INFOs redaktion:

Ansvarshavende redaktør:
Underdirektør Ane Marie Christensen
☎ 33 33 10 75
E-mail: anem@unibank.dk
Unibank

Øvrig redaktion:

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

Specialkonsulent Tina Mollerup Laigaard
☎ 33 92 91 94
E-mail: tml@oes.dk
Økonomistyrelsen

Revisor Gert Stubkjær
☎ 33 55 42 84
E-mail: gst@codan.dk
Codan Forsikring

Revisionsdirektør John Tyrrestrup
☎ 43 86 49 34
E-mail: john_tyrrestrup@fdb.dk
FDB

Revisor Louise Claudi Westh
☎ 33 42 1780
E-mail: lcw@nykredit.dk
Nykredit

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

Redaktionens adresse
IIA INFO
c/o Post Danmark
Vester Farimagsgade 31
1606 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/Niels Thor Mikkelsen

Risk Management er et begreb, der længe har været optaget i den interne revisors ordbog. Men begrebet er under stadig udvikling og er nu langsomt ved at blive integreret i den interne revisors arbejdsfelt, jfr. IIA's nye definition af intern revision, der blev formuleret i 1999. Heraf fremgår bl.a., at intern revision har til opgave at hjælpe til med at "evaluate and improve the effectiveness of risk management".

INFO bringer denne gang en artikel om emnet med titlen Enterprise-wide Risk Management, hvor der arbejdes med et udvidet risikobegreb, der ikke kun tager udgangspunkt i trusler, men også i risikoen for ikke at udnytte muligheder. Det bliver spændende at følge udviklingen i Danmark og opleve, når interne revisorer for alvor tager begrebet til sig og begynder at redefinere arbejdsområdet og tilpasse metodikker og værktøjer for at styrke leveringen af "value added services".

Anvendelsen af Internettet er stadigt stigende, og der "opfindes" hele tiden nye anvendelsesmuligheder. Samtidig er der stigende opmærksomhed mod de risici, der uvægerligt følger med. Senest har hackerprogrammet BackOrifice været fremme i medierne igen efter, at programmets source-kode er lagt på Internettet til fri afbenyttelse. Dette øger en hackers mulighed for at omgå virus-kontroller.

INFO følger emnet op med en artikel om Internet Sikkerhed. Artiklen behandler to af de væsentligste risici: Virus og Hacking.

Virus angreb kan antage forskellige former og have forskellige konsekvenser, men fælles er, at der "plantes" et program på en server eller pc, hvorefter det er programmet, der afgør det videre forløb uden indgreb af menneskehænder. Det seneste større virus angreb blev kendt under navnet ILOVEYOU.

Et hacker angreb indebærer, at en fremmed person overtager kontrollen med ens computer og dens indhold af data. Målet kan være at få adgang til fortrolige informationer eller anvende computeren som springbræt for andre hacker angreb.

Der findes effektive beskyttelsesforanstaltninger mod såvel Virus som Hacking, men vigtigt er det, at der er tale om en målrettet og styret indsats, som også involverer virksomhedsledelsen. Herudover kræver det adgang til den nødvendige kompetence for at kunne håndtere advarsler og alarmer. Dette er måske en af de væsentligste årsager til, at privatpersoner almindeligvis ikke har installeret firewalls i forbindelse med Internet-adgang – hvilket efterhånden er en defacto standard i enhver virksomhed.

Nyt fra bestyrelsen

Af Ane Marie Christensen

Foreningens årsmøde den 8. juni 2000 blev i år holdt på Langeliniepavillonen i tilknytning til et velbesøgt heldagsseminar om Fraud med Mike Comer, Chief Executive, Maxima Group plc.

Forhenværende revisionschef og vicedirektør i BG bank Verner Søgaard var dirigent på årsmødet.

Formandens beretning indeholdt en redegørelse for udviklingen i medlemstallet, der er steget fra 129 i 1998/99 til 134 i 1999/2000. Stigningen er bl. a. påvirket af to modsatrettede bevægelser, en stigning i medlemmer fra den finansielle sektor på 9 og et fald i medlemstallet fra Industri og Service på 5.

Der var ligeledes en redegørelse for medlemsmøderne i det forløbne foreningsår. De fleste medlemsmøder havde været velbesøgt. Halvdagsseminar om applikationsrevision i praksis havde således haft 50 deltagere.

Foreningens nye hjemmeside med den mere brugervenlige adresse (www.iia.dk) blev også omtalt ligesom INFO indgik i beretningen, herunder med en tak til den tidligere ansvarshavende redaktør revisionschef Thorkild Jakobsen og medlem af redaktionen Claus Deela, begge Told & Skat.

Foreningens kursusvirksomhed, der er relativt omfattende, byder på kurser i såvel generel intern revision som IT-revision og statistisk revision. Foreningen søger til stadighed at udvide kursusudbuddet, og gode ideer til nye kurser er velkomne.

Mange har ytret interesse for at tage en CIA-eksamen. Desværre er det imidlertid kun få, der tager det endelige skridt og melder sig til eksamen. Foreningen håber på fremskridt på dette vigtige område.

Internationalt deltager foreningen fortsat i aktiviteter i USA og Europa (ECIIA), ligesom der også er et nordisk samarbejde bl. a. om et fælles nordisk forberedelseskursus til CIA-eksamen.

I Danmark er der et positivt samarbejde med FSR, FIK, Revisionschefkredsen og Rigsrevisionen.

Årsregnskabet viste et resultat på 35 tkr. (1998/99: 116 tkr.). Nedgangen i resultatet skyldtes primært lavere indtægter ved kursusvirksomhed og en væsentlig nedgang i afkast af fondsbeholdning. Kontingentet blev fastholdt på et uændret niveau til 1.000 kr., og 300 kr. for pensionister og studenter.

Bestyrelsen ændrede sammensætning, idet underdirektør John Rasmussen, Danske Bank og revisionschef Thorkild Jakobsen, Told & Skat begge havde ønsket at træde ud af bestyrelsen. Formanden takkede for deres mangeårige store indsats for foreningen. Underdirektør Niels Thor Mikkelsen Danske Bank blev nyvalgt medlem af bestyrelsen og ny kasserer. Bestyrelsen fortsætter herved med 7 medlemmer i stedet for 8 og Søren Kongsbo som formand og Tage Rasmussen som næstformand.

Her ses fra venstre:
Ane Marie Christensen, Peter Birkholm Laursen, Niels Thor Mikkelsen, Søren Kongsbo, John Tyrrestrup, Tage Rasmussen og Frede Bech Poulsen.

Redaktøren

Medlem af foreningens bestyrelse Peter Birkholm Laursen forsvarede den 9. juni sin Phd-afhandling på Handelshøjskolen i København. Afhandlingen har titlen "En komparativ analyse af udviklingen i international revisionsregulering med hensyn til intern kontrol og IT-revision". Redaktionen ønsker hermed Peter et stort til lykke.

INFO har desværre måttet sige farvel til to af sine flittige redaktionsmedlemmer Claus Deela og Mette Larsen. De har begge ydet en rigtig god indsats, som bestyrelsen og INFO's redaktion takker dem for.

edlemmer

INFO byder velkommen til:

Intern revisor Peter Hærning,
Dansk Olie & Naturgas A/S.

Revisionschef Hans-Jørgen Andresen,
Lån og Spar Bank.

IT audit manager, Per Rhein Hansen,
Post Danmark.

Kontorchef Kurt Wagner,
Post Danmark.

Kursuskalender

Intern revision

modul 1	forår 2001
modul 2	forår 2001
modul 3	5. - 6. oktober 2000

IT-revision

modul 1	7. - 8. sept. 2000
modul 2	12. - 13. okt. 2000
modul 3	23. - 24. nov. 2000

Operationel revision 28. - 29. sept. 2000

Tilmelding kan foretages på skemaet i kursuskatalogets sidste side eller på IIA´s hjemmeside.

Aktivitetskalender

I den kommende periode er der planlagt følgende aktiviteter:

7. september 2000
Halvdagsseminar inkl. frokost fra kl. 12 - ca. kl. 16.
Emne: Statistisk revision
v/ lektor Lars Kiertzner.

26. oktober 2000
Programmet er ikke endelig fastlagt.

7. december 2000
Programmet er ikke endelig fastlagt.

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

Tilmelding til månedsmøder skal foretages til:
Bente Christensen, Post Danmark, Intern Revision,
☎ 3375 6402 eller
FAX nr. 3332 9010 eller
E-mail bcc@post.dk
senest mandagen før afholdelse af månedsmødet.

Anmeldelse af månedsmøder i IIA

Aktiviteter i IIA…
Indlæg omkring Helle Bank Jørgensens materiale af Pui Fong Yau

På foreningens månedsmøde den 16. marts 2000 holdt Statsautoriseret revisor Helle Bank Jørgensen fra PricewaterhouseCoopers et indlæg om de nye regnskabsformer.

Til deltagerne på mødet har Helle Bank Jørgensen efterfølgende fremsendt en flot mappe indeholdende en cd-rom om ValueReporting og flere pjecer omkring emnet udover de plancher, der blev fremvist på mødet. Et meget interessant og inspirerende materiale.

SEMINAR om FRAUD

Den 8. juni 2000 bød formanden for IIA, Søren Kongsbo, velkommen til Chief Executive, Mike Comer, der var foredragsholder på seminaret om FRAUD.

Chief Executive, Mike Comer.

Anmeldelse af seminar om FRAUD

Af Hans Heltborg, Nykredit, Intern Revision

Emnet Fraud er jo et emne, som vi som interne revisorer må til at forholde os mere til i tiden der kommer "best practice" og også set i lyset af vejledning nr. 21 fra FSR omhandlende misligheder.

Indledningsvis skal det siges, at ovennævnte seminar oprindeligt var tiltænkt at skulle strække sig over 2 dage, hvilket naturligvis har haft indflydelse på min vurdering.

Mike Comer er en meget levende og energisk foredragsholder som helt sikkert ved, hvad han taler om, men som nævnt ovenfor var programmet meget sammenpresset, og dette har naturligvis haft en indflydelse på det budskab, som Mike Comer ville have frem. Til gengæld var materialet, som blev udleveret, det fulde materiale for et 2 dages seminar, så yderligere inspiration kan hentes deri.

De vigtigste budskaber som jeg synes kom frem var følgende:

Virksomheden bør have "holdningsprægede" politikker for området, som beskriver værdier og regler, som virksomheden ønsker efterlevet. (Business Ethics Policy)

"Control Self Assessment" er et begreb, som nok vil vinde mere og mere indpas.

Intern revision er en vigtig brik i spillet. Intern revision bør være stærk og uafhængig og rapportere til ledelsen udenfor Finansområdet.

Etablering af Compliance afdelinger og Audit Committees vil nok også blive mere og mere udbredt.

Som nævnt tidligere er det udleverede materiale meget omfangsrigt og kan give mere inspiration til egen udvikling. Her tænkes blandt andet på risici, typer af bedrageri, årsager til bedrageri samt interviewteknik mv.
Seminaret havde stor relevans og foredragsholderen var uden tvivl meget kompetent, men tiden var desværre for kort.

Artikel bragt i Berlingske Tidende, Erhverv, søndag den 30. juli 2000
Af Uffe Gardel.

"Bedrageri og plat: Om golfspillende svindlere, forbrydere i pæne sko og værdien af etisk ledelse. En engelsk ekspert i bedrageriske ansatte var på besøg i Danmark.

På jagt efter svindlere.

"Lad aldrig nogen slippe afsted med at skjule sandheden", siger den cirka 60-årige, tætbyggede englænder.

"En løgner vil afsløre sig gennem sit kropssprog, for eksempel ved at røre sig i ansigtet. Kopier hans mimik og se, hvad reaktionen er. Hvis det bare er understregende gesti, kommer der ingen reaktion, men en løgner vil sænke hænderne."

Uden for Langeliniepavillonens store vinduer skinner solen, og turisterne fotograferer Den Lille Havfrue. Verden er normal.

"Hvis folk sværger ved deres kones liv, eller ved Gud, på at noget passer, så passer det med 90 % sandsynlighed ikke," siger foredragsholderen, som er i lyseblå skjorteærmer.

"En som taler sandt, vil kræve at få lov at forklare sig. En løgner vil derimod kræve ret til at tie, eller bede om at få sin advokat eller tillidsmand tilkaldt."

En flyvebåd sejler gennem havneløbet. Helt almindelige mennesker passer deres arbejde, men det er en illusion, for de svindler og bedrager, kassedamerne tager af kassen, indkøbscheferne bliver bestukket, og salgschaufførerne laver plat.

Vi er til seminar i svindel hos Foreningen af Interne Revisorer, og de 40 - 50 tilhørere lytter opmærksomt til den engelske svindel-ekspert Mike Comer. Han er ved at forklare dem , hvordan man som intern revisor forhører en mistænkt ansat.

Sandhed kommer fra hukommelsen, løgn kommer fra fantasien. Når man henter noget fra fantasien, kigger man til højre, derfor skal man prøve at stille sig til venstre for den mistænkte for at tvinge hans øjne til venstre.

Comer må vide, hvad han snakker om. Han har 40 års erfaring i svindel, han har arbejdet i det britiske toldvæsen, været sikkerhedschef i to olieselskaber og siden 1979 selvstændig konsulent.

Hans tilhørere kommer fra velrenommerede firmaer som A.P. Møller, Post Danmark og ISS, og de har ikke det bitterste lyst til at fortælle små anekdoter hjemme fra firmaet, når Berlingske Tidende prøver at småsludre i kaffepausen. Dette er seriøs svindelbekæmpelse, og diskretion er en æressag.

Svært at opdage

Heldigvis kan Mike Comer masser af anekdoter. Der var engang en direktør, som tog 180 millioner dollar af kassen; han indkasserede simpelt hen en masse lån, som hans firma havde fået bevilget. Han havde så mange penge, at han ikke anede, hvad han skulle bruge dem til: han ejede fem huse i Californien, heraf ét med en privat zoologisk have, og hans kone trak for 385.000 dollar om måneden på kreditkortet. Men ingen i firmaet bemærkede noget. Han blev knaldet, fordi en eller anden nabo sladrede til skattevæsenet.

Morale: Svindel er svært at opdage.

"51 procent af de svindeltilfælde, jeg kender til, er blevet opdaget ved et tilfælde," siger Mike Comer.

I gamle dage var det så nemt at finde svindlerne: man skulle bare holde øje med, hvem der aldrig tog ferie, hvem der mødte tidligt og gik sent hjem. Men den regel holder ikke i IT-alderen, forklarer Mike Comer.

"Forbrydere holder udmærkede ferier," siger Comer.

Der er heller ingen mønstre. Der findes ingen typisk svindler, som er 35 år, har en universitetsuddannelse og syv års anciennitet, eller sådan noget. Alle kan blive svindlere.

Mike Comer anbefaler i stedet at kigge efter folks sko. Svindlere går i pæne sko.

"Jeres sko trænger til at blive pudset, og det er et godt tegn," siger han. Tilhørerne fortrækker ikke en mine, og kigger ikke på deres sko.

Eller kig efter afvigere. Folk der altid vil gøre tingene på deres egen måde.

En direktør, som havde bedt Comer om hjælp, advarede ham mod en bestemt medarbejder.

"Gener ikke ham der, han er en hidsig skotte, som hader revisorer," sagde direktøren.

For Comer havde skotten et skilt i panden, hvor der stod: "jeg er en forbryder".

Vi skaffede nøglerne til hans skrivebord og fandt bankkonti med 4½ million dollar på Kanaløerne. Han modtog 35.000 dollar om måneden i bestikkelse, og hans aggressive opførsel var et bevidst forsøg på at undgå spørgsmål," forklarer Mike Comer.

Men mindre kan også gøre det. Comer fortæller om firmaet i Singapore, der havde så mange dumme uheld med deres lastbiler. Dumme, dumme uheld, hvor chaufføren var kørt ind i en mur eller ind i en lygtepæl, men heldigvis ikke var kommet noget til selv. Uheldene var også gerne sket om fredagen, så chaufførerne kun skulle undvære bilen en enkelt dag.

Det var naturligvis svindel, som nogle lokale autoværksteder deltog i.

Man skal i det hele taget passe på med chauffører, især salgschauffører.

"Giv en almindelig arbejder en lagerbeholdning og en adgang til at fakturere kunderne - så får man problemer," siger Comer.

Lejlighed gør tyve, og andre gode svindelmuligheder opstår, hvor en virksomhed tjener ekstraordinært store penge - eller tror, den kan komme til det.

Og Comer fortæller om direktøren i det store schweiziske firma, som fortalte sin bestyrelse om en enestående forretningsmulighed i Rusland. Man skulle bare betale en engangsbestikkelse på én million dollar. Det tog bestyrelsen to minutter at sige ja. Men der kom ingen kæmpefortjeneste fra det russiske marked. I stedet blev firmaet presset i Indien og Pakistan af en mystisk parallelimportør, der solgte dets varer til lavpris. Og direktøren gik til bekendelse.

"Jeg har aldrig været i Rusland," tilstod han.

"Bestikkelsen på én million dollar står på min bankkonto på Kanaløerne. Det gør fem millioner dollar i fortjeneste på parallelimport også - og de bliver der. Jeg har nemlig optaget bestyrelsesmødet på bånd."

Her bliver Mike Comer lidt teoretisk. Han henviser til den franske filosof Durkheim og hans teori om anomali: Der skal være balance mellem muligheder og ambitioner, ellers bliver der problemer. Alle mennesker stræber efter denne balance.

Pas på golfspillere

"Svindlere er ofte folk, som føler sig forfordelt." bemærker Mike Comer.

Anomali - uindfriede ambitioner - behøver dog ikke at føre til svindel.

"Det er blandt britiske embedsmænd, at man finder de førende eksperter i rosendyrkning eller dueavl. Det er folk, der ikke kunne avancere," forklarer Comer.

"Man kan ikke sætte lighedstegn mellem "golf" og "svindel", men det er tæt på. Hvis der er en god golfspiller i firmaet, så pas på! Høje ambitioner uden tilsvarende karrieremuligheder, det skal man passe på."

Her er det at et spørgsmål trænger sig på: Er svindelbekæmpelse i virkeligheden et spørgsmål om at behandle sine ansatte ordentligt ?

"Det er et spørgsmål om værdier, om virksomhedens værdier," bekræfter Mike Comer i en privat samtale med Berlingske Tidende i en pause under foredraget.

"Det handler om lederskab, stil og kultur. Hvis virksomheden opfattes som rimelig, behandler sine ansatte rimeligt, og opfører sig samfundsmæssigt ansvarligt, så falder risikoen for svindel.

Hvis man for eksempel er nødt til at betale bestikkelse for at komme ind på et mellemøstligt marked, så lader man være med at gå ind på det forbandede marked. Man lader være, hvis man er et ærligt og etisk firma. Ville man måske gå ind på et marked, hvis det betød, at man var nødt til at myrde mrs. Smith ? eller forgifte 2.000 mennesker ?"
Nogle ville måske.

"Ha-ha. Ja, der er altid nogle, der vil."

Fakta:
Mike Comer var inviteret til Danmark af Foreningen af Interne Revisorer, som kan besøges på Internet: www.iia.dk. "

Koordinering af ERFA-grupper

Foreningen hører gerne om interesse for oprettelse af ERFA-grupper og vil så kunne bistå med oprettelsen. Henvendelse kan ske til Tina Mollerup Laigaard, Økonomistyrelsen på mail tml@oes.dk

Erfagruppe vedrørende revision af finansielle instrumenter

Som bekendt er finansielle instrumenter et kompleks område i en virksomhed, og revision heraf kan være en jungle. Skulle nogen være interesserede i at deltage i erfaringsudveksling vedrørende revision af finansielle instrumenter vil redaktionen hermed gerne tage initiativ hertil.

Kontakt Louise Claudi Westh, Intern Revision, Nykredit på mail lcw@nykredit.dk

Anmeldelse af www.retsinfo.dk

Af Cand. merc. aud. Louise Brouer, Unibank A/S

Retsinformation er statens juridiske online informationssystem. Her finder man alle normerede retsforskrifter så som love, bekendtgørelser, cirkulærer samt Folketingets dokumenter. Dokumenterne i Retsinformation opdateres løbende af Folketinget og ministerierne i henhold til retningslinierne i 2 cirkulærer fra 28. februar 1996 (nr. 27 og 28). Opdatering sker minimum en gang i døgnet ifølge Retsinformations egen indholdsbeskrivelse.

Der er flere forskellige indgange til søgning af information. Man kan søge via registrene i Lovtidende A, via registrene i Ministerialtidende, via en lovbog, som indeholder en samlet oversigt over alle gældende love, via en ministerieindgang, som indeholder oversigter over de enkelte ministeriers regler samt via direkte søgning som har adgang til de forskellige databaser. Der er både fordele og ulemper ved de forskellige indgange til informationssøgning.

Anvendes registrene i Lovtidende A til søgning får man en meget overskuelig emneopdelt oversigt, således at man kan søge på alle nye regler, der er vedtaget inden for et bestemt emne i et givet år. Svagheden ved denne indfaldsvinkel er selvfølgelig, at man, hvis man leder efter en bestemt lov, på forhånd skal vide hvilket år den pågældende lov er vedtaget. Det

samme gør sig gældende for søgning via registrene i Ministerialtidende.

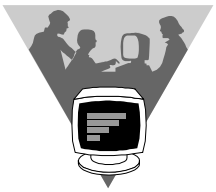
Lovbogen, som indeholder en samlet oversigt over alle gældende love er oplistet efter underskriftsdato. Denne søgeindgang giver et overblik over gældende ret, men stiller krav om, at man som minimum har en ide om, hvornår en given lov er vedtaget.

Den direkte søgning giver mulighed for at søge på en række udvalgte kriterier, hvor man selv bestemmer, hvor mange af de pågældende kriterier man vil anvende. Denne søgeindgang giver mulighed for at søge meget bredt og er den søgeindgang som giver den største frihedsgrad i forbindelse med søgning. Der er dog to ting man skal være opmærksom på:

For det første skal man ved udvælgelse af søgekriterier tænke på, dels at indsnævre sin søgning ved hjælp af specielle søgeord og/eller flere forskellige kriterier, dels at man ikke skal indsnævre den for meget, så eventuelt relevant materiale ikke kommer med.

For det andet skal man være opmærksom på, at Retsinformation er opdelt i nogle underliggende databaser og at man selv skal definere, hvilken database søgningen skal foretages i. Som udgangspunkt foretages informationssøgning i Regelbasen, som indeholder love, bekendtgørelser, cirkulærer, vejledninger samt internationale overenskomster mv. (aktuelle såvel som historiske). Anden information så som afgørelser, lovforslag, betænkninger mv. skal findes i en af de andre baser. Endvidere er skatteministeriets store vejledninger indlagt i en særlig database.

Første gang man anvender Retsinformation, kan det anbefales at læse Retsinformations egen beskrivelse af indhold og databaser. Her gives en kort beskrivelse af indholdet i de forskellige databaser samt en kort introduktion til, hvilke muligheder der er for at søge efter dokumenter. Derudover bør man nok afsætte lidt tid til at gøre sig fortrolig med de forskellige databaser og deres indhold samt forsøge sig lidt frem med, hvilken søgemetode der passer en bedst. Giver man sig selv lidt tid til at prøve sig frem, er der ingen tvivl om, at man med tiden vil finde Retsinformation meget anvendelig bl.a. fordi man altid vil have det sidste nye lovgrundlag at arbejde med.



Internet sikkerhed

Af Peter Petersen, CISA
Codan Forsikring

Anvendelse af internettet bliver mere og mere udbredt og antallet af brugere stiger. Opkobling til internettet giver adgang til et meget stort udbud af forskellige services, fx informationer fra hjemmesider, e-mail og nyhedsgrupper. Mange firmaer har oprettet egen hjemmeside, eventuelt suppleret med diverse tilbud på varer og tjenesteydelser. Anvendelse af e-mail bliver anvendt i stort omfang. Mange typer af interessegrupper har etableret nyhedsgrupper, hvor emner og indhold kun begrænses af deltagernes egen fantasi (chat). Firmaer såvel som private er "på nettet".

Deltagelse i dette store informationsunivers giver næsten uanede muligheder for at skaffe sig oplysninger om alt mellem himmel og jord. Desværre er der ikke kun seriøse deltagere og seriøs information på internettet. Der er visse forstyrrende elementer fx hackere og virus. Hackere interesserer sig for alle computere, både dem, der er placeret i firmaer, og dem, der er placeret i private hjem. Et andet forstyrrende element er virus, dvs. få linier programkode med flere funktioner, både generende og ødelæggende. En stor kilde til spredning af virus er e-mail. Udbuddet omfatter også "stødende" info i form af børneporno og racistiske sider. For at komme på nettet, er det nødvendigt at installere en browser (kigger), og gennem denne browser er der mulighed for at komme i kontakt med de mange web-servere, hvor de mange hjemmesider er placeret. Browseren giver også mulighed for at udveksle e-mails med omverdenen.

Der er næppe tvivl om, at internettet er kommet for at blive, og derfor gør den seriøse del af IT-verdenen, hvad der er mulig, for at beskytte egne systemer og informationer mod såvel virus som hackere. Af naturlige grunde er det de større installationer som erhvervslivet og det offentlige, der anvender de fleste midler til at beskytte sig mod vira og hackere. Med henvisning til førnævnte stødende info skal det pointeres, at denne artikel vil koncentrere sig om virus og hacking.

De mest almindelige risici

Virus.
Virus kan være generende eller direkte ødelæggende fx ved at slette alt på hard-disken eller fylde harddisken op med unyttige ting og dermed blokere for brug af computeren. Inficering med virus kan ske ved at indlæse inficerede disketter eller cd-rom direkte i computeren. En anden måde at inficere computeren er via e-mails fra internettet med vedhæftede filer, hvor den vedhæftede fil indeholder virus.

Hacking.
Man kan blive udsat for hacking uanset om man er privatperson eller et firma. Som privatperson kan det fx ske ved at man modtager en uskyldig e-mail. Når man åbner denne e-mail tapper et program, som er aktiveret uden at brugeren ved det, computeren for fx bankkontooplysninger, bruger-id og password. Disse oplysninger og måske andre fortrolige oplysninger om computerens bruger, sendes til den person, der har foranlediget, at den lille programstump bliver downloadet sammen med et helt normalt program, uden at brugeren ved det. Disse små programmer kan være ualmindelig ondsindede. Det er således yderst vigtigt, at man kender det pågældende firma og har tillid til det. I denne situation kan et anti-virus program ikke opdage et sådan program. Det er blot et lille "normalt" program, der er beregnet til at overføre oplysninger. Antivirus-programmet vil opfatte programmet som værende "virusfrit".

IT-Sikkerhedspolitik
For at beskytte sig mod disse risici er det væsentligt at ledelsen etablerer en IT-sikkerhedspolitik, som anvendelse af internettet er en del af. Det er af yderste vigtighed, at ledelsen engagerer sig i sikkerhed og at dette engagement kanaliseres ned i organisationen. Sikkerhedspolitikken bør være kendt i organisationen og udformet så detaljeret, således at medarbejdere er i stand til at efterleve politikken i overensstemmelse med ledelsens forventninger. Sikkerhedspolitikken kan være den overordnede beskrivelse af sikkerhed. Denne sikkerhedspolitik kan suppleres med mere detaljerede bestemmelser, fx brug af internettet, logisk adgang til data og systemer og lignende.

Virusforsvar
Sikkerhedspolitik alene gør det ikke. Detaljerede retningslinier bør suppleres med andre tiltag. Den mest udbredte måde at sikre sig mod virus er ved at installere anti-virus programmer, at etablere et virusforsvar. Der findes flere forskellige udbydere af antivirus programmer. Udbyderne konkurrerer med hinanden ved hyppige opdateringer med forsvar mod de nyeste vira. Anti-virus programmerne virker ved at være i stand til at identificere kendte vira og dermed at kunne forhindre, at den pågældende virus lagres på computeren. Ofte er de i stand til at rense de modtagne informationer for vira, og dermed gøre informationerne anvendelige for modtageren. Erhvervslivet har naturligt forsynet sig med et virusforsvar, som bør være en del af et betryggende IT-miljø. Ligesom erhvervslivet benytter sig af virusforsvar er det nu almindeligt, at også mange private computere har installeret et anti-virus program.

Værdien i et anti-virusprogram er afhængig af, hvor ofte det opdateres og hvor mange vira, det kender. Man regner med, at der produceres ca. 1.500 nye vira om måneden, så derfor er det vigtigt, at de installerede virusforsvar er opdateret og kender de nyeste vira. Afhængig af, hvilket produkt, der er installeret, kan opdatering af virusmønstre ske ved at hente opdateringen fra udbyderens hjemmeside og dermed ajourføre sit anti-virus program. At hente programmer eller opdateringer fra internettet (downloade) er en af kilderne til at få inficeret sin computer.

En anden måde at få inficeret sin computer med virus, er ved at modtage e-mails, hvor der til den modtagne e-mail er vedhæftet et dokument. Risikoen består i, at det vedhæftede dokument kan indeholde en virus i form af en eksekverbar fil, som aktiveres når man åbner dokumentet og således inficerer computeren. Denne virus kan være mere eller mindre harmløs. Eksempler på sådanne vira er de vira, der har været omtalt i pressen som "Iloveyou". Den og andre vira blev distribueret via adresselister i e-mail systemer. Risikoen ved disse vira består i at den vedhæf-

tede fil blev åbnet og dermed aktiverede skjulte virus.

Fordi denne virus var ny, var der ikke noget antivirusprogram, der kendte den og derved kunne de ikke lukke dem ude eller fjerne viruskoden. Dette paradoks vil formentligt vare evigt, idet virus selvsagt skal være "produceret" før anti-virus programmet er i stand til at genkende den. Og iøvrigt er der ikke tegn på at antal af virus vil reduceres, tværtimod.

Routere og firewall

Virusforsvar anvendes både af erhvervslivet og private. Det samme er ikke tilfældet med routere og firewall. Det er ikke særlig udbredt at private har installeret en firewall, hvorimod erhvervslivet ofte benytter denne enhed for at beskytte sit IT-miljø. Routere mod internettet er ofte placeret hos internetudbyderen, men uden at den derfor yder beskyttelse.

Signaler til og fra internettet transmitteres gennem routere og firewalls, som kan opsættes til at begrænse trafikken.

Alle modtager internetsignaler gennem en router. Routeren er ofte placeret hos internetudbyderen, hvor private har en bruger-id og et password. Erhvervsvirksomheder anvender ligeledes routere, der er placeret hos internet-udbyderen. Nogle virksomheder har selv status som udbyder og har således router placeret hos sig selv. Disse forhold har betydning, såfremt man ønsker at filtrere trafikken gennem routeren.

Routeren er den første enhed, som signalet fra internettet møder. Routeren er en indgangsenhed, som signalet skal passere. Routeren kan opsættes med filtre, der udelukker bestemte signaler, fx således at e-mails signaler ikke kan accepteres.

Såfremt man ikke ønsker at basere sine sikkerhedstiltag på, at udbyderen forsyner routeren med filtre kan firmaet evt. selv opsætte en router med filtre i sin egen installation. Efter routeren placeres typisk en firewall (brandmur).

En firewall er en enhed, som trafikken til og fra internettet ledes igennem. I firewall'en findes et stort antal porte, der hver benyttes til specifikke services. I forbindelse med at firmaet opsætter sin firewall, er det af stor vigtighed, at de ikke benyttede porte spærres, således at kun de aktuelle porte, der benyttes, er åbne.

Hackere "scanner" netop firewalls for ubenyttede porte, der er åbne. Disse porte benytter de til at få adgang til det pågældende firmas computersystem og dermed overtage rettighederne til computeren, og måske benytte den pågældende computer som springbræt til at angribe andre computere i verden. Derved bliver det vanskeligt at spore hackeren og eventuelt retsforfølge ham. En anden måde at genere servere på, er ved spam-mail. Populært sagt sender man så mange breve til serveren, at den ikke kan overkomme at modtage dem. Dette kaldes et "denial of service-angreb". Derved sættes serveren ud af kraft i en periode. Serveren skal så renses for disse nytteløse breve, før den igen kan være aktiv. Flere af de store søgemaskiner har været ude for dette, bl.a. Yahoo.

Ud over at begrænse adgangen ved at spærre ubenyttede porte er der mulighed for at definere, hvilken typer af trafik, som firmaet ønsker gennem firewall'en, ligesom det er muligt at definere, hvilke ydelser, man ikke ønsker, skal passere. Derved er der mulighed for, i et vist omfang, at forhindre en del af de odiøse services. Anvendelse af internettet bør håndteres således, at man i størst muligt omfang, styrer trafikken. Man bør være opmærksom på, at ved at anvende fornuftige tiltag, der kan sikre IT-miljøet mest muligt, kan man begå sig nogenlunde trygt på internettet. Der er visse færdselsregler, som i trafikken, og når disse regler overholdes og man er opmærksom på, at der kan opstå uventede situationer, kan internettet anvendes rimeligt sikkert.

Afslutning

De ovennævnte tilfælde er eksempler, der viser, at der er en risiko, stor eller lille, ved anvendelse af internettet. Der er mange forhold, der kan udnyttes af mindre seriøse personer. Til gengæld er der også mulighed for at styre anvendelse i et vist omfang. Digital signatur og web trust er et par måder, som erhvervslivet kan benytte sig af for at sikre sig, at de parter på internettet, som man har kontakt til, virkelig er de korrekte personer/firmaer. Tillid til handelspartnere på internettet er vigtig. Firmaernes indstilling til sikkerhed er væsentlig, således at firmaet informerer medarbejderne om, hvilke tiltag, der er taget fra firmaets side, samt at medarbejderne er be-

kendt med, at internet-trafikken overvåges centralt og at eventuelt misbrug vil medføre sanktioner.

Enterprise-Wide Risk Management

Af statsautoriseret revisor Morten Egelund og civilingeniør Jon Blønd Sørensen, Arthur Andersen.

Risk Management (RM) er et begreb, som har eksisteret i mange år. I Danmark er RM nok primært knyttet til styringen af forsikringsbare risici såsom ulykker, brand, produktionsstop m.v. Organisatorisk er RM-funktionen i de fleste tilfælde en stabsfunktion, hvis primære funktion er at varetage virksomhedens forsikringspolicer, forsikringssager, garantier m.v. I enkelte tilfælde er området en del af revisionschefens ansvarsområde.

I finanssektoren og flere større virksomheder er der tillige etableret RM-funktioner, som er knyttet til styringen af finansielle risici. Inden for dette område er der udviklet relativt sofistikerede modeller til at identificere, måle og styre rente-, kredit- og valutarisici m.v.

Den internationale udvikling

I flere lande, særligt i England, USA og senest i Tyskland, har en række virksomheder udvidet det traditionelle RM-begreb til at omfatte mere end til blot forsikringsbare risici og risici tilknyttet finansfunktionen.

I flere af disse virksomheder har RM ligeledes bevæget sig fra udelukkende at være et internt styringsværktøj til også at være en del af den eksterne afrapportering over for selskabets ejere og øvrige interessenter. Afrapporteringen omhandler eksempelvis virksomhedens risikoprofil og processen for risikostyring.

Nogle af de væsentligste drivkrafter bag denne udvikling har været:

- Corporate Governance
- Lokal lovgivning (eksempelvis Turnbull (Combined Code) i England og KonTraG i Tyskland)
- Shareholder Value
- Styrkelse af konkurrencefordele
- Aktuelle "blow-ups"

I de seneste år er fokus på Corporate Governance udvidet kraftigt, hvilket dels har udmøntet sig i en "frivillig" fokus herpå fra virksomhedernes side, men også i en "lovgivningsdrevet fokus". Med hensyn til sidstnævnte er der inden for det seneste år kommet ganske vidtrækkende lovgivning i England i form af den såkaldte Turnbull rapport og i Tyskland i form af KonTraG (Law on control and transparency in business). I begge tilfælde stilles der krav, om at offentligt noterede virksomheder skal have en proces for risikostyring og tillige med væsentligt risici afrapportere herom i årsregnskabet.

I de nordiske lande har vi ikke set tilsvarende lovgivning, men det må formodes, at eksempelvis fortolkningen af Aktieselskabslovens § 54 om direktionens og bestyrelsens ansvar og ledelse af selskabet, i takt med at der internationalt udvikles en god skik for RM, vil udvides til også i et eller andet omfang at omfatte RM.

Shareholder value og styrkelse af konkurrencefordele er begreber, der efterhånden høres i mange sammenhænge. Men ikke desto mindre bør det være indlysende, at den virksomhed, som evner bedre at forudse, bedre at vurdere, bedre at fokusere på og bedre styre risici og usikkerhed, alt andet lige vil være bedre rustet til at forfølge strategiske muligheder hurtigere og med større selvtillid og i sidste ende skabe mere værdi for ejerne. Det er også her værdien af det, der kaldes Enterprise-Wide Risk Management (EWRM), ligger.

Hvad er risici?

Før vi kikker nærmere på EWRM er det interessant at stille spørgsmålet – Hvad er risici?

Forretningsmæssige risici defineres forskelligt af folk, som følge af forskellig baggrund, erfaring med risici og ikke mindst organisatorisk placering og fokus.

Tidligere har man ofte tillagt risici en negativ betydning – *truslen* om at noget kan gå galt, men risici handler i høj grad også om muligheder og risikoen for ikke at gribe disse muligheder.

I Arthur Andersen har vi defineret risici som:

Business Risk is the level of exposure to uncertainties that the enterprise must understand and effectively manage, as it creates value.

Entreprise Wide Risk Management

Folk reagerer forskelligt, når de konfronteres med EWRM, men en første reaktion er ofte "vi kender vore risici, og vi reagerer derpå". Reaktionen har naturligvis delvis sin berettigelse, da ledelsen og virksomhedens medarbejdere mere eller mindre bevidst tager risici i betragtning i deres daglige arbejde.
Risikostyringen vil imidlertid i langt de fleste tilfælde være karakteriseret ved at være

- fragmenteret
- negativt fokuseret
- reaktiv
- ad hoc
- omkostningsfokuseret
- snævert fokuseret
- funktionsdreven

I modsætning hertil er de væsentligste karakteristika ved EWRM:

- integreret
- positiv fokus
- proaktiv
- løbende proces
- værdi baseret
- bredt fokuseret (holistisk)
- procesdrevet

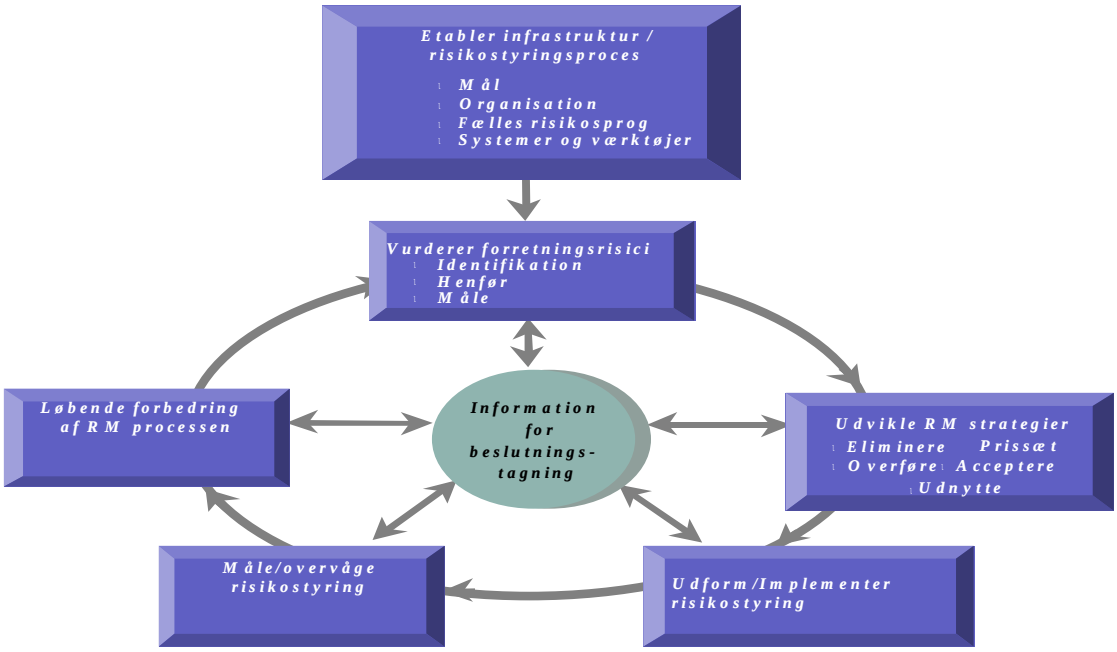
I Arthur Andersen har vi defineret EWRM som:

EWRM is a truly holistic, integrated, forward-looking and process-oriented approach that alligns strategy, processes, technology and knowledge.

Definitionen kræver nok et par ganges gennemlæsning! Den signalerer et ambitionsniveau, som for langt de fleste virksomheder vil kræve en rejse hen imod et højere stadie for risikostyring. EWRM er derfor i høj grad et spørgsmål om at opgøre ønsker og behov og tage et skridt ad gangen.

I figur 1 er konceptet for (EWRM) skitseret. De forskellige faser forklares efterfølgende. Faserne vil ofte overlappe hinanden.

Figur 1: Koncept for EWRM



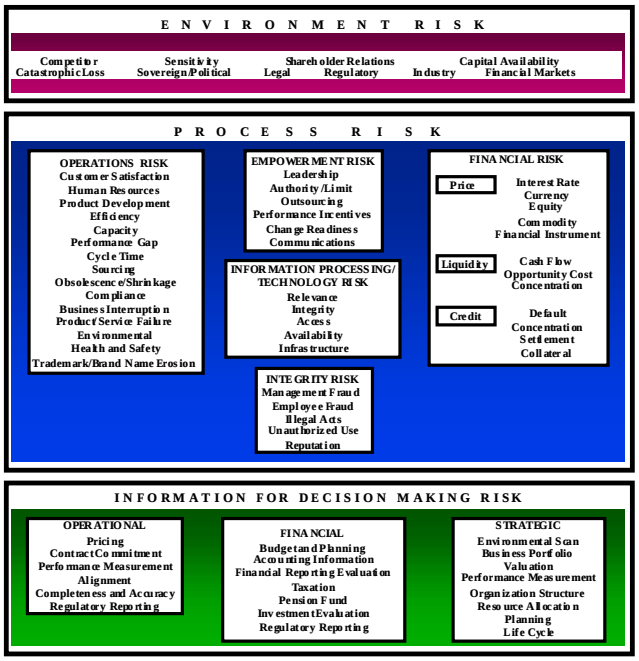
Etablering af RM-infrastruktur

Som netop omtalt er det essentielt, at der defineres en målsætning og en strategi for RM, som udmyndes i en egentlig politik for området. Det skal besluttes, på hvilke niveauer RM skal anvendes: operationelle, taktiske og strategiske. Hvis det fulde udbytte ønskes, bør alle niveauer inddrages. Organisationens ledelse må på denne baggrund tage stilling til, hvorledes RM-funktionen skal organiseres, dens ansvarsområde, rapportering og forankring i organisationen. For at sikre at de grundlæggende forudsætninger, for at RM kan blive en succes, er tilstede, bør RM-funktionen være synlig, evt. bestående af en risk manager og ledere fra forskellige forretningsenheder og frem for alt have opbakning fra den øverste ledelse.

Funktionen vil indledningsvist evaluere den eksisterende risikostyring og udvikle en fælles opfattelse af risici - et *fælles risikosprog*, som yderligere detaljeres i risikoanalysen.

I figur 2 er vist et eksempel på et udgangspunkt for et fælles risikosprog i form *af Arthur Andersen Business Risk Model*. Modellen har opdelt de risici som en organisation kan stå over for i 3 hovedkatagorier – *Environment risk, Process risk og Information for decision making risk* – samt i et antal underkategorier.

Figur 2 Arthur Andersen Business Risk Model



Vurdering af forretningsrisici

Første skridt i denne fase er en detail-identifikation af risici. Der kan anvendes flere forskellige metoder hertil, men det typiske forløb består af en række faciliterede workshops, som tager udgangspunkt i det fælles risikosprog, samt interviews med virksomhedens nøglepersoner. Resultatet er en liste med risici, der defineres og kategoriseres, og som derefter anvendes ved risikovurderingen. Risikoen udtrykkes som produktet af frekvens og konsekvens og afbildes ofte i et *risk map*. Frekvensen kan udtrykkes ved hjælp af sandsynlighedsintervaller, men ofte opstilles relationer mellem værdier for begge variabler. IT kan anvendes til at understøtte processen, således at vurderingerne sker udfra en fælles opfattelse af frekvens og konsekvens.

Udvikling af RM-strategi

Over for en risiko har man 5 mulige strategier:

- *eliminere*
- *prissætte*
- *overføre*
- *acceptere*
- *udnytte*

For hver risiko udarbejdes en strategi, som baseres på, hvilket risikoniveau der findes acceptabelt efter RM-politikken, og de ressourcer, der er til stede i organisationen. Et eksempel på en strategi for en klassisk risiko kunne være risikoen for brand, som overføres til en tredjepart ved forsikring.

Udformning og implementering af risikostyring

Når strategien for de enkelte risici og grupper af risici er fastlagt, udpeges *risikoejere*. Risikoejeren vil herefter skulle designe og implementere de *egenskaber* i form af processer, mennesker, rapporter, metodologier og teknologier, som skal til for at gennemføre en strategi. Tiltagene kan selvsagt spænde vidt lige fra ændring af procedurer og forretningsgange over ændrede rapporteringsformer og IT-systemer til outsourcing af aktiviteter. Ved både design og implementering skal der lægges vægt på bløde faktorer, og man skal være opmærksom på organisationens kultur, modstand mod forandringer og medarbejderindflydelse.

Overvågning af risikostyringen

For at sikre at de implementerede tiltag virker efter hensigten, bør risikostyringen løbende overvåges. Dette kan ske efter definerede aktivitets- og resultatstandarder. Det centrale spørgsmål er "hvordan ved vi, at ...", eksempelvis grundlaget for vurderingen af de enkelte risici stadig er aktuelt, at de valgte strategier er valide o.s.v.

Løbende forbedring af RM

På baggrund af overvågningen skal det løbende vurderes, om de etablerede risikostyringstiltag virker tilfredsstillende.

Benchmarking mod *best practices* eller andre enheder i organisationen kan være eksempler på værktøjer til løbende at forbedre RM-processen. Herved synliggøres de områder, der halter efter, og de, der viser fremskridt.

Information for beslutningstagning

De forskellige faser er afhængige af informationer fra andre faser, og i hver enkel fase vil der ligeledes blive genereret betydelige mængder af information. Eksempelvis vil der ved design af risikostyringsaktiviteter skulle være information til stede om den identificerede risiko, hvem ejer risikoen og størrelsen af risikoværdien, ligesom selve risikostyringsaktiviteten

vil skulle afrapporteres og indgå i ledelsens beslutningsgrundlag.

Informationsudveksling mellem faserne er en central forudsætning for EWRM. RM-funktionen vil have den centrale rolle i at sikre, at information indsamles, bearbejdes og udveksles.

Intern revisions placering i EWRM

Intern revision gennemgår i disse år meget store forandringer. En række danske og udenlandske revisionsafdelinger re-definerer deres arbejdsområde, metodologier og værktøjer for fortsat at være relevante og værdiskabende for organisationen.

Som bekendt kom der sidste år en ny definition af intern revision:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance process.

Definitionen lægger op til, at den interne revision bør have en central rolle i relation til virksomhedens værdiskabelse, RM-aktiviteter og governance-processer.

Den interne revision har ofte erfaring med risikovurderinger i kraft af en risikofokuseret revisionsplan og gennemfører eller deltager ofte i større projekter på tværs af organisationen. Den interne revision har derfor gode muligheder for at introducere og "sælge" EWRM i organisationen, gennemføre pilotprojekter og deltage i en passende og bæredygtig implementering af EWRM, og ikke mindst ændre revisionsmetodikken til at fokusere på forretningsmæssige risici og på risikostyringsprocessen**.**

Styring af valutarisici

Af Joan Nielsen og Louise Claudi Westh, Intern Revision, Nykredit A/S

Denne artikel tager udgangspunkt i styring af valutarisici i et pengeinstitut.

Valutarisikoen udtrykker risikoen for tab på beholdninger eller forpligtelser i fremmed valuta ved bevægelse i markedskursen.

Styring af valutarisici i et pengeinstitut vil primært være styring af det cash flow, der er i et pengeinstitut af valuta. Her tænkes på fx køb og salg af udenlandske værdipapirer og arbitrage samt betalinger. Endvidere foretager de fleste pengeinstitutter spekulation i valuta og påfører sig derved risici. Der udover har instituttet ofte positioner i værdipapirer, lån og garantier, som ligeledes skal styres.

Styring af valutarisici foretages oftest på 3 niveauer:

- strategisk niveau
- taktisk niveau
- operationelt niveau

På strategisk niveau tager bestyrelsen stilling til, hvilken risikoprofil pengeinstituttet skal have, herunder under hvilke rammer Direktionen kan tage risici.
I henhold til bank- og sparekasseloven § 18 skal bestyrelsen udarbejde skriftlige retningslinier mellem direktionen og bestyrelse, hvori arbejdsdelingen mellem parterne fastlægges. Disse retningslinier benævnes i praksis bestyrelsens instruks til direktionen.

På taktisk niveau råder direktionen over et sæt rammer for pådragelse af risici, som kan videredelegeres til afdelingschefer og dealere i pengeinstituttets handelsfunktion. Direktionen kan ved videredelegering sætte yderligere begrænsninger.

På operationelt niveau har handelsfunktionen fået udstukket rammer, som denne skal holde sig indenfor. Organisatorisk adskilt fra handelsfunktionen forestår en kontrolfunktion kontrol af, at dealerne, afdelingschefer og direktion holder sig indenfor de udstukne begrænsninger.

Nedenfor vil vi skitsere en metode til brug for styring af valutarisici.

Styring af valutarisici kan tage udgangspunkt i de af Finanstilsynet definerede risikomål. Risikomålene samt beregningsmetoderne herfor er defineret i Finanstilsynets kapitaldækningsbekendtgørelse.

Valutaindikator 1
Valutaindikator 1 defineres som den største af summen af positive henholdsvis summen af negativer positioner og beregnes kun for positioner i de 19 valutaer der er noteret på Københavns fondsbørs. Det vil sige lange positioner lægges sammen og korte positioner lægges sammen, det største tal af disse er valutaindikator 1.

Indikator 1 benyttes til at begrænse modsatrettede positionstagning i valutaer, der varierer i takt overfor danske kroner.

Valutaindikator 2
Valutarisikoen kan måles som det maksimale tab, der med 99% sandsynlighed kan pådrages indenfor en 10-dagesperiode. Det vil sige, at banken har sat grænser for hvad man indenfor 10 dage med 99% sandsynlighed tror at man kan tabe.

Metoden baseres på statiske registreringer af valutaernes varianser og indbyrdes covarianser. Der anvendes variansberegninger for de mest almindelige valutaer i henhold til Finanstilsynet og Nationalbankens model.

Ved anvendelse af valutaindikator 2 tages højde for at nogle valutaer svinger mindre og andre svinger mere end gennemsnittet i forhold til den danske krone, og at kursen på nogle valutaer svinger mere eller mindre i takt med hinanden.

Indikator defineres som en value at risk metode, hvor der tages hensyn til de enkelte valutaers volatilitet og indbydes samvariation. Valutaindikator 2 beregnes som valutaindikator 1 kun ud fra de 19 valutaer, som er noteret på Københavns fondsbørs.

Øvrige valutaer
For øvrige valutaer stilles pengeinstituttet frit for hvorledes styringen af valutarisici kan foretages, det foreslås, at der fastsættes en særskilt ramme for gruppen af øvrige valutaer, der opgøres som summen af de numeriske nettopositioner omregnet til danske kroner i lighed med valutaindikator 1.

Positionstagning
I forbindelse med fastlæggelse af rammer for styring af valutarisci kan ovenstående risikomål benyttes. Der udover bør bestyrelsen i det enkelte pengeinstitut vurdere og fastsætte rammer for intraday handel og overnight handel. Det vil sige, at indenfor dagen skal dealerne have rammer, som de kan handle indenfor, og når dagen er omme skal de fastlægge en ny ramme for hvilke positioner, som dealerne må have natten over.

Intraday rammen kan være højere end overnight rammen, da man hurtigere kan nedbringe en position i løbet af dagen.

Fordelingen kunne tage udgangspunkt i følgende måle punkter:

Indikator 1
Indikator 2 O/N
Indikator 2 I/D

Konklusion

Det vigtigste ved styring af valutarisici er at instituttet definerer sin risikoprofil samt klarlægger sine risici og med udgangspunkt heri får afdækket styringen af enhver form for risiko, som vil kunne påføre instituttet et tab. Ovenfor er skitseret forskellige metoder til brug herfor.

Præsentation af Intern Revision i Novo Nordisk

Af Pui Fong Yau, Novo Nordisk

Baggrund
Novo Nordisk Intern Revisions afdeling (Group Internal Audit, forkortes GIA) blev stiftet i 1993 på foranledning af et ønske fra bestyrelsen for at styrke organisationens interne kontrolmiljø.

Organisation og uafhængighed
GIA udgør Novo Nordisk koncernens eneste Intern Revisions afdeling. Organisatorisk er GIA placeret således, at vi refererer og rapporterer til Chief Financial Officer (CFO).

I praksis planlægger og styrer GIA selv hvilke opgaver, der løses i årets løb. Uafhængigheden af den daglige og den forretningsmæssige ledelse sikres og opretholdes dels via vor Charter og dels via vor direkte rapportering til bestyrelsen, idet vi afrapporterer kvartalvist til bestyrelsesformanden omkring vore aktiviteter, og om der har været væsentlige problemstillinger.

I starten bestod GIA af 3 personer, men gennem de senere år har GIA beskæftiget 7 - 8 mand m/k. P.t. er vi 7 personer, 4 finansielle revisorer og 3 IT revisorer, hvoraf den ene person (IT revisor) er udstationeret hos et af vore amerikanske datterselskaber for en 1½ års periode. De fleste GIA medarbejdere har en cand.merc.aud. baggrund og har tidligere arbejdet i revisionsfirmaer, men enkelte medarbejdere har andre baggrunde.

Afhængig af de enkelte opgavers omfang arbejder vi i teams. Mindre eller afgrænsede opgaver løses typisk af 1-2 personer sammen, mens lidt større opgaver løses af teams på op til 4 personer.

Opgaver
GIA har mange forskelligartede opgaver, herunder beskæftiger vi os bl.a. med:

- Finansiel revision, herunder gennemgang af brugersystemer, der omfatter forretningsgange og tilhørende edb-systemer samt revision af årsregnskabet i samarbejde med ekstern revision.
- Gennemgang af nye væsentlige IT-systemer eller ændringer til eksisterende væsentlige IT systemer, herunder rådgivning om business- og applikationskontroller før, under og efter implementering.
- Gennemgang af miljø- og socialrapporten i samarbejde med eksterne verifikatorer.
- Control Risk Self Assessment (CRSA).
- Diverse ad hoc opgaver, forespørgsler fra ledelsen eller vore kundeafdelinger, medvirken til erklæringsopgaver m.v. i samarbejde med ekstern revision.

Novo Nordisk koncernen har datterselskaber, filialer og salgskontorer i bl.a. USA, Canada og Sydamerika, Asien, Australien, Centraleuropa og Nordafrika.

De fleste opgaver ligger i moderselskabet, men der udføres også opgaver hos de danske datterselskaber og enheder med beliggenhed i udlandet. Revision af de udenlandske enheder giver en noget varierende rejseaktivitet.

Vi arbejder ikke med nogen faste rammer for hvilke eller hvor mange udenlandske enheder, der skal besøges i løbet af et år. Nogle enheder besøges hyppigere end andre under afvejning af væsentlighed og risici, mens andre enheder alene besøges foranlediget af ad hoc forespørgsler fra den daglige eller forretningsmæssige ledelse.

Service
Samarbejde, dialog og høj etik er nøgleord i stort set alt, hvad vi foretager os. Vor arbejdsform og vore service ydelser til resten af organisationen betinger en proaktiv holdning, det at kunne forholde sig konstruktiv kritisk til eksisterende rutiner og kunne yde rådgivning, der er etisk forsvarligt og som så vidt muligt frembringer holdbare løsninger.

I nogle projekter medvirker GIA som ex-officio medlem i styregruppen, således at vi kan holde os orienteret om, hvorledes væsentlige projekter skrider frem.

Forslag til forbedringer eller ændring til eksisterende rutiner drøftes løbende med kunden under revisionens udførelse, hvilket åbner mulighed for en god og konstruktiv dialog, der medvirker til at inspirere begge parter.

Rapporter udarbejdes og fremsendes i udkast til kunden, findings og forslag vægtes efter væsentlighed, og den endelige rapport indeholder både afdelingslederens svar og deres tidsfrist for implementering af forslagene. Alle rapporter fremsendes til bl.a. kunden, CFO og ekstern revision.

Samarbejde med ekstern revision og andre eksterne verifikatorer
Vi indgår aftaler for et år ad gangen med ekstern revision og andre eksterne verifikatorer, hvilke opgaver vi skal løse i samarbejde med disse, herunder aftaler om scope, tidsplaner standard for rapportering m.v.

Der udarbejdes detaljerede revisionsplaner og arbejdsprogrammer for de enkelte revisionsområder, der godkendes af vor ekstern revision/ eksterne verifikatorer.

Der føres en løbende dialog med eksterne verifikatorer omkring, hvorledes arbejdet skrider frem, og om der evt. på et tidligt tidspunkt er identificeret væsentlige problemområder (early-warnings).

Efter endt arbejde gennemgår vore arbejdspapirer en intern kvalitetssikring, hvorefter disse overleveres til ekstern revision/ eksterne verifikatorer til deres brug. Diskussioner omkring problemstillinger eller evt. behov for yderligere diskussion eller opfølgning sker i en dialog med disse.

Nye aktiviteter
Efter en vellykket pilotfase, er vi for alvor gået i gang med at afholde CRSA workshops, hvor vi bl.a. anvender OptionFinder som afstemningsredskab. Indtil videre afholdes CRSA workshops udelukkende for de afdelinger, der har relation til regnskabsfunktionen. På længere sigt er det hensigten at CRSA workshops også tilbydes andre afdelinger.

Med hensyn til anvendelsen af OptionFinder, som er et temmelig bekosteligt teknisk redskab, har vi bl.a. et fint samarbejde med 2 andre store firmaer, om at vi gensidigt kan leje udstyr hos hinanden, såfremt vor eget udstyr ikke findes i tilstrækkeligt antal.

Karrieremuligheder
Novo Nordisk gør meget ud af medarbejderudviklingen. Der afholdes halvårlige medarbejdersamtaler (Annual Performance Improvement System, forkortes APIS). Udviklingsplaner, herunder behov for videreuddannelse samt fremtidige karriereplaner evt. i andre afdelinger drøftes i en åben og konstruktiv dialog mellem den enkelte medarbejder og leder.

GIA har haft en relativ stor personaleomsætning ift. organisationens størrelse i de seneste år. De fleste af de medarbejdere, der har forladt GIA er rejst videre til andre karrierestillinger i Novo Nordisk.

Afrunding
Novo Nordisk er en spændende organisation at arbejde for. Jeg har været i GIA siden efteråret 1996, og jeg synes fortsat at intern revision er et spændende og udviklende område med mange fremtidsmuligheder.

Mærkedage

Foreningen har i forbindelse med årsmødet gratuleret

Ulla Hansen fra Topdanmark A/S i anledning af 10 års jubilæet som medlem af Foreningen.

Endvidere havde Hans Peter Slot fra Kuwait Petroleum A/S 10 års jubilæum som medlem af Foreningen.

Bestået CIA eksamen

Redaktionen ønsker tillykke til

Revisor, Pui Fong Yau, Novo Nordisk

Pui er blevet CIA´er, d.v.s., at alle 4 eksaminer er bestået.

Bagsmækken

Oplysninger om Foreningen af Interne Revisorer

Foreningens adresse:
Foreningen af Interne Revisorer (IIA)
Vester Farimagsgade 31
1606 København V

☎ 3375 6400 Søren Kongsbo
☎ 3375 6402 Bente Christensen (indmeldelser, tilmeldinger til kurser, månedsmøder m.v.)
E-mail: bcc@post.dk
Telefax 3332 9010
☎ 3253 0989 Frede Bech Poulsen

Foreningen af Interne Revisorers bestyrelsesmedlemmer:

Søren Kongsbo (formand)	**Post Danmark**
Tage Rasmussen (næstformand)	**Handelshøjskolen, Århus**
Niels Thor Mikkelsen (kasserer)	**Den Danske Bank**
Frede Bech Poulsen (sekretær)	
Ane Marie Christensen	**Unibank**
Peter Birkholm Laursen	**Handelshøjskolen, København**
John Tyrrestrup	**FDB**

Jobannoncer
Jobannoncer kan bringes i INFO for kr. 1.500.
Annonceudkast sendes til Foreningens adresse jf. ovenfor.

CIA-eksamen
Henvendelse angående CIA-eksamen samt forberedelse hertil kan rettes til Tage Rasmussen.
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.

Artikler
Artikler i INFO honoreres med 3 flasker god rødvin.

Næste nummer
Udkommer i december 2000

Udlån
System Control & Auditability (SAC-Rapporten)

Foreningen har et fuldstændigt eksemplar af SAC-Rapporten, som kan lånes ved henvendelse til Foreningens sekretær på ☎ 3253 0989.

Formålet er at give de medlemmer, der endnu ikke har anskaffet den, en chance for at danne sig et indtryk af den inden bestilling.

COSO rapporten (Internal Control Integrated Framework), som tidligere har været omtalt på månedsmøderne samt på kurset "Operationel Revision" kan lånes til gennemsyn, før man evt. selv vil anskaffe den fra Orlando.

Rapporten er delt op i 4 bind:
- Executive Summary (7 sider)
- Reporting to External Parties (25 sider)
- Framework (118 sider)
- Evaluation Tools (203 sider)

Henvendelse til Foreningens sekretær på
☎ 3253 0989

Oplysninger om diverse hjemmesider

IIA´ hjemmeside	www.theiia.org Se endvidere IIA-INFO nr. 12 www.itaudit.org
IIA, DK´ hjemmeside	www.iia.dk
IIA, UK Chapter	www.iia.org.uk
Outsourcing	www.outsourcing.com Se endvidere IIA-INFO nr. 8
AuditNet	Users.aol.com/auditnet
Fraud	Users.aol.com/auditnet (derefter vælges FraudNet). Se endvidere IIA-INFO nr. 7
WebTrust	www.fsr.dk www.aicpa.org www.cica.org www.cpaWebTrust.org www.verisign.com (Her findes også en liste over WebTrust certificerede virksomheder).