

Den finansielle infrastruktur og bruk av informasjonsteknologi

Risiko- og Sårbarhetsanalyse

Version: 2002-03-10/1.0

Author: Kredittilsynet, R-avdelingen, IT tilsyn

Innholdsfortegnelse

1	Innledning.....	1
1.1	Bakgrunn	1
1.2	Hensikt.....	1
2	Gjennomføring.....	3
2.1	Fremgangsmåte.....	3
2.1.1	Utvelgelse av områder	3
2.1.2	Intervjuobjekter.....	3
2.1.3	Sannsynlighet og konsekvens	4
2.1.4	Deltagelse i utførelsen av prosjektet	4
2.2	Avgrensninger	4
3	Teknologisk utvikling	5
3.1	Elektroniske løsninger	5
3.2	Utviklingstrekk	5
4	Utkontraktering	8
5	Teknologiens betydning for finansnæringens utvikling	9
6	Aktørenes roller	11
6.1	Finansnæringens IT-infrastruktur	11
6.1.1	Betalingssystemer	11
6.1.2	Innsamlings-/avregnings- og oppgjørssystemer.....	11
6.1.3	Verdipapirområdet	11
6.1.4	Verdipapiroppgjøret.....	12
6.1.5	Finansnæringens IT-infrastruktur	13
6.1.6	Spesielt om NICS avregnings-/oppgjør- og likviditetssystem	13
6.1.7	Bankenes roller	15
6.2	Noen viktige aktører i IT-infrastrukturen	15
6.2.1	NORGES BANK	15
6.2.2	Den norske Bank (DnB).....	15
6.2.3	Gjensidige NOR Sparebank	15
6.2.4	Oslo Børs	15
6.2.5	BBS	16
6.2.6	VPS	16
6.2.7	NOS	16
6.3	Transaksjonsvolum.....	17
6.3.1	Volumutvikling av transaksjoner og nettbank kunder	17
7	Nye tjenestetilbud.....	18
7.1	Den nye teknologiske hverdag.....	18
7.2	Om utbredelsen av e-tjenester	19
8	Sikkerhet og sikkerhetsløsninger.....	21
8.1	Tillit, en kritisk suksessfaktor for institusjonene	21

8.2	Forhold vedrørende sikkerhet	22
9	Kritiske risiko- og sårbarhetsområder	23
9.1	Hva fant vi ut gjennom analysen?	23
9.2	Sårbare områder	23
9.2.1	Utkontraktering av IT-tjenester	23
9.2.1.1	Konsentrasjon av datatjenester og EDB Business Partner ASA	24
9.2.2	Personavhengighet og kompetanse	24
9.2.3	Katastrofeløsninger	24
9.2.4	Endringshåndtering	25
9.2.5	Opplisting av samlepunkter	25
10	Foreslåtte tiltak	26
10.1	Hva gjør vi med informasjonen?	26

1 Innledning

1.1 Bakgrunn

Bankene har gjennom de siste 3 til 5 år gjennomgått store forandringer. Ikke minst har det skjedd mye på teknologiområdet, noe som har gitt grunnlag for introduksjon av nye produkter og tjenester. Endringer i måten å distribuere produktene ut til kundene på har vært et av områdene med store forandringer og Internett-teknologien må betegnes som et generasjonsskifte. Oppbyggingen av Internett som en åpen ny infrastruktur fungerer som en premissgiver og har gitt grunnlag for lansering av en ny og mer effektiv distribusjon mellom kunde og tjenesteyter. I finansmarkedet har bankene vært de mest aktive til å ta i bruk denne nye muligheten, særlig for distribusjon av nye tjenester gjennom Internett som distribusjonskanal.

Et annet forhold som også har hatt betydning er den relativt dramatiske restrukturering som har skjedd på det norske leverandørmarkedet for IT tjenester til finansnæringen. Det som tidligere i stor grad var relatert til Fellesdata (sparebankene) og IDA (forretningsbankene) (ble avviklet i 90 årene) som datasentraler, de store bankenes egne relativt tunge IT miljøer og mange alternative leverandører på enkeltområder, har i stor grad nå begrenset seg til EDB Business Partner som en meget dominerende aktør. Det er kun ErgoData, IBM, WM-Data og Merkantildata som på det norske markedet kan representere et realistisk leverandør alternativ til EDB Business Partner.

Dette skaper på den ene siden, en viss risikoeksponering, og på den andre siden et dårlig utgangspunkt for bankene når de skal forhandle nye avtaler. En slik konsentrasjon på IT siden gir imidlertid også nye muligheter ved at samlet IT miljø blir tyngre og samordning av ulike oppgaver blir enklere.

Leverandørendringene på det norske IT markedet har skjedd samtidig som bankene i større grad enn tidligere har utkontraktert sine IT oppgaver. Samlet sett har derfor effekten av endringene fått store dimensjoner. Samordningen er ikke lenger basert på et frivillig samarbeid av type ”spleiselag”, men er regulert i form av kommersielle kontrakter mellom partene og hovedmålsettingen til IT leverandøren er å skape økonomiske resultater for sine eiere. Dette gir på mange måter en helt ny ”setting”.

Internett har etablert seg som en ny og åpen infrastruktur og har på mange måter gitt støtet til en internasjonal bølge av nye muligheter. Aktørene ser på dette som nye muligheter som bør utnyttes. Sikkerhetsnivået vil bli begrenset av tilgjengelige teknologiske muligheter og økonomiske begrensninger. Konkurransen mellom bankene er hard. Etablering av nordiske finanskonsern har gitt grunnlag for å se på Norden som en stor markeds plass, hvor teknologi gjør at bankene kan nå kundene på en helt annen måte enn tidligere med sine produkter. Presset på å lansere nye produkter hurtig i denne infrastrukturen kan lett føre til eksponering av nye og sårbare områder.

1.2 Hensikt

Sett fra Kredittilsynets side har dette gitt en ny situasjon for den finansielle IT infrastruktur i Norge, noe som kan gi større grad av sårbarhet og dermed økt risiko for den daglige operasjon.

Med dette som bakgrunn besluttet Kredittilsynet seg for å skaffe seg bedre innsikt i dette området ved å kartlegge IT infrastrukturen for hele finanssektoren, på tvers av den enkelte institusjon. Basert på denne kunnskap ønsket Kredittilsynet å gjøre en vurdering av sårbarheten og analysere aktuell risiko for eventuelt å foreslå tiltak.

En bieffekt er at arbeidet kan bidra til å gi Kredittilsynet et bedre grunnlag for utforming av et nytt IT tilsynsprogram med sterkere fokus på operasjonell risiko. Arbeidet kan også gi oss bedre

innsikt i den teknologiske utviklingen og en mer aktiv bruk av IT-forskriften som et mer preventivt element i tillegg til den regulerende effekt.

Videre har Kredittilsynet til hensikt å foreta en årlig oppdatering av IT benyttet i den finansielle infrastruktur og kartlegging av sårbarhet og vurdering av risiko. Resultatet skal gi grunnlag for tiltak der dette ansees som nødvendig.

2 Gjennomføring

2.1 Fremgangsmåte

2.1.1 Utvelgelse av områder

Første del av arbeidet bestod i å kartlegge finansnæringens IT-infrastruktur. Oppmerksomhet ble gitt til de endringer og tillegg i infrastrukturen som følge av innføringen av Internett. For å kunne identifisere de kritiske IT-komponenter og enheter i infrastrukturen, var det nødvendig først å få en oversikt over de kritiske forretningsprosesser sett i forhold til de elektroniske tjenestene som institusjonene tilbyr markedet. Nøkkelpersoner i de sentrale institusjonene og deres datasentraler ble intervjuet og dokumentasjon av infrastrukturen ble innhentet.

Under arbeidet var vi spesielt oppmerksom på å få kartlagt de komponenter eller enheter som mangler reserveløsninger; "Single-point-of-failure".

Kartleggingen omfattet:

- De kritiske forretningsprosesser og de systemer som behandler disse.
- Internettrelatert utstyr og systemer med tilhørende sikkerhetssystemer og systemer som grenser opp mot Internett funksjoner.
- De datasystemer, nettverk, utvikling, drift, vedlikehold, administrasjon og sikring av de systemer som våre tilsynsenheter benytter.
- Beskrivelser av institusjonenes roller og funksjoner, oversikt over avtaler, lover og instruksjoner som næringen må etterleve, og over produkter og tjenester i finansmarkedet.
- Transaksjonsflyt, oppgjørs- og avregningsfunksjoner beskrives. Teknologi, sikkerhetsmekanismer og teknologiske løsninger som er involvert vurderes og kartlegges.
- Systemer som de siste 5 årene er blitt vesentlig endret med mulig innvirkning på nye tjenester.
- Meglernes elektroniske tilknytning til Oslo Børs handelssystem.

2.1.2 Intervjuobjekter

Andre del av arbeidet som bestod i å vurdere risiko- og sårbarhet, startet med en intervjurunde i institusjonene hvor vi ønsket å identifisere risikoområder. Institusjonenes interne risikorapporter ble brukt i arbeidet. De viktigste intervjuobjekter var:

-Den norske Bank, Nordea (daværende Kreditkassen), Gjensidige NOR (Sparebanken NOR og Gjensidige NOR Spareforsikring), skadeforsikringsselskapet if. Et møte ble også avholdt hos Nordea AB (daværende MeritaNordbanken) i Stockholm.

-EDB Fellesdata, Bankenes betalingssentral (BBS), Oslo Børs, Verdipapirsentralen og NOS Clearing.

-Andre relevante institusjoner:

Møter er avholdt hos Financial Services Authority, Storbritannia og Federal Reserve Bank i Chicago. Diskusjoner er blitt gjennomført med nordiske tilsynsmyndigheter. Møte med CSC Solution Norge AS ble holdt for å se på utkontraktering av tjenester.

2.1.3 Sannsynlighet og konsekvens

Det er vanskelig å forutsi sannsynligheten for at en hendelse kan inntreffe. Skadeomfanget er vanligvis avhengig av hvor lenge en tjeneste er utilgjengelig.

Under arbeidet ble det tatt hensyn til fungerende reserveløsninger hvis deler av tjenestene eller systemene svikter. Hvis en reserveløsning trer inn under svikt av en driftsfunksjon, blir risikoen vurdert på bakgrunn av sannsynligheten for at også reserveløsningen skal svikte.

Ringvirkninger blir vurdert der slike effekter kan forventes. Noen enkle feil kan forårsake ringvirkninger som kan lamme større systemer. Mulige kjedereaksjoner er vanskelig å identifisere.

2.1.4 Deltagelse i utførelsen av prosjektet

Prosjektet har hatt deltagere fra flere avdelinger i Kredittilsynet. Kvalitetssikring er utført av Ingvald Thuen, Advanced Information Security (AIS).

Per Steinar Davidsen, IT tilsyn.

Svein Erik Dovran, IT tilsyn.

Harald A. Hammer, Finans- og Forsikringsavdelingen.

Aud Kogstad, Markedsavdelingen.

Anders N. Kvam, Finans- og Forsikringsavdelingen.

Stig Ulstein, IT tilsyn.

Observatør: Steinar Guribye, Norges Bank

2.2 Avgrensninger

I arbeidet med risiko- og sårbarhetsanalysen har vi gitt prioritet til forhold som er av betydning for den videre utarbeidelse av en relevant oppjustert IT-forskrift og IT tilsynsprogrammer.

Følgende forhold omfattes ikke:

- De tradisjonelle systemene i infrastrukturen, som for eksempel basissystemene, er ikke sett på uten at det er spesielle forhold som også berører den nye teknologien.
- Oppgjørssystemer hos BBS for tradisjonelle tjenester.
- Institusjoner som er mindre kritiske i IT-infrastrukturen.
- Telefon- og datatjenesteleverandører, el-kraft, vann og annen ekstern infrastruktur. Det refereres til Willoch-utredningen som beskriver sårbarhet i denne del av infrastrukturen.
- Finansdepartementet og Norges Bank.

3 Teknologisk utvikling

Den teknologiske utviklingen relatert til bank- og finansvirksomhet har gjennomgått store forandringer de siste årene. Fra å være et hjelpemiddel til behandling av store masserutiner sentralt, gikk utviklingen i retning av direkte koplet ("online") distribusjon internt i finansinstitusjonene. Det neste skrittet var å gi støtte til bedre arbeidsflyt og kommunikasjon, noe som førte til en vesentlig bedring av informasjons- og beslutningsstøtte-systemer. I dagens situasjon er det teknologiske løpet kommet så langt at nye distribusjonskanaler for produkter og tjenester direkte til kunden etableres for en stadig større del av finansinstitusjonenes produkt- og tjenestespekter. En viktig del av dette har også vært introduksjon av kunde- og produktlønnsomhetsløsninger kombinert med kunderelasjonssystemer.

Basistjenestene er på mange måter de samme, mens det særlig på betalingsformidlingssiden har foregått en produktutvikling etter hvert som ny teknologi har gjort dette mulig. Driverne her har vært en kombinasjon av konkurranse og teknologisk utvikling hvor etablering av Internett som infrastruktur, sammen med introduksjon av en internasjonal industristandard for brukergrensesnitt (Microsoft), nok har vært viktige premiss. Samlet har dette gitt grunnlag for store rasjonaliseringsgevinster for finansinstitusjonene. De nye Internett-baserte løsningene har også introdusert nye problemstillinger knyttet til sikkerhet og risiko og kan dermed gi økt sårbarhet. Et annet forhold er økt kjøp av ferdige løsninger, kjøp av konsulenttjenester og utkontraktering av betydelige deler av IT aktivitetene, som også introduserer nye problemstillinger.

3.1 Elektroniske løsninger

Det som følger av denne utviklingen, er ofte at ny teknologi tas i bruk i stor skala før en har vunnet erfaring av teknologien og vet nok om hvordan tjenestene best kan sikres. Det konkurransemessige presset for å komme først i markedet med nye elektroniske tjenester er så betydelig at det kan være fare for at sikkerheten ikke alltid blir tilstrekkelig ivaretatt. Videre er lojaliteten fra kundene i ferd med å forsvinne. En ny bankforbindelse kan etableres med noen tastetrykk. Markedet er i konstant endring og i mange situasjoner er det teknologien som driver forretningsprosessene, ofte på bekostning av rutiner og sikkerhetsløsninger. I finansnæringen har bankene hittil vært de viktigste pådrivere i denne utviklingen, men også i verdipapirmarkedet er det etablerte flere nettbaserte løsninger for handel i verdipapirer. Forsikring ligger noe etter når det gjelder å ta i bruk teknologi på dette området.

Det som regnes som elektroniske tjenester i bank, er kundebetjente systemer uten kontakt med bankens ansatte, og består hovedsakelig av følgende: Minibank, Bedriftsterminaler, Banktjenester over Internett, Debet- og kredittkort, e-penger, e-faktura, eGiro og Kontofontjenester.

3.2 Utviklingstrekk

Følgende utviklingstrekk synes å være sentrale på teknologiområdet:

Finanskonsernarkitektur. Dette er systemløsninger der basissystemer og databaser knyttet til et finanskonserns virksomhetsområder og produkter ligger i bunnen, f.eks innlåns-, utlåns-, liv- og skadeforsikringssystemer. Over dette nivået utvikles det saksbehandlings- og kontorstøttesystemer, samt datavarehus som integrerer all informasjon fra produktsystemene. Her sentraliseres også alle kundedata. På toppen ligger dialog- og kommunikasjonssystemer (Internettbasert) som integrerer all informasjon fra de øvrige systemer og som samtidig representerer grensesnittet og kanalen mot kundene.

Etablering av større finanskonserner. Sammenslåinger er ofte motivert ut fra større volum = lavere enhetskostnad. En effekt av dette, sammen med økt bruk av elektroniske løsninger, er en

reduksjon av de manuelt betjente ekspedisjonsenheter. Samtidig skjer en sentralisering og konsentrasjon av backoffice (sentralisert manuell/maskinell behandling av data) kombinert med en ytterligere automatisering. Resultatet av dette er reduserte kostnader, men en uønsket bieffekt er også redusert kompetanse og faglige miljøer både sentralt i bankene og andre enkeltselskaper i konsernet, men ikke minst ute i de enkelte distriktskontor. Dette i seg selv gir en økt sårbarhet og dermed en økt risiko.

Multikanalkonsepter og delte arbeidsprosesser. Dette innebærer at finansforetaket har flere måter å kommunisere med kundene på, f.eks bankkontor, callsenter, nettbank via PC eller PDA (Personal Digital Appliance/håndholdt device). Et fellestrekk er at kundene gjør mer selv og at virksomheten i større grad vil dreie seg om håndtering av kundeavtaler, produktutvikling og bruk av informasjonsteknologi. En distribusjonskanal som vil bli viktigere, er bruken av håndholdte enheter som mobiltelefon og håndholdte PDA'er. Det er et klart trekk at mobiltelefon-teknologien og PC-teknologien vokser nærmere hverandre og nye hybrider oppstår med basis i de to teknologier. Dette vil representere et økende brukt grensesnitt mot bankens kunder.

Utkontraktering av driftsoperasjon til IT-leverandør (datasentral), som har vært den tradisjonelle løsningen og som i stor grad har vært benyttet av norske banker, eller ved sentralisert computing, gjennom avtale med en såkalt ASP leverandør (Application Service Provider). Dette er løsninger som brer om seg og innebærer at et foretak betaler en viss pris for å sette driften av IT-systemet ut til en ASP leverandør. All prosessering skjer gjerne utenfor foretaket, og foretakets ansatte sitter på såkalte "tynne" klienter, i praksis standard PC'er. Det er ASP operatøren sin oppgave å sørge for at bedriften til enhver tid har tilgang til de aktuelle program og data. I dette inngår også programvaredistribusjon og kontroll med lisenser.

Utvikling av datavarehus. Dette gjelder særlig kundedatabaser og skreddersøm av brev og dokumenter der kundeinformasjon inngår (DM –Direct Mail utsendelser). Dette gir også grunnlag for etablering av nye løsninger for kunde- og produktlønnsomhet, kunderelasjoner og mer aktiv bruk av kundetilpassede produktløsninger.

Imaging/elektronisk arkiv inkl elektroniske signaturer. Dette innebærer scanning, overføring og lagring av informasjon, som muliggjør en fullstendig elektronisk saksbehandling. Enkelte banker har allerede kommet langt på dette området.

Systemstøtte næringslivskunder. Dette kan være e-faktura, factoring, cash management og direkte grensesnitt til kundens egne løsninger, som igjen gir grunnlag for videre rasjonaliseringer både hos kunden og i finansinstitusjonen.

Det er en generell trend at standard programvares størrelse og funksjonalitet økes kraftig. Dette skjer i stor grad basert på en fortsatt tredelt arkitektur (arbeidsstasjon, server og sentralmaskin), men hvor arbeidsstasjonens rolle og kapasitetsbehov øker for hvert år. Summen av dette har gitt større krav til lagring og administrasjon av data og funksjoner og introdusert nye problemstillinger. Teknologiske arkitekturer i dag er fortsatt basert på stormaskiner, kombinert med servere i nettverket, sammen med stadig mer kapasitet til arbeidsstasjoner. I hvilken grad denne utviklingen vil fortsette er uvisst. En helt klar trend er at sentrale organisasjoner tar hånd om operasjon og drift av sentrale maskiner, servere og nettverk. Interoperabilitet er kravet for å få til internasjonale IT-løsninger. Systemer må også kunne virke over grensene. De store kredittkortselskapene leder an her, men også finanskonsern over landegrenser vil være en kraftig pådriver for å utvikle og etablere slike løsninger. Danske Bank og Fokus Bank i Norge er et eksempel på dette. Det er sannsynligvis kun et tidsspørsmål før vi vil se det samme i relasjon til Nordea og andre nordiske konstellasjoner. IT-kompetanse kan bli en mangelvare når det gjelder nisjeløsninger. Dette er en naturlig følge av etableringen av internasjonale finanskonsern hvor synergi og kostnadsreduksjon er viktige parametre. IT-kostnadene utgjør en økende andel av de totale kostnader, anslått til mellom 15 til 25% av totale kostnader i dagens situasjon.

Det er liten tvil om at teknologiutviklingen legger til rette for nye aktører i finansnæringen, særlig innenfor enkelte nisjer. Rene nettbanker (Skandiabanken) og nye aktører som f.eks ICA-

bank (nylig fått konsesjon i Sverige) er eksempler på det. En observasjon er at det foreløpig er få i det norske markedet som opptrer som nisjeaktører.

4 Utkontraktering

Finansnæringen i Norge har i over 30 år satt ut drift av datatjenester til eksterne leverandører. Hensikten har vært kostnadsreduksjoner, økt fleksibilitet, redusert risiko og bedre effektivitet. Fra kundenes side har dette gitt store fordeler i form av høy grad av samordning, særlig når det gjelder betalingstjenester.

Utkontraktering av IT-tjenester er et generelt utviklingsstrekk i finansnæringen internasjonalt. I Norge er situasjonen den at alle banker har satt ut IT-driften av sine kjerneløsninger og store deler av utviklings- og forvaltningsarbeidet av systemløsningene. Det er et spørsmål om dette fenomenet har hatt betydning for strukturen i norsk bankvesen. I andre land har behovet for investeringer i bl.a. IT-løsninger m.v. vært en driver for alliansebygging og fusjoner for å utnytte stordriftsfordeler. I Norge har dette så langt ikke vært dominerende. Selv de minste banker har vært i stand til å dra nytte av avanserte teknologiske løsninger til en overkommelig pris pga samarbeid og utkontraktering.

Ulempene knyttet til slik utkontraktering er imidlertid flere. Det er lett å bli for avhengig av sine leverandører ved at institusjonen får redusert kontroll og autonomi i kritiske deler av virksomheten. Det kan være praktisk vanskelig å skifte til annen leverandør, og det er kostbart og vanskelig å bygge opp igjen denne delen av virksomheten i egen institusjon. Styrkeforholdet mellom kunde og leverandør kan lett endre seg. Når tjenesten er satt bort, er mulighetene for læring og innovasjon redusert, og institusjonen har ikke lenger egen kompetanse på området. Dette gjør at det kan bli vanskelig å forhandle på like fot med sin leverandør når det gjelder kontraktsinngåelser, endringer eller å få balanserte avtaler. Konkurransesituasjonen og den teknologiske utviklingen gjør at det er viktig for bankene å beholde en stor grad av frihet. Dette kan være vanskelig å kombinere i samband med inngåelse av langsiktige kontrakter for vitale IT funksjoner.

I Norge har avhengigheten til tjenesteleverandører som EDB Business Partner økt dramatisk. EDB Business Partner har i løpet av de siste 2-3 år overtatt flere av finansnæringens felles datasentraler, og er nå så godt som enerådende på det norske bankmarkedet. Et annet forhold er en tendens til en videre ”utkontraktering” av tjenester fra den primære tjenesteleverandør til andre underleverandører, dels innenfor og utenfor eget konsern. Dette gir større risiko og utfordringer for så vel institusjonene som tjenesteleverandører mht. oppfølging av leveranser, service og kvalitet.

Hvis institusjonen kan benytte en alternativ (”second source”) leverandør, blir det mer reell konkurranse og leveransen blir mer sikker fordi en har reserveleverandør hvis hovedleverandøren skulle svikte. Dette er imidlertid en kostbar løsning som få nytter seg av. Reserveleverandøren må minst ha 20 – 30% av volumet for at det skal kunne gi akseptable priser og lønnsomhet.

Nye former for utkontraktering er ASP (se side 6) for Internett baserte løsninger eller ISP (Internet Service Provider) som er en tilsvarende løsning for kommunikasjonsnettverk og teledataløsninger.

5 Teknologiens betydning for finansnæringens utvikling

Bankene har også tidligere kunnet tilby sine kunder brukergrensesnitt mot sine banksystemer som gjorde det mulig for bankkunden å utføre banktjenester selv. Bankenes markedsstrategier er noe endret etter at Internett ble tatt i bruk som en kanal for å nå kundene. Drivkreftene i utviklingen av nettbaserte løsninger er:

Konkurranse; flere rapporter viser at det er konkurransemessige forhold som er hovedgrunnen til at bankene innfører nettbank. Kostnadsreduksjoner og omsetningsvekst ligger henholdsvis på annen og tredje plass. Ved å innføre nettbank ser de en mulighet til å beholde eksisterende kunder og tiltrekke nye kunder. Utenlandsk konkurranse i privatkundesegmentet er relativt nytt. Skandiabanken har ved inngangen til år 2001 fått 100 000 norske nettbankkunder. Det er viktigere for banken å beholde den direkte kundetilknytningen, ansiktet mot kunden og lojaliteten enn nødvendigvis selv å utføre de øvrige ledd i verdikjeden.

Kostnadseffektivitet; kundene utfører arbeidet med oppdraget selv og banken stiller til rådighet et fullelektronisk automatisert banksystem. Bankenes transaksjonskostnader blir på denne måten vesentlig lavere enn før. Den reelle kostnaden ved å gjennomføre en transaksjon vil variere avhengig av den kanal som blir brukt. En tjeneste utført ved skranken koster i gjennomsnitt 22 kroner, en minibanktransaksjon og en kortbetaling kan koste 1,50 kroner og en nettbanktransaksjon er estimert til 20 øre. Store besparelser kan oppnås når for eksempel utsendelse av kontoutdrag til kundene blir erstattet med elektroniske løsninger.

Ubegrenset tilgjengelighet i forhold til geografi og tid; tjenestene er tilgjengelig når kunden måtte ønske det og hvor kunden måtte befinne seg. Tilbakemeldinger fra banken kan skje raskt.

Branding; det er viktig for banken å vise omgivelsene hvilke merker eller samarbeidspartnere den har og at den gir sine kunder fordeler av samarbeidet. Bankenes betalingskort, hvor Visa og bankens logo vises sammen, er et eksempel. Branding er antatt å øke i omfang når blant annet smartkort blir tatt i bruk for betalingskort og elektroniske penger. Smartkort med digitale sertifikater kommer til å bli brukt for autentiseringsformål i elektronisk handel, disse forventes å vise logo for samarbeidspartnere med produkter. Branding bidrar til å bygge opp kundelojalitet og kryssalg.

Bruk av Internett og oppbygging av datavarehus er høyt prioritert av de store institusjonene. Gamle og nye systemer samler data i et sentralt datavarehus, som muliggjør felles bruk av kundedata og ledelsesdata i hele konsernet, samtidig med at alt tilrettelegges for at kundene betjener seg selv. Dette skaper rom for økt effektivitet, kostnadsreduksjoner og synergier mellom virksomhetsområder, men også økt press i forhold til styring og strategivalg.

I en rapport utarbeidet av Finlands sentralbank i juli 2000 konkluderes det med at teknologiutviklingen skaper store strategiske utfordringer for finansnæringen. Tilsvarende blir det i en rapport fra den svenske Finansinspektionen (april 2000) pekt på de strategiske utfordringer i denne sammenheng. Umiddelbare konsekvenser er:

- Økt press for å redusere antall ekspedisjonssteder og ansatte for å oppnå kostnadsbesparelser. Nettbaserte løsninger innebærer at kundene betjener seg selv, noe som frigjør institusjonenes egne ressurser. Dessuten blir geografisk tilstedeværelse ikke i samme grad en markedsfaktor, da nettløsningen alltid er ”åpen” og ”tilstede”. Distribusjon av tjenester får en annen form og ekspedisjonsapparatet kan reduseres vesentlig.
- Endring i finansnæringens medarbeiderprofil i retning av økt kompetanse innenfor rådgivning, markedsføring, IT og mer sofistikerte tilleggstjenester. Det legges større vekt på produktutvikling og markedsbearbeidelse enn tradisjonell betjening av kunder.
- Kundelojaliteten er synkende, og det kreves mer for å beholde eksisterende kunder og enda mer for å øke kundegrunnlaget. Finansnæringen må derfor demonstrere høy kompetanse på produkt, markedsføring og markedsbearbeidelse. Kompetanse innen IT blir en forutsetning, da teknologien i seg selv er en av drivkreftene for produktutvikling og distribusjon av tjenester
- Intensivert utkontraktering av IT-relaterte aktiviteter. Behovet for spesialisering medfører generelt at aktiviteter som ikke er knyttet til kjerneaktiviteter utkontrakteres. Utkontraktering av IT-tjenester har i Norge lang tradisjon og øker i omfang.
- Strukturendring i form av fusjoner, alliansebygging og samarbeid mellom aktører i finansmarkedet både når det gjelder produksjon og distribusjon av tjenester. Synkende kundelojalitet og økt prispress er drivkrefter for rimeligere og mer effektive tjenester.
- Flere allianser mellom finansnæringen, IT-selskaper og teleoperatører for å optimalisere produktutviklingen. Dette er en sannsynlig utvikling på grunn av at skillene mellom finansielle produkter og applikasjonene som presenterer dem blir visket ut.
- Økt konkurranse og bransjeglidning. Teknologiens muligheter for lønnsomhetsvekst gjennom at distribusjonskanaler blir rasjonalisert er konkurransedrivende. Dessuten skaper bruk av nettbaserte løsninger muligheter for e-handel, der f.eks en banks web-side kan knytte sammen selgere og kjøpere av varer og tjenester, der nettbanken blir ”oppgjørssted”. Dette åpner for en viss bransjeglidning der banktjenester kan integreres med andre ikke-finansielle produkter som ”bank i butikk konsept”.
- Økt operasjonell risiko. Finansnæringens sårbarhet øker ved at kundene har et direkte grensesnitt til driftssystemene slik at alle feil og uregelmessigheter blir blottlagt umiddelbart. Tidligere var det slik at foretakenes kontrollrutiner fanget opp slike forhold før kundene fikk sin informasjon. Dette, i kombinasjon med at tilnærmet alle IT-tjenester er utkontraktert, medfører at store deler av foretakenes virksomhet faktisk er utenfor den umiddelbare, daglige direkte kontroll. Dessuten er sårbarhets- og sikkerhetsaspektene knyttet til den nye teknologien er meget utfordrende, spesielt hva gjelder uautorisert inntrengning.

Disse utfordringene krever mye av institusjonenes strategiske og operative tilpasningsevne, og innebærer på ulike måter en annen måte å drive finansvirksomhet på enn før. Det knytter seg både strategisk og operativ risiko til teknologiutviklingen. Et annet forhold er de ulike strategier som bankene velger. Enkelte banker satser på å være universalbank (full service bank), mens andre satser på kun å være en nisjebank. Ut fra konkurransesituasjonen vil nok hvert enkelt produkt ut mot markedet allikevel bli målt ut fra pris, tilgjengelighet og kvalitet. Dette vil gi et stort konkurransemessig press på universalbankene med hensyn til pris, funksjonalitet og kvalitet. Resultatet kan bli merkbart større forskjell på bankenes resultater.

6 Aktørenes roller

6.1 Finansnæringens IT-infrastruktur

Figur 1) på side 11 viser et bilde av hovedstrukturen for den finansielle IT infrastruktur. Denne struktur kan også fremstilles mer som et teknologisk bilde med kommunikasjonsforbindelser. Det er også viktig å merke seg noen hovedroller som inngår i begrepene:

- Betalingssystemer
- Innsamlings-/avregning og oppgjørssystemer
- Verdipapirområdet

Utforming og drift av avregningssystemene kan ha betydning for landets finansielle stabilitet.

Nedenfor vil vi forklare hvert av de nevnte områder nærmere:

6.1.1 Betalingssystemer

Et betalingssystem har som formål og sørge for overføring av betalingsmidler. Et slikt system er en formalisert ordning bestående av tekniske innretninger, prosedyrer og avtaler som kan beskrives og avgrenses til en enhet og som er til for å sikre pengestrømmen. Begrepet betalingssystem benyttes som en samlebetegnelse for både systemer for betalingstjenester (bankene) og for interbanksystemer (Norges Bank). Det er bankene som har kontakt med kundene når et betalingsoppdrag skal formidles. Har kundene konti i samme bank, avregnes kontiene lokalt. Har kundene konti i ulike banker, oppstår det fordringsforhold mellom bankene som skal gjøre opp. Avregningen er en regneoperasjon hvor den enkelte banks fordringsposisjon i forhold til de øvrige deltakere beregnes. Norges Bank foretar avregningen mellom bankene og fungerer som en oppgjørsbank, og de enkelte banker hhv. godskrives eller belastes i henhold til de beregnede disposisjoner. Større banker som, DnB, Gjensidige NOR Sparebank og Nordea Bank Norge kan fungere som oppgjørsbank for grupperinger av banker.

Bankene har etablert egne rutiner for bilateral avregning av større transaksjoner, den såkalte mellomavregningen som nyttes av store banker. Disse transaksjoner består hovedsakelig av overførslar fra utlandet, innenlandske overførslar mellom kunder, forretninger som bankene gjør seg imellom og betaling for verdipapirhandel. Transaksjonene avregnes bilateralt mellom par av banker og gjøres opp ved kontoregulering i Norges Bank. Slike meldinger sendes via SWIFT direkte til Norges Bank. Bankenes likviditetssystem NICS hører under Norges Bank og driftes av BBS.

6.1.2 Innsamlings-/avregnings- og oppgjørssystemer

De fleste betalingsoverføringer blir i dag kanalisert inn i masseavregnings- og oppgjørssystemer via datasentralene Bankenes Betalingssentral eller EDB Fellesdata. Avregningen resulterer i netto posisjoner for den enkelte deltakerbank og gjøres opp i en oppgjørsbank. De fleste forretningsbankene og de største sparebankene deltar i avregningen i BBS. Nettoposisjonen fra BBS-avregningen gjøres opp ved regulering av bankenes foliokonti i Norges Bank.

6.1.3 Verdipapirområdet

Verdipapirområdet består av Oslo Børs, Mellommenn (verdipapirforetak og banker), Verdipapirsentralen (VPS) og NOS Clearing (NOS). Børsen er markedsplass for børsmedlemmene som hovedsakelig er meglere, banker og utenlandske investorer. Avregningen i forbindelse med verdipapiroppgjøret blir imidlertid utført i VPS, mens pengeavregningen i forbindelse med handel i derivater blir utført i regi av NOS. VPS registrerer og avregner transaksjoner og posisjoner både for oppgjør med verdipapirer og penger. For verdipapirsiden er

VPS både rettighetsregister og oppgjørsenhet. Verdipapirforetak som deltar i oppgjøret, har en oppgjørskonto i Norges Bank som ikke har trekkrettigheter. NOS er en avregningssentral for standardiserte finansielle derivater. Sentralen har i hovedsak ansvaret for avregning og risikokontroll av opsjoner og futures handlet på Oslo Børs. Opsjonene avregnes i VPS på vegne av NOS, mens futures avregnes i NOS' egne systemer. NOS er en sentral motpart både i opsjons- og futureskontrakter. Penge delen av futuresoppgjøret fortas ved at hver deltaker er tilknyttet en depotbank for margininnbetalinger og oppgjør, og posisjonene i futureoppgjøret blir et rent interbankoppgjør mellom depot-bankene. For opsjonsoppgjøret har verdipapirforetakene oppgjørskonti i Norges Bank, og har en egen garantiordning. Det er ingen trekkrettigheter knyttet til disse konti. Utligningen av posisjonen i opsjonsoppgjøret foretas over bankenes foliokonti i Norges Bank.

6.1.4 Verdipapiroppgjøret.

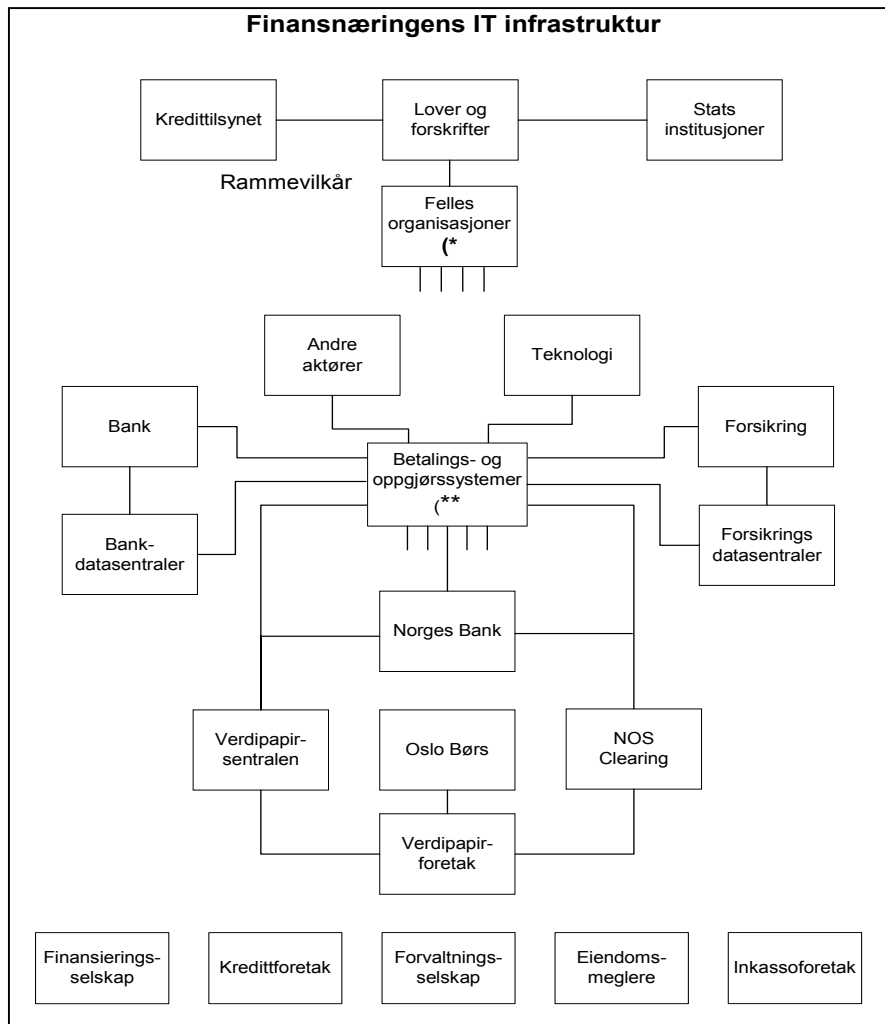
Levering av finansielle instrumenter mot samtidig betaling skjer i verdipapiroppgjørssystemet (VPO) ved at det foretas et pengeoppgjør og et verdipapiroppgjør. VPS utfører verdipapiroppgjøret. VPS foretar dessuten pengeavregning mellom de sentrale deltakerne. Pengeoppgjøret mellom deltakerne i VPO skjer gjennom Norges Bank. VPS slutfører verdipapiroppgjøret når Norges Bank har akseptert pengeoppgjøret.

Pengeoppgjøret gjennomføres på nettobasis i Norges Bank etter at VPS i løpet av kvelden før oppgjørslag har beregnet den enkelte oppgjørslagers nettoposisjon i oppgjøret. Nettooppgjør fremkommer ved at to eller flere oppgjørslagers fordringsforhold motregnes slik at den enkelte oppgjørslager får en nettoposisjon i oppgjøret. Meglerne melder handlene til VPS med angivelse av oppgjørslag. Dette oppgjøret skjer i VPS. Pengeavregningen mellom meglerne oversendes Norges Bank til oppgjør. Når dette er gjennomført kan VPS flytte papirene mellom deltakernes verdipapirkonti.

Nordic Electricity Clearing House ASA (NECH), har, fra 5.mars 2002, lisens som clearing operatør for vare derivater med strøm produkter som underliggende instrumenter.

6.1.5 Finansnæringens IT-infrastruktur

Figur 1. Oversikt over finansnæringens IT-infrastruktur



* Sparebankforeningen, Finansnæringens Hovedorganisasjon, Bankenes standardiseringsorganer.

** Et viktig element her er NICS avregnings-, oppgjørs- og likviditetssystem operert av BBS.

6.1.6 Spesielt om NICS avregnings-/oppgjør- og likviditetssystem

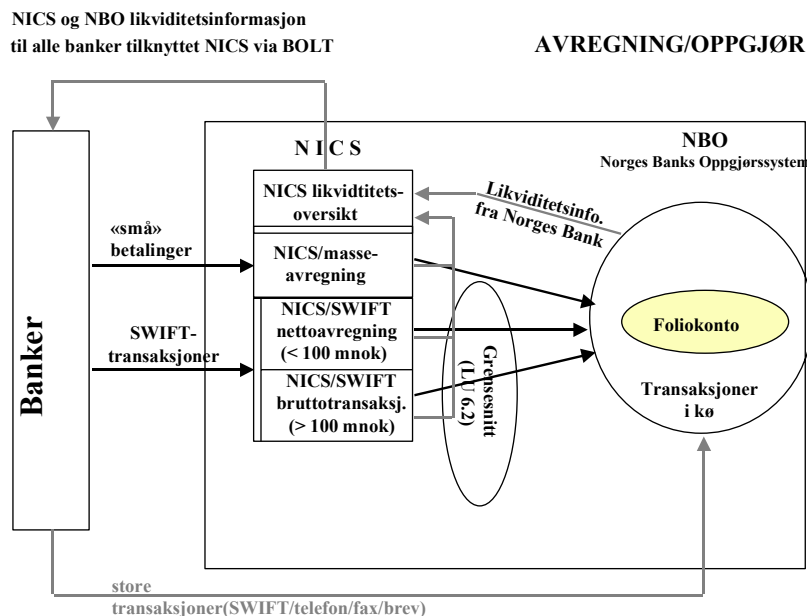
Nedenfor vil vi gi en kort forklaring av NICS (Norwegian Interbank Clearing System) samt vise et logisk bilde av hovedfunksjoner:

NICS omfatter tre hovedområder:

- **NICS MASSE** - avregning og generering av oppgjørsposter for massetransaksjoner fra banker/ datasentraler og fra mottaks-/innsamlingssystemer i BBS

- **NICS SWIFT** - avregning og generering av netto oppgjørsposter for SWIFT-transaksjoner med beløp mindre enn 100 mill NOK, umiddelbar oversendelse av brutto oppgjørsposter for SWIFT-transaksjoner med beløp på 100 mill NOK eller mer, samt transaksjoner merket "HASTE" eller "REG".
- **NICS LIKVIDITET** - likviditets- og oppgjørsinformasjon fra NICS og NBO (Norges Banks Oppgjørssystem) via BOLT (BBS On-Line Tjenester).

Figur 2. Oversikt over NICS funksjonalitet og grensesnitt



NICS er utviklet, og videreutvikles av BBS på vegne av Norges Bank og bankene, for å samle avregning i NOK på ett sted og slik at bankene kan eliminere bruk av mellomregningskonti og få mindre manuell oppfølging.

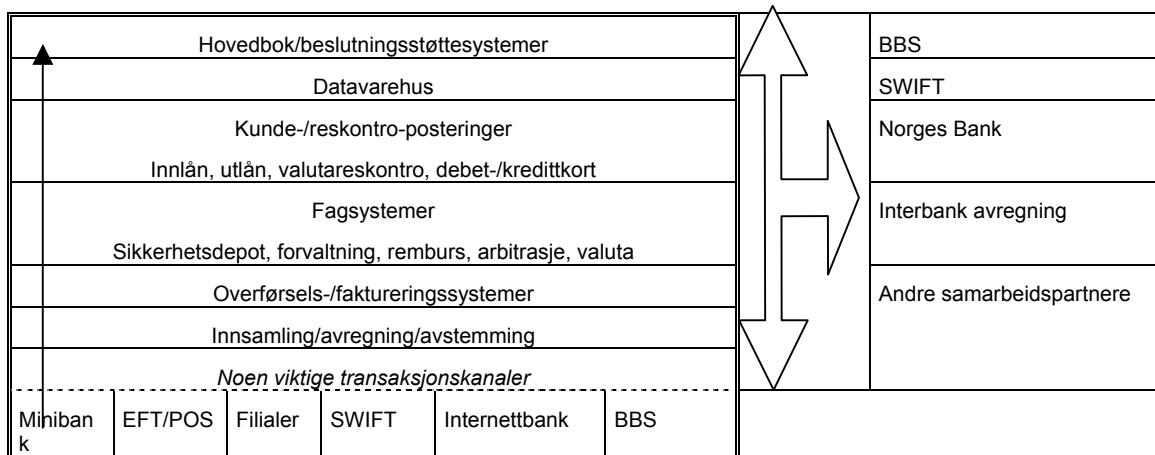
NICS/ NBO Likviditetsoversikt er utviklet i et prosjektsamarbeid mellom bankene og Norges Bank, i henhold til avtale mellom Norges Bank og de to bankforeningene. Likviditetsoversikten gir informasjon både fra NBO og fra NICS, og er et automatisert, og til enhver tid ajourført, likviditetssystem. NICS/ NBO Likviditetsoversikt er i dag et nødvendig verktøy for bankens daglige likviditets- og risikostyring.

BBS er driftsenhet for NICS gjennom avtale med Sparebankforeningenes Servicekontor (SPS) og Bankforeningens Servicekontor (BAS).

Forholdet mellom NICS og NBO er regulert i egen avtale mellom Norges Bank og BAS/ SPS.

6.1.7 Bankenes roller

I tillegg til den felles IT infrastruktur er det viktig å kunne se dette i sammenheng med bankenes egne logiske hovedfunksjonsområder og hvordan dette samvirker med den felles finansielle infrastruktur. Et skjematisk bilde av en banks hovedfunksjoner kan fremstilles på følgende måte:



Figur 3. Oversikt over en banks hovedfunksjoner

Bankens egen virksomhet mottar og avleverer transaksjoner til kunder og samvirkende instanser. Deler av bankens virksomhet kan være utkontraktert til en leverandør som utfører tjenesten på vegne av banken eller banken kan ivareta denne i egen regi. Dette endrer ikke bankenes logiske bilde av funksjoner og transaksjonsflyt.

6.2 Noen viktige aktører i IT-infrastrukturen

6.2.1 NORGES BANK

Norges Bank har etablert Norges Banks Oppgjørssystem (NBO) som ivaretar realtidsoppgjør og saldooppdateringer på bankenes foliokonto i Norges Bank, dekningskontroll og køordning. NBO driftes og forvaltes av Norges Bank.

6.2.2 Den norske Bank (DnB)

DnB har konsesjon fra Norges Bank som oppgjørspartner for egne kontorer og sine samarbeidsbanker.

6.2.3 Gjensidige NOR Sparebank

Gjensidige Nor Sparebank har konsesjon fra Norges Bank som oppgjørspartner for sine samarbeidsbanker.

6.2.4 Oslo Børs

Oslo Børs opererer på 3 markedsplasser, aksjer, obligasjoner og derivater.

Oslo Børs tilbyr sine brukere et moderne handelssystem for aksjer.

Introduksjonen av det nye handelssystemet medførte en overgang fra det gamle handelssystemet, der handel i aksjer og grunnfondsbevis hovedsakelig ble utført over

telefon, til et system basert på automatisk slutning av ordre som er innlagt elektronisk av kjøpere og selgere.

Oslo Børs er dermed over fra sentralisert handel, der det tidligere systemet krevde meglernes fysiske tilstedeværelse i børsbygningen, til desentralisert handel. Børsens medlemmer utfører dermed nå all handelsaktivitet fra eget kontor.

6.2.5 BBS

BBS besørger innsamling, autorisasjon og oppgjør av transaksjoner for en rekke transaksjonstyper. I 2000 behandlet BBS ca. 750 millioner transaksjoner i den fysiske verden og på Internett. Ved årsskiftet 2001 hadde norske banker ca. 52.500 terminaler utplassert til bruk i handel og næringsliv.

NICS er bankenes felles system for avregning mellom banker med oppgjør via foliokonto i Norges Bank. Driften av systemet er utkontraktert til BBS. NICS omfatter avregning av ordinære betalingstransaksjoner (NICS Masse) og avregning av høyverditransaksjoner så som låneforretninger mellom banker og store kundetransaksjoner (NICS SWIFT). I løpet av år 2000 avregnet BBS gjennom NICS betalinger til en samlet verdi av 43.081 milliarder kroner.

6.2.6 VPS

VPS har fire kundegrupper:

- Avtale Kontofører (Investorer)

VPS er et offisielt rettighetsregister hvor eiendomsrett og andre rettigheter til et verdipapir registreres. Det sentrale elementet i denne tjenesten er Investors VPS konto, som kan benyttes for aksjer, grunnfondsbevis, andeler i verdipapirfond, obligasjoner, sertifikater og derivater.

- Utsteder

VPS administrerer eierregisteret for verdipapirer. Flere tjenester tilbys med bakgrunn i eierregisteret, som f.eks rutiner for utbetaling av utbytte, splitt eller sammenslåing av aksjer og fondsemisjoner.

- Verdipapirforetak

VPS yter tjenester for avregning og oppgjør av handel med verdipapirer. Gjennom muligheten ved å knytte seg opp mot Norges Banks oppgjørssystem sørger VPS for at både aksje og obligasjonshandel inngår i samme pengeoppgjøret.

- Fonds-/Forvaltningsselskap

VPS yter tjenester til forvaltningsselskaper, distributører og agenter for utenlandske fond, som f.eks sikrer administrasjon av andelseiere.

6.2.7 NOS

NOS tilbyr følgende tjenester til det norske verdipapirmarkedet:

- Clearing av norske og svensk aksjer og indeksderivater.
- Clearing av norske rentefutures.
- Clearing av norske OTC aksje- og aksjeindeksderivater.
- Clearing for verdipapir lån i 2 ulike låneordninger for verdipapir.
- Rapporteringstjenester.

6.3 Transaksjonsvolum

6.3.1 Volumutvikling av transaksjoner og nettbank kunder

Volumtall BBS transaksjoner:

BBS transaksjoner	1997	1998	1999	2000
Giro blanketter	223	257	121	73
Korttransaksjoner	122	162	211	320
Interbank transaksjoner	180	236	209	310
Avtalegiro/ Autogiro	17	21	23	25
Direkte remittering	29	30	32	24

Figur 4. Volumutvikling av transaksjoner i BBS målt i millioner.

Utvikling nettbankkunder:

Nettbankvolumer	1997	1998	1999	2000	30.06.01
DnB & Postbanken		0 10 000	26 035 54 000	113 898 137 000	163 239 180 000
Nordea Bank Norge	7 300	21 000	76 000	148 000	165 000
Sparebanken NOR	7 000	21 000	53 000	112 000	175 000
Sparebank 1			Ca. 60 0000	130 000	160 000
Skandiabanken				54 000	109 000
Terra gruppen	1000	-	-	-	75 000
Fokus		9000	15000	33 000	41 000

Figur 5. Volumutvikling, antall nettbank-kunder

7 Nye tjenestetilbud

7.1 Den nye teknologiske hverdag

De større institusjonene har løpende langsiktige utviklingsprosjekter som i stor grad kommer til å endre forretningsprosessene og måten kundene vil forholde seg på.

Eksempler på dette er :

- Innkjøpsportaler som knytter bedrifter og forretninger sammen til en felles handelsplass hvor betalingsfunksjonen er integrert.
- On-line kreditt og lån.
- WAP aksjehandel.
- Dokumenthåndtering (inkasso, remburs, garantier etc.).
- Utenlandsk aksjehandel.
- Internasjonal betalingsformidling.
- Forsikringstjenester.

En ytterligere utvikling innenfor dette området er interaktiv TV (iTV). På dette området forventes det stor vekst når infrastrukturen er utbygget. Utstyret som nyttes er en boks som kobles til fjernsynsapparatet. En har da direkte tilgang til Internett hvor TV'en brukes som dataskjerm. Løsningen gir mulighet for en personlig kundeveileder på fjernsynsskjermen. (The Banker, Feb.01).

Det er en klar trend at telekommunikasjon og datakommunikasjon, samles i håndholdte enheter som mobiltelefon og Personal Digital Appliance (PDA). PDA er en elektronisk adresse og avtalebok med muligheter for tilknytning til Internett. Teknologier som Blue Tooth (trådløs måte å kommunisere på) vil forenkle oppkoblinger mellom mobiltelefoner, PDAs, bærbare PC'er og digitale telefoner mot betalingstjenester. Sikkerhet er her en stor utfordring.

Programvarens lagringsbehov og dens funksjonalitet øker kraftig. Større krav settes følgelig til lagring og administrasjon av data. Trenden innen IT-arkitektur har vært bruk av distribuerte løsninger og i mindre grad bruk av stormaskin. Ser en framover vil nok stormaskinløsningene benyttes ennå en tid. De distribuerte løsningene får stadig sterkere servere men dette vil ikke dempe bruk av stormaskin for å behandle on-line oppgaver eller sanntids enkelttransaksjoner. Siden serverne i de distribuerte løsningene stadig blir kraftigere vil antallet servere i løsningene avta. Etter noen år med PC-baserte nettverksløsninger og minimaskiner, synes nå trenden å gå i retning av færre små servere samtidig som en opprettholder stormaskinmiljøene. Dette er en naturlig utvikling ved at kundene betjener seg selv i stadig større grad og færre transaksjoner går gjennom bankens interne organisasjon (=arbeidsstasjoner og nettverk).

Interoperabilitet er kravet for å få til internasjonale IT-løsninger. Systemer må også kunne virke over grensene. Multinasjonale konsern (kunder som stiller krav) og at bankene selv etablerer finanskonsern på tvers av landegrenser (lanseres som konkurransefortrinn) bidrar til at det blir et økende behov for slike løsninger.

Det antas at kompetanse innen drift av stormaskin, dens operativsystem, programvare og applikasjoner vil kunne bli mangelvare. Den samme antagelsen gjelder de mange Internett-baserte nisjeløsningene som er under utvikling.

7.2 Om utbredelsen av e-tjenester

Norge ligger sammen med de øvrige nordiske land på Europa-toppen når det gjelder nettbanktjenester. De nordiske land skiller seg klart ut når det gjelder markedspenetreringen av nettbank, og ifølge en rapport fra ECB (sept 2001) er det bare her nettbank virkelig har "tatt av". En forklaring kan være at de nordiske land tradisjonelt har hatt avanserte IT-løsninger og høy grad av samordnet betalingsformidling, som kan ha gjort overgangen til elektroniske banktjenester på nettet enklere. Et moment for Norges del er sannsynligvis også at utkontraktering og felles datasentraler har medført at hver eneste bank, også den minste sparebank, er i stand til tilby avanserte nettbanktjenester. Det legges til grunn at dette er et nordisk særtrekk som har gjort det mulig for de fleste nordiske banker å tilby slike tjenester. For hver enkelt bank har kostnadene vært overkommelige, siden datasentralene har medført en fordeling av kostnadene på flere. I mange andre land vil alliansebygging og samarbeid være eneste måte å oppnå det samme på.

En av tre nordmenn mellom 15 og 64 år (rundt 880 000 personer) opplyser at de bruker slike tjenester, viser tall fra Norsk Regnesentral og Markeds- og medieinstituttet (nov 2000). Det forventes at antall kunder øker til over 1,2 millioner innen utgangen av 2001.

Banker har i mange år eksperimentert med on-line banktjenester. Flere av disse har vært tungvinte å bruke og har medført ekstrakostnader i form av telefon og tilleggsutstyr for kundene. Når bruken av Internett har vokst i volum og spredning, kan denne teknologien brukes for å få tilgang til banken uavhengig av tid og sted. Internett har gitt bankene muligheter til å nå flere kunder med sine tjenester, der geografisk nedslagsfelt ikke lenger spiller noen rolle. Internett-løsningene er blitt standardiserte med mange konkurrerende leverandører av utstyr til fordel for banker og kunder.

Sparebankforeningen har foretatt en undersøkelse for å kartlegge markedet for nettbank og nettbankbrukere. Norsk Gallup gjennomførte spørreundersøkelsen i februar 2001 og noen resultater fra undersøkelsen er:

- Til sammen 59 prosent av befolkningen over 15 år (mer enn 2 millioner personer) bruker Internett.
- 30 prosent av alle personer over 15 år bruker nettbank. Dette tilsvarer ca. 1 million kunder.

For 1 år siden var tilsvarende tall ca. 17 prosent, altså 600.000 kunder. Veksten vil bli mer dempet i årene fremover, men en overveiende andel av kundene vil i fremtiden ha denne tilgangen.

Den yngste aldersgruppen er de ivrigste Internett-brukerne. Disse blir de neste nettbankkundene. En regner med at andelen av de som benytter nettbank, (30 prosent i begynnelsen av 2001), vil øke ytterligere de nærmeste årene. Bankene satser tungt på denne distribusjonskanalen og tilknytning til og bruk av Internett er fortsatt økende. Til sammenligning ligger tilsvarende andel som bruker nettbank i Finland på 50 prosent og i Sverige på 20 prosent (ihht rapport fra ECB sept 2001). Norsk Gallup kom med en ny undersøkelse vedrørende bruk av nettbank i januar 2002 som bekreftet at det pr siste årsskiftet var 1,5 millioner nettbankkunder i Norge, der Sparebank 1 og Skandiabanken er de største nettbankene.

Innføring av Internett som kanal for elektroniske tjenester har medført nye forretningsmessige muligheter og nye problemstillinger for finansinstitusjonene. Den hurtige omstillingen har vært og er krevende å forholde seg til i forhold til sikkerhet. De norske finansinstitusjonene har til nå mestret innføringen av Internett tilfredsstillende. Ingen større kriser har oppstått i finansmarkedet rundt de elektroniske banktjenester som tilbys via Internett. Sammenliknet med utenlandske aktører er Norge på flere områder ledende når det gjelder bruk av Internett til finanstjenester. Likevel er store deler av den norske befolkningen fortsatt usikker på om sikkerheten er god nok. Finansinstitusjonene har vært forsiktige med å spre informasjon til publikum om de sikkerhetsforanstaltninger institusjonene benytter. Etter det Kredittilsynet

kjenner til har det ennå ikke vært registrert noe vellykket tyveri av penger fra nordiske nettbanker.

De karakteristiske trekkene ved Internett har bl.a. bidratt til endring av risikobildet.

- Hurtige endringer i teknologi, forretningsprosesser og nye konkurrerende tjenester på markedet har bidratt til sterk konkurranse. "Time to market" presser frem situasjoner som kan gå på bekostning av sikkerheten.
- Bruk av ny teknologi med ukjente konsekvenser. Transaksjoner er automatiske og styrt av kundene. Autentisering foretas datateknisk. Avhengigheten til IT er stor da det er få forretningsprosesser som kan erstattes med manuelle beredskapsrutiner.
- Kompleksiteten i systemene og kravene til tilgjengelighet er økende. Samarbeid mellom institusjoner øker og utkontraktering av kritiske tjenester øker i forsøk på å redusere risiko og kostnader. Det er en illusjon at samfunnet blir sikrere gjennom økt bruk av teknologi. Virkeligheten viser at forretningsprosesser, IT-systemer og styringsprosesser blir mer omfattende og kompliserte. Det siste bidrar til at det er krevende å ha en totalforståelse av systemenes oppbygning og hvordan de virker sammen, samtidig som det er nødvendig med spesialistens detaljforståelse for å hindre at "en liten tue kan velte det store lasset".

8 Sikkerhet og sikkerhetsløsninger

Den nye teknologien medfører at sluttbruker får et direkte forhold til nettverk og applikasjoner. I dette ligger vesentlig større utfordringer enn før når det gjelder sikkerhet. Finansnæringen er avhengig av tillit for å fylle sin rolle og markedet vil sannsynligvis ikke tåle mange hendelser i relasjon til sikkerhetsaspektene før tillitsforholdet er svekket. I tillegg til det forhold at kundene har direkte tilgang til systemene, noe som i seg selv øker eksponeringen for tilgang til og mulig misbruk av data, er det også et moment at alle feil og svakheter blir synlige for kundene.

Tilfredsstillende sikkerhetsløsninger i datasystemene er dermed av avgjørende betydning for finansnæringen. Datasystemene må beskyttes fra ulovlige inntrengere og virus. Problemet er at trussel bildet endrer seg kontinuerlig og når en får kjennskap til et nytt virus eller uønskede nettadresser, må sikkerhetskomponentene på nytt justeres. Oppdatering av sikkerhetsløsningene henger ofte etter, og kan derfor utsettes for nye virus og inntrengningsforsøk uten adekvat beskyttelse.

Sikkerhetsløsningene knytter seg til fysisk sikkerhet, sikkerhet med nettverket, sikkerhet ved operativsystemet og sikkerhet ved å anvende programmet.

De mest vanlige sikkerhetsløsninger er:

- Autentisering – funksjonalitet for bekreftelse av identitet til kunde og tjenesteleverandør. Det vanligste her er passord.
- Autorisering – funksjonalitet for å gi kunden adgang til bestemte typer tjenester.
- Kryptering – funksjonalitet for dekoding av data slik at det for uvedkommende blir uforståelig. Brukes ved overføring av data.
- Brannmur – teknologi for å hindre uvedkommende adgang til egne systemer.
- Antivirusprogrammer – programvare som avdekker virus på vei inn i systemene.
- Intelligent overvåking – programvare som gjennomfører overvåking av trafikken på nettet og som rapporterer mistenkelig aktivitet.
- Digitale sertifikater – et ”pass” som inneholder identiteten til personen eller selskapet som passet er utstedt til.

Det må vurderes som en stor utfordring for finansnæringen å utvikle og forbedre sikkerhetsløsningene, slik at den generelle tillit til elektroniske kundesystemer ikke svekkes. Det må antas at dette vil bli den avgjørende suksessfaktor når det gjelder videre utvikling og bruk av nettbank løsninger.

8.1 Tillit, en kritisk suksessfaktor for institusjonene

Langsiktig bank- og finansvirksomhet er basert på tillit. Dette er avhengig av at avtalen mellom partene gjennomføres med forutsigbarhet. Virksomhetene må heller ikke utsettes for kriminelle handlinger som svekker virksomhetens økonomiske fundament. Tillit oppnås ved bruk av sikringsmekanismer og kontroller for å gi driftsstabilitet og tilgjengelighet på tjenestene, sikre dataintegritet og konfidensialitet. Både kunder og myndigheter stiller høye krav til at tjenestene er sikre.

8.2 Forhold vedrørende sikkerhet

Flere sikkerhetsrådgivere antyder at hele 80% av alvorlige innbrudd i norske foretak, blir gjort av foretakets egne ansatte. Mange grunner for sikkerhetsbruddene angis :

- Uklare ansvarsforhold
- Liten forståelse hos ledelsen
- Mangel på rutiner som avdekker sikkerhetsbrudd
- Budsjettbegrensninger
- Ansattes likegyldighet
- Manglende sanksjoner

Det er nødvendig å ha høy sikkerhet i betalingssystemene for at det finansielle system i Norge skal fungere tilfredstillende. Derfor kan en sammenligne nettbankens sikkerhet med andre betalingsinstrumenter i forhold til tyveri av penger. Informasjonen nedenfor er hentet fra BBS i juni 2001:

- | | |
|------------------|--------------------------------------|
| ▪ Bankkort | Økende |
| ▪ Kredittkort | Økende |
| ▪ Sjekk | Mange før, nesten null nå |
| ▪ Bankgiro | Drastisk redusert, overgang Brevgiro |
| ▪ Brevgiro | Maks. 40 stk siden 1992 |
| ▪ Autogiro | Ingen |
| ▪ Avtalegiro | Ingen |
| ▪ Internett-bank | Ingen |

Norge har svært få tyveri av penger fra bankkort sammenlignet med andre land. Etter at bruk av sjekk nesten er opphørt, er det svært lavt antall svindler med sjekk. Foreløpig har Kredittilsynet ikke registrert tyveri av penger fra nettbank i Norge.

9 Kritiske risiko- og sårbarhetsområder

9.1 Hva fant vi ut gjennom analysen?

Det gjennomgående temaet i arbeidet med risiko- og sårbarhetsvurderingene, har vært å se på de sikkerhetsløsninger og kontroller som skal hindre at følgende oppstår:

- avbrudd og svikt i kontinuitet i leveranse av tjenester
- feil vedrørende transaksjoner og oppgjør
- svindel og kriminelle handlinger

Resultatet av vurderingen viser at beredskapsløsninger og planverk rundt disse ser ut til å være på plass, som en generell iakttagelse. Likevel er vi usikre på om beredskapsløsningene er gode nok, spesielt etter de store omstillingene som har funnet sted i bransjen med oppkjøp, fusjoner og utkontraktering.

Identifiseringen av områder som kan være utsatt for sårbarhet og dermed risiko er listet opp under kapittel 9.2 og er basert på Kredittilsynets egne vurderinger:

9.2 Sårbare områder

9.2.1 Utkontraktering av IT-tjenester

Finansnæringen i Norge har i over 30 år i stor grad samlet driften av datatjenester i større datasentraler som IDA for forretningsbankene og Fellesdata for sparebankene.

Argumentasjonen for å gjøre dette har vært besparelser, økt fleksibilitet, redusert risiko og bedre effektivitet. Fra bankkundes side har dette hatt store fordeler i form av produktutvikling og høy grad av samordning når det gjelder bl.a. betalingstjenester.

Noen av ulempene som kan knyttes til utkontraktering er av mer langsiktig karakter. Det er lett å bli avhengig av sine leverandører ved at institusjonen får redusert kontroll og autonomi i kritiske deler av egen virksomhet. Det kan være praktisk vanskelig å skifte leverandør, og det er kostbart å bygge opp igjen denne delen av virksomheten i egen institusjon. Styrkeforholdet mellom kunde og leverandør kan lett endre seg. Settes tjenesten bort, er mulighetene for erfaring og innovasjon redusert, og institusjonen kan miste egen kompetanse på området. Det bør være en forutsetning at institusjonene selv har den nødvendige kompetansen som kreves for å forvalte sine utkontrakterings-avtaler.

ASP (Application Service Provider) er i stor grad et nytt navn for fjerndrift eller servicebyrå. Leverandørens oppgave er å sørge for at institusjonene har tilgang til programvare og applikasjoner som de abonnerer på. Et av foretningsområdene til en ASP er programvaredistribusjon og lisenskontroll. En ASP må ha sikkerhetsløsninger som tilsvarer de policyer og retningslinjer som institusjonen har, ettersom institusjonens data forlater foretaket og overføres via datalinjer til ASPen for lagring. Det er også her viktig at institusjonen har tilstrekkelig kompetanse for vurdering av de funksjonelle og sikkerhetsmessige aspektene. En meget alvorlig situasjon kan her være at en ASP blander data mellom to institusjoner. Data til to eller flere institusjoner kan gjerne ligge på fysisk samme disk.

Generelt for denne type leverandører gjelder at profesjonalitet, kompetanse og interne rutiner blir svært viktig for finansinstitusjonene. Det kan være ønskelig at kundene av slike leverandører stiller krav om dokumentasjon av visse minimumsstandarder, som for eksempel ISO sertifisering.

9.2.1.1 Konsentrasjon av datatjenester og EDB Business Partner ASA

Det er en ny problemstilling at det nærmer seg en monopolsituasjon på det norske markedet når det gjelder utkontraktering av IT-banktjenester.

EDB Business Partner ASA, med sine selskaper EDB Fellesdata og EDB Teamco, har en meget sterk stilling som tjenesteleverandør til banknæringen. Etter at DnB utkontrakterte store deler av sin IT virksomhet til EDB Teamco 1. juli 2001, er monopolsituasjonen praktisk talt et faktum.

En foreløpig betraktning knyttet til sårbarhet og sikkerhet er at selv om driften av tjenestene skjer i ulike selskaper med skilte tekniske driftsmiljøer, vil det likevel være felles ledelse- og styringsfilosofi innenfor konsernet. Felles prinsipper for risikostyring, prioriteringer og ressursbruk vil kunne avleire de samme svakheter i alle driftsmiljøer, noe som i krisesituasjoner vil kunne slå uheldig ut.

Det er grunn til å tro at EDB Business Partner har planer om å etablere seg utenlands. Erfaringer har vist at ved for sterk eksponering i utenlandske virksomheter eller prosjekter, kan det norske morselskapet bli truet i nedgangstider eller ved selskapets endring av fokus.

Det er antatt at konsentrasjonen av slike tjenesteleverandører vil øke ytterligere. Som følge av restrukturering av finansnæringen i retning av nordiske løsninger, er det naturlig at også IT-siden vil få en "nordisk" løsning.

9.2.2 Personavhengighet og kompetanse

Som en konsekvens av at stadig flere av institusjonenes tjenester utkontrakteres, flyttes kompetansen for disse tjenestene fra institusjonen til tjenesteleverandør. Det er derfor viktig at institusjonene har et aktivt forhold til utkontraktørs kompetanseprofil. Institusjonene bør til enhver tid være sikker på at tjenesteleverandør har tilgang til den kompetansen som trengs for å utføre inngåtte avtaler. Institusjonene bør med jevne mellomrom gjennomgå tjenesteleverandørs utdanningsprosesser for å se at disse fungerer og at disse oppdager og tetter eventuelle kompetanse hull. Slike prosesser skal også avdekke at tjenesteleverandør ikke gjør seg avhengig av en person for å kunne drifte en institusjons tjenester.

Det er viktig at tjenesteleverandør har en langsiktig kompetanseoppbyggingsplan som tar høyde for å tilføre organisasjonen tilstrekkelig kompetanse for å opprettholde kvaliteten i driftsmiljøenes grunnstamme.

Som en generell betraktning ser vi på behovet for tilstrekkelig kompetanse på viktige funksjonsområder som en stor utfordring videre fremover. Noen stikkord relatert til dette området er:

- Tilstrekkelig kompetanse hos leverandør ved utkontraktering.
- Tilstrekkelig kompetanse i egen organisasjon på det områder som er utkontraktert.
- Beholde kompetanse på viktige områder som på lengre sikt er under avvikling.
- Skaffe tilstrekkelig kompetanse på nye teknologiområder.
- Beholde kompetanse på områder som er i stadig endring.
- Ha tilstrekkelig egen kompetanse både på funksjonelle og teknologiske områder og ha nok kunnskap om sammenhengen mellom disse.

9.2.3 Katastrofeløsninger

For å holde høy tilgjengelighet av finansinstitusjonenes tjenester og hindre at f.eks. betalingssystemene lammes over lengre tid, er det nødvendig å ha fungerende beredskapsløsninger / reserveløsninger klar. Beredskapsløsninger må testes med jevne mellomrom for å få en bekreftelse på at både mennesker og utstyr er beredt til å tre inn når situasjonen krever det.

Det er en omfattende operasjon å koble inn en reserveløsning når deler av et større system svikter. Det er også en omfattende operasjon å returnere til normal drift etter at skaden er utbedret.

Noen av områdene vedrørende kontinuitets- og beredskapsløsninger som en bør fokusere på er

- Bankenes krav og forventninger til underleverandør i katastrofesituasjoner
- Realismen i katastrofetesting
- Katastrofeinstallasjonens kapasitet Realisme i katastrofetesting er et område det knyttes usikkerhet til. Så langt Kredittilsynet kan se, er alle de gjennomførte testene planlagt i lang tid på forhånd. Uannonserte tester bør innføres og gjennomføres årlig.

Kvaliteten på beredskapsløsningene hos institusjoner og tjenesteleverandører har vist seg å være svekket i perioder ved omstillinger eller sammenslåinger.

I situasjoner der funksjonsområdet/tjenesten er utkontraktert blir det å opprettholde god nok beredskap på katastrofeløsninger et stor utfordring. Slike tester vil da sannsynligvis få en synliggjort pris. Leverandøren kan også fristes til å prise dette relativt høyt. Dette kan samlet resultere i færre tester enn det som er ønskelig på at beredskapen er god nok.

9.2.4 Endringshåndtering

Den raske innføringstakten av nye tjenester fører til flere risikoelementer i betalingstjenestene og kan derfor innebære økt operasjonell risiko. Gode endringsrutiner, og oppfølging av disse, er kritisk for institusjonene siden dagens applikasjoner har en langt hyppigere oppgraderingstakt enn sine forgjengere.

Endringer i omgivelser, teknologi og tjenester medfører forstyrrelser i bestående leveranser. Enhver endring må vurderes separat og konsekvensene av endringen må forelegges eier før denne godkjenner gjennomføringen. Årsakene til driftsstans pga endringer kan være mange; mangelfull utvikling og testing av programmer og tjenester, mangelfull oppfølging av rutiner, vanskeligheter med å teste for en reell driftssituasjon. Endringskontroll er særskilt krevende når endringen berører flere selskaper.

IT-systemene er komplekse og det må settes krav til kompetanse om systemenes innbyrdes avhengighet for å vurdere konsekvenser av endringer i teknologi og tjenester. Rutiner for endringskontroll som omfatter konsekvensutredninger, testing, godkjenning og beredskap må utarbeides og etterleves. Ved at samme leverandør opererer samme løsning for mange banker, og at disse er integrert i samme fysiske løsning, øker også behovet for samordning ved endringer som gjennomføres på tvers av flere banker.

Eksempler som bidrar til høyt endringstempo er:

- Endringer i bruk av teknologi.
- Introduksjon av nye tjenester (kan endre både bruk av teknologi og løsninger).
- Feilhåndtering og påfølgende rettelser.
- Utkontraktering.
- Fusjoner.
- Omorganiseringer.

9.2.5 Opplisting av samlepunkter

I tillegg til hvert enkelt punkt vi har redegjort nærmere for her har vi også potensielle sårbare områder som er viktige, men som vi her vil peke på mer stikkordsmessig:

- Virus som kan ha en meget ødeleggende effekt.

- Organisert kriminalitet.
- Tidsfaktoren før en feil blir oppdaget, pga kompliserte teknologiske løsninger, hvor få personer har tilstrekkelig kompetanse til at problemet blir oppdaget tidlig nok.
- Digital identifisering og beskyttelse.
- Internett som introduserer og eksponerer ikke identifiserte problemer.

10 Foreslåtte tiltak

10.1 Hva gjør vi med informasjonen?

- Sørge for at vi har kunnskapen og informasjonen fra vår risiko og sårbarhetsanalyse som del av vår prioritering og som planlagte underlag når vi gjør dokumentbaserte og stedlige tilsyn i 2002.
- System for årlig ajourføring av vår risiko og sårbarhetsanalyse.
- Gradvis dreining mot et risikobasert IT-tilsyn.
- Kommunikasjon med partene i den finansielle IT infrastruktur (=fokusere).
- Preventive tiltak gjennom lover og forskrifter hvor de viktigste for Kredittilsynet i denne sammenheng vil være Intern-kontrollforskriften og IT-forskriften.
- Direkte kommunikasjon med aktuell institusjon der vi har funnet forhold det er grunn til å gå nærmere etter.