INFOs redaktion:

Ansvarshavende redaktør:
Revisionschef Thorkild Jakobsen
☎35 29 28 50
Told- og Skatterevisionen

Øvrig redaktion:

Frede Bech Poulsen
☎32 53 09 89

Revisor Nina Belcaid
☎33 33 10 37
Unibank A/S, Finansrevisionen

Revisor Bente Hallberg
☎33 75 64 08
Post Danmark, Intern Revision

Revisor Tina Mollerup Laigaard
☎35 29 28 61
Told- og Skatterevisionen

EDB-revisor Claus Deela
☎35 29 28 66
Told- og Skatterevisionen

Revisor Pui Fong Yau
☎44 42 11 49
Novo Nordisk

Revisor Gert Stubkjær
☎33 55 42 84
Codan Forsikring

- - - - - - - - - - - - - - - -

Redaktionens adresse:
IIA INFO
c/o Told- og Skatterevisionen
Toldbodgade 57 - 61
1253 København K
☎35 29 28 50

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/ Tage Rasmussen

Den "Ideelle" uddannelse til intern revisor

Flere har spurgt mig, hvordan den ideelle uddannelse til intern revisor bør designes. Efter at have tænkt over problemstillingen i nogen tid, er jeg kommet til følgende konklusion: Der er ikke én ideel uddannelse til intern revisor, men mange gode veje. Årsagerne til konklusionen er primært to:

1. Den enkelte person starter sit arbejde som intern revisor på vidt forskellige tidspunkter i sit karriereforløb og dermed med vidt forskellig teoretisk og praktisk uddannelse.
2. Den enkelte person har vidt forskellig hensigt med at beskæftige sig med intern revision.

Som illustration af disse forskelle kan nævnes nogle få praktiske eksempler:

- En cand. merc. aud., der måske også er blevet statsautoriseret revisor, men som prioriterer at beskæftige sig i dybden med én virksomhed i stedet for at sprede sit arbejde over mange virksomheder.
- En brancheuddannet person (fx. bank- eller etatsuddannet), der fristes af den mere analyserende tilgang, der er indeholdt i intern revision.
- En person med en anden videregående uddannelse end revision, der ønsker at anvende fx. et tre-årigt ophold i en intern revisionsafdeling til at skabe sig et overblik over en kompliceret virksomhed med henblik på yderligere karriereudvikling.
- En person der fra starten af sin faglige uddannelse ønsker at gennemføre en uddannelse / et studium, der er målrettet mod en længerevarende karriere indenfor intern revision.

Det er ret klart, at disse forskellige profiler har behov for en meget forskellig uddannelse eller efteruddannelse. Én ting er dog sikkert. Der stilles fremover store krav til praktisk forståelse for intern revision og ikke mindst til teoretisk viden indenfor de mange fagområder, der er omfattet af intern revision.

Heldigvis er det danske uddannelsessystem også klædt rimelig godt på til at løse denne opgave. Som eksempler på nogle af de mange muligheder kan nævnes:

- Deltagelse i enkeltfag på cand. merc. aud.-studiet. Personer med en teoretisk eller praktisk uddannelse, der modsvarer en bachelor-uddannelse (fx. HA), eller som på anden måde har erhvervet de tilstrækkelige forudsætninger, kan under lov om åben uddannelse deltage i undervisning og eksamen i studiets enkeltfag, fx. revision. Tilsvarende gælder for deltagelse i HD-uddannelsens enkelte fag.
- Deltage på Foreningen af Interne Revisorers Grundkurser i Revision, IT-revision, Statistisk Revision, Operationel Revision mv. Kursuskataloget for 1999 er netop udkommet. Der udstedes bevis for deltagelse.
- Sammen med andre ligesindede som selvstuderende forberede sig til at deltage i den internationale CIA-eksamen. Kontakt undertegnede, hvis optagelse i netværk omkring forberedelse til CIA frister. Såfremt der viser sig et væsentlig behov for specielle workshops i forbindelse med forberedelsen, etablerer Foreningen af Interne Revisorer sådanne workshops.
- Deltage i internationale konferencer, workshops, seminarer mv. I forskellige lande i Europa men især i USA arrangeres sådanne aktiviteter i stor udstrækning. Nærmere oplysninger herom kan fås hos foreningens sekretær Frede Bech Poulsen.
- En forventet og ønsket fornyelse af cand. merc. aud.-uddannelsen kunne også tænkes at medføre, at der åbnes mulighed for en specialisering. Man kunne således forestille sig, at væsentlige dele af skatteretten og de juridiske specialiteter erstattes af moduler, der fokuserer på intern kontrol / controlling, økonomistyring og IT / IT-revision. En sådan speciali-

sering fortjener næsten titlen: cand. merc. i intern revision!

Uanset tidligere formel uddannelse og efteruddannelse har alle et udtalt behov for at kunne dokumentere, at et højt niveau mht. målrettet faglig uddannelse, viden og forståelse er opnået. Dokumenteret deltagelse i mange kurser, konferencer, workshops osv. er selvfølgelig udmærket, men det sandsynliggør ikke i tilstrækkelig grad, at der er opnået en brugbar kompetence.

Gennemførelse af den internationale anerkendte eksamen CIA (Certified Internal Auditor), der fx. i USA vurderes at være på samme faglige niveau som den amerikanske revisoreksamen (CPA), er derfor et godt værktøj i en internationalt orienteret karriereplan. Det kan derfor varmt anbefales, at en gennemført praktisk og/eller teoretisk uddannelse indenfor fagområder, der er relevante for intern revision, afsluttes med en CIA-eksamen.

Krav til og indhold i CIA-eksamen er kort beskrevet i foreningens uddannelsesfolder for 1999. Yderligere beskrivelse af eksamen, forudsætninger for indstilling til eksamen, anbefalet litteratur til selvstudier, ønske om deltagelse i det danske netværk, tilmelding til eksamen og i øvrigt praktiske problemer i forbindelse med planlægning og gennemførelse af forberedelsesarbejdet kan formidles af undertegnede.

God held på uddannelsesrejsen!

Redaktøren
v/ Thorkild Jacobsen

Bestyrelsen har løbende focus på foreningens uddannelsesprogram, som er en markant hjørnesten i foreningens virksomhed. Tilbuddene kommer til udtryk i det årlige uddannelsesprogram, som netop er tilgået medlemmerne. I tilknytning hertil har redaktionen anmodet Tage Rasmussen, som er ansvarlig for kursusvirksomheden, i INFO`s leder at sætte focus på de veje, der kan føre til en god uddannelse af interne revisorer.

I øvrigt er dette nummer af INFO præget af tankevækkende indlæg fra Jesper Koefoed, KPMG om besvigelser i dansk erhvervsliv, fra Finn Morell, Unibank om revision af homebanking systemer og fra Claus Deela, Told- og Skatterevisionen om begrebet datawarehouse.

INFO indeholder endvidere et referat fra et møde, som bestyrelsen og INFO`s redaktion afholdt i november om INFO, dets udformning og tilrettelæggelse. Redaktionen håber, at medlemmerne herigennem kan få et indtryk af det virkelyst, der præger arbejdet med at udgive et blad, der tilgodeser foreningens medlemmer i videst muligt omfang.

For yderligere at skaffe artikler og inspiration har redaktionen truffet aftale med vores norske og svenske redaktionskollegaer, at vi fremover kan udnytte hinandens artikler i egne publikationer. Endvidere er det aftalt, at de 3 redaktører i starten af næste år mødes for at udveksle erfaringer.

Med disse ord ønsker redaktionen sine læsere en rigtig god jul og et godt nytår.

Nye medlemmer
v/Frede Bech Poulsen

INFO byder velkommen til:

A.P.Møller
Chief internal auditor Stephen C. Glover

ABN AMRO Bank
Intern revisor Lars Bo Jeppesen

Novo Nordisk

EDB-revisor Carole Seymour

Nyt fra bestyrelsen
v/ Thorkild Jakobsen

Den 11. november afholdtes et møde mellem IIA´s bestyrelse og INFO´s redaktion. Formålet var at diskutere INFO, dets udformning og tilrettelæggelse. Nedenfor ses en oversigt over de på mødet trufne beslutninger, som INFO´s læsere vil mærke mere til i løbet af 1999:

- Artikler i bladet bør veksle mellem teori og praksis og fortsat lægge op til erfaringsudveksling.
- Der bør bringes flere artikler om de forskellige branchers interne revisioner.
- INFO´s ledere bør så vidt muligt være holdningsprægede og relateres til indholdet i INFO.
- Mærkedage bør i højere grad markeres (medlemmerne opfordres til at meddele disse til INFO).
- Der bør bringes artikler om IIA´s guidelines evt. sammenlignet med FSRs vejledninger.
- Der bør bringes artikler om responsumsager, svig og uregelmæssigheder, det elektroniske arbejdspapir.
- Der bør bringes artikler fra interne revisorer udstationeret i udlandet (opfordring er hermed givet)
- Opfølgning af månedsmøder med artikler om emnet.
- Artikler honoreres med 3 flasker god vin.
- INFO´s forside skal fange opmærksomheden.
- Antal eksemplarer af INFO tilgår medlemmerne udfra et oplyst behov.
- Bestyrelsen og redaktionen mødes en gang årligt angående INFO´s tilrettelæggelse.
- Påmindelse fra redaktøren om, at INFO bør cirkulere internt i den interne revision.
- Indførelse af en fast bagside: ”Bagsmækken”.
- Anmeldelse af internationale kurser.
- Drøftelser af de tiltag/bidrag vi får fra IIA, Orlando og Europe.

“Frit Forum”
v/Nina Belcaid

Noter fra en revisorkonference:

En redaktør er en, der skiller hveden fra klinten og bruger klinten.

Styrken ved demokratiet er ytringsfrihed. Svagheden er, at denne frihed bliver brugt.

Man støder først på den virkelige sandhed, når den ikke længere er interessant.

Love skal ikke være fælder, der fanger forbrydere, men lamper der advarer mod risiko for skibsbrud.

Journalister har svært ved at se forskel på et cykeluheld og et civiliseret samfunds sammenbrud.

Et dementi defineres som den benægtende bekræftelse af en nyhed, der indtil nu kun har været et rygte.

Fremskridt er kun muligt, hvis man intilligent overtræder regler.

Aktivitetskalender
v/Ane Marie Christensen

For 1999 er der foreløbig planlagt månedsmøder på følgende datoer:

Torsdag den 11. marts
Torsdag den 15. april
Torsdag den 10. juni (årsmøde)

Reserver datoerne allerede nu.

Tilmelding til månedsmøder sker til Bente Christensen, Post Danmark, Intern Revision,
☎ 3375 6402 eller FAX nr. 3332 9010
senest mandagen før afholdelse af månedsmødet.

Kursuskalender
v/Tage Rasmussen

Foreningens uddannelsesfolder for 1999 er netop færdiggjort. Det er vores håb, at mange af medarbejderne hos foreningens medlemmer også vil tilmelde sig kurserne i 1999. Uddannelsesudvalget har gjort sig stor umage i forbindelse med ajourføring af kurserne.

En del af vores kursister og medlemmer har foreslået, at kurserne flyttes til Sjælland, hvor de fleste af kursusdeltagerne kommer fra.

Bestyrelsen har derfor rettet henvendelse til flere kursussteder på Sjælland for at få et samlet tilbud. Resultatet af undersøgelsen er blevet, at vi foreløbig fastholder Ebelftoft Parkhotel som kursussted. De to væsentligste årsager til beslutningen er:

Omkostningerne til kursusstedet vil være mellem 600 kr. og 800 kr. større pr. kursusdeltager på Sjælland.

Fleksibiliteten m.h.t. fastlæggelse af antal deltagere til kort før kursernes gennemførelse og en eventuel aflysning er langt mindre på de sjællandske kursussteder end på Ebeltoft Parkhotel. Dette vil i gennemsnit gøre det enkelte kursus væsentligt dyrere at gennemføre.

Da foreningen fortsat ønsker at kunne gennemføre nogle relativt billige kurser med et forholdsvist lavt antal deltagere pr. kursus, har vi vurderet, at ulempen og omkostningen for den enkelte kursist ved at skulle rejse til Ebletoft, er væsentlig mindre end den prisstigning, der nødvendigvis må gennemføres ved at flytte kurserne til Sjælland.

Vi håber, at medlemmerne og deres medarbejdere har forståelse for dette.

Såfremt foreningens medlemmer er uenige i beslutningen, hører vi gerne herom.

Information fra IIA i Orlando
v/Frede Bech Poulsen

IIA lancerer ny "IT Audit Web" side, som kan findes på adressen:

www.itaudit.org

og omfatter "The IT Audit Forum", "The Reference Library", " The Conference Center" og "The Yellow Pages". Sidstnævnte er en database over IT produkter m.m. af interesse for IT professionelle.

ECIIA (Europian Confederation of Institutes of Internal Auditing) er af EU inviteret til at deltage i "The Technical committee on Auditing". Dermed har ECIIA "fået foden indenfor".

Evaluering af foreningens kurser
v/Nina Belcaid

Kurser i Intern Revision, modul 1 og 2.
Af cand. merc. aud. Kim Petersen, Finansrevisionen Unibank

I september og oktober har foreningen afholdt de to første moduler af en kursusrække, der forløber over efteråret 1998 og forår/sommer 1999.

Kursusrækken henvender sig til interne revisorer og har til formål at give interne revisorer en opdateret og ajourført indsigt i den interne revisions funktion.

Indholdet i de to første moduler var grundlæggende. I første modul fik vi indsigt i emner, som revisionens funktioner, revisorlovgivningen og revisionsprocessen, mens andet modul berørte emnerne revisionens afsluttende arbejder, revisoransvar og samarbejde mellem interne og eksterne revisorer. Beggge moduler indeholdt udbytterige og lærerige casearbejder.

Deltagerne kom fra forskellige brancher og med forskellige uddannelses- og erfaringsmæssig baggrund. Der var lige fra den helt nye uerfarne interne revisor til revisoren med flere års erfaring. Dette har stillet store krav til kursets undervisere lektor, statsautoriseret revisor Peter Birkholm og lektor, statsautoriseret revisor Mogens Christensen. Begge formåede, til trods de hårde odds, at gøre undervisningen interessant og medlevende, så nye revisorer kunne lære nyt stof og dem med erfaring fik en god repetition heraf.

Begge moduler var to dages kurser, der blev afholdt på Parkhotel i Ebeltoft, og undervisningen blev udført med skiftevis indlæg af de to undervisere. Der var hele tiden mulighed for at stille spørgsmål og komme med kommentarer hertil. Ved anden modul var spørgelysten større en på første, da vi kursusdeltagere tilsyneladende havde lært hinanden bedre at kende.

Det generelle indtryk af kurserne er, at de var lære- og udbytterige. Det eneste umiddelbare minus ved de to moduler var, at de blev afholdt i Ebletoft. En køn liggende by, men ikke den mest centralt beliggende. Foreningen burde overveje, om nogle af dets kurser fremover kunne afholdes på Sjælland, eller som alternativ på Fyn, hvortil der er gode forbindelsesmuligheder fra alle landsdele.

Koordinering af ERFA-grupper
v/Nina Belcaid

Der har vist sig interesse for at oprette en erfaringsgruppe omkring revision af SAP R/3, som nu vil blive etableret. Interesserede kan stadig henvende sig til Tina Mollerup Laigaard på telefon 3529 2861.

Besvigelser i dansk erhvervsliv
Af statsautoriseret revisor Jesper Koefoed, KPMG

I 1997 offentliggjorde KPMG den hidtil mest omfattende undersøgelse af besvigelser i dansk erhvervsliv. Undersøgelsen omfatter svar fra 208 større virksomheder med en samlet omsætning på ikke under 250 mia. kr., 160.000 medarbejdere og 150 mia. kr. i aktiver.

Formålet med undersøgelsen var at fastslå arten og omfanget af besvigelser i Danmark samt fastslå, hvorledes virksomhederne opfatter og håndterer problemet med besvigelser.

Hovedresultaterne af undersøgelsen kan resumeres således:

- 29% af virksomhederne opfatter besvigelser som et problem i dagligdagen.

- 29% af virksomhederne har oplevet besvigelser det seneste år med et samlet estimeret tab på 162 mio. kr.
- Besvigelserne begås af såvel ledelsen (8%), medarbejderne (34%), og eksterne personer (58%). De største tab er dog rapporteret for besvigelser begået af ledelsen.
- Opdagelsen af besvigelser sker i 63% af tilfældenne som følge af virksomhedernes interne kontroller.

Tankevækkende er det dog, at opdagelsen i 30% af tilfældene sker ved en tilfældighed, og at der i 38% af tilfældene eksisterede advarselssignaler, som blev ignoreret.

Undersøgelsens resultater danner et godt grundlag for bestyrelsens/direktionens diskussion af virksomhedens risici i denne forbindelse, således at forebyggende foranstaltninger kan iværksættes. Undersøgelsens resultater kan endvidere anvendes som grundlag for controllers / interne revisorers indsats på dette område.

Det kan i mange tilfælde være velbegrundet at udarbejde en egentlig handlingsplan mod besvigelser. Handlingsplanen bør omfatte en forebyggende del, som bl.a. fokuserer på medarbejderoplysning om risici for besvigelser, etablering af hensigtsmæssige forretningsgange, kontrol af medarbejdere ved ansættelse samt holdningsbearbejdelse vedrørende etik og moral i virksomheden. Endvidere bør handlingsplanen omfatte forholdsregler, når skaden er sket eller der foreligger en mistanke herom. Eksempler på forholdsregler kan være udmeldelse af en ansvarlig for undersøgelsen, procedurer for sikring af aktiver og regnskabsmateriale, bortvisning/retsforfølgning af skadevolder, procedurer for kontakt til politi, forsikringsselskab, offentlige myndigheder og pressen.

Revision af homebanking systemer
Af kontorchef Finn Morell, Unibank

Forstået i bredeste forstand vil denne overskrift bringe revisorerne vidt omkring. Der er mange risici, som skal afdækkes, og der er mange parter involveret. For at overskue problematikken har jeg i denne artikel valgt en 'geografisk' opdeling af kontrollerne:

- hos kunden
- i datacentralen
- transmission
- i pengeinstituttet.

Hos kunden

For at kunne anvende disse systemer kræves at kunden har investeret i en PC af en vis størrelse og med tilknyttet modem.

De systemer, som leveres til kunden ved tilmelding til homebanking, er ofte et antal serviceprogrammer, som kan bruges på PC'en uden opkobling, og programmer som skal anvendes i forbindelse med selve bankforretningerne.

Servicesystemerne er typisk skatte- beregningsprogrammer, budgetprogrammer og andre økonomiprogrammer, men kan være alt muligt andet som vinkartoteker o.lign.

Er disse serviceprogrammer risikofyldte nok til at være væsentlige for revision ?

Jeg tror det næppe. Det tab banken kan påføres består af et imagetab, som kan være vanskeligt at beregne. Når man ser, hvad der i øvrigt bliver trykt i aviserne om PI'erne og deres systemer uden at det får den store imagemæssige betydning, så kan en fejl i et budgetsystem nok klares med en beklagelse og et hurtig rettelse. Endvidere vil eventuelle fejl i program- merne allerede være fundet og rettet.

Noget ganske andet er de programmer, som installeres på kundens PC til brug for bankforretninger med PI'et. De sendes til kunden på CD eller disketter, og kunden skal derefter selv installere dem. Risici i forbindelse med disse programmer er, at de ikke fungerer, som kunden forventer det, og det kan give alvorligere image-tab, og at de kan misbruges, hvilket kan medføre direkte tab.

Allerede ved installationen kan kunden få problemer. I teorien er det nemt, men ofte er det et område med store problemer. Dels fordi det tit er uerfarne (edb-mæs- sigt) mennesker, der udfører installa- tionen, og dels fordi der meget nemt kan opstå konflikter med andre kommunikationsprogrammer, som i forvejen ligger på PC'en. Uanset hvad der er grunden, vil PI'ets programmel få skylden, og kunden vil opleve et dårligt produkt.

Efter vellykket installation skal program- met fungere hver gang kunden ønsker det (inden for den lovede oppetid). Ellers vil produktet også blive opfattet dårligt.

Kontrollerne, som skal revideres på disse områder er, at det udsendte programmel bliver gennemgået og testet inden det sendes ud, at udsendelsen er vedlagt en god brugervejledning (gerne med illustrationer) - både til installation og til den efterfølgende anvendelse, og endelig er en on-line 'hotservice' vigtig. Kunden skal kunne få hurtig hjælp, hvis noget går galt.

Forsendelsesproceduren skal omfatte viruskontrol af disketter eller CD-rom. Hvis det utænkelige skulle ske, at PI'et får spredt virus ud til kunderne, er image-tabet nok til at tage og føle på !

Større risici end de hidtil omtalte image- tab er de direkte tab, som kan påføres PI'et, som følge af misbrug eller fejl i de beløbsmæssige transaktioner.

Da datacentralen stoler på, at trans- aktionerne stammer fra den kunde, som kender bruger-ID og password, er det nødvendigt, at der også hos kunden er kontroller i forbindelse med edb-anvendelsen.

De stærke edb-kontroller, som anvendes i datacentralen, kan nok ikke forventes, at være på plads i de private hjem. Set ud fra et sikkerhedsmæssigt synspunkt alene, vil det være ønskeligt, at kundens PC ikke er koblet op mod andet end datacentralen. Hackere har i TV vist, at det er muligt via en tilfældig Internet adgang, at skaffe sig adgang til brugerens password og banksystemer, og derved overføre penge til egne konti. Men da de fleste kunder ønsker, at blive koblet op mod Internettet, og PI'erne støtter dette ved også at udbyde homebanking over Internettet, er denne kontrol i praksis illusorisk.

I mange tilfælde vil kunden ikke engang være særlig 'kontrolminded'. PC'en vil stå frit fremme, koblet op til Internettet, og den vil blive benyttet af familiens unge mennesker og deres kammerater. For nylig kunne man i et 'Komputerblad' læse om anvendelse af makroer. Som et af eksemplerne i artiklen var nævnt, at man til brug for 'homebanking' kunne lægge bruger-ID og password ind i en makro, hvorved man blot ved et enkelt tasta- turtryk kunne sende sine transaktioner til banken.

Hvilke kontroller kan så eliminere eller minimere risiciene ?

Det væsentligste er, at password, som anvendes til bankforretninger, ikke findes i klar tekst på harddisken. Det skal systemet sikre, men derudover skal kunden ved tilmelding til systemet modtage en skrivelse, der påpeger hvilke risici, der er i forbindelse med 'homeban- banking', og hvilke forholdsregler der bør tages.

Skrivelsen bør som minimum indeholde anvisninger for

1. brug af kodeord til PI'et
2. sikring af PC'en ved opstartadgangskode
3. sikker opbevaring af programmer og backup

4. kritisk vurdering af andet programmel, der hentes ind fra Internettet
5. viruskontrol
6. spærring ved brudt kodeord eller ulovlig kopiering af programmel.

Ved revisionen gennemgås procedurer- ne, og indholdet af skrivelsen vurderes.

I datacentralen

Her 'bestemmer' datacentralen selv sikkerheden, så her bør være et højt kontrolniveau. De generelle edb-kontroller skal være på plads, og revisionen skal omfatte eventuelle routere, firewalls og andet netværks-udstyr, som skal være sat op i overensstemmelse med datacentralens politik.

En del af de anvendte systemer er de samme, som normalt anvendes til transaktioner, der fødes i PI'et. Derfor bør sikkerhedskrav for de PC-skabte transak- tioner være mindst lige så højt, som det er for filialskabte transaktioner. Det vigtigste er opnå sikkerhed for, at mod- tagne transaktioner kommer fra den kunde, som de udgiver sig fra at komme. Kunden identificeres ved en bruger-ID, og i dag bekræftes denne bruger-ID normalt ved brug af et password, som kunden selv har bestemt. (Da password ikke er en speciel stærk identifikation arbejdes med at indføre andre identifikations- metoder, som f.eks. chipkort). Kon- trollerne i datacentralen er, at kundens bruger-ID skal være kendt, og det anvendte password skal være korrekt. Password må endvidere ikke være kendt i datacentralen, hvilket vil sige, at det skal opbevares krypteret, men såfremt det sædvanlige adgangskontrolsystem anvendes (RACF el. lign.) er det ikke noget problem. Andre kontroller som tvungent skift af password hver 30. dag eller kontrol med, at kunden ringer op fra et forud defineret telefonnummer kan etableres, men det strider ofte mod pengeinstituttes politik, hvor man ønsker at kunden skal kunne bruge systemet fleksibelt (Internettet).

En væsentlig kontrol er udsendelse af fysiske kontoudskrifter med aftalte intervaller, som kan være for hver bevægelse, en gang om måneden eller mere, men helst ikke for stort. Ganske vist kan kunderne i 'homebanking' systemet selv se bevægelserne på kontiene og derigennem føre kontrol, men ikke alle vil gøre det, og i hvert fald ikke på konti, som kunden ved ikke bliver benyttet. Eventuelle fejl (eller misbrug) på den type konti vil ikke blive opdaget i tide uden udsendelse af kontoudskrifterne.

Revisionen består i, at vurdere om kontrollerne efterlever politikken, og at de fungerer (test).

Når brugeren er identificeret behandles selve transaktionerne. De væsentligste transaktioner er de beløbsmæssige. Der skal være kontrol med kontonumre og med beløb. Kontonumre til debitering skal være kundens egne, eller fuldmagtsregistrerede konti, men der er kontotyper, som ikke må anvendes (pensionskonti). Beløbsmæssige kontroller skal sikres mod uønskede overtræk på kontiene. Bedst er en direkte overtrækskontrol, men som minimum bør der være en maksimum-beløbsgrænse i systemet. Overførsel til andre konti kan sikres ved, at kunden kun kan overføre mellem egne konti eller at der oprettes en liste for hver kunde med kontonumre, som der kan overføres til. Det vil sikre mod at eventuelle hackere kan få penge ud af systemet, men igen er det en kontrol, som ofte ligger ud over det ønskede sikkerheds- niveau, da PI'et ønsker at kunden skal kunne overføre penge til alle konti i alle pengeinstitutter.

Revisionen består i, at undersøge og vurdere om de etablerede kontroller er i overensstemmelse med PI'ets politik, og at teste at de fungerer.

Transmission

En potentiel risiko for datamanipulation er, at transaktioner kan manipuleres under transmission. Risikoen er tilstede i alle tilfælde, men anvendes Internettet til transportvej, er der en stor gruppe skumle personer liggende på lur, for at finde svagheder, som de ikke vil tøve med at udnytte.

Kryptografering eller mac-beregning er derfor en kontrol, som ikke kan undvæ- res. Teoretisk kan andre kontroller anvendes, som f.eks. at kunden efter at have sendt transaktioner til datacentralen, ringer til PI'et og meddeler, hvad trans- aktionen omfatter, men det er en tung løsning, som nok ikke vil blive benyttet.

Kryptografering/MAC-beregning revideres ved gennemgang af systembeskrivelsen, og test, hvor man vurderer kontrollernes effektivitet herunder nøglernes længde og opbevaring.

I pengeinstituttet

Pengeinstituttet bør have en politik for hvem, man vil tilbyde systemet. Kunderne bogfører direkte i systemerne på egne og andres konti, uden at nogen i PI'et ser, at det foregår. Først hvis noget går galt vil transaktionerne blive gennemgået, og det kan være for sent. En anden risiko er, at en eventuel fejloverførsel ikke kan tages tilbage uden kontoejers samtykke. Hvis en medarbejder i PI'et kommer til at lave en manuel fejloverførsel lykkes det som regel, at skaffe pengene tilbage ved hjælp af et par telefonsamtaler og måske et brev. Men hvis kunden eller en der misbruger hans password foretager en forkert overførsel, er der ingen vej uden om modtagerens velvilje, når pengene skal hentes tilbage.

Derfor bør revisionen omfatte en gennemgang af regler for oprettelse af homebanking adgang - herunder aldersgrænse, og revisionen skal omfatte en stikprøvevis kontrol med, at reglerne er overholdt.

Der skal endvidere være udarbejdet en skriftlig aftale med kunden, som specificerer hvad kunden og PI'et er ansvarlige for. Denne aftale skal gennemgås og vurderes, og det skal kontrolleres, at der er underskrevne aftaler tilstede for 'homebanking' adgangene.

Forretningsgangen for fremsendelse af PIN-koder til kunden skal vurderes med henblik på at sikre, at de altid sendes direkte til den korrekte kunde.

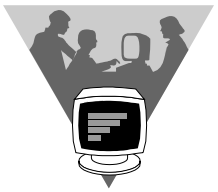
Eksterne krav

Området er omfattet af en række eksterne krav, og revisionen bør omfatte handlinger, der sikrer disse kravs overholdelse. De væsentligste regler fastlagt i 'kodeks for homebanking', og systemerne er endvidere omfattet af betalingskortloven.

År 2000

Som lidt ekstra krydderi til dette spændende område vil jeg til slut nævne årets (og næste års) hit - år 2000 problematikken. Er disse systemer og hardwarekomponenter omfattet af datacentralernes og PI'ernes år 2000 planlægning og test, således at systemerne er parate og aftestede i god tid inden det afgørende årsskifte ? Har PI'erne taget stilling til, om kunderne skal have meddelelse om, hvilke krav de skal leve op til på deres PC'er ? Vil man eventuelt sende kunden en 'testplan' for aftestning af 'homebanking' systemet ? Hvordan vil man tackle de kunder, som ikke klarer år 2000 overgangen (altså hardwaremæssigt) ?

Revisorerne bør også her vurdere beslutningerne for området og de etablerede planer.



Datawarehouse

Af Claus Deela, HD(IØ), Told- og Skatterevisionen

Artiklen er baseret på artikel i Internal Auditor/februar 1998 [1] og formålet er en kort indføring i begrebet datawarehouse og sikkerhed ved samme. Hovedbudskab er at sikkerhed og datawarehouse udmærket kan forenes.

Hvad er datawarehouse (DW)
Et datawarehouse (DW) er i følge artiklen en samling af integrerede databaser designet til beslutningsstøtte for ledelsen samt problemløsning/analysering ved hjælp af en kopi af organisationens egne data.

Der foretages kopiering af data fra produktionsmiljøet med "real life" data til et isoleret miljø, hvor virksomhedens data gøres tilgængelige for de sammenhænge og informationsbehov, som brugeren måtte have behov for og lov til. Data kan lagres på nederste dataniveau og/eller som sumtal. Både produktionsmiljøet og datawarehouse forvaltes driftsmæssigt typisk af en IT-afdeling, hvilket indicerer at DW formentlig er mest fremherskende i større og mellemstore organisationer. Et DW kan medvirke til at minimere den tid IT-afdelingen ellers anvender på at forsyne organisationen med organisationens egne data i forskellige opstillinger og sammentællinger.

Hele tankegangen er som sådan ikke ny, herunder har jeg bl.a. stiftet bekendtskab med emnet i begyndelsen af 80-erne. I den mellemliggende periode er den nødvendige datalagring (diske mm.) blevet endnu billigere, mere effektiv og hurtigere, og endvidere har det nødvendige programmel ligeledes gennemgået en stor udvikling.

Gennemgang af sårbarhed og styring af datawarehouse

Sikkerhedsaspekter bør altid være fremtrædende, hvilket ligeledes er gældende med hensyn til et datawarehouse. Der bør gennemføres reviews af administrationen af DW, og hovedvægten bør lægges på det forebyggende arbejde.

Der er efterfølgende vist et sammendrag med tilhørende stikord til et 7-punkts program fra artiklen til brug ved gennemgang af sårbarhed og styring af datawarehouse.

1. Identificering af data
Komplet oversigt over alle tilgængelige data i i datawarehouse (inventarliste).

2. Klasificering af data
Sikkerhedsbehov med hensyn til data's fortrolighed, integritet og tilgængelighed.

Forslag om anvendelse af tre kategorier af data:

- Fælles (public) / mindst sensitive data (alle har adgang).
- Fortrolige / moderat sensitive data (tilgængelig når nødvendigt for arbejdsudførelse).
- Top hemmelige / mest sensitive data (tilgængelig for brugere med ubegrænset adgang).

3. Kvantificering af data's værdi
Værdien kan ses som omkostningen ved (1) rekonstruktion af tabte data, (2) rekonstruere datasammenhænge, (3) forringet beslutningsgrundlag, (4) omkostninger ved afsløring af fortrolige data.

4. Identificer sårbarheder
Identificering af sårbarheder i datawarehouse miljøet, herunder åbenhed i datastrukturen, den menneskelige faktor, samt interne og eksterne trusler.
Specifik teknisk sikkerhed (i det anvendte databaseprogrammel, backup mm.).

- Identificering af de mest effektive sikkerhedsoranstaltninger og de tilhørende omkostninger (brugerprofiler, adgangskontroller, kryptering af data, segmentering af data osv.).

- Vælg de nødvendige sikkerhedsforanstaltninger

Hovedmålet er her, at omkostningerne til at imødegå tab o.lign. af data ikke overstiger den maksimale værdi som tabet af data repræsenterer.

- Evaluering af sikkerhedsforanstaltninger
  Tænk på at alle foranstaltninger kan brydes, samt at de til tider ikke er effektive nok.

Det er vigtigt, at brugerne får den rette forståelse for den nødvendige sikkerhed.

Afrundning
Af revisionsmæssige aspekter er det min opfattelse, at indsatsen primært skal lægges i.f.m. de generelle edb-kontroller, herunder betryggende funktionsadskillelse og vedligeholdelse af hvilke data, der indgår i DW. Selvfølgelig sker der et skift i organisationens edb-anvendelse, men i de rigtige hænder repræsenterer skiftet kun en mindre risiko, som med hensyn til organisationens ve og vel ikke vurderes at være af nævneværdig betydning. Førnævnte er dog ikke gældende, hvis organisationens eneste aktiv er fortrolig information, og endnu værre hvis den kun er opbevaret i et datawarehouse. En faldgrube kan fx. være at organisationen ikke ender op med at være ejer af data i datawarehouse, men at ejerskab bliver "hængende" i IT-afdelingen, der typisk tager de indledende tiltag i.f.m. etableringen af et DW.

Det skitserede 7-punkts program kan anvendes til opstilling af et omkostningsbevidst sikkerhedsmiljø omkring et datawarehouse, hvor der er balance mellem organisationens udbytte og omkostninger.

IIA International har flere udviklingsprojekter igang, herunder et om Data Warehousing / Data Mining, hvilket kan følges på IIA's hjemmeside under 'The IIA Research Foundation'. Derigennem forventes der opstillet information til interne revisorer om et revisionsprogram til evaluering af risici og opstilling af nødvendige kontroller i et DW-miljø. Forventet færdiggørelse af rapport er angivet til første kvartal 1999.

Afslutningsvis skal der lyde en appel til vores læsere om, at såfremt de selv har praktisk erfaring med revision af et datawarehouse, så er de meget velkommen til at henvende sig til redaktionen med henblik på endnu en artikel om emnet.

Kilder

I.Datawarehouse Control & Security, Slemo Warigon, Internal Auditor Februar 1998

Opslagstavlen

Foreningen af Interne Revisorers bestyrelsesmedlemmer:

Søren Kongsbo (formand)	***Post Danmark***
Tage Rasmussen	***Handelshøjskolen, Århus***
John Rasmussen	***Den Danske Bank***
Peter Birkholm Laursen	***Handelshøjskolen, København***
John Tyrrestrup	***FDB***
Frede Bech Poulsen	
Ane Marie Christensen	***Unibank***
Thorkild Jakobsen	***Told-og Skatterevisionen***

Jobannoncer
Jobannoncer kan bringes i INFO for kr. 1.500. Annonceudkast sendes til: Bente Christensen, Post Danmark, Bernstorffsgade 23, 1577 København V.

Næste nummer af bladet udkommer i april 1999.

CIA-eksamen
Der er i november måned afholdt CIA-eksamen, redaktionen ser frem til at høre om resultatet, som dog først foreligger i februar 1999.

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

Indlæg om svig
Indlægget kan sendes til Tina M. Laigaard og kan evt. bringes anonymiseret.

Oplysninger om mærkedage
Oplysninger om mærkedage bedes meddelt til Bente Hallberg, Post Danmark, Intern Revision på telefon 3375 6408.

Oplysninger om IIA
Hvis man ønsker oplysninger om
Foreningen af Interne Revisorer
henvises til Bente Christensen, Post Danmark, Intern Revision på ☎ 33 75 64 02 .

Oplysninger om diverse homepages

IIAs homepage	www.theiia.org
	www.itaudit.org
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