



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Evaluerings skjema

Foretakets virksomhet knyttet til
Systemer for Betalingstjenester.

Foretakets navn :
Dato:
Underskrift :

Dato: 24.11.2008
Versjon: 1.0

Evalueringsskjema for foretakets virksomhet knyttet til Systemer for Betalingstjenester

Side	Antall spørsmål			Gjennomført dato:
------	-----------------	--	--	-------------------

1. Beskrivelse av betalingssystem og betalingsinfrastruktur.

<u>2. Styring og Kontroll (SKx)</u>				
SK1	Strategi og Organisering	6	19	
SK2	Betalingskanaler	8	9	
SK3	Betalingsinstrumenter	9	10	
SK4	Meldingsstandarder i Betalingsnettverk	10	11	

3. Forvaltning og Drift av betalingssystemer (FDx)

FD1	Dokumentasjon av betalingssystemer	12	5	
FD2	Nyutvikling og kjøp	13	11	
FD3	Endringsledelse og -håndtering	14	14	
FD4	Risiko ved nyutvikling/kjøp eller endringer	16	11	
FD5	Informasjon om nyutvikling/kjøp eller endringer	17	4	
FD6	Testing ved nyutvikling/kjøp eller endringer	18	21	
FD7	Produksjonssetting og drift	20	18	
FD8	Beredskap ved produksjonssetting og drift	22	9	
FD9	Kompetanse	23	6	
FD10	Behandling av hendelser	24	10	
Kommentarer:		25		
Antall spørsmål:			158	

1. Beskrivelse av systemer for betalingstjenester og betalingsinfrastruktur.

Systemer for betalingstjenester.

Handel med varer og tjenester i moderne velregulerte samfunn fungerer optimalt gjennom bruk av effektive betalingssystemer.

Lov om betalingssystemer m.v.(Lov 1999-12-17 nr. 95) definerer interbanksystemer(avregning og oppgjør) og systemer for betalingstjenester(betalingsystemer) som to systemer i et betalingsoppgjør mellom ulike parter.

Denne tilsynsmodulen fokuserer på systemer som i loven er betegnet som systemer for betalingstjenester.

I hovedsak omfatter dette systemer som gjør det mulig for kunder i finansforetak å overføre penger mellom egne og til andres konti ved bruk av ulike betalingsinstrumenter.

De anvendte systemer håndterer nødvendige prosesser mellom kunde og kundens bank og mellom banker enten direkte eller gjennom oppgjørssentraler og Norges bank.

Finansforetakenes drift av betalingssystemer er for det meste basert på bruk av elektronisk databehandling, IKT, som normalt er en kombinasjon av interne og utkontrakterte prosesser. Regelverket rundt drift og utvikling av slike prosesser dekkes av IKT forskriften (FOR 2003-05-21 nr. 630: Forskrift om bruk av informasjon- og kommunikasjonsteknologi(IKT)).

Tilsynsmodulen skal dekke området for systemer for betalingstjenester for å sikre at hensynet til sikker, effektiv betaling og rasjonell og samordnet utførelse av betalingstjenester blir ivaretatt.

Styring og kontroll av betalingssystemer inngår som et viktig element i vurderingen av operasjonell risiko basert på reglene i Basel II som er innarbeidet i norsk finanslovgivning.

Ved nyutvikling, kjøp eller endringer av et system for betalingstjenester, skal Kredittilsynet informeres gjennom "Egenmelding for systemer for betalingstjenester"(Rundskriv 17/2004).

Tilsynsmodulen omfatter:

- Styring og Kontroll.
- Forvaltning og Drift.
- Nyutvikling, Kjøp eller Systemendring.

Betalingsinfrastruktur.

Betalingsinfrastruktur omfatter fysiske komponenter, operativsystem, nettverk, standarder, systemer for overvåking, organisering, avtaler, oppfølging, dokumentasjon og kontroll når det gjelder drift av finansforetakenes betalingssystemer. Infrastrukturen vil kunne omfatte foretakets egen organisasjon inkludert avtaler om utkontraktering og samarbeidsavtaler med andre foretak.

Infrastrukturens ulike elementer og aktører(se Fig.1. side 5) må samarbeide for å oppnå kostnadseffektivitet og sikker transaksjonsflyt innenfor rammen av tilfredstillende operasjonell risiko.

Betalingskanaler, betalingsinstrumenter og meldingsstandarder i betalingsnettverk er elementene som spiller sammen i den finansielle leverandørkjede når betalingstjenester utføres i betalingssystemene.

Eksempler på slike elementer er:

Betalingskanaler

- a. Brev
- b. Bankfilial/Bank i butikk
- c. Elektronisk betalingsterminal(nettbank, mobilbank, butikkterminal o.l.)
- d. Elektronisk overførte datafiler

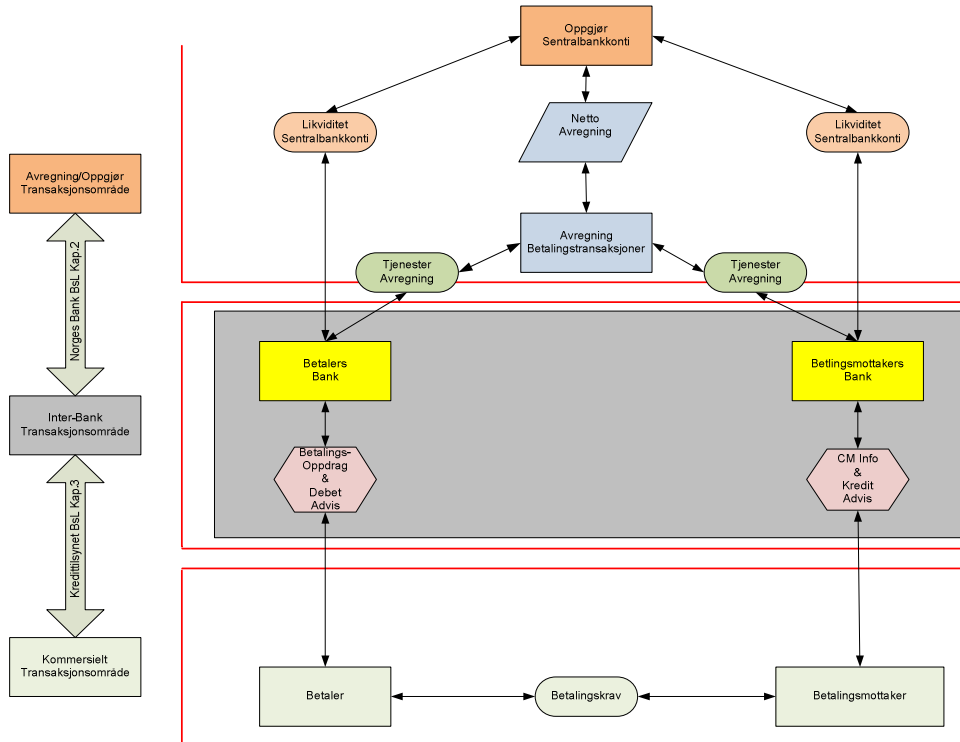
Betalingsinstrumenter

- a. Koder(i forbindelse med nettbank, mobilbank, butikkterminal o.l.)
- b. Debetkort
- c. Kredittkort
- d. E-faktura
- e. Avtalegiro
- f. Brevgiro
- g. Giro(enkel og masse)

Meldingsstandarder i Betalingsnettverk

- a. Egenkontrollerte meldingsstandarder
- b. Felleskontrollerte meldingsstandarder
 - i. NIBE
 - ii. SWIFT MT og MX
 - iii. EMV(Internasjonale betalingskort)
 - iv. OCR
 - v. BOLS
 - vi. Telepay
 - vii. EdiFact
 - viii. ISO(8583, 2002 XML)

Fig.1.



	SK1	Kontroll- spørsmål		Sårbarhet		
	Styring og Kontroll			H	M	L
	Strategi og Organisering	Ja	Nei			
	1. Er det etablert en egen strategiplan med konkrete mål for forretningsområdet betalingssystemer?					
	2. Er strategi for betalingssystemer koordinert med IT-strategien?					
	3. Er mål og strategi for betalingssystemer forankret hos foretakets øverste ledelse?					
	4. Er det etablert rutiner for å informere ledelsen om IT-teknologiske synergier relatert til systemer for betalingstjenester?					
	5. Er mål og strategi for betalingssystemer hensyntatt i foretakets forretningsmessige mål?					
	6. Er det organisatoriske ansvaret for betalingssystemer knyttet til ansvaret for IT-systemer ?					
	7. Er det organisatoriske ansvaret for betalingssystemer knyttet til ansvaret for betalingstjenester?					
	8. Finnes et overordnet klart definert ansvar for alle betalingssystemer?					
	9. Er eksterne leverandører kritiske for betalingssystemene?					
	10. Er operasjonelle ansvarsforhold mellom betalingssystemenes leverandører klart definert og avtalt?					
	11. Er betalingssystemene elektronisk STP (Straight Through Processing)?					
	12. Hvis nei på 11. Er betalingssystemene delvis basert på manuelle prosesser?					

	13. Har betalingssystemene automatisk feilsøking og feilretting?			
	14. Er katastrofeberedskap for betalingssystemene klart organisert med dokumentert arbeids- og rapporteringsplan?			
	15. Er det gjennomført faktisk bruk eller test av planen for katastrofeberedskap i løpet av de siste 12 måneder?			
	16. Finnes det planer for erstatning av identifiserte nøkkelressurser (personer/leverandører) dersom disse skulle bli utilgjengelig?			
	17. Finnes det operative planprosesser for inneværende/neste år hvor ressurser og tiltak til akutt forvaltning, preventiv forvaltning samt viderertuving blir planlagt og avtalt.			
	18. Er foretaket representert i samarbeidsfora med leverandører, myndigheter og samarbeidspartnere av personell med riktig kompetanse.			
	19. Er det oppdaterte ressursplaner for området på brukersiden og IT siden?			
<u>Kommentarer:</u>				

	SK2	Kontroll- spørsmål		Sårbarhet		
	Styring og Kontroll			H	M	L
	Betalingskanaler	Ja	Nei			
	1. Er alle betalingskanaler dokumentert og beskrevet?					
	2. Har alle betalingskanaler en entydig organisatorisk forankring?					
	3. Er det felles avhengige operasjonelle funksjoner mellom betalingskanalene?					
	4. Er alle betalingskanalene elektroniske?					
	5. Hvis nei på 4. Er det etablert kontroller for de manuelle kanaler (for eksempel sluttsum, sekvens, siffer)?					
	6. Finnes plan for bruk av alternativ betalingskanal dersom en betalingskanal er utilgjengelig?					
	7. Loggføres alle avvikshendelser i forbindelse med tilgang/bruk av betalingskanal?					
	8. Logges alle feilmeldinger/klager fra kunder/brukere av de forskjellige betalingskanalene?					
	9. Føres statistikk på bruk/endring i bruk av hver enkelt betalingskanal?					
<u>Kommentarer:</u>						

	SK3	Kontroll- spørsmål		Sårbarhet		
	Styring og Kontroll			H	M	L
	Betalingsinstrumenter	Ja	Nei			
	1. Er alle betalingsinstrumenter dokumentert og beskrevet?					
	2. Har alle betalingsinstrumenter en entydig organisatorisk forankring, internt og eksternt?					
	3. Er det felles avhengige operasjonelle funksjoner mellom betalingsinstrumentene?					
	4. Er alle betalingsinstrumentene elektroniske?					
	5. Hvis nei på 4. Er det knyttet kontroller til behandlingen av de manuelle?					
	6. Finnes plan for bruk av alternativ betalingsinstrument dersom ett betalingsinstrument er utilgjengelig?					
	7. Loggføres alle avvikshendelser i forbindelse med tilgang/bruk av hvert enkelt betalingsinstrument? (eks. som påvirker STP grad)					
	8. Logges alle feilmeldinger/klager fra kunder/brukere av de forskjellige betalingsinstrument?					
	9. Føres statistikk på bruk/endring i bruk av hvert enkelt betalingsinstrument?					
	10. Finnes det plan for jevnlig fornying av aktive betalingsinstrument samt makulering av passive hos hver enkelt bruker?					
<u>Kommentarer:</u>						

	SK4	Kontroll- spørsmål		Sårbarhet		
	Styring og Kontroll			H	M	L
	Meldingsstandarder i Betalingsnettverk	Ja	Nei			
	1. Brukes det bare egenkontrollerte meldingsstandarder i betalingsnettverk?					
	2. Hvis nei på 1. Er anvendte meldingsstandarder i betalingsnettverk en kombinasjon av egenkontrollerte og felleskontrollerte valg?					
	3. Hvis ja på 2. Er felleskontrollerte meldingsstandarder i betalingsnettverk vurdert som kritiske?					
	4. Har foretaket en full dokumentert oversikt over alle anvendte meldingsstandarder i betalingsnettverk som er knyttet til betalingssystemene?					
	5. Er ansvaret for meldingsstandarder i betalingsnettverk klart organisatorisk forankret?					
	6. Deltar foretaket i styringen av bankenes selvregulering (Blåboken)?					
	7. Deltar foretaket i styringen av SWIFT NNG (Norge)?					
	8. Deltar foretaket i standardiseringsarbeidet knyttet til betalingssystemene?					
	9. Hvilke selskap er leverandør av tele nettverk? Kommenter!					
	10. Finnes det fast rutine for varsling av berørte parter ved endringer i meldingsstandarder?					
	11. Er det klart hvem som representerer foretaket i samarbeidsfora rundt forvaltning av meldingsstandarder?					

Kommentarer:

	FD1	Kontroll- spørsmål		Sårbarhet		
	Forvaltning og Drift av betalingssystemer			H	M	L
	Dokumentasjon av betalingssystemer	Ja	Nei			
	1. Er relevant systemdokumentasjon oppdatert og godkjent i henhold til interne kvalitetssikringsrutiner?					
	2. Er relevant rutinedokumentasjon utarbeidet (oppdatert) og godkjent i henhold til interne kvalitetssikringsrutiner?					
	3. Foreligger komplett oversikt over konfigurasjon, berørte systemkomponenter, versjonsnr., m.m.?					
	4. Foreligger det en dokumentert prosess for oppdatering av all relevant dokumentasjon ved endringer?					
	5. Foreligger det rutine for konsistenssjekk av de forskjellige deler av dokumentasjon mot hverandre ved nyutvikling/endringer? (eks. Markedsføringsmateriell, Brukerdokumentasjon, Systemdokumentasjon, Driftsdokumentasjon. Kravspesifikasjon.)					
<u>Kommentarer:</u>						

	FD2	Kontrollspørsmål		Sårbarhet		
	Forvaltning og Drift av betalingssystemer			H	M	L
	Nyutvikling og kjøp	Ja	Nei			
	1. Har foretaket etablert dokumenterte rutiner for håndtering av nyutvikling/kjøp av betalingssystemer?					
	2. Behandles forespørsler om nyutvikling/kjøp iht. etablerte rutiner?					
	3. Blir nyutvikling/kjøp kategorisert og prioritert iht. fastsatte kriterier?					
	4. Gjennomføres kost-/nyttevurderinger som grunnlag for valg av løsning?					
	5. Sikrer organisasjonens rutiner for nyutvikling/kjøp at konsekvenser og risiki ved gjennomføring av de aktuelle valg blir identifisert og vurdert, før de blir godkjent, evt. avvist?					
	6. Er det etablert rutiner som sikrer at nyutvikling/kjøp som påvirker beredskapsløsningen, initierer oppdatering av denne?					
	7. Er det dokumentert hvem som har myndighet til å godkjenne nyutvikling/kjøp?					
	8. Har foretaket etablert en egen prosedyre for hastebeslutninger?					
	9. Organiseres nyutvikling/kjøp av vesentlig omfang som egne prosjekter med representasjon fra berørte parter?					
	10. Prioriteres representasjon i fellesfora for utvikling med riktig kompetanse i henhold til fastsatte rutiner?					
	11. Er det rutine for å avtale kvalitetsnivå på alle leveranser internt og eksternt?					
<u>Kommentarer:</u>						

	FD3	Kontrollspørsmål		Sårbarhet		
	Forvaltning og Drift av betalingssystemer			H	M	L
	Endringsledelse og -håndtering	Ja	Nei			
	1. Har foretaket etablert dokumentert rutine for endringshåndtering?					
	2. Blir alle forespørsler om endringer i foretakets IT-løsninger dokumentert, og behandles disse iht. rutine for endringshåndtering?					
	3. Blir alle endringer kategorisert og prioritert iht. fastsatte kriterier?					
	4. Gjennomføres kost-/nyttevurderinger som grunnlag for valg av løsning?					
	5. Sikrer organisasjonens rutiner for endringshåndtering at konsekvenser og risiki ved gjennomføring av den aktuelle endringen blir identifisert og vurdert, før den blir godkjent, evt. avvist?					
	6. Er det etablert rutiner som sikrer at endringer som påvirker beredskapsløsningen, initierer oppdatering av denne?					
	7. Er det dokumentert hvem som har myndighet til å godkjenne endringer?					
	8. Foreligger det kontrollrutiner som sikrer at dette følges?					
	9. Har foretaket etablert en egen rutine for hasteendringer?					
	10. Implementeres endringer i planlagte nye releaser?					
	11. Hvis ja på 10, koordineres slike planer med tilsvarende releaseplaner fra eksterne nettverk?					
	12. Finnes det egen rutine for konsistenssjekk av konfigurasjoner mellom programmer og dokumentasjon?					
	13. Avsjekkes forståelse av løsningsbeskrivelse mot endringsforespørsel i forhold til bestiller før implementering av endring?					
	14. Sikres det at endringer til produksjonssystemer autoriseres på rett nivå?					

Kommentarer:

	FD4	Kontrollspørsmål		Sårbarhet		
	Forvaltning og Drift av betalingssystemer			H	M	L
	Risiko ved nyutvikling/kjøp eller endringer	Ja	Nei			
	Gjennomføres risiko og sårbarhetsanalyse for å avdekke:					
	1. Vesentlige økonomiske konsekvenser for banken eller dens kunder?					
	2. Vesentlige økonomiske konsekvenser for andre banker, deres kunder eller andre aktører??					
	3. Driftsavbrudd eller vesentlige driftsavvik for andre systemer i banken?					
	4. Driftsavbrudd eller vesentlige driftsavvik for bankens datasentral (herunder andre banker tilknyttet samme sentral), eller andre aktører i betalingsinfrastrukturen?					
	5. Gjennomføres risiko- og sårbarhetsanalyse for nyutvikling/kjøp eller endringer knyttet til avbrudd og svikt i kontinuitet i leveransen av tjenester ?					
	6. Gjennomføres risiko- og sårbarhetsanalyse for nyutvikling/kjøp eller endringer knyttet til feil vedrørende transaksjonsflyt og betalingsoppgjør?					
	7. Hvis svar på spørsmål 4-6 er ja. Håndteres alle identifiserte svakheter?					
	8. Gjennomføres risiko- og sårbarhetsanalyse for endringer knyttet til svindel og kriminelle handlinger?					
	9. Er det etablert en dokumentert rutine for hvordan egenmeldinger for nyutvikling/kjøp eller endringer av betalingssystemer blir meddelt Kredittilsynet ?					
	10. Risiko for at sensitive data kommer på avveie i forbindelse med utvikling/testing/migrering av data?					
	11. Risiko for at uautoriserte endringer blir implementert i produksjonssystemer?					
<u>Kommentarer:</u>						

	FD5	Kontroll- spørsmål		Sårbarhet		
	Forvaltning og Drift av Betalingssystemer			H	M	L
	Informasjon om nyutvikling/kjøp eller endringer	Ja	Nei			
	1. Er det utarbeidet plan for intern og eksternt informasjon om nyutvikling/kjøp eller endringer i betalingssystem og deres konsekvenser for alle berørte parter?					
	2. Er alle relevante eksterne aktører informert i god tid og i henhold til informasjonsplan? (Norges Bank, Kredittilsynet, BBS, Finansdepartementet, Bankforeningene, infrastrukturleverandører, andre banker, kunder)					
	3. Er alle relevante interne aktører informert i god tid og i henhold til informasjonsplan? (Kundeansvarlige, produkt- og systemansvarlige, driftsansvarlig)					
	4. Er alle relevante underleverandører informert i god tid og i henhold til informasjonsplan? (datasentral/driftsleverandør, nettverksleverandør, osv.)					
<u>Kommentarer:</u>						

	FD6	Kontrollspørsmål		Sårbarhet		
	Forvaltning og Drift av betalingssystemer			H	M	L
	Testing ved nyutvikling/kjøp eller endring	Ja	Nei			
	1. Gjennomføres ende-til-ende test med alle relevante eksterne aktører og brukere?					
	2. Gjennomføres fullverdig regresjonstest i produksjonslik miljø?					
	3. Gjennomføres tilstrekkelige funksjonelle tester?					
	4. Gjennomføres test av driftsopplegg og driftsrutiner?					
	5. Gjennomføres test av evt. konverteringsrutiner?					
	6. Gjennomføres volum og ytelsestester?					
	7. Er alle kjente avvikssituasjoner testet mht. varsling, recovery og restart?					
	8. Gjennomføres test av migreringsrutiner.					
	9. Blir testene gjennomført på siste versjon av systemkomponenter iht. produksjonskonfigurasjonen?					
	10. Vil migrering til produksjon ta utgangspunkt i de versjoner av systemkomponenter som er godkjent i test?					
	11. Gjennomføres hele/deler av testingen på (kopi av) reelle data?					
	12. Hvis ja på 11: Finnes sikre rutiner for at slike data ikke kommer på avveie?					
	13. Bygges testplan/testtilfeller og gjennomføres testingen med hjelp av representanter fra forretningssiden i foretaket?					
	14. Finnes og brukes etablerte testmiljø for komplett ende-ende testing også for endringer?					
	15. Er godkjent konfigurasjonsstyringprosess spesifisert?					
	16. Er konfigurasjonsansvarlig for test og produksjon pekt ut?					
	17. Lages testplan i god tid før testingen skal starte?					

	18. Loggføres alle avvik/feilsituasjoner?			
	19. Kategoriseres alle feilsituasjoner i forhold til avtalte kvalitetskriteria internt/eksternt?			
	20. Korrigeres slike avvik i henhold til prioritering i kategoriseringen?			
	21. Er forventet nivå på feilsituasjoner planlagt/avtalt internt/eksternt?			
<u>Kommentarer:</u>				

	FD7	Kontrollspørsmål		Sårbarhet		
	Forvaltning og Drift av betalingssystemer			H	M	L
	Produksjonssetting og drift	Ja	Nei			
	1. Foreligger klare kvalitetskrav og kriterier for å akseptere omlegging til produksjon?					
	2. Er det definert et kontrollopplegg for omlegging til produksjon som sikrer at evt. avvik avdekkes internt så tidlig som mulig og før avvik påvirker evt. eksterne parter?					
	3. Foreligger det plan for hvordan eksterne parter skal informeres ved evt. avvik i forbindelse med omlegging?					
	4. Gir oppstartsplanene tilstrekkelig rom for stabilisering før frysperiode eller ferie?					
	5. Finnes rutiner som sikrer at nøkkelpersoner er tilgjengelige i oppstarts- og stabiliseringsfasen?					
	6. Tar oppstartsplanene hensyn til behov for utvidet bemanning og overvåking i oppstartsfasen?					
	7. Blir relevante driftsrutiner utarbeidet/oppdatert?					
	8. Blir relevante brukerrutiner utarbeidet/oppdatert?					
	9. Godkjenner driftsleverandøren en omlegging til produksjon?					
	10. Definerer driftsleverandøren rutiner for overvåking av ytelse, nødvendig diskplass, maskinbelastning osv?					
	11. Vil miljø for katastrofeberedskap oppdateres med ny konfigurasjon samtidig med omlegging til produksjon?					
	12. Vil testmodellen være tilgjengelig for feilrettere ved evt. regresjonstest etter retting av produksjonsavvik?					
	13. Er berørte serviceavtaler oppdatert?					

	14. Koordineres produksjonssetting med tilsvarende produksjonssetting hos samarbeidspartnere slik at forutsatte konfigurasjoner fungerer sammen som forutsatt?			
	15. Beregnes og tas det hensyn til kapasitetsøkning i serviceapparat, teknisk lagringskapasitet, kommunikasjonskapasitet i forbindelse med ny løsning og/eller avvikssituasjon i forbindelse med oppstart?			
	16. Er tilstrekkelig sikring mot uautorisert adgang tatt hensyn til også i selve oppstartsperioden?			
	17. Er tidspunkt for ”back-out” og ”point-of-no-return” planlagt med god margin?			
	18. Dersom produksjonssetting innebærer migrering/konvertering av produksjonsdata, er disse vurdert ”vasket”/konsistenssjekket?			
<u>Kommentarer:</u> 				

	FD8	Kontrollspørsmål		Sårbarhet		
				H	M	L
	Forvaltning og Drift av betalingssystemer					
	Beredskap ved produksjonssetting og drift	Ja	Nei			
	1. Er det utarbeidet kontinuitetsplan eller er eksisterende kontinuitetsplan oppdatert?					
	2. Blir kontinuitetsplanen testet i forbindelse med nyutvikling/kjøp eller endringer? Hvis nei, oppgi når den sist ble testet/ vil bli testet.					
	3. Er det utarbeidet plan for gjenoppretting av normal drift på gammel systemløsning dersom nye løsninger skulle vise seg ikke å fungere godt nok?					
	4. Er det definert klare kriterier for overgang til gammel systemløsning og hva som er "point of no return"?					
	5. Blir gjenopprettingsplanen testet i produksjonslik miljø?					
	6. Er det utarbeidet ny beredskapsplan eller er eksisterende beredskapsplan oppdatert?					
	7. Er beredskapsplanen testet i forbindelse med endringer?					
	8. Er beredskapsplanen avtalt med alle parter som kan tenkes å måtte bidra i planen?					
	9. Er brukere/kunder informert dersom det er nødvendig med ekstra kontroller, nye kontaktveier eller lignende?					
<u>Kommentarer:</u>						

	FD9	Kontrollspørsmål		Sårbarhet		
	Forvaltning og Drift av betalingssystemer			H	M	L
	Kompetanse	Ja	Nei			
	1. Har foretaket etablert en opplæringsplan som sikrer at medarbeidere, brukere og IT personell får tilstrekkelig opplæring ved innføring av nyutviklete/kjøpte eller endrete systemer for betalingstjenester?					
	2. Er tilstrekkelig kompetanse overført fra eventuelle systemleverandører som sikrer forsvarlig drift?					
	3. Hvis svar på spørsmål 2. er nei; Foreligger det konkrete og forpliktende planer for kompetanseoverføring?					
	4. Hvis svar på spørsmål 3. er nei; Er det inngått avtale med systemleverandører om den nødvendige bistand?					
	5. Har driftspersonalet fått den nødvendige opplæring for å kunne ivareta driften på en forsvarlig måte?					
	6. Er dekning av behov for kjernekompetanse ved hendelser der nøkkelressurs blir utilgjengelig, vurdert?					
<u>Kommentarer:</u>						

	FD10	Kontrollspørsmål		Sårbarhet		
	Forvaltning og Drift av Betalingssystemer			H	M	L
	Behandling av hendelser	Ja	Nei			
	1. Er det etablert et definert 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 rutiner for eskalering og overføring av hendelser til prosedyre for krisehåndtering?					
	5. Foreligger det oversikt over IT-leverandørers ansvar i en problemsituasjon?					
	6. Er det etablert prosedyrer for varsling av hendelser til Kredittilsynet?					
	7. Loggføres og kategoriseres all hendelser?					
	8. Håndteres alle hendelser hos rette vedkommende i henhold til eskaleringsplan?					
	9. Finnes eskaleringsplan?					
	10. Vurderes kommersielle og sikkerhetsmessige konsekvenser av hver hendelse?					
<u>Kommentarer:</u>						

Kommentarer: