

IT-revisjon

Siste forelesning Rev3576

Klassisk IT-revisjon

Cobit

ITIL

1

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.)
 - Revisors håndbok RS500 p. 9
- Ikke bare sitater fra loven
 - Eksempler og konkretisering
 - Praktiske utfordringer ved etterlevelse av reglene

2

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

3

IT-relatert risiko

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

4

Revisjonskonseptet

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

5

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

6

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

7

Risikoreduksjon ?

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

8

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

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

9

IT-ledelse

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

10

Bevisinnsamling

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

11

Bevisvurdering

- Vurdere aktivbeskyttelse og dataintegritet
- Vurdere systemenes
 - målrettethet
 - kostnadseffektivitet

12

Kontrollmiljøet

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

13

Sikkerhetskontroller (som påvirker revisjonen)

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

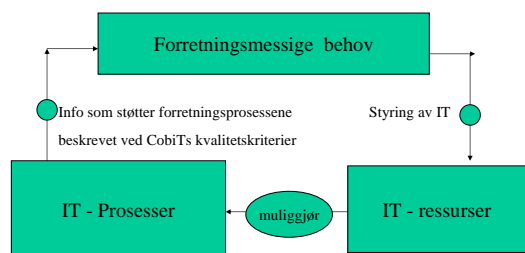
14

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

15

Cobits Rammeverk “Understanding the business”



16

Ledelsen må

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

17

Styring (kontroll)

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

18

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

19

Forretningsmessige behov: Kvalitet

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

20

Forretningsmessige behov: IK

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

21

Kriterier for informasjonskvalitet

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

22

IT-ressursene

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

23

Cobit-områdene

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

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

24

ITIL IT Infrastructure Library

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

25

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

26

Tjenestestøtte

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

27

Tjenestelevering

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

28

Styring, planlegging og implementering

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

29

Sikkerhet

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

30

Kontroll på infrastrukturen

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

31

Applikasjoner

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

32

Forretningsperspektivet

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

33