



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Egenevalueringsskjema

for foretakets IT-virksomhet
basert på 34 COBIT prosesser

Dato: 26.01.2009

Versjon 5.0

Evalueringsskjema for foretakets IT-virksomhet

Oppdatert i henhold til CobiT 4.0

Rangering av prosess

Planlegging og organisering (POx):

| | | |
|------|--|--|
| PO1 | Definere en IT-strategi | |
| PO2 | Definere en informasjons-/systemarkitektur | |
| PO3 | Bestemme teknologisk retning | |
| PO4 | Utforme IT-organisasjonen | |
| PO5 | Forvalte IT-investeringer | |
| PO6 | Formidle ledelsens mål og retning | |
| PO7 | Personalledelse | |
| PO8 | Kvalitetsstyring | |
| PO9 | Vurdere risiko | |
| PO10 | Prosjektstyring | |

Anskaffelse og implementering (AIx)

| | | |
|-----|---|--|
| AI1 | Identifisere løsninger | |
| AI2 | Anskaffelse og vedlikehold av applikasjoner | |
| AI3 | Anskaffelse og vedlikehold av teknologisk infrastruktur | |
| AI4 | Utvikle og vedlikeholde prosedyrer | |
| AI5 | Anskaffelse av IT-ressurser | |
| AI6 | Endringsledelse og -håndtering | |
| AI7 | Installasjon og godkjenning av systemer | |

Leveranse og støtte (DSx):

| | | |
|------|--|--|
| DS1 | Definere og styre servicenivået | |
| DS2 | Styre tjenester fra eksterne IT-leverandører | |
| DS3 | Styring av ytelse og kapasitet | |
| DS4 | Sikre kontinuerlig service-/kriseplanlegging | |
| DS5 | Sikre systemsikkerhet | |
| DS6 | Identifisere og fordele kostnader | |
| DS7 | Brukeropplæring | |
| DS8 | Mottak for behandling av hendelser | |
| DS9 | Konfigurasjonshåndtering | |
| DS10 | Håndtering av problemer og hendelser | |
| DS11 | Håndtering av data | |
| DS12 | Fysiske omgivelser | |
| DS13 | Styring av driften | |

Overvåkning (MEx):

| | | |
|-----|-------------------------------------|--|
| ME1 | Overvåke og vurdere IT ytelse | |
| ME2 | Vurdere internkontroll | |
| ME3 | Sikre etterlevelse av eksterne krav | |

| | | |
|-----|---------------------|--|
| ME4 | Styring og kontroll | |
|-----|---------------------|--|

Foretakets navn :

Dato :

Underskrift :

| Grad av viktighet, rangering 1 til 34 | PO1 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|--|--|-------------------|-----|-----------|---|---|
| | | | | H | M | L |
| | Definere en IT-strategi | Ja | Nei | | | |
| | 1. Er IT-strategien forankret i foretakets øverste ledelse? | | | | | |
| | 2. Understøtter IT-strategien foretakets foretningmessige mål? | | | | | |
| | 3. Er det samsvar mellom IT-strategien og IT-virksomhetens operasjonelle mål? | | | | | |
| | 4. Er det etablert en prosess for periodisk oppdatering av IT-strategien? | | | | | |
| | 5. Er IT-investeringer basert på dokumenterte forretningsplaner? | | | | | |
| | 6. Er det etablert prosesser for å informere ledelsen om muligheter IT-teknologien åpner for som forretningsområdene i neste omgang kan dra fordel av? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO2 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|--|--|-------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Definere en informasjons-/systemarkitektur | | | | | |
| | 1. Har IT-virksomheten en dokumentert data- og funksjonsmodell? | | | | | |
| | 2. Er det prosedyrer som sikrer integritet og konfidensialitet i datamodellen? | | | | | |
| | 3. Er IT-virksomhetens tekniske arkitektur dokumentert? | | | | | |
| | 4. Samsvarer data- og funksjonsmodell og teknisk arkitektur med foretakets forretningsprosesser? | | | | | |
| | 5. Er systemer gradert inn i ulike nivåer av kritiskhet? | | | | | |
| | 6. Er ansvarlig oppnevnt for de enkelte systemer og applikasjoner? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO3 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | | | H | M | L |
| | Bestemme teknologisk retning | Ja | Nei | | | |
| | 1. Er det etablert standarder for infrastruktur, maskin og programvare som understøtter foretakets forretningsplan? | | | | | |
| | 2. Er det etablert tiltak som sikrer at anskaffelser følger foretakets etablerte standarder for maskin og programvare? | | | | | |
| | 3. Er det etablert en rolle for å overvåke relevant teknologisk utvikling? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO4 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|---------------------------------------|---|-------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Utforme IT-organisasjonen | | | | | |
| | 1. Gjennomfører foretaket en vurdering av IT-organisasjonen slik at funksjoner og ansvarsforhold samsvarer med vedtatte mål? | | | | | |
| | 2. Gjennomføres det jevnlig vurderinger av om organisasjonsstrukturen i IT-virksomheten er hensiktsmessig? | | | | | |
| | 3. Er det etablert funksjoner som sikrer effektiv koordinering mellom IT-leveranser og foretakets forretningsmessige behov? | | | | | |
| | 4. Er tilstrekkelige IT-ressurser tilgjengelig for utføring av IT-virksomhetens oppgaver? | | | | | |
| | 5. Har IT-virksomheten utarbeidet funksjons-/rollebeskrivelser for de ulike arbeidsoppgaver, hvor det fremgår hvilket ansvar den enkelte har? | | | | | |
| | 6. Er det etablert eierskap og ansvar for IT-risiko, sikkerhet og etterlevelse av lover og forskrifter på ledelsesnivå? | | | | | |
| | 7. Er det etablert eierskap til de enkelte elementer i IT-virksomheten? | | | | | |
| | 9. Er ansvar for sikkerhet, kvalitet og internkontroll i IT-virksomheten ivaretatt? | | | | | |
| | 10. Har IT-virksomheten vurdert og etablert arbeidsdeling av funksjoner i kritiske prosesser? | | | | | |
| | 11. Har IT-ledelsen vurdert om tilstrekkelig myndighet er delegert til den enkelte, slik at myndighet står i forhold til ansvar? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO5 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|--|---|-------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Forvalte IT-investeringer | | | | | |
| | 1. Er det etablert en prosess for å utarbeide budsjett og årsplaner for IT-virksomheten? | | | | | |
| | 2. Er IT-virksomhetens budsjett koordinert med foretakets budsjett og prioriteringer? | | | | | |
| | 3. Er det etablert en prosedyre for kontroll og rapportering av avvik fra budsjettet for IT-virksomheten? | | | | | |
| | 4. Gjennomføres det kost-/nyttevurderinger og etterkontroll av større IT-investeringer? | | | | | |
| | 5. Er det etablert kontroller som sikrer at lisenshåndtering er ivaretatt? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO6 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Formidle ledelsens mål og retning | | | | | |
| | 1. Er det etablert en plan/strategi som sikrer at IT-virksomhetens målsetninger og beslutninger formidles på en effektiv måte? | | | | | |
| | 2. Har foretaket utarbeidet og formidlet etiske retningslinjer? | | | | | |
| | 3. Er det definert og dokumentert kvalitetsmål for IT-leveranser som er i samsvar med IT-virksomhetens kvalitetskrav? | | | | | |
| | 4. Har foretaket utarbeidet strategi og retningslinjer for sikkerhet og er disse gjort kjent i foretaket? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO7 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Personalledelse av IT-virksomheten | | | | | |
| | 1. Er det laget opplæringsplaner som sikrer at ansatte i IT-virksomheten får kunnskap om og forståelse av foretakets forretningsområde? | | | | | |
| | 2. Er nøkkelpersonell definert og identifisert slik at man kan etablere tiltak for å minske nøkkelmansrisiko? | | | | | |
| | 3. Har foretaket etablert et opplæringsprogram for ansatte som inneholder sikkerhetsforståelse? | | | | | |
| | 4. Er det etablert prosedyrer som ivaretar sikkerhet ved opphør av ansettelsesforhold eller endring av arbeidsoppgaver? | | | | | |
| | 5. Finnes det et program for rekruttering og utvikling av medarbeidere basert på dokumentert kompetansebehov? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO8 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|--|---|-------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Kvalitetsstyring | | | | | |
| | 1. Har foretaket etablert kvalitetsmål for de enkelte deler av IT-virksomheten, og er disse knyttet opp mot foretakets øvrige mål? | | | | | |
| | 2. Har foretaket etablert prosedyrer for hvordan IT-virksomheten skal følge opp at kvaliteten på leveransene er i henhold til de fastsatte kvalitetsmålene? | | | | | |
| | 3. Benyttes resultater fra kvalitetsmålingene i en forbedringsprosess? | | | | | |
| | 4. Har foretaket utpekt ansvarlige som skal sikre organisasjonens kvalitetsstyring? | | | | | |
| | 5. Har de kvalitetsansvarlige en uavhengig rolle i forhold til operativt ansvarlige? | | | | | |
| | 6. Gjennomføres det uavhengig vurderinger av IT-virksomhetens leveranseevne og servicegrad? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO9 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|--|--|
| | | H | M | L | | |
| | Vurdere risiko | Ja | Nei | | | |
| | 1. Har foretaket inkludert vurdering av IT-risiko og styring og kontroll av IT-virksomheten i foretakets øvrige rammeverk for risikohåndtering? | | | | | |
| | 2. Har foretaket etablert en prosess for risikoanalyser av IT-virksomheten? | | | | | |
| | 3. Har foretaket etablert retningslinjer / metode for hvordan ny risiko skal identifiseres? | | | | | |
| | 4. Har foretaket etablert ansvarsfordeling for gjennomføring og oppfølging av risikoanalysen? | | | | | |
| | 5. Har foretaket fastsatt kriterier for akseptabel risiko forbundet med bruk av IT-systemene? | | | | | |
| | 6. Er det etablert tiltak som sikrer at det blir gjennomført systematiske vurderinger av forskjellige typer risiko som f. eks. innføring av ny teknologi, endringer, single point of failure, sikkerhet, lover, beredskap, organisasjon og grensesnitt? | | | | | |
| | 7. Har foretaket etablert tiltak som sikrer at risikoanalyse av IT-virksomheten gjennomføres minst årlig og ved større endringer? | | | | | |
| | 8. Blir risikovurderingene brukt som verktøy i utformingen av interne kontrollrutiner, strategiske planer, samt ved overvåkning og evaluering? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | PO10 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|--|--|-------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Prosjektstyring | | | | | |
| | 1. Foreligger det et rammeverk (prosjekthåndbok, prosjektmetode) for gjennomføring av prosjekter? | | | | | |
| | 2. Sikrer rammeverket at berørte parter involveres tilstrekkelig, med klar beskrivelse av roller, ansvar og myndighet for prosjektorganiseringen? | | | | | |
| | 3. Sikrer rammeverket at prosjektmål, omfang, avgrensning, og kost/nytte vurdering utarbeides som beslutningsgrunnlag for oppstart av prosjekt? | | | | | |
| | 4. Sikrer rammeverket tilstrekkelig kvalitet ved gjennomføring av prosjekter? | | | | | |
| | 5. Er det etablert prosedyre for endringskontroll ved gjennomføring av prosjekter? | | | | | |
| | 6. Sikrer rammeverket at det planlegges og rapporteres på et tilstrekkelig detaljeringsnivå (ressurser, avhengighet, milepæler, aktiviteter, risiko, avvik, økonomi, etc.) som gjør det mulig å fatte nødvendige beslutninger? | | | | | |
| | 7. Sikrer rammeverket tilstrekkelig kvalitet ved gjennomføring av prosjekter? | | | | | |
| | 8. Sikrer rammeverket tilstrekkelig vurdering og oppfølging av prosjektrisiko? | | | | | |
| | 9. Er det etablert prosedyrer og kontroller som sikrer overgangen fra utvikling til drift som blant annet skal inkludere testing, opplæring, dokumentasjon og godkjenning? | | | | | |
| | 10. Gjennomføres det en systematisk evaluering av gjennomførte prosjekter som ledd i en forbedringsprosess? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | AI1 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|--|--|-------------------|-----|-----------|--|--|
| | | H | M | L | | |
| | Identifisere løsninger | Ja | Nei | | | |
| | 1. Er det innført prosedyrer som sikrer at anskaffelse av programvare og maskinvare følger foretakets IT-strategi og innkjøpsprosedyre? | | | | | |
| | 2. Er det etablert tiltak som sikrer at alternative løsninger blir vurdert, også med hensyn til risiko, før man velger en bestemt løsning? | | | | | |
| | 3. Gjennomføres det kost-/nyttevurderinger, basert på forretningsmessige krav, som grunnlag for valg av løsning? | | | | | |
| | 4. Er det etablert tiltak som sørger for at de operasjonelle krav til løsninger blir ivaretatt med hensyn til ytelse, sikkerhet, pålitelighet og kompatibilitet? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | AI2 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Anskaffelse og vedlikehold av applikasjoner | | | | | |
| | 1. Er anskaffelse av IT-løsninger basert på foretakets behov for å oppnå sine forretningsmessige mål? | | | | | |
| | 2. Utarbeides kravspesifikasjoner i samarbeid mellom brukere, forretningsansvarlig (eier), IT-organisasjonen og andre berørte parter? | | | | | |
| | 3. Har foretaket prosedyrer som benyttes for utvikling, kjøp og implementering av IT-løsninger? | | | | | |
| | 4. Er det i kravspesifikasjonen utarbeidet krav til dataintegritet, tilgangskontroll, backup / recovery og revisjonsspor? | | | | | |
| | 5. Gjennomføres det risikovurderinger ved anskaffelser og endringer av eksisterende løsninger? | | | | | |
| | 6. Er det dokumentert hvordan forvaltning og vedlikehold av applikasjoner skal foretas? | | | | | |
| | 7. Er det etablert tiltak som sikrer at det utarbeides brukerhåndbøker og støttemateriell som en del av anskaffelsen? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | AI3 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Anskaffelse og vedlikehold av teknologisk infrastruktur | | | | | |
| | 1. Har foretaket definert hvilke krav som skal ligge til grunn for kjøp av ny maskin- og programvare? | | | | | |
| | 2. Er det etablert prosedyrer som sikrer at installasjon, konfigurasjon og vedlikehold av teknologisk infrastruktur imøtekommer forretningsmessige og sikkerhetsmessige krav? | | | | | |
| | 3. Er det etablert prosedyrer som sikrer at default brukerid fra leverandør blir endret etter at programvaren er installert? | | | | | |
| | 4. Er det etablert prosedyrer som sikrer etablering av vedlikeholds kontrakter for maskin- og programvare? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | AI4 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Utvikle og vedlikeholde prosedyrer | | | | | |
| | 1. Har foretaket utarbeidet retningslinjer for utvikling, endring, og godkjenning av prosedyrer? | | | | | |
| | 2. Foreligger det driftsdokumentasjon for foretakets IT-løsninger og er det etablert prosedyrer for oppdatering av denne? | | | | | |
| | 3. Foreligger det systemdokumentasjon for foretakets IT-løsninger og er det etablert prosedyrer for oppdatering av denne? | | | | | |
| | 4. Foreligger det brukerdokumentasjon for foretakets IT-løsninger og er det etablert prosedyrer for oppdatering av denne? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | AI5 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Anskaffelse av IT-ressurser | | | | | |
| | 1. Har foretaket etablert prosedyrer for innkjøp av IT-løsninger? | | | | | |
| | 2. Foreligger det kontroller som sikrer at foretakets prosedyrer og etiske retningslinjer følges ved anskaffelser? | | | | | |
| | 3. Foreligger det prosedyrer som sikrer at relevante forhold ved innkjøp av IT-tjenester er regulert i avtalen, for eksempel lisensrettigheter, akseptansekriterier og eventuelle reaksjoner ved ikke oppnådde krav til akseptanse? | | | | | |
| | 4. Foreligger det retningslinjer for innkjøp av konsulent tjenester? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | AI6 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Endringsledelse og -håndtering | | | | | |
| | 1. Har foretaket etablert prosedyre for endringshåndtering? | | | | | |
| | 2. Blir alle forespørsler om endringer i foretakets IT-løsninger dokumentert og behandles disse iht. endringsprosedyren? | | | | | |
| | 3. Blir alle endringer kategorisert og prioritert iht. fastsatte kriterier? | | | | | |
| | 4. Har foretaket etablert en egen prosedyre for hasteendringer? | | | | | |
| | 5. Sikrer organisasjonens prosedyre for endringshåndtering at konsekvenser/risiko ved gjennomføring av den aktuelle endringen blir identifisert og vurdert, før den blir godkjent/avvist? | | | | | |
| | 6. Er det etablert prosedyrer som sikrer at endringer som påvirker beredskapsløsningen initierer oppdatering av denne? | | | | | |
| | 7. Er det dokumentert hvem som har myndighet til å godkjenne endringer, og foreligger det kontrollrutiner som sikrer at dette følges? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | AI7 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Installasjon og godkjenning av systemer | | | | | |
| | 1. Har organisasjonen etablert en opplæringsplan som sikrer at medarbeidere, brukere og IT-personell får tilstrekkelig opplæring ved innføring av nye løsninger? | | | | | |
| | 2. Har foretaket etablert en teststrategi, som er grunnlaget for utvikling av testplaner? | | | | | |
| | 3. Har foretaket utarbeidet en implementeringsplan for innføring av nye og endrede IT-løsninger? | | | | | |
| | 4. Gjennomføres testing av nye/endrede IT-løsninger i et relevant testmiljø? | | | | | |
| | 5. Foreligger det prosedyrer og kontroller for godkjenning av testresultater? | | | | | |
| | 6. Foreligger det prosedyrer og kontroller for produksjonssetting av IT-løsninger, med krav til akseptanse, "roll-back" og kontinuitets løsninger? | | | | | |
| | 7. Bli erfaringer dokumentert og brukt til forbedringer? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS1 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Definere og styre servicenivået | | | | | |
| | 1. Er det utarbeidet retningslinjer for hvordan foretaket definerer, måler og følger opp servicenivået på virksomhetens IT-tjenester/-leveranser? | | | | | |
| | 2. Dekker avtalene sentrale punkter for en sikker og stabil drift av spesifiserte systemer/tjenester som for eksempel: tilgjengelighet, ytelse, kapasitet, support, integritet, overvåkning, konfidensialitet, problem- og endringshåndtering, testing, beredskap, eskalering og rapportering? | | | | | |
| | 3. Er ansvar, forpliktelser og forutsetninger beskrevet i avtalene? | | | | | |
| | 4. Har foretaket oppnevnt en ansvarlig for å sikre at leveransene er i henhold til avtalene om servicenivå og nødvendig rapportering? | | | | | |
| | 5. Foreligger det retningslinjer for hvordan informasjon til kunder og andre berørte skal ivaretas ved avvik? | | | | | |
| | 6. Er det etablert en prosess for regelmessig gjennomgang av serviceavtalene? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | IT-Prosesser | DS2 | | Kontrollspørsmål | | Sårbarhet | | |
|--|---|-----|-----|------------------|--|-----------|---|---|
| | | | | | | H | M | L |
| | Styre tjenester fra eksterne IT-leverandører | Ja | Nei | | | | | |
| | 1. Foreligger det retningslinjer for inngåelse og håndtering av avtaler, og sikrer disse at sikkerhetsmessige, lovmessige og driftsmessige krav ivaretas? | | | | | | | |
| | 2. Foreligger det retningslinjer som sikrer at eierskap og ansvar for avtalene er etablert? | | | | | | | |
| | 3. Foreligger det retningslinjer som sikrer at avtaler er utarbeidet og vedtatt før leveranser foretas? | | | | | | | |
| | 4. Gjennomføres det risiko- og sårbarhetsvurdering før valg av IT-leverandører og/eller når større endringer skjer hos IT-leverandøren? | | | | | | | |
| | 5. Er ulike krav til sikkerhet for IT-leverandører, som for eksempel taushetsplikt, identifisert og avtalt? | | | | | | | |
| | 6. Er driftskontinuitet i egen virksomhet sikret hvis ekstern IT-leverandør skulle få problemer på grunn av driftsmessige-, økonomiske eller juridiske forhold? | | | | | | | |
| Kommentarer: | | | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS3 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Styring av ytelse og kapasitet | | | | | |
| | 1. Hvis IT-drift ivaretas i eget foretak, er det etablert en prosess for regelmessig vurdering av kapasitet og ytelse? | | | | | |
| | 2. Hvis IT-drift er utkontraktet, sikrer avtalen at det er etablert en prosess for regelmessig vurdering av kapasitet og ytelse? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS4 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Sikre kontinuerlig service-/kriseplanlegging | | | | | |
| | 1. Foreligger det en kontinuitetsplan og er det etablert en prosess for oppdatering av denne? | | | | | |
| | 2. Er det etablert en prosess for årlig evaluering av kontinuitetsløsningen? | | | | | |
| | 3. Inneholder kontinuitetsplanen prosedyrer for back-up og recovery? | | | | | |
| | 4. Brukes risikovurderinger i prosessen med å etablere kontinuerlig service og katastrofeplanen? | | | | | |
| | 5. Foreligger det en tilgjengelig katastrofeplan og er det etablert en prosedyre for oppdatering av denne? | | | | | |
| | 6. Er det sikret at katastrofeplanen er tilgjengelig ved alle katastrofesituasjoner? | | | | | |
| | 7. Gjennomføres det testing av og øving i katastrofeplanen og er resultatet dokumentert? | | | | | |
| | 8. Er det utarbeidet klare kriterier for aktivering av katastrofeplan? | | | | | |
| | 9. Omfatter katastrofeplanen informasjon til ansatte, leverandører, kunder, offentlige myndigheter og media? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS5 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Sikre systemsikkerhet | | | | | |
| | 1. Er det utarbeidet IT-sikkerhetspolicy og er denne forankret i foretakets ledelse? | | | | | |
| | 2. Har foretaket retningslinjer for klassifisering av informasjon og utveksling med hensyn til konfidensialitet? | | | | | |
| | 3. Har foretaket retningslinjer for styring av tilgangskontroll for de ulike systemer og brukergrupper? | | | | | |
| | 4. Har foretaket retningslinjer for sikkerhetsadministrasjon? | | | | | |
| | 5. Er det utarbeidet prosedyrer for håndtering og administrasjon av sertifikater og krypteringsnøkler? | | | | | |
| | 6. Er det utarbeidet prosedyrer for håndtering av sikkerhetsbrudd og som beskriver hva som skal gjøres, for eksempel rapportering, eskalering og oppfølging? | | | | | |
| | 7. Er det utarbeidet prosedyrer for å forhindre, oppdage og fjerne uautorisert kode som for eksempel virus? | | | | | |
| | 8. Har enheten prosedyrer for oppfølging, vedlikehold og overvåking av nettverksinfrastruktur med hensyn på sikkerhet? | | | | | |
| | 9. Er det etablert en prosedyre for å sikre tilstrekkelig opplæring i sikkerhetsforståelse for foretakets brukere? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS6 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|--|---|-------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Identifisere og fordele kostnader | | | | | |
| | 1. Er det innført retningslinjer for hva og hvordan man måler kostnader på IT-leveranser? | | | | | |
| | 2. Foretas det en regelmessig ajourføring av prissystemet knyttet til IT-leveranser? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS7 | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | | | H | M | L |
| | IT-Prosesser | | | | | |
| | Brukeropplæring | Ja | Nei | | | |
| | 1. Er det etablert en opplæringsplan som beskriver de ulike brukergruppernes behov for IT-opplæring? | | | | | |
| | 2. Er det utpekt en ansvarlig for å tilrettelegge og følge opp brukeropplæringen? | | | | | |
| | 3. Er det etablert rutiner for å evaluere at opplæringsplanene er i samsvar med behovet for opplæring? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS8 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Mottak for behandling av hendelser | | | | | |
| | 1. Er det etablert et mottak for behandling av hendelser? | | | | | |
| | 2. Er det etablert prosedyrer som sikrer at kunnskap om hendelser benyttes til forbedring? | | | | | |
| | 3. Er det etablert prosedyrer som sikrer brukere / kunder oppfølging og tilbakemeldinger på henvendelser til brukerstøtte? | | | | | |
| | 4. Er det etablert prosedyrer for eskalering og overføring av hendelser til problemløsningsprosedyren? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS9 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Konfigurasjonshåndtering | | | | | |
| | 1. Foreligger det prosedyrer som sikrer at IT-komponenter blir identifisert? | | | | | |
| | 2. Er det utarbeidet prosedyrer som ivaretar konfigurasjonskontroll og oppfølging? | | | | | |
| | 3. Er det utarbeidet prosedyrer for å hindre bruk av uautorisert programvare, for eksempel lisenskontroll? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS10 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Håndtering av problemer | | | | | |
| | 1. Foreligger en prosedyre som sikrer at problemer registreres, analyseres og at nødvendige aksjoner blir avtalt og foretatt? | | | | | |
| | 2. Kan saksgangen for håndtering av problemer vise status i behandlingen og kan saksgangen spores i ettertid? | | | | | |
| | 3. Er det etablert samordning mellom problemhåndtering og endringshåndtering? | | | | | |
| | 4. Inneholder prosedyren for problemhåndtering retningslinjer for eskalering? | | | | | |
| | 5. Gjennomføres det vurderinger av alle registrerte problemer som ledd i forbedringsarbeidet? | | | | | |
| | 6. Foreligger det oversikt over IT-leverandørers ansvar i en problemsituasjon? | | | | | |
| | 7. Er det etablert en rutine for rapportering av alvorlige og kritiske hendelser til Finanstilsynet? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS11 | | Kontrollspørsmål | | Sårbarhet | | |
|--|---|--|------------------|-----|-----------|---|---|
| | | | | | H | M | L |
| | IT-Prosesser | | | | | | |
| | Håndtering av data | | Ja | Nei | | | |
| | 1. Foreligger det prosedyrer som sikrer at datagrunnlag (inndata) for transaksjoner er kvalitetssikret? | | | | | | |
| | 2. Er det etablert retningslinjer for arbeidsdeling og internkontroll for behandling av data? | | | | | | |
| | 3. Foreligger det prosedyrer som sikrer at gjenoppretting, oppbevaring og arkivering av datagrunnlag for transaksjoner gjennomføres i henhold til egne krav, retningslinjer og lovpålagte krav? | | | | | | |
| | 4. Finnes det innebygde kontroller i systemene som sikrer at data blir underlagt kontroller knyttet til konfidensialitet, integritet og tilgjengelighet? | | | | | | |
| | 5. Foreligger det prosedyrer for sikring og distribusjon av gradert informasjon? | | | | | | |
| | 6. Foreligger det prosedyrer som sikrer en rutinemessig kontroll av transaksjoner, herunder også avstemming? | | | | | | |
| | 7. Lager IT-løsningene revisjonsspor som gjør det mulig å følge en transaksjon gjennom prosesseringen? | | | | | | |
| | 8. Foreligger det prosedyrer for lagring, gjenoppretting og sletting av data som ivaretar hensynet til sikkerhetsmessige og lovbestemte krav? | | | | | | |
| | 9. Er oppbevaringstid og lagringsvilkår definert for krypteringsnøkler og sertifikater? | | | | | | |
| | 10. Er det prosedyrer som sikrer at backup/recovery av data (sikkerhetskopi) gjennomføres, og at integritet, fysisk sikkerhet og ansvarsforhold er ivaretatt? | | | | | | |
| | 11. Foreligger det prosedyrer som sikrer data som overføres over åpne nettverk? | | | | | | |
| <u>Kommentarer:</u> | | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS12 IT-Prosesser | Kontroll-spørsmål | | Sårbarhet | | |
|--|--|-------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Fysiske omgivelser | | | | | |
| | 1. Er plasseringen av og utformingen av lokalene til IT-virksomheten basert på gjennomført risikoanalyse? | | | | | |
| | 2. Foreligger det prosedyrer for adgangskontroll til foretakets lokaler? | | | | | |
| | 3. Foreligger det prosedyre som sikrer håndtering av innbrudd? | | | | | |
| | 4. Foreligger det prosedyrer som sikrer jevnlig vurdering og oppdatering av systemene for adgangskontroll? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | DS13 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Styring av driften | | | | | |
| | 1. Foreligger det driftshåndbøker for IT-løsningene? | | | | | |
| | 2. Gjennomføres det logging av driften som gjør det mulig å identifisere og løse avvik og feil som oppstår? | | | | | |
| | 3. Gjennomføres det logging av driftsoppgaver som gjør det mulig å reetablere driften etter oppstått feil? | | | | | |
| | 4. Er det etablert prosedyrer for vedlikehold av maskinvare? | | | | | |
| Kommentarer: | | | | | | |

| Grad av viktighet, rangering 1 til 34 | ME1 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Overvåke og vurdere IT ytelse | | | | | |
| | 1. Er det etablert tiltak for å sikre at IT-leveransene understøtter forretningsmessige mål og vedtatte strategier? | | | | | |
| | 2. Blir resultatene fra IT-virksomheten (for eksempel utviklingsprosjekter og driftsleveranser) benyttet som grunnlag for overordnet styring og kontroll? | | | | | |
| | 3. Gjøres det vurderinger av brukertilfredshet med hensyn på den service som blir levert? | | | | | |
| | 4. Blir det rapportert til ledelsen i hvilken grad målsettinger og måltall blir nådd, leveranser gjennomført og risiko håndtert? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | ME2 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Vurdere internkontroll | | | | | |
| | 1. Er det etablert prosedyrer for overvåking, kontroll og vurdering av internkontroll i virksomheten? | | | | | |
| | 2. Blir feil og avvik avdekket ved gjennomgang av internkontrollen, som kan medføre risiko, rapportert til ledelsen? | | | | | |
| | 3. Er det i avtalene med IT-leverandører sikret at det gjennomføres kontroll av internkontrollen? | | | | | |
| | 4. Blir resultatet av gjennomgang av internkontrollen fulgt opp i foretaket? | | | | | |
| <u>Kommentarer:</u> | | | | | | |

| Grad av viktighet, rangering 1 til 34 | ME3 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|--|---|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Sikre etterlevelse av eksterne krav | | | | | |
| | 1. Er det etablert rutiner som sikrer at eksterne krav til IT-virksomheten identifiseres og dokumenteres? | | | | | |
| | 2. Er det etablert rutiner som sikrer etterlevelse av eksterne krav, for eksempel lover og forskrifter? | | | | | |
| | 3. Finnes det en oversikt over alle eksterne kontrakter og hvilke forpliktelser disse medfører? | | | | | |
| | 4. Er foretaket kjent med meldeplikten for systemer for betalingstjenester i henhold til lov om betalingssystemer? ¹ | | | | | |
| <u>Kommentarer:</u> | | | | | | |

1

<http://www.Finanstilsynet.no/wbch3.exe?ce=13764>

| Grad av viktighet, rangering 1 til 34 | ME4 IT-Prosesser | Kontrollspørsmål | | Sårbarhet | | |
|---------------------------------------|--|------------------|-----|-----------|---|---|
| | | Ja | Nei | H | M | L |
| | Styring og kontroll | | | | | |
| | 1. Foreligger det et rammeverk for styring av IT-virksomheten som omfatter prosesser, roller og ansvar og som sikrer at IT-virksomheten understøtter foretakets mål og strategier? | | | | | |
| | 2. Blir det gjennomført kost-/nytteanalyser forut for beslutning om IT-investering? | | | | | |
| | 3. Foretas det regelmessig kvalitetsgjennomgang av IT-virksomheten som for eksempel omfatter økonomi, ressurser, kompetanse, avtaleverk, risiko og ledelse? | | | | | |
| | 4. Er det gjennomført sertifisering av IT-virksomheten, for eksempel ISO-sertifisering? | | | | | |
| | 5. Gjennomføres det regelmessig uavhengig ekstern kontroll / revisjon av IT-virksomheten? | | | | | |
| <u>Kommentarer:</u> | | | | | | |