus/program
- Datoen for deltagelse
- Kursussted
- Kursusudbyder
- CPE timer anbefalet af kursusudbyder
- Brev, certifikat eller anden skriftlig uafhængig attestation for fuldførelse af kursus
- Dokumentation, der understøtter artikler, mundtlige præsentationer, komite arbejde eller anden deltagelse

Rapporteringskategorier

IIA opererer med forskellige kategorier af CIAs: Udøvende, ikke praktiserende, kommende, pensionerede, inaktive og genindtrædende. For hver kategori er der speciferet krav til antallet af CPE timer for hver periode.

1. Udøvende CIAs

CIAs, der arbejder med intern revision, skal fuldføre 80 timer accepterede CPE for hver 2 års rapporteringsperiode.

2. Ikke praktiserende CIAs

Kandidater, der arbejder med intern revision, kan søge status som *ikke praktiserende* ved at rette skriftlig henvendelse til IIA, Certification Department. Ikke praktiserende CIAs skal fuldføre 40 timers godkendt CPE for hver 2 års rapporteringsperiode. Så længe CPE kravet er opfyldt, kan CIA betegnelsen fortsat bruget.

3. Kommende CIAs

Kandidater, der har bestået eksamen, men ikke opfylder alle krav for at blive certificerede, skal overholde CPE kravet om 80 CPE timer de foregående 2 år, når de ansøger om certificeringen. 80 CPE vil blive tildelt, når man består eksamen, 40 CPE timer, når man består eksamen og 40 CPE timer det efterfølgende år.

4. Pensionerede CIAs

CIAs, som ikke arbejder med intern revision, fordi de er blevet pensionerede, kan ansøge om status som pensioneret ved skriftlig henvendelse til IAA, Certication Department. Pensionerede CIAs skal ikke opfylde CPE krav. Pensionerede CIAs kan bruge CIA betegnelsen men må ikke udføre intern revision.

5. Status som inaktiv

CIAs bliver automatisk omplaceret til status som inaktiv af IIA Certification Departement, når de etablerede CPE krav ikke opfyldes. CIAs, med status som inaktiv, må ikke bruge betegnelsen. Uretmæssig brug af betegnelsen CIA vil blive rapporteret til The IIA's Ethics Committee med henblik på disciplinær proces.

6. Genindtrædelse i status som aktiv

Inaktive CIAs kan ansøge om aktiv CIA status ved skriftlig henvendelse til IIA, Certification Department. CIAs med status som inaktiv skal indrapportere 80 CPE timer for den seneste 2-års periode, når de ansøger om genindtrædelse.

Kvalificerende CPE aktiviteter

IIA forudsætter/forventer, at CIAs vil bibeholde den høje professionelle standard ved at vælge uddannelse af kvalitet for at leve op til CPE kravene og har opstillet følgende generelle kriterier skal tilfredsstilles for at CPE timer kan blive godkendt:

> Den altoverskyggende overvejelse for at bestemme om et specifikt program er acceptabelt er, at det skal være et formelt program for indlæring som bidrager direkte til professionel kompetence for en CIA.

Et acceptabelt formelt program skal:
- bidrage til deltagerens professionelle kompetence
- fastslå formål og specificere niveauet for den viden deltageren skal have opnået eller niveauet for den kompetence, som skal kunne demonstreres, når programmet er fuldført.
- beskrive kravet til uddannelse eller erfaring, som er passende for programmet
- være udviklet af personer, der er kvalificerede i såvel emnet som i undervisning
- tilbyde et programindhold, der er opdateret
- være på et professionelt niveau

Følgende generelle emner er positivt defineret som acceptable, når de er sammenfaldende med øvrige CPE kriterier:
- revision og regnskab
- ledelse og kommunikation
- computer videnskab
- matematik, statistik og kvantitative applikationer
- økonomi
- erhvervsret
- specifikke emner som finans, produktion, marketing og HR
- specialiserede erhvervsemner som offentlig virksomhed, bankvæsen, olie- og gas.

Andre aktiviteter end de nævnte kan være acceptable, hvis de medvirker til professionel kompetence. Det er den certificeredes ansvar at bevise at sådanne aktiviteter opfylder kravene.

Beregning af CPR timer

CPE timer bliver tildelt for hele timer, således at 50 minutter svarer til 1 CPE time., dvs. at 100 minutter uafbrudt undervisning svarer til 2 CPE timer. Der tildeles ikke halve eller kvarte timer, hvorfor "formlen" for udregningen er antal minutter delt med 50 nedrundet til nærmeste hele tal.

For konferenser, møder etc., hvor hvert enkelt præsentation er kortere end 50 minutter, beregnes summen af præsentationerne for et helt program. F.eks. 5 præsentationer af 30 minutter svarer til 150 minutter og dermed 3 CPE timer.

Hvad kvalificerer til CPE timer

Det er alene klasseundervisning eller accepteret selvstudier der til tilladt. Skemaet nedenfor viser opgørelse og max antal CPE timer per 2 års periode.

Kategori[1]	**Max CPE timer pr 2-års periode**	**Bemærkning**
CIA eksamen	80	40 CPE timer i det år eksamen bestås og 40 CPE timer det efterfølgende år
Uddannelse	80	Jf. ovenfor
Offentliggørelse af bøger, artikler, forskning	50	Generelt svarer 1 side til 2 CPE timer. Dog med følgende begrænsning for hver publikation: bøger 50 CPE, artikler 25 CPE og forskningspapirer 25 CPE
Mundtlige præsentationer	50	Både forberedelse og selve præsentationen udløser CPE timer. Præsentationen vil første gang give CPE timer i henhold til præsentationens længde plus CPE timer for forberedelse svarende til 3 gange præsentationens længde. Efterfølgende præsentationer vil alene give CPE timer for præsentationen og er begrænset til max 10 CPE timer for hver 2-års periode.
Deltagelse i udvalg, komiteer mv. samt kvalitetssikrings gennemgang	25	1 CPE time per time deltagelse.

[1] For en nærmere gennemgang af de enkelte kategorier se www.theiia.org

IIA *kan* gennemgå de indberettede CPE timer for en bedømmelse af om indberetningerne opfylder kravene.

Andre IIA certificeringer

Andre IIA certificeringer som Certification in Control Self-Assessments Professionals (CCSA), Certified Financial Services Auditors (CFSA) og Certified Government Auditing Professionals (CGAP) har tilsvarende krav for vedligeholdelse af certificering[1].

Det krævede antal CPE timer for opretholdelse af status som praktiserende indenfor disse certificeringer er 40 per 2-års periode. En CIA, der opfylder CPE kravene jf. ovenfor, opfylder samtidig CPE kravene for de øvrige IIA certificeringer.

Nyt fra IIA

Af Henning Jørgensen, Tryg

Kildemateriale: www.iia.org

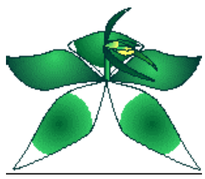
IIA signs agreement with IFAC (11-11-04)
Aftalen er designet således, at der sker vidensdeling og fælles undersøgelser af områder af generel fælles interesse. Aftalen fokuserer på 4 hovedområder: IT Audit, Revision af den offentlige sektor, gensidig opmærksomhed/bevidsthed og anerkendelse af professionelle standarder.

Assessment Guide (8-12-04)
IIA research Foundation har opdateret 'Assessement Guide for U.S. Legislave, Regulatory, and Listing Exchange Requirements Affecting Internal Auditing'. Det kan være relevant for virksomheder som skal være i SOX compliance.

AICPA, Ny vejledning (1-02-04)
AICPA har udgivet en ny vejledning 'Management Override of Internal Controls: The Achilles´ Heel of Fraud Prevention'. Det er en vejledning til hjælp i Audit committees.

COSO i mindre målestok (24-2-2004)
COSO har annonceret, at de arbejder på et projekt, hvor designet skal være med til at hjælpe mindre selskaber til at opfylde kravene i COSO.

Ny IIA plan for offentlig revision (3-3-04)
IIA præsident Dave Richards har skitseret en 10 trin plan for at forbedre service og programmer for revisorer indenfor den offentlige sektor.



[1] For en nærmere gennemgang henvises til IIAs hjemmeside www.theiia.org

Nye medlemmer

INFO byder velkommen til:

Ernst & Young
Konsulent Thomas Hansen
Revisor Bo Langhoff
Partner Otto E.P. Winterskov

Spar Nord Bank
Revisor Kirsten Jensen

PBS
Chefrevisor Thomas Balzer Jensen

Nordea
Revisor Marianne Van Berkel
Revisor Peter Bache

Handelsbanken
Revisionschef Thorkil Nielsen

Jyske Bank
Revisor Dorthe Lilleris

Egnsbank Han Herred
Revisionschef Knud Kristensen Kragh

GE Money Bank
Revisor Audi Simon

Finansministeriet
Koncernrevisionschef Doris T. Jørgensen

Danfoss
Team leader HE Team Jens N. Andresen

AP Møller – Maersk
Business Audit Weilian Ge

Novo Nordisk
Intern revisor Maria Johansson
Intern revisor Lars Ingemann

Københavns Universitet
Professor Jesper Lau Hansen

Danmarks Nationalbank
Revisionschef Jan Birkedal

SEB
Intern revisor Tom Ejlsborg
Intern revisor Vibeke Arnholst

Bagsmækken

Oplysninger om Foreningen af Interne Revisorer

<u>**Foreningens adresse:**</u>
Post Danmark
Intern Revision
Foreningen af Interne Revisorer (IIA)
Tietgensgade 37
1566 København V

☎ **3375 6400** **e-mail:** ***shk@post.dk***	**Søren Kongsbo** Formand
☎ **3587 2668** **e-mail:** ***vibeke.aggerholm@dk.ey.com***	**Vibeke Aggerholm** Sekretær
☎ **3375 6402** **Telefax: 3332 9010** **e-mail:** ***bentec@post.dk***	**Bente Christensen** Tilmelding til kurser.
☎ **7733 1465** **Telefax: 7733 1477** **e-mail:** **ano@sampension.dk**	**Anne Nordberg** Indmeldelse i Foreningen. Tilmelding til medlemsmøder.

Foreningen af Interne Revisorers bestyrelses-medlemmer:

Søren Kongsbo **(formand)** **e-mail:** ***shk@post.dk***	**Post Danmark**
Ane Marie Christensen **(næstformand)** **e-mail:** ***ane.marie.christensen@nordea.com***	**Nordea**
Jens Galsgaard **(kasserer)** **e-mail:** ***jga@sampension.dk***	**SAMPENSION**
Vibeke Aggerholm **(sekretær)** **e-mail:** ***vibeke.aggerholm@dk.ey.com***	**Ernst & Young**
Claus Okholm **e-mail:** ***co@nykredit.dk***	**Nykredit**
Jens Peter Thomassen **e-mail:** ***jens.peter.thomassen@danskebank.dk***	**Danske Bank**
Alex Bremner **e-mail:** ***alb@novonordisk.com***	**Novo Nordisk**
Hans Kristian Møller **e-mail:** ***hkm@dffe.dk***	**Direktoratet for FødevareErhverv**
Margit Nicolajsen **e-mail:** ***mnc@sparnord.dk***	**Spar Nord Bank**

Jobannoncer
Jobannoncer for medlemmer kan bringes i INFO. Helsides annoncer koster 2.000 kr.

Halvsides eller mindre annoncer koster 1.000 kr.

Annonceudkast sendes til foreningens adresse jf. ovenfor.

For ikke medlemmer aftales prisen særskilt.

Eksamen
Henvendelse angående CIA-, CGAP-, CCSA- og CFSA-eksamen samt forberedelse hertil kan rettes til Bente Christensen, Post Danmark, Intern Revision
☎ 3375 6402
e-mail: bentec@post.dk

Der kan søges yderligere oplysninger på IIA`s hjemmeside (se efterfølgende).

Oplysninger om mærkedage
Oplysninger om mærkedage bedes meddelt til:
Bente Hallberg, Post Danmark, Intern Revision
☎ 3375 6408
e-mail: beh@post.dk

Indlæg til INFO
Artikler i INFO honoreres med 3 flasker rødvin. Anmeldelser af hjemmesider, kurser, månedsmøder m.v. honoreres med 2 flasker rødvin.

Næste nummer
INFO 30 udkommer i august 2005.

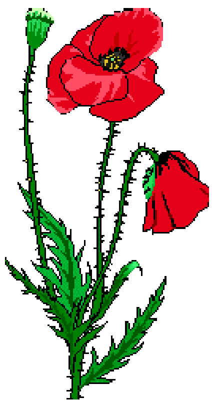
Oplysninger om diverse hjemmesider

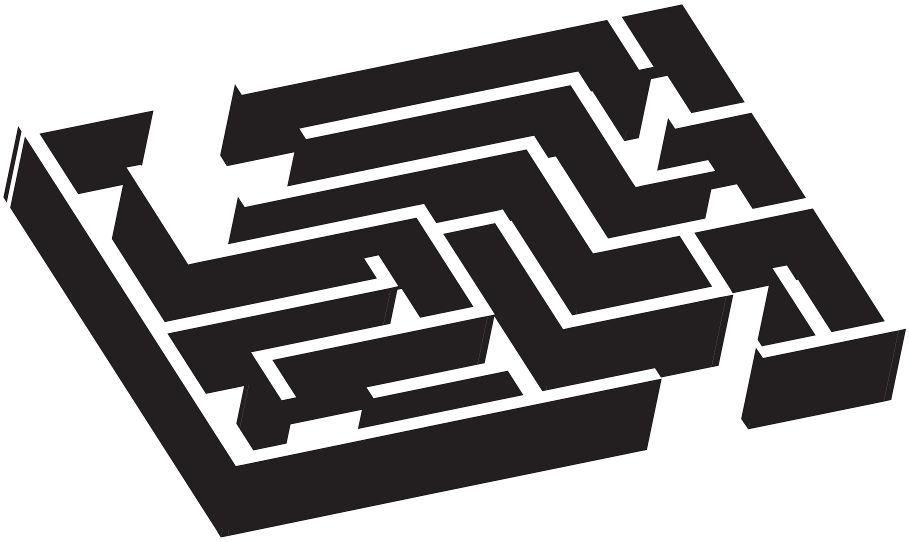
IIAs hjemmeside	www.theiia.org www.itaudit.org
IIA, DKs hjemmeside	www.iia.dk
IIA, UK Chapter	www.iia.org.uk

Redaktionen kan oplyse, at INFO også kan ses på foreningens hjemmeside på **www.iia.dk**

IIA standarder, der er præsenteret i INFO

IIA-Standarder	Emne	Præsenteret af	INFO nr.
2410 og PA 2410-1	Rapportering	Frank Sundgaard Nielsen	**24**
2010, 2200 og 2240	Planlægning	Solveig Petersen	**25**
1300-1340	Kvalitetsstyring af revisionsarbejder	Carsten Damø	**26**
2110	Risk Management	Solveig Petersen	**27**
2230.A1, 2330.A2 og 2330.C1	Opbevaring og beskyttelse af dokumentation	Birgitte Rousing Svenningsen	**29**





Gør det komplicerede enkelt

Rådgiver til den Statslige Task Force

Ernst & Young Risk Advisory Services søger endnu en medarbejder til at rådgive ministerier og statslige institutioner i forbindelse med den nye statslige regnskabs- og bevillingsreform. Du får et selvstændigt job i et stærkt fagligt og til tider hektisk miljø. Vi har fokus på de udfordringer, vores kunder har i forbindelse med overgangen til omkostningsbaserede regnskabsprincipper. Du er uddannet inden for regnskab og økonomistyring. Herudover har du 2-4 års praktisk erfaring inden for regnskabsvæsen eller revision. Besøg os på www.ey.com/dk/karrierecenter

Ernst & Young er et af verdens førende revisions- og rådgivningsfirmaer med 100.000 ansatte inden for revision, skat samt transaction advisory services (corporate finance) i mere end 140 lande. Vores kundesammensætning rummer virksomheder af enhver størrelse og inden for alle brancher. Ernst & Young's målsætning er gennem værdi og tillid at bidrage til vores kunders og medarbejderes succes.

www.ey.com/dk

ERNST & YOUNG

Quality In Everything We Do