God IT-skikk

ISACA, Norway Chapter
Den norske dataforening
(Revisors håndbok)

Grunnlag

- generelt aksepterte grunnprinsipper for sikkerhet og kontroll
- å etablere et tilfredsstillende kontroll- og sikkerhetsnivå er vanskelig
- Objektive standarder for
  - god intern kontroll på IT-siden er derfor et nyttig verktøy for
    - bedriftenes ledelse
    - kontrollorganer
    - revisor
- Asl/Asal§6-12,14 styrets og adm dir ansvar for den interne kontroll
- Selskapslovens paragraf 2-13 og 2-18
- Økonomireglement for Staten, § 15 og § 21.

Grunnleggende retningslinjer for God IT-Skikk (nr.0)

- utvikling og vedlikehold av IT-systemer
- drift av IT-systemer
- bruk av IT-systemer
- nettverk
- informasjonsutveksling
- ekstern informasjonsbehandling
- katastrofeplanlegging.

Dokumentasjon av IT-systemer(nr 1)

- Retningslinjer for utforming av:
  - brukerdokumenstasjon
  - systemdokumentasjon
  - driftsdokumentasjon

Tilgangskontroll (nr 2)

- ledelsens styring
- holdninger
- tap av informasjon og misbruk av ressurser
- aktivitetsoppfølging
- beskytte brukere mot unødig mistanke
- arbeidsdeling
- styring av IT-bruk innenfor administrasjon av brukere, sikkerhetsrutiner,
- sanksjoner og etterkontroll.

Tilgangskontroll (nr 2)

- 1.4 Aktuell lovgivning
  - IKT-forskriften
  - Personopplysningsloven
  - Strl §145.2
- 2.6 Beskytte brukere mot uberettiget mistanke

Kontinuitet i den operasjonelle drift av sentrale og desentrale IT-systemer (nr 3)

- ansvarsforhold
- situasjons- og behovsanalyser, herunder risikoanalyser og konsekvensanalyser
- forebyggende tiltak
  - avtaler, dokumentasjon, sikring av data, beredskapsplaner og fysisk sikring
- endringskontroll, prosedyrer, driftsplanlegging,
- logging
- driftsforstyrrelser
- beredskapsplan
  - organisering, situasjonsbedømmelse, manuelle rutiner, alternativ datakraft samt gjenoppbygging av egen datakraft og overgang til normal drift.
  - opplæring, testing og ajourføring av beredskapsplaner.

Endringsadministrasjon (nr 4)

- Styrt endring
- Organisasjon
- Rutiner
- IT-systemer

internettforbindelse (nr 5)

- Risiko
  - ulike tilknytningsformer
  - tjenestetyper
- Beskyttelse
- Teknikker
- Organisering og ansvar