IT-revisjon

Klassisk IT-revisjon

Cobit

ITIL

Dokumentasjon av balansen

- Nøyaktighet og gyldighet har dere drøftet
- Fullstendighet har de fleste ikke tenkt på (utfordring: gjeld)
- Kilder
  - BOL §11, FOR-01.12.2004 nr 1558
  - NOU 2002:20
  - Tvedt: Ny bokføringslov
  - Norsk regnskapsstiftelse GBS
  - RF-1052 (Avstemmingsskjema for egenkapital m.v.)
  - Jf Revisors håndbok ISA500 p. 9: revisjonsbevis
- Ikke bare sitater fra loven
  - Eksempler og konkretisering
  - Praktiske utfordringer ved etterlevelse av reglene

E-post som bevis (regnskapsmateriale)

- Autentisk ?
  - Autorisert prosedyre
  - Integritet
- PDF (GBS 02-05-2006-4)
  - Ikke "direkte redigerbart", men . . .
- Elektronisk signatur
  - E-signaturloven LOV-2001-06-15-81 m endringslover
    - §3 definisjoner
  - Asymmetrisk kryptering, off / priv nkl
    - Integritet: signer med utstederens priv nkl
  - Konfidensialitet (sign m mottagers off nkl lite relevant for bevis-spørsmålet)
  - Tilgjengelighet: Problemer?
  - Praktisk gjennomføring

IT-relatert risiko

- Revisjon er risikostyrt
- Risiko som skyldes bruk av IT (foreslå med eksempler)
  - Riktig regnskap?
  - Lovbrudd?
  - Effektiv drift?

Revisjonskonseptet

- Tester av kontroller (tidl.: systemtest)
- substanskontroller
  - detaljtesting av transaksjoner og saldoer
  - analytiske kontrollhandlinger
- Vurdering av IK
  - virkningen av IT
    - kontrollsporet
    - Generelle / applikasjons-kontroller

Metodeutvikling i finansiell revisjon

- Bekrefte regnskapspostene
  - i årsregnskapet
- Transaksjonskontroll / bilagskontroll
  - bokføringsarbeidet
- Test av kontroller
  - vekt på systemer og internkontroll
- Balansekontroll: tester uavhengig av bokf
  - eksistens og tilhørighet

Gir IT forbedret IK?

- Maskinelle kontroller
  - hyppige, konsistente, bedre informasjon
- Kontrollrisiko kan også øke
  - systemers tilgjengelighet
  - kontrollspor
  - redusert menneskelig involvering
  - systematiske feil vs. tilfeldige feil
  - uautorisert tilgang
  - datatap
  - mindre arbeidsdeling

Risikoreduksjon ?

- Generelle kontroller
  - IT-ledelse
  - Arbeidsdeling
  - Systemutvikling
  - Fysisk og on-line sikkerhet
  - Reservedrift
- Applikasjonskontroller
  - Inndatakontroll og validering
  - Behandlingskontroll
  - Utdatakontroll

IT-baserte IK-verktøy (i tillegg til styringsrapportene)

- Datagranskning
- Data og prosessgranskining
  - logger
  - spørrespråk og rapportgeneratorer
- Rutinemessige feilkontroller og avstemminger
  - kontrollpunkter
  - restartpunkter

IT-ledelse

- Forankret hos toppledelsen
- Systemutvikling
- Programmering
- Databiblioteker (dataressurser)
- Sikkerhetsadministrasjon
- Drift

Bevisinnsamling

- Generell revisjonsprogramvare
- Annen programvare
- Programgranskning, testdata og programsammenligning
- revisjon i sann tid
- Ytelsesmåling

Bevisvurdering

- Vurdere aktivabeskyttelse og dataintegritet
- Vurdere systemenes
  - målrettethet
  - kostnadseffektivitet

Kontrollmiljøet

- Arbeidsdeling
  - IT-avd / brukerne
  - innen IT-avd
- Ansvar
- Personalledelse
- Rutiner

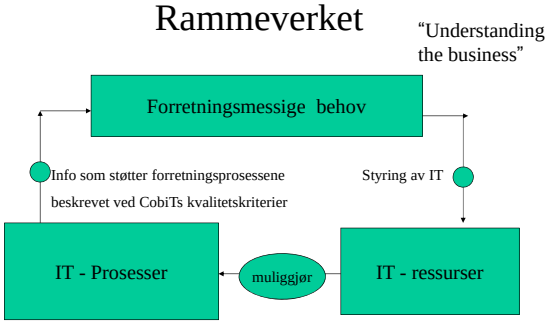
Sikkerhetskontroller (som påvirker revisjonen)

- Forebyggende
  - sikkerhetsledelse, fysisk s., biblioteksk., tilgangskontr.
- Oppdagende kontroller
  - overvåkning, autentisering, systemlogger
- Gjenvinnende kontroller
  - brannslukning, forsikring, reservedrift, gjenvinningsplan og gjenvinningsprosedyrer

Fra klassisk IT-revisjon til Cobit

- Klassisk IT-revisjon fokuserte på
  - Gode IT-systemer
    - Programmene
    - Maskinvare
    - Rutinene
    - Etterhvert også på dataene
- Cobit fokuserer på
  - Organisasjonens forutsetninger for å skape gode IT-systemer

Rammeverket



Ledelsen må

- Bestemme investeringsomfang / ressursbruk
  - sikkerhet og styring
  - risiko vs styringsinvestering
- utvikle og iverksette IK
  - fordelaktig med et rammerverk
- for å forvalte selskapets verdier riktig

Styring (kontroll)

- Policier, prosedyrer, praksis, organisasjon
- som gir
- rimelig sikkerhet for
- oppnåelse av forretningsmål
  - og uønskede hendelser motvirkes eller oppdages og korrigeres

Kontrollmål (styringsmål)

- Utsagn om ønsket resultat, som
- oppnås ved å implementere en kontrollprosedyre
  - målt mot kontrollmål
- i en IT-aktivitet
  - som definert innen fire CobiT-områder

Forretningsmessige behov: Kvalitet

- Riktig kvalitetet (jf. Kvalitetsrevisjon)
  - "negativ": feilfritt, pålitelig
  - Ikke så mye "posistiv": tiltrekning, skjønnhet, ytelse utover forventning
- balansert mot kostnad
- målt etter levering
  - (tilgjengelighet, brukbarhet og "kundeperspektiv")

Forretningsmessige behov: IK

- Effektivitet
- Informasjonspålitelighet
  - objektivitet, nøytralitet, prognosekraft, fullstendighet
- Samsvar med lover og regler

Kriterier for informasjonskvalitet

- Målrettethet
- Kostnadseffektivitet (økonomisk ressursforbruk)
- Sikkerhet
  - Konfidensialitet
  - Integritet
  - Tilgjengelighet
- Samsvar
- Pålitelighet

IT-ressursene

- Data
- Applikasjonssystemer
- Teknologi
  - maskinvare, OS, DBMS, . .
- Fasiliteter
- Mennesker
  - kompetanse, miljø og ledelse

Cobit-områdene

- Planlegning og Organisering
- Anskaffelse og implementering
- Levering og støtte
- Overvåkning

- Områdene deles i
  - IT-prosesser som igjen deles i
  - IT-aktiviteter

ITIL
IT Infrastructure Library

- Syv områder
  - tjenestestøtte
  - tjenestelevering
  - styring, planlegning og implementering av tjenester
  - Sikkerhet
  - Kontroll på infrastrukturen
  - Applikasjoner
  - Forretningsperspektivet

Metode

- Erfaringsbasert: Best Practice
- Engelsk ++
- I forhold til Cobit:
  - noe mer fokus på drift, mindre på strategi
  - IT-prosess
    - Cobit: en prosess for styring av IT
    - ITIL: en IT-støttet applikasjon
- ISO/NS 17799: standard for informasjonssikring og -kvalitet

Tjenestestøtte

- Beskriver prosesser for daglig
  - støtte
  - vedlikehold
  - av IT-tjenestene

Tjenestelevering

- Prosesser for
  - planlegging og levering av it-tjenester
  - langsiktige muligheter for forbedret bruk

Styring, planlegning og implementering

- Forbedre styringen av it-tjenestene
- Virkninger på organisasjonen av IT
  - Kulturelle
  - Organisatoriske
- IT-visjon
- IT-strategi

Sikkerhet

- Valg av sikkerhetsnivå
  - for informasjon
  - for it-tjenestene
- plan for risikohåndtering

Kontroll på infrastrukturen

- Alle sider ved tele og datatrafikk
- testing, implementering og optimalisering av infrastruktur

Applikasjoner

- Styring og håndtering av applikasjoner
- Alle faser i applikasjonens livssyklus
  - definere behov
  - systemutvikling og programmering
  - implementering
  - vedlikehold
  - utfasing

Forretningsperspektivet

- Organsisasjonens måloppnåelse
- Etablere mål
- Spre kunnskap om og kjenne mål
- Kostnadseffektive løsninger