



FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Evaluerings skjema

Foretakets nettbankvirksomhet

Foretakets navn :
Dato:
Underskrift :

Dato: 13.11.2007

Versjon: 1.0

Evalueringsskjema for foretakets nettbankløsning

Rangering av prosess				Gjennomført dato:
----------------------	--	--	--	-------------------

Nettbank 1	Avtaler					
Nettbank 2	Krav til nettbankløsningen					
Nettbank 3	Sikkerhet					
Nettbank 4	Endringshåndtering og installasjon					
Nettbank 5	Kontinuitets- og katastrofehandtering					
Nettbank 6	Avviks- og hendelseshåndtering					
Nettbank 7	Overvåkning					

	Nettbank 1		Sårbarhet		
	IT-Prosesser	Kontroll-spørsmål	H	M	L
	Avtaler	Ja	Nei		
	1. Er det definert krav til servicenivå (tilgjengelighet, konfidensialitet, integritet) for nettbankløsningen?				
	2. Er det gjort en vurdering av om avtaler med deltagende institusjoner ¹ er tilstrekkelige til å sikre regulering av de forhold som berører nettbankløsningen ?				
	3. Dersom det er inngått avtaler med eksterne IT-leverandører, regulerer disse partenes rettigheter og plikter?				
	4. Er det utarbeidet krav til servicenivå i avtalene med eksterne IT-leverandører?				
	5. Er det utført en risikovurdering av avtalene med eksterne IT-leverandører?				
	6. Er de ulike krav til sikkerhet for eksterne IT-leverandører (for eks. taushetsplikt) identifisert og avtalt?				
	7. Er det laget avtaler om kundenes rettigheter, plikter og finansielle risiko?				
<u>Kommentarer:</u>					

¹ Deltagende institusjoner kan være andre banker, BBS, Norges Bank o.a.

	Nettbank 2	Kontrollspørsmål		Sårbarhet		
				H	M	L
IT-Prosesser						
Krav til nettbanken		Ja	Nei			
1. Er eierskap og ansvar for nettbankløsningen avklart?						
2. Har banken sikret at kunden blir informert om hvordan nettbanktjenesten virker og skal brukes?						
3. Har foretaket dokumentert data- og funksjonsmodell og teknisk arkitektur for nettbankløsningen?						
4. Foreligger det driftsdokumentasjon for nettbankløsningen og er det etablert prosedyrer for oppdatering av denne?						
5. Foreligger det systemdokumentasjon for nettbankløsningen og er det etablert prosedyrer for oppdatering av denne?						
6. Lages det revisjonsspor som gjør det mulig å følge en transaksjon fra nettbanken gjennom prosesseringen ?						
7. Er det etablert kontroller som sikrer tilgang til kritisk kompetanse i forhold til IT-løsningene for nettbanken?						
8. Er det gjennomført en vurdering av nettbankløsningen som sikrer etterlevelse av lover, forskrifter, andre avtaler eller interne retningslinjer?						
<u>Kommentarer:</u>						

	Nettbank 3	Kontrollspørsmål		Sårbarhet		
				H	M	L
IT-Prosesser						
Sikkerhet		Ja	Nei			
	1. Har foretaket fastsatt kriterier for akseptabel risiko forbundet med bruk av nettbankløsningen?					
	2. Er det utarbeidet beskrivelser og gjort vurderinger av sikkerhetsmekanismene som benyttes til å autentisere kunden?					
	3. Er det etablert sikkerhetsmekanismer for å autorisere kunden for tjenester i nettbankløsningen?					
	4. Er det utarbeidet prosedyrer for håndtering og administrasjon av sertifikater og krypteringsnøkler?					
	5. Blir det utført årlig risikovurdering av nettbankløsningen ?					
	6. Blir kompetansen på nettbankløsninger oppdatert gjennom systematiske vurderinger av resultater fra internasjonale samarbeidsfora og ny teknologi?					
	7. Er det planlagt eller igangsatt utvikling av mobile løsninger for nettbank?					
	8. Hvis det er igangsatt utvikling av mobile løsninger for nettbank, er det utført sikkerhetsvurderinger av disse?					
<u>Kommentarer:</u>						

	Nettbank 4	Kontroll- spørsmål		Sårbarhet		
				H	M	L
IT-Prosesser						
Endringshåndtering og installasjon		Ja	Nei			
1. Blir alle forespørsler om endringer i nettbankløsningen dokumentert og behandlet gjennom endringshåndteringsprosessen?						
2. Sikrer rutinene for endringshåndtering at konsekvenser og risiko ved gjennomføring av en endring blir identifisert og vurdert før endringen blir godkjent/avvist?						
3. Blir det foretatt tester av løsningen før den settes i produksjon for å sikre at definerte krav til servicenivå blir opprettholdt etter at endringen er gjennomført?						
4. Blir plan for gjenoppretting utarbeidet og testet før omlegging til drift?						
5. Godkjennes produksjonssetting av endringer av den som er ansvarlig for nettbankløsningen?						
6. Er det etablert rutiner som sikrer at kunden blir informert om hvordan endringen påvirker tjenesten?						
7. Blir plan for katastrofeberedskap oppdatert ved endring?						
8. Blir endringer vurdert i forhold til meldeplikten for system for betalingstjenester ref. Kredittilsynets rundskriv 17/2004 av 30.november 2004? http://www.kredittilsynet.no/wbch3.exe?ce=13764						
<u>Kommentarer:</u>						

		Nettbank 5		Sårbarhet		
IT-Prosesser		Kontroll- spørsmål		H	M	L
		Ja	Nei			
Kontinuitets- og katastrofehandtering						
1. Foreligger det en kontinuitetsplan og er det etablert en prosess for oppdatering av denne ?						
2. Er kontinuitetsplanen samordnet med leverandørens kontinuitetsplan på området ?						
3. Gjennomføres det testing og trening i kontinuitetsplanen ?						
4. Er kontinuitet av nettbankløsningen sikret hvis ekstern IT-leverandør får problemer på grunn av egne driftsmessige, økonomiske eller juridiske -forhold ?						
5. Foreligger det en katastrofeplan og er det etablert en prosess for oppdatering av denne ?						
6. Er det utarbeidet kriterier for aktivering av katastrofeplanen ?						
7. Er katastrofeplanen samordnet med leverandørens katastrofeplan på området ?						
8. Gjennomføres det testing og trening i katastrofeplanen ?						
<u>Kommentarer:</u>						

	Nettbank 6	Kontrollspørsmål		Sårbarhet		
				H	M	L
IT-Prosesser						
	Avviks- og hendelsehåndtering	Ja	Nei			
	1. Er det prosedyrer som sikrer at problemer og hendelser som oppstår i den daglige driften av nettbankløsningen, registreres, analyseres og løses til avtalt tid ?					
	2. Er det utarbeidet prosedyrer for håndtering av forsøk på identitetstyveri mot nettbanken som for eksempel phishing, som omfatter informasjon til kundene og stenging av nettstedet?					
	3. Er det utarbeidet prosedyrer for håndtering av DDoS (Distributed Denial of Service) angrep mot nettbanken som beskriver hva som skal gjøres, for eksempel informasjon til kundene, gjenoppretting, eskalering, rapportering, oppfølging?					
	4. Gjennomføres det løpende vurderinger av alle hendelser som et ledd i forbedringsarbeidet?					
<u>Kommentarer:</u>						

	Nettbank 7	Kontroll- spørsmål		Sårbarhet		
				H	M	L
	IT-Prosesser					
	Overvåkning	Ja	Nei			
	1. Gjennomføres det uavhengig vurderinger av nettbankløsningens leveranseevne og servicegrad for å bekrefte at avtalte kvalitetskrav holdes?					
	2. Gjøres det vurderinger av brukertilfredshet, med hensyn på den service som blir levert ?					
	3. Er det en prosess for løpende overvåking av leveranser fra ekstern IT-leverandør for å sikre at disse skjer i henhold til avtalen ?					
<u>Kommentarer:</u>						