



**FINANSTILSYNET**  
THE FINANCIAL SUPERVISORY  
AUTHORITY OF NORWAY

# Egenevalueringsskjema

for foretakets IT-virksomhet  
forenklet versjon basert på  
12 COBIT prosesser

Dato: 21.01.2009

Versjon 2.5

**Finanstilsynet**

Tlf. 22 93 98 00

post@finansilsynet.no

www.finanstilsynet.no

# Evalueringskjema for foretakets IT-virksomhet

Rangering av  
prosess

## **Planlegging og organisering (POx):**

PO1	Definere en IT-strategi	
PO7	Personalledelse	
PO8	Kvalitetsstyring	
PO9	Vurdere risiko	
PO10	Prosjektstyring	

## **Anskaffelse og implementering (AIx)**

AI6	Endringsledelse og -håndtering	
AI7	Installasjon og godkjenning av systemer	

## **Leveranse og støtte (DSx):**

DS2	Styre tjenester fra eksterne IT-leverandører	
DS4	Sikre kontinuerlig service-/kriseplanlegging	
DS5	Sikre systemsikkerhet	
DS10	Håndtering av problemer	

## **Overvåkning (MEx):**

ME3	Sikre etterlevelse av eksterne krav	
-----	-------------------------------------	--

Foretakets navn :

Dato :

Underskrift :

Link til Finanstilsynets veiledning i etterlevelse av IKT-forskriften for mindre foretak:  
<http://www.Finanstilsynet.no/wbch3.exe?ce=17379>

Grad av viktighet, rangering 1 til 12	PO1 IT-Prosesser	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	<b>Definere en IT-strategi</b>	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 12	IT-Prosesser	PO7		Kontroll-spørsmål		Sårbarhet		
				H	M	L		
	<b>Personalledelse</b>	Ja	Nei					
	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 12	PO8 IT-Prosesser	Kontroll-spørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	<b>Kvalitetsstyring</b>					
	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 12	PO9 IT-Prosesser	Kontrollspørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	<b>Vurdere risiko</b>					
	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?					
<u>Kommentarer:</u>						

Grad av viktighet, rangering 1 til 12	PO10 IT-Prosesser	Kontrollspørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	<b>Prosjektstyring</b>					
	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 12	AI6 IT-Prosesser	Kontrollspørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	<b>Endringsledelse og -håndtering</b>					
	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 12	AI7 IT-Prosesser	Kontrollspørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	<b>Installasjon og godkjenning av systemer</b>					
	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 12	DS2 IT-Prosesser	Kontrollspørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	Styre tjenester fra eksterne IT-leverandører					
	1. Foreligger det retningslinjer for inngåelse og håndtering av avtaler, og sikrer disse at sikkerhetsmessige, lovmessige og driftsmessige krav ivaretas?					
	2. Ivaretar retningslinjene 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 12	DS4 IT-Prosesser	Kontrollspørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	<b>Sikre kontinuerlig service-/kriseplanlegging</b>					
	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 12	DS5 IT-Prosesser	Kontrollspørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	<b>Sikre systemsikkerhet</b>					
	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 12	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 12	ME3 IT-Prosesser	Kontrollspørsmål		Sårbarhet		
		Ja	Nei	H	M	L
	<b>Sikre etterlevelse av eksterne krav</b>					
	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? <sup>1</sup>					
<u>Kommentarer:</u>						

---

1

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