Risiko- og sårbarhetsanalyse (ROS) 2006

Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Kredittilsynet, 21. mars 2007

1 Innledning

Kredittilsynets erfaringer med å gjennomføre en årlig ROS-analyse som vurderer finansforetakenes bruk av informasjonsteknologi i forhold til risiko, har vist seg nyttig, både som grunnlag for tiltak og som preventivt virkemiddel. Informasjonen som ROS-analysen bygger på, gir Kredittilsynet gode tilbakemeldinger om kvaliteten på tilsynsopplegget, etterlevelse av IKT-forskriften og den generelle tilstanden i finansforetakenes bruk av informasjonsteknologi. Analysen for 2005 var i stor grad retningsgivende for prioriteringen av tilsynsaktiviteter og øvrige temaområder som ble vektlagt i 2006.

Kredittilsynet kan gjennom resultatet av ROS–analysene se positive endringer i hvordan IKT-prosessene i foretakene implementeres for områdene planlegging, innkjøp/utvikling, drift og kontroll. Etter Kredittilsynets vurderinger la finanssektoren i 2006 større vekt på bruken av etablerte standarder og ”best practices” enn tidligere. Standarder og metoder som ITIL, ISO-27000, COSO og CobiT benyttes i stadig økende grad. En ser også en økning i bruken av de sertifiseringsordningene som enkelte av standardene kan tilby.

2 Bakgrunn og formål

2006 føyde seg inn i rekken av år med store endringer innenfor IKT-området i sentrale foretak innenfor finanssektoren. Dette gjaldt både områder innenfor infrastrukturtjenester og bruk av ny informasjonsteknologi som grunnlag for nye produkter og tjenester. Kredittilsynet ser det som viktig å gjennomføre ROS-analysen for å identifisere trender og for å kunne peke på områder som er særlig risikoutsatte. I finanssektoren har foretakene i stor grad utkontraktert IKT-tjenestene til eksterne IKT-leverandører. Dette medfører en stor utfordring i foretakenes arbeid med kontroll og oppfølging av IKT-leveransene. Den tradisjonelle nærheten mellom foretak og leverandør er borte, og er i større grad enn tidligere basert på rene forretningsmessige prinsipper. Dette kan gjøre det vanskelig å opprettholde tilstrekkelig kompetanse på IKT-området over tid.

Formålet med Kredittilsynets ROS-analyse er å identifisere hovedtrekk knyttet til risikoeksponering og sårbarhet. Gjennom informasjon og vektlegging av disse områdene ønsker Kredittilsynet å bidra til at nødvendige tiltak settes i verk.

3 Utviklingstrekk, risiko og sårbarhet

I dette kapitlet vil vi forsøke å beskrive de utviklingstrekkene som er identifisert fra ulike åpne kilder og samarbeidsorganisasjoner. Dette er informasjon som hver for seg og samlet har betydning for risikobildet når det gjelder finanssektorens bruk av og avhengighet av IKT. På grunnlag av informasjonen identifiseres både utviklingstrekk som kan gi økt risiko og enkelttemaer som allerede representerer høy risiko.

3.1 Ytre trusler

Det er identifisert en rekke ytre trusler hvor eksempelvis kraft og telekommunikasjon er vesentlige. Arbeid med å sikre dette inngår som en naturlig del av kontinuitetsarbeidet og katastrofeplaneverket. En ny type ytre trussel som kan vise seg å bli viktig, er utbrudd av pandemi som i større eller mindre grad kan lamme institusjonene selv og publikums tilgang på bank- og betalingstjenester over lengre tid.

3.1.1 Pandemi og fugleinfluensa

Den britiske regjeringen ser på en influensapandemi som en av de største risikoene for Storbritannia. Derfor har de gjennomført flere øvelser med dette som tema. I 2006 ble det gjennomført den hittil største øvelsen, som særlig la vekt på den første sykdomsbølgen av en influensapandemi. Øvelsen ble gjennomført over seks uker og simulerte 22 uker av et utbrudd. Øvelsen ble arrangert av The Financial Services Authority (FSA), Bank of England og det britiske finansdepartementet, HM Treasury. Det var 70 organisasjoner innen finansnæringen som deltok i øvelsen. Totalt var det 3500 deltagere med.

Det som kjennetegner situasjonen ved en pandemi, er at det er tilgang på personell og ikke til fysiske eiendeler som er utfordringen. For å simulere omfanget, besto scenariet av en gradvis økning i sykefravær, hvor en startet på 15 prosent og økte til 49 prosent når utbruddet var på det kraftigste. Hensikten med dette var å få foretakene til å legge vekt på hvordan personalet organiseres geografisk og benyttes for å kunne ivareta sine forpliktelser. Øvelsen viste at i en slik situasjon er det nødvendig at en har planer for karantenebestemmelser, vaksinering, foreldre som er hjemme med syke barn, redsel og også hvordan organisasjonen skal håndtere dødsfall.

Der hvor testen viste at utbruddet medførte størst problemer, var i den delen av organisasjonen som utøvde fysisk arbeid. Scenariet viste allerede på et tidlig tidspunkt at distribusjon av kontanter ble en stor utfordring både for bankene og offentlige myndigheter. Ved stadig færre ressurser å benytte, måtte

stadig flere bankfilialer stenge, noe som påvirket kundenes tilgang til banktjenester, som for eksempel bruk av minibank og nattsafe.

I forbindelse med bruk av debet- og kredittkort oppsto det utfordringer i områder som distribusjon av nye kort på grunn av at gamle kort har passert utløpsdato. Noen deltagere greide å etablere løsninger hvor utløpsdatoen ble utsatt for fortsatt å kunne bruke eksisterende kort.

Leverandører av tjenester til den finansielle infrastrukturen rapporterte jevnlig i testen. Det er grunn til å tro at først ved et stort antall syke hos en slik leverandør vil dette kunne påvirke deres leveranseevne av kritisk infrastruktur siden en stor del av operasjonen er automatisert. Derimot vil håndtering av feilsituasjoner, feilretting og nyutvikling bli skadelidende.

Kredittilsynet har vektlagt kontinuitets- og katastrofeløsninger i IKT-forskriften, hvor områdene fikk egne bestemmelser. Erfaringene vi har gjort gjennom IT-tilsyn og intervju, er at finansnæringen er opptatt av områdene. Det som etter vår vurdering gjenstår, er å se på planene i et tverrsektorielt perspektiv hvor grunnleggende infrastruktur som strøm, telekommunikasjon, samferdsel og helse får en mer sentral del i foretakenes planverk og testing.

3.2 Utviklingstrekk i finanssektoren som påvirker bruk av IKT

3.2.1 Automatisering av den finansielle leverandørkjeden

Den finansielle leverandørkjeden er ofte definert som kjeden av finansielle transaksjoner som foregår i interbankmarkedet, eller mellom andre profesjonelle finansielle markedsaktører som for eksempel finansforetak eller meglere. Finansnæringen har lenge jobbet for å øke produktiviteten og effektivisere transaksjonsutvekslingen gjennom automatisert transaksjonsflyt (STP[1]). Dette har vært mulig å oppnå ved å utnytte tilgjengelig IKT sammen med sikkerhetsløsninger. Norge er et av foregangslandene for å drive denne utviklingen videre, noe som har ført til at den automatiserte finansielle leverandørkjeden strekker seg lenger enn bare mellom de finansielle markedsaktørene og integreres med bankkundenes egne administrative systemer (ERP[2]). På denne måten kobles den finansielle og den kommersielle leverandørkjeden sammen til en sømløs automatisert transaksjonsflyt. Internett, åpne internasjonale standarder som XML, utvikling av et integrert internasjonalt betalingsmarked i SEPA[3] og økt etterspørsel fra krevende kunder, forsterker hverandre gjensidig og driver denne utviklingen i større fart enn tidligere.

[1] STP = Straight Through Processing
[2] ERP = Enterprise Resource Planning
[3] SEPA = Single Euro Payments Area

3.2.2 Bankkundene blir en integrert del av den finansielle leverandørkjeden

Denne utviklingen medfører at standardisert kommunikasjon i den kommersielle og den finansielle leverandørkjeden vil kunne smelte sammen. Informasjon som er kritisk for de ulike aktørene i leverandørkjedene, kan lett kobles av eller hektes på, avhengig av bruk. Dette vil kunne møte behovet fra bankkundene om en reell automatisert transaksjonsflyt (STP) mellom sluttbrukerne. Behovet for IKT-løsninger mellom kundene og finanssektoren forsterkes ytterligere av ønske om færrest mulig manuelle transaksjoner mellom kunder og finansforetak og behov for hyppig oppdaterte rapporter. Dette vil samtidig sikre at foretakenes styringssystemer møter nye krav.

3.2.3 Økt bruk av åpne standarder

Initiativet fra FN og ISO om å etablere felles internasjonale ISO-standarder for finansnæringen ble i første omgang gjennomført med ISO 15022 for meldingsutveksling mellom verdipapirforetak. Den tekniske styringskomiteen for finansielle tjenester, ISO TC 68, videreførte dette initiativet og etablerte en egen organisasjon for ISO 20022 (XML-standarder for finansielle tjenester) i 2005. Dette har medført en økt integrasjon mellom ulike standardiseringsorganisasjoner, noe som har redusert antall særegne standarder. I særdeleshet gjelder dette verdipapirhandel, handel med verdipapirfond og finansielle instrumenter og betalingsoppdrag fra bankkunder (C2B[4]). SWIFT forvalter biblioteket for ISO 20022 XML på vegne av ISO. Utviklingen av nye felles europeiske betalingstjenester innenfor SEPA forutsetter bruk av ISO 20022 i interbankmarkedet, og anbefaler at standardene benyttes i bankenes kommunikasjon med egne kunder. Likeledes forutsettes det at chipstandarden EMV[5] blir brukt for alle betalingskort.

3.2.4 IKT-leverandørenes rolle

Finansnæringen har over lang tid utkontraktert sentrale deler av sine IKT-løsninger til selvstendige, hel- eller deleide IKT-leverandører. Dette omfatter også avregningen i NICS og VPO. Selv om ny teknologi og åpne standarder kan være en trussel mot nasjonale løsninger, er det viktig at IKT-leverandørene og finanssektoren følger denne utviklingen slik at det blir tatt høyde for internasjonale standarder ved utarbeidelse av IKT-strategier og utviklingsplaner. Dette er spesielt viktig for IKT-leverandørene EDB Business Partner ASA og BBS AS som begge har særlige roller innenfor finanssektoren.

3.3 Leverandørsidens teknologiske utvikling med virkning for finanssektoren

Det skjer hele tiden en teknologisk utvikling som også påvirker finanssektorens bruk av IKT. Dette kan inndeles i 2 hoveddeler,

[4] C2B = Consumer to Business
[5] EMV= Europay International, MasterCard International and Visa International

a) Der den teknologiske utviklingen krever at bruk av nåværende teknologi endres for å sikre support og oppgraderinger fra leverandører. Dette kan innebære plattformskifte som kan medføre store utfordringer for enkeltforetak, ikke minst risiko under gjennomføring av endringen.

b) Der ny teknologi gir finanssektoren nye muligheter for blant annet lansering av nye produkter og nye distribusjonsformer.

3.3.1 Teknologisk plattformskifte

Det er registrert at mange aktører i finanssektoren, både finansforetak og aktuelle IKT-leverandører har startet prosjekter for overgang til ny teknologisk plattform eller utskifting av viktige deler av teknisk infrastruktur. Slike endringsprosesser representerer i seg selv stor risiko som krever stor oppmerksomhet på styring og kontroll. Det er registrert ulike feilsituasjoner med til dels alvorlige konsekvenser.

3.3.2 Innføring av ny teknologi

Ved innføring av ny teknologi er det viktig at det gjennomføres tilfredsstillende ROS-analyser før nye tjenester basert på ny teknologi lanseres.

Eksempler på ny teknologi:

- Bruk av trådløs kommunikasjon
  Bruk av mobiltelefon og håndholdt PC som distribusjonskanal for betalingsformidling
- Bruk av betalingskort på Internett

Vi vet fra USA at banker har tatt trådløs kommunikasjon i bruk uten at løsningen tilfredsstilte et minimum av sikkerhetskrav. Kredittilsynet ønsker å ha en proaktiv holdning til dette, og har derfor kartlagt bankenes bruk av trådløs kommunikasjon. Med bakgrunn i den informasjonen som er innhentet, finner vi at det ikke er noen som så langt hadde tatt i bruk trådløse nettverk i sine produksjonsmiljøer.

Likeledes har vi en pågående prosess knyttet til bruken av betalingstjenester via mobiltelefon.

3.3.3 Økt anvendelse av IKT på nye funksjonsområder

De fleste funksjonsområder i finansnæringen er helt eller delvis avhengig av leveranser av IKT-tjenester. Samtidig skjer det en stadig sterkere konvergens mellom de enkelte elementene i foretakets IKT-løsninger. Kompleksiteten i løsningene som større aktører innen finanssektoren benytter seg av, er omfattende. Dette gjelder på alle områder innen aktørenes IKT-virksomhet.

Konsulentselskapet McKinsey har gjennomført en analyse av foretak som foretar IKT-investeringer og om forbruk og kvalitet henger naturlig sammen. Analysen så nærmere på kostnader og inntekter totalt og hvilken andel kostnadene forbundet med IKT utgjorde av de totale kostnadene. Undersøkelsen viser at de foretakene som kom best ut, har sentralisert IKT-virksomheten og har sterk styring av IKT, færre løsninger totalt og høy grad av integrasjon. Dette er en god indikasjon om at den utviklingen vi har sett

i Norge med sterkere grad av integrasjon mellom de ulike løsningene, er formålstjenlig. Undersøkelsen indikerer videre at det å ha omfattende bruk av kostnader på IKT, ikke alltid betyr bedre løsninger: Det var også en klar indikasjon på at det ved bruk av utkontraktering var nødvendig med sterk egenkontroll, kompetanse og organisatorisk forankring og med avtaler som ga kunden stor grad av fleksibilitet ved reforhandling av innhold og betingelser. Sterkere integrasjon mellom de ulike delene av totalløsningen kan likevel gi økt sårbarhet og øke konsekvensene når det oppstår alvorlige problemer. Sannsynligheten for at dette skjer, vurderes som høy. Problemstillingen blir om foretaket gjennomfører en tilstrekkelig risikoanalyse før iverksetting.

3.4 Datakriminalitet rettet mot finanssektoren

3.4.1 Internett som distribusjonskanal

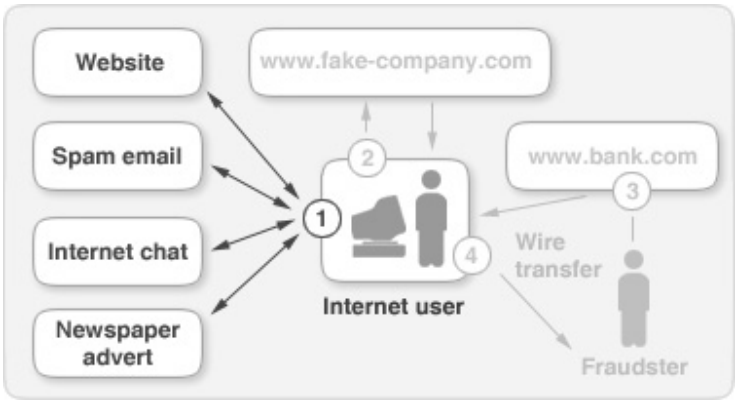
Det er grunn til å tro at antallet forsøk på å bryte seg inn i finanssektorens IKT-systemer vil øke. Dette vil kunne gjelde angrep både utenfra og innenfra i det enkelte foretak og kan rette seg mot mange ulike deler av foretakets virksomhet. Ulike undersøkelser og registrerte hendelser særlig i de større vestlige land, men også Norge, viser at dette er et reelt og økende problem. Det er særlig bruk av Internett til distribusjon av produkter og tjenester og utbetalingsautomater av kontanter som er spesielt utsatt.

Foreløpig har oppmerksomheten særlig vært rettet mot identitetstyveri hvor de kriminelle skaffer seg tilgang til enkeltelementer av informasjon om offerets personalia for deretter å sette dette sammen i et forsøk på uautorisert tilgang til, for eksempel en bankkonto. Enkeltelementer kan være: navn, adresse, telefonnummer, fødselsdato, fødselsnummer, sertifikatnummer, kredittkortnummer, utløpsdato på betalingskort og annen informasjon om relasjonen mellom kunden og banken, eksempelvis kontonummer, bank- og kredittkort, dato for utstedelse av pass og lignende. Det at bankene i stadig større grad benytter elektroniske distribusjonskanaler ut til kundene, kan bidra til å eksponere det antatt svakeste ledd i kjeden, nemlig kundens egen datamaskin (pc). Det er vanskelig å kontrollere at alle kundene er like opptatt av sikkerhet og sørger for tilstrekkelig grad av beskyttelse gjennom brannmur og antivirusprogrammer. Det kan se ut til at det er dette leddet i kjeden de kriminelle i første rekke retter aktiviteten mot. Et eksempel er ”phishing”, hvor noen forsøker å avlure kunden informasjon via en e-post som utgir seg for å komme fra kundens bankforbindelse. E-posten kan for eksempel inneholde en trojaner (har navnet sitt fra det historiske ”trojansk hest”) som er en type datavirus (ondsinnet programkode) som blir installert på kundens pc og utgir seg for å ha annen funksjonalitet. Programkoden er laget slik at den overvåker aktivitetene på pc-en og sender denne informasjon til en annen datamaskin som kan være hvor som helst på Internett.

Et nytt begrep som har dukket opp i den senere tid, er ”Money Mules”. Money Mules opptrer som en agent for overføring av penger basert på resultat av informasjon fra trojanere og phishing. Handel på nettet er en annen type problem hvor noen bestiller varer i kundens navn betalt med for eksempel kredittkort. Dette er kun ment som noen aktuelle eksempler fra et økende risikoområde. Temaet er blant annet tatt opp i Kredittilsynts ROS-analyse både for 2004 og 2005. Nedenfor er det gjengitt en

illustrasjon av Money Mules fra Bank Safe Online (assosiert med APACS – Association for Payment Clearing Services / The UK payments association) som er et nettsted satt opp av myndighetene i Storbritannia.

Figur 1: Money Mules



Kilde: Bank Safe Online

3.4.2 Angrep mot nettbanker

I Kredittilsynets ROS-analyse for 2005 ble det lagt vekt på at det hadde vært en økning i organisert kriminalitet. Internettbaserte banktjenester er et utsatt område hvor trojanere og phishing stadig øker. I 2006 ble det registrert flere hendelser knyttet til bruk av nettbank. Dette hadde grunnlag i både manglende funksjonalitet, tilgjengelighet og sikkerhetsløsninger.

I løpet av 2006 innførte de siste av bankene to-faktorautentisering. To-faktorautentisering er en viktig del av sikkerhetsløsningen som er i nettbankløsningene, og er sammensatt av en pin-kode som kunden selv vet og en engangskode som enten genereres av en kodekalkulator eller som kunden plukker fra en serie forhåndsgenererte koder som banken har sendt kunden.

Flere banker tilbyr sine kunder gratis nedlasting og bruk av antivirusprodukter. Kredittilsynet anser dette tiltaket som nyttig, og som et av mange tiltak for å høyne sikkerhetsnivået i de norske nettbankene. Sammen med jevnlige oppdateringer av operativsystem og nettleser, bidrar antivirusproduktene nettopp til dette. Det er imidlertid svært usikkert om sikkerhet knyttet til den enkeltes kundes pc kan gjøres avhengig av at kunden selv følger opp uten at dette på annen måte er under kontroll av banken.

3.4.3 Angrep rettet mot bankautomater

Et område som har vært kjent i lang tid, er organisert kriminalitet rettet mot bankenes kontantautomater. Det er mange ulike former for denne type kriminalitet hvor hovedhensikten er å

kopiere innholdet i betalingskortets magnetstripe samtidig som en tilegner seg PIN-koden. Ulike former for filming skjer gjennom montering av et minikamera inne i selve bankautomatåpningen eller filming med videokamera fra en nærliggende plass. En liten mikroprosessor som er montert på bankautomatåpningen og som kopierer innholdet i magnetstripen, kan være vanskelig å oppdage. Basert på informasjonen som skaffes gjennom identitetstyveri, produseres nye, falske betalingskort med magnetstripe. Disse blir deretter benyttet i kombinasjon med den innhentede PIN-kodeinformasjonen. I mange tilfeller sendes denne informasjonen via Internett til andre kriminelle på annet sted hvor produksjon av falske kort foregår. Bankene i Norge iverksatte i 2006 tiltak for å redusere problemet med "skimming" (avkopiering av informasjon). Det er derfor ikke usannsynlig at de kriminelle miljøene vil utforske andre områder som EFT/POS og andre e-handelsløsninger for å samle inn informasjon, eller for å gjøre direkte svindelforsøk.

3.4.4 Økning i hvitvasking

En økning generelt i organisert kriminalitet mot finanssektoren vil åpenbart også føre til økt hvitvasking av penger som er resultater av slike kriminelle handlinger. Det skjer en stadig bedring i rapportering og oppfølgingsaktiviteter på dette området, men økt omfang av internasjonal betalingsformidling fører til nye utfordringer. Et eksempel på dette er opprettelse av en debetkortkonto i et "skatteparadis" og deretter bruk av den aktuelle kontoen gjennom de internasjonale betalingssystemene. Kontoinnehaver kan da ta ut penger i en norsk minibank og bli oppfattet som en valutautlending i kontrollsystemet og dermed ikke bli registrert. Dette er et vanskelig område å arbeide med som krever langsiktighet og internasjonalt samarbeid.

3.4.5 Organisert kriminalitet

Det er ikke tvil om at det vil komme nye angrep av organisert kriminalitet og at noen vil lykkes. Tendensen på flere av områdene som det er redegjort for ovenfor, er temmelig klare. I hvilken grad finansnæringen vil klare å beskytte seg, vil avhenge av flere forhold. Det er grunnleggende at foretakene legger stor vekt på styring og kontroll og benytter anerkjente verktøy for å følge opp prosessene som inngår i et slikt opplegg. Likeledes at det legges vekt på risiko og gjennomføring av relevante risikoanalyser i en årlig syklus og ved endringer i bruk av IKT. Dette blir gjort både for å identifisere sårbare områder og for å iverksette nødvendige tiltak.

På det operative planet vil det være avhengig av hensiktsmessige opplegg for autentisering, integritet og sikkerhet. Det betyr at foretakene må ha relevante løsninger for å sikre at det er rett person som blir autentisert og får tilgang og at det skjer en beskyttelse av dialogen slik at uvedkommende ikke får tilgang til sensitive data. Løsninger for brannmur (f.eks. fra CISCO eller IBM), antivirusbeskyttelse (f.eks. fra Norman, Symantec (Norton) eller F-Secure) og påloggingsmekanismer (f.eks. BankID) inngår i dette. For at de nevnte løsningene skal kunne fungere optimalt, må det foreligge relevante prosedyrer for nødvendig ajourhold og oppfølging.

Det er viktig å ligge foran de kriminelle med tiltak. BankID for bruk ved autentisering av brukere i internettbaserte tjenester, er en løsning som bidrar i riktig retning. Likeledes innebærer bankenes nye kontobaserte betalingstjeneste BankAxess ved kjøp av varer og tjenester på Internett en forbedring

(avgrenset til norske brukersteder). Det svakeste leddet i kjeden vil ofte være hjemmepc-er hvor den enkelte bruker ikke sørger for nødvendig oppdatering og oppfølging av sikkerhetsmekanismer.

Økt organisert kriminalitet på de områdene som det er redegjort for her, kan få store samfunnsmessige konsekvenser, både kostnadsmessige og gjennom redusert tillit til betalingssystemene. I prinsippet kan økt kriminell aktivitet for eksempel føre til at en banks nettbankløsning må stenge i kortere eller lengre tid. Dette vil få betydning for et bredt spekter av finansielle tjenester. Det å sørge for å ligge i forkant med utvikling av beskyttelsessystemer for å hindre utvikling av løsninger i kriminelle miljøer, krever store anstrengelser og kostnader. Det samme gjelder for svindel i forbindelse med bruk av betalingskort, som også vil føre til større kostnader, både for forbruker, brukerstedsleddet og kortutsteder (f.eks. bank).

3.5 Utkontraktering av IKT og risikoeksponering

3.5.1 Utkontraktering

Utkontraktering er finanssektoren i Norge godt kjent med da norske banker har brukt felles IT-løsninger siden datasentralene Fellesdata og IDA, som den gangen var eid av bankene, ble opprettet i midten av 1960-årene. Inntil nylig har utkontraktering av IT-tjenester i hovedsak vært levert av norske leverandører. De trendene som vi ser både innenfor finanssektoren i Norge og i det globale utkontrakteringsmarkedet, er at utkontraktering over landegrensene øker i omfang. Internasjonalt gjelder dette særlig utkontraktering av IT-tjenester til foretak i land som India, Kina og Russland. I USA kalles dette ”offshore outsourcing”.

Det er i første rekke India som har bidratt til den sterke veksten i denne typen utkontraktering. Eksport av IT-baserte tjenester og BPO (Business Process Outsourcing) hadde en vekst på 59 prosent i 2004. Det forventes at den samme veksten vil fortsette i årene som kommer. Ifølge McKinsey vil IT-tjenester og back-office-arbeid i India femdobles innen 2008, til 57 milliarder US-dollar i årlig eksportindustri, og 4 millioner ansatte.

I Norge har utkontraktering til lavkostland som India så langt vært liten. Men dette kan imidlertid bli mer aktuelt siden de større tilbyderne av utkontrakteringstjenester begynner å ansette IT-personell i land som India for å redusere sine egne kostnader. I India kan kostnadene til en kvalifisert IT-arbeider være en tidel av tilsvarende stilling i Vest-Europa eller USA. Ifølge McKinsey koster en software-utvikler i USA ca. 60 dollar pr. time, mens den samme timeprisen for en indisk utvikler er 6 dollar. IT-kompetansen er også minst like god, kanskje bedre?

Alle de store IT-leverandørene har allerede etablert seg i India, og antall ansatte blant disse vil trolig øke i denne regionen. Grunnlaget for dette er de store utdanningsinstitusjonene i India som årlig utdanner store kull med høyt kvalifiserte IT-studenter. I tillegg har arbeidsmarkedet innenfor

informasjonsteknologi i løpet av det siste året blitt strammere slik at det er vanskelig for foretakene å rekruttere nøkkelressurser med riktig kompetanse her hjemme.

Finansnæringen i Norge er av ulike historiske grunner preget av:

- tradisjon for samarbeid
- samarbeid på en rekke strategiske IT-områder
- høy kostnads- og kompetanseterskel for etablering av infrastruktur på IT-området
- bruk av avanserte bank- og finansløsninger
- små volum

Indirekte har dette medført utkontraktering av viktige deler av foretakenes IKT-virksomhet. Dette har pågått siden IT-løsninger ble tatt i bruk i 1960-årene. I lang tid foregikk dette gjennom ulike samarbeidskonstellasjoner, og finansforetakene eide i stor grad IT-leverandørene. De tidligere datasentralene Fellesdata, IDA og NOVIT er i dag en del av EDB Business Partner ASA. Det skjer stadige endringer i dette markedet. IBM AS og den nordiske IBM-organisasjonen har i de senere årene blitt en stor og viktig leverandør av IT-tjenester til finanssektoren. Også ErgoGroup AS, TietoEnator, CSC (Computer Sciences Corporation) og WM-data leverer i økende grad IKT-tjenester til finansnæringen.

3.5.2 Myndighetskrav til utkontraktering

Utkontraktering kan være en hensiktsmessig løsning for leveranser av IKT-tjenester både for å sikre kvalitet, effektivitet og kostnadsstyring. Forutsetningen er imidlertid at en utkontrakteringsstrategi er basert på en forretningsplan som klart definerer hva foretaket ønsker å oppnå med utkontraktering og hvordan dette skal styres og kontrolleres av foretaket. I IKT-forskriften §§ 2 og 12 er det gitt spesifikke krav til foretak i finansnæringen om bestemte krav som skal ivaretas ved utkontraktering:

> ***§ 2 Planlegging og organisering***
> *Foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten. Det skal foreligge beskrivelse av den enkelte prosess og hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte.*
> ***Ved utkontraktering av deler eller hele IKT-virksomheten skal foretaket ha egne retningslinjer som skal sikre leveransen.***
> *Det skal oppnevnes en ansvarlig i foretaket for de ulike deler av IKT-virksomheten. Med ansvarlig menes en funksjon eller stilling.*
> ***§ 12 Utkontraktering***
> *Foretaket har ansvar for at IKT-virksomheten oppfyller alle krav som stilles etter denne forskrift. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Det skal foreligge en skriftlig avtale som sikrer dette. Avtalen må sikre at foretak under tilsyn også gis rett til å inspisere og kontrollere de av leverandørens aktiviteter som er knyttet til avtalen. Avtalen skal også sikre håndtering av taushetsbelagt informasjon.*

> *Avtalen skal videre sikre at Kredittilsynet gis tilgang til opplysninger fra og tilsyn hos IKT-leverandøren der Kredittilsynet finner det nødvendig som et ledd i tilsynet med foretaket. Foretaket skal sikre, i egen regi eller gjennom et formalisert samarbeid med andre foretak enn IKT-leverandøren, at organisasjonen besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalen.*

Basert på kravene i § 12 har det vært mulig for Kredittilsynet å gå gjennom IKT-leverandørenes aktiviteter som danner grunnlag for leveranser til det enkelte foretak som er under tilsyn av Kredittilsynet. Dette har gjort at Kredittilsynet kan foreta en samlet gjennomgang av IKT-virksomheten til foretaket, både den som ivaretas internt og den som foretas av ekstern leverandør. Kredittilsynet ser at det i stor grad gjennomføres utkontraktering av IKT-tjenester gjennom flere ledd. Dette er ofte en stor utfordring for foretaket å ha kontroll med og oppfølging av. Om vi ser på utkontraktering av IKT, kan figuren nedenfor gi et bilde av hovedelementene i dette:

Figur 2. Opplegg for utkontraktering

Hittil har ITO vært den mest vanlige formen for utkontraktering og følgelig også den med mest erfaringsdata. Denne type utkontraktering medfører at IT-leverandøren overtar definerte oppgaver for å levere konkrete resultater med avtalt kvalitet eller oppfylt servicenivå innenfor forvaltning og drift av den teknologiske infrastrukturen. AO er det neste nivået, og dette innebærer utkontraktering av utvikling, forvaltning og drift av applikasjonsporteføljen. Dette stiller ofte store krav til leverandør siden løsningene i større grad enn for ITO er spesialtilpassede for hver enkelt kunde. BPO betyr å overlate en eller flere IKT-intensive forretningsprosesser i sin helhet til en ekstern leverandør. Dette er en relativt ny form for utkontraktering, og den anses fremdeles som umoden.

3.6 Utarming av IKT-kompetanse innen bank og finans i Norge

En viktig forutsetning for utkontraktering av IKT, er at foretaket har ressurser og kompetanse til å være i stand til å forvalte avtalene, samt kontrollere og følge opp leveransene. Det er en utfordring å sikre tilstrekkelig kompetanse over tid, men helt avgjørende for at utkontrakteringen skal bli vellykket. Det er også klart definerte krav i IKT-forskriften om å beholde tilstrekkelig bestillerkompetanse ved utkontraktering.

Norge har i stor grad vært et foregangsland i bruken av IKT innenfor de næringene som Kredittilsynet har tilsynsansvar for. Den nærheten som det har vært mellom foretak, samarbeidsorganisasjoner og IKT-leverandører, har ført til at norske leverandører har kunnet utvikle løsninger som andre land fortsatt ikke har etablert. Felles infrastruktur innenfor betalingsformidling, oppgjør og verdipapirområdet, er løsninger som har gitt norske forbrukere en stor sikkerhet i bruken av tjenester som tilbys innenfor disse områdene. Også gjennom utstrakt samarbeid mellom bankene om utkontraktering, særlig når det gjelder banktjenester, har både store og små foretak kunnet tilby et stort spekter av tjenester til tilnærmet samme enhetspris for både store og små volumer.

Gjennom de endringene vi ser, med stadig større grad av utkontraktering ut over landegrensene, vil den norske andelen av IT-leveranser avta, og følgelig vil antall IT-ansatte avta. Sikkerhetsmessig og næringspolitisk er dette en betenkelig utvikling. Norsk finanssektors IT-virksomhet har ligget langt fremme og har hatt stor betydning, først og fremst for utviklingen av IKT-løsninger i finanssektoren, men også generelt for den totale IT-industrien i Norge gjennom at finanssektoren har vært en stor IT-aktør. Samspillet mellom de ulike delene av foretakenes forretnings- og IT-utviklere vil bli svekket og kan over tid redusere innovasjonen og nyskapningen på dette området. Om vi ser dette i sammenheng med filialisering og flytting av hovedkontorsfunksjoner ut av landet, vil dette forsterke den trenden som allerede er til stede. Norge kan langt på vei komme til å bli et ”filialland” når det gjelder finansforetakenes utvikling og forvaltning av egen IKT-virksomhet. Dette kan igjen svekke beredskapen og over tid resultere i større risiko samlet sett. Det er ingen tvil om at Norge i europeisk sammenheng har en høy andel IKT-virksomhet som blir ivaretatt utenfor landegrensene. Norge er dessuten et lite land med relativt begrensede ressurser knyttet til dette området. Over tid vil dette kunne få økt negativ virkning på den operasjonelle risikoen.

4 Kilder og informasjonsbearbeiding

Et viktig bidrag til ROS-analysen for 2006 er analysen av informasjonen fra ulike eksterne informasjonskilder. I kapittel 4 gis det et bilde av den informasjonen som har fremkommet gjennom våre egne arbeidsoppgaver. Samlet vurdering av konsekvensene av informasjonen som er dokumentert her, gis i kapittel 5.

4.1 IT-tilsyn

Kredittilsynet gjennomførte 21 IT-tilsyn i 2006 fordelt på bank, forsikring og verdipapirforetak, datasentraler og andre. Antall stedlige IT-tilsyn er noe lavere enn i fjor. Derimot ble det gjennomført flere forenklede IT-tilsyn enn tidligere år. Som en del av Kredittilsynets ordinære tilsyn, svarer foretakene på et egenevalueringsskjema om IKT-virksomheten. Svarene og tilsendte dokumenter blir gjennomgått, og svake områder fulgt opp med kommentarer og merknader i de ordinære tilsynsrapportene.

I 2006 var verdipapiroppgjøret i Norge et eget tema for IT-tilsyn. Gjennom møter med verdipapirforetak, Oslo Børs, VPS og dokumentasjon fra Norges Bank, har vi tegnet et bilde av IT-systemene som støtter dataflyten fra verdipapiret legges ut for salg til det er solgt og penger og papirer gjort opp. Arbeidet med å sluttføre denne gjennomgangen vil fortsette inn i 2007, blant annet med en vurdering av spesielle risikoområder og kontrolltiltak med disse.

Vi ser en positiv utvikling i foretakenes håndtering av IKT-virksomheten. Resultatene fra IT-tilsynene viser at foretakene har blitt bedre til å organisere IT-virksomheten på en mer hensiktsmessig måte. Foretakene har i større grad enn tidligere satt IT-prosessene på dagsorden som utgangspunkt for organisering av IT-virksomheten. Mange foretak har, eller er i gang med å implementere ITIL[6] i IKT-organisasjonen. Mens vi gjennom IT-tilsynene for noen år tilbake ofte påpekte mangler på en rekke områder, er det færre områder vi nå har anmerkninger til. Risikoanalyser er fortsatt et vanskelig område. Tidligere var problemet at risikoanalysen manglet. Nå er problemet heller at risikoanalyse er utført, men måten den er utført på, og innholdet i den, er ikke alltid av tilstrekkelig god kvalitet.

[6] Information Technology Infrastructure Library (ITIL) er et internasjonalt rammeverk for ”best practice” på de operative områdene av IT-virksomheten.

Kredittilsynet fører tilsyn med et stort spekter av ulike foretakstyper som har ulike utfordringer på IT-siden. Mens det for bank ofte er tilgjengelighet og beskyttelse av de webbaserte applikasjonene som står i sentrum, kan den største utfordringen for andre bransjer være håndteringen av et komplisert regelverk. For forsikringsbransjen er tilpasning av IT-systemene til regelverket og endringer i dette, svært arbeidskrevende. Her kan kompleksiteten i regelverket innebære en risiko ved at det kan være vanskelig å kontrollere og verifisere at IT-systemene faktisk produserer resultater som er i henhold til reglene.

4.2 Intervjuer med sentrale aktører

Tolv foretak, med nøkkelpersonell fra foretaket og IKT-området, og som samlet dekker vesentlige deler av den finansielle sektoren, deltok i intervjuene. Erfaringene med gjennomføringen av intervjuene vurderes som gode. En nærmere bearbeiding av resultatene viser følgende hovedtrekk fra svarene på de enkelte spørsmålene:

1) Hva ser foretaket på som den/de største risiko/er ved foretakets bruk av IKT?

De viktigste forholdene vi vil trekke frem fra intervjuene er:

- Introduksjon av ny teknologi gir høy risiko for alvorlige feilsituasjoner.
- Muligheten til å identifisere latente feil der konsekvensene blir store, særlig av typen Single Point of Failure i teknisk infrastruktur, er et risikoområde som krever mer oppmerksomhet.
- Mangel på tilstrekkelig nøkkelkompetanse og dermed kontroll over egen situasjon kan gi sårbarhet.
- Bruk av såkalt åpne løsninger, for eksempel Internett, krever stadig større oppmerksomhet, med bakgrunn i den innsatsen som organisert kriminalitet representerer og behovet for å ligge i forkant med preventive tiltak. Det er særlig produktområdene nettbank, handel på Internett og tjenestekanaler som benytter kort, som viser seg å være utsatte. Her blir det spørsmål om evne til å reagere og iverksette raske tiltak når en hendelse inntreffer.
- Endringer representerer en risiko og krever etablering av gode prosedyrer for endringshåndtering og kvalitet i håndteringen. Forretningsmessige og myndighetspålagte krav gir stort press på endringsbehovet.
- Organisasjonsmessige endringer, særlig når dette skjer over landegrenser i nordiske konsern, vurderes som problematisk når det gjelder oversikt over og styring av potensielle feilsituasjoner. Nødvendig samordning er tidkrevende og blir et problem i seg selv for å kunne reagere tilstrekkelig med adekvate tiltak.
- Skifte av teknologisk plattform vurderes å gi høy risiko under endringsprosesser. Dette krever stram kontroll.
- I en prosess med store endringer er det særlig viktig å sikre relevant backup. Backup-løsningen må være tilstrekkelig testet for å sikre at denne fungerer i en plutselig oppstått katastrofesituasjon. Dette stiller store krav til ressurser og praktisk tilrettelegging ved

endringer som gjennomføres med høyt krav til tempo og forutsigbarhet (overholde fastlagte planer).
- Det ble pekt på at foretakene ser på mulig tap av omdømme som en tilleggsrisiko og følgeskade av en oppstått feilsituasjon om denne blir kjent offentlig.

2) Hva har vært de største problemene knyttet til IKT-området i 2006?

- Mangler i prosjektetablering, -planlegging og -gjennomføring og de følgeskader dette ga ved driftssetting.
- Manglende evne til styring og kontroll ved gjennomføring av prosjekter og større endringer.
- Store endringer i myndighetskrav og nye tjenester innenfor pensjonsforsikring samtidig med plattformendringer.
- Problemer knyttet til nettbank.
- Mangler i bestillerkompetanse ved utkontraktering og ved kjøp av tjenester.
- Utilstrekkelig testing.
- Feil i endringskontroll.
- Sikre tilstrekkelig nøkkelkompetanse.
- Feil knyttet til utvikling og kontroll med teknisk nettverk hvilket resulterer i manglende tilgjengelighet og stabilitet på teknisk nettverk med tilhørende store konsekvenser.

3) Hva er grunnlaget for å kunne identifisere disse?
a) I stor grad var det med grunnlag i foretakenes ROS-analyser at problemstillingene ble identifisert.

b) I tillegg var arbeidet med registrering og behandling av hendelser en annen viktig kilde til informasjon om feil og problemer som var oppstått.

4) Hva ser foretaket på som de største utfordringene i 2007 mht. risiko ved bruk av IKT?
- Plattformskifte som krever større endringer i eksisterende applikasjonsporteføljе.
- Sikre en virksom og korrekt backup-løsning som grunnlag for gjenoppretting ved katastrofelignende situasjoner.
- Sikre etterlevelse av myndighetskrav (Basel II, Solvens II, OTP og annet regelverk, f.eks. EU-direktiver) som samlet krever store endringer samtidig som forretningssiden også stiller krav til endringer.
- Beholde og sikre tilstrekkelig kompetanse internt i en situasjon med stor grad av utkontraktering.

5) Hva ser foretaket på som viktige problemstillinger mht. IKT-risiko i 2007 og hvor det kreves iverksatt egne tiltak?
- Sikre funksjonell og sikkerhetsmessig tilfredsstillende PKI-løsning.
- Plattformskifte.
- Bedre sikkerheten knyttet til nettbank og kunderettede kanaler.
- Bedre sikring mot angrep via Internett.

- Møte krav til endringer, samtidig med effektivisering og kostnadsreduksjon.
- Bedre sikkerheten knyttet til nettverk og infrastruktur.

4.3 Spørreundersøkelser som ledd i ROS-analysen

Kredittilsynet gjennomførte i 2006 flere spørreundersøkelser som relaterte seg til kartlegging av mulige sårbare områder i IKT-virksomheten. Også tidligere har vi benyttet denne metoden for å få oppdatert informasjon fra foretakene om status på ulike områder i IKT-virksomheten. Ofte er spørreundersøkelsene rettet mot en foretakstype og omhandler et konkret tema som for eksempel bruk av trådløse nett eller introduksjon av betalingstjenester på mobiltelefon i bankene. Basert på den informasjonen vi innhenter gjennom spørreundersøkelser, får vi et bredt bilde av status på det aktuelle området og mulighet for å sammenligne på tvers av foretakene. I noen tilfeller der spørreundersøkelsen fokuserer på betalingssystemer, kan svarene til en viss grad avdekke om foretakene er flinke nok til å etterleve meldeplikten etter lov om betalingssystemer, se kapittel 4.5. I 2006 brukte vi spørreundersøkelser også til å kartlegge hendelsesregistreringen i foretakene. Dette er nærmere beskrevet i kapittel 4.4.2. All informasjon Kredittilsynet benytter fra spørreundersøkelsene, er anonymisert.

4.4 Hendelser

Kredittilsynet fikk i 2006 mer informasjon om hendelser enn tidligere år. Årsaken til dette kan være at det var mange alvorlige hendelser i 2006. Vektlegging av hendelsesrapportering i forrige års ROS-analyse, samt fokusering på dette området i gjennomførte IT-tilsyn, kan også ha bidratt til at foretakene i større grad har rapportert uoppfordret om hendelser til Kredittilsynet.

4.4.1 Vesentlige hendelser

Hendelser som Kredittilsynet er gjort kjent med, er en god illustrasjon på at det er mange ulike årsaker til at en hendelse kan kategoriseres som alvorlig eller kritisk, og at en hendelse kan være kritisk selv om den ikke fører til direkte tap av penger. I 2006 var det eksempler på:

- Større driftsforstyrrelser som førte til at kundekanaler og tjenester var utilgjengelige over flere dager.
- Synliggjøring av andre kunders konti.
- Feil på komponenter i sentral infrastruktur førte til kortvarige brudd, men rammet bredt på tvers av foretak og viste sårbarheten ved bruk av felles infrastruktur.
- Nye former for avanserte kriminelle angrep mot nettbankkanalene.
- Tjenester med gjennomsnittlig dårligere tilgjengelighet og stabilitet enn tidligere som følge av nye teknologiske plattformer.

4.4.2 Kartlegging av bankenes hendelsesregistrering

Som ledd i å kartlegge foretakenes egen hendelsesregistrering og kategorisering, gjennomførte Kredittilsynet en spørreundersøkelse høsten 2006. Kredittilsynet sendte brev til et utvalg banker og banksammenslutninger i Norge, som til sammen utgjorde ca. 95 prosent av bankene. Bankene ble blant annet spurt om de hadde et system for kategorisering av hendelser etter alvorlighetsgrad og videre om hvor mange kritiske og hvor mange alvorlige hendelser det hadde vært i perioden 1. september 2005 til 1. september 2006.

4.4.3 Resultatet av undersøkelsen – bankenes kategorisering

Alle bankene svarte at de hadde et system for kategorisering av hendelser på en skala fra 1–3 eller fra 1–4, der de alvorligste hendelsene var kategorisert til 1. De største bankene la også ved detaljerte beskrivelser av hvordan de kategoriserte hendelsene, noe som vitnet om at det var lagt ned mye arbeid i denne sammenheng. Kategoriseringen er basert på konsekvens av hendelsen målt mot ulike kvantitative parametere – som antall brukere som ble berørt, antall systemer som ble berørt og antall minutters varighet av hendelsen.

4.4.4 Antall hendelser

Undersøkelsen viste et stort sprik mellom foretakene i antall registrerte alvorlige og kritiske hendelser. Noen banker og banksammenslutninger pekte seg ut ved at de hadde registrert et langt større antall hendelser enn de andre. Tallene varierte mellom 370 og 7 kritiske hendelser og 850 og 35 alvorlige hendelser. Dette indikerer at bankene kategoriserer hendelsene på ulike måter. Dersom foretakene hadde rapportert alle hendelser de selv hadde kategorisert som kritiske i perioden, ville det ført til rapportering av rundt 900 hendelser med en overvekt av rapporteringer fra enkelte banker og banksammenslutninger uten at disse foretakene reelt sett hadde flere feil eller større ustabilitet i driften enn de andre. Kredittilsynet vurderer det som positivt at det foreligger hendelsesrapporteringer, men ser at ensrettede kriterier kunne være formålstjenlige.

4.5 Meldeplikten for systemer for betalingstjenester

I lov om betalingssystemer § 3-2 om meldeplikt heter det: ”Det skal uten unødig opphold gis melding til Kredittilsynet om etablering og drift av system for betalingstjenester.”

Kredittilsynet utarbeidet høsten 2004 et rundskriv med 19 kontrollspørsmål som skal besvares og sendes til Kredittilsynet ved innføring av nye betalingssystemer eller endringer i eksisterende betalingssystemer. Foretakene har blitt flinkere til å melde fra om nye eller endrede betalingssystemer. Det var en markert økning i antall mottatte skjemaer i 2006. For Kredittilsynet betyr dette tidlig informasjon om planlagte systemer og en oversikt over hva foretakene arbeider med.

Samlet gir de mottatte egenevalueringsskjemaene en bekreftelse på at meldeplikten kan utgjøre et viktig bidrag til å holde tilsynsmyndighetene løpende orientert om foretakenes aktiviteter på

betalingssystemssiden. Samtidig ser vi at slik skjemaet er utformet i dag, er det begrenset hvilken reell informasjon om systemet som avdekkes gjennom svarene på de 19 ja/nei-spørsmålene i egenmeldingen. En justering av utformingen av egenmeldingen er derfor aktuell. Så langt har rapporteringen i stor grad fokusert på IKT-relaterte forhold. Dette vil bli vurdert å utvide egenmeldingen slik at den bedre kan fange opp hensynet til sikker og effektiv betaling og rasjonell og samordnet utførelse av betalingstjenestene.

5 Kredittilsynets vurderinger

Kredittilsynet har med bakgrunn i det informasjonstilfanget vi har hatt tilgang til, og som det er redegjort for i kapittel 3 og 4, analysert informasjonen for å identifisere aktuelle risikoområder. Vurdering av forholdet mellom sannsynlighet og konsekvens er vektlagt, og på bakgrunn av analysen har vi kommet frem til områder vi mener det er særlig grunn til å legge vekt på og som krever at det blir iverksatt risikoreduserende tiltak. Nedenfor har vi redegjort nærmere for hvert av de aktuelle risikoområdene.

5.1 Nettbank

I 2005 var 93 prosent av betalingstransaksjonene elektroniske. Om lag 2,3 millioner personer i Norge brukte nettbank i 2005.[7] I tillegg benyttet også en rekke bedrifter nettbank. Tallene er antagelig tallene enda høyere for 2006. Nettbanken er den sentrale betalingskanalen som også brukes til å utføre en rekke andre finansielle tjenester. Dette viser hvor viktig det er å ha funksjonelle og sikre nettbankløsninger. I 2006 var det flere ulike hendelser og alvorlige problemer knyttet til bruk av nettbank. Dette skyldtes manglende funksjonalitet, manglende tilgjengelighet og manglende sikkerhetsløsninger.

5.1.1 Brukergrensesnitt i nettbank

Kundenære løsninger som nettbank stiller store krav til funksjonalitet. Nettbanken skal kunne betjenes av alle, og bør derfor ha et brukergrensesnitt der funksjonaliteten er selvforklarende. Den skal ikke kreve spesielle forkunnskaper hos brukeren eller spesiell opplæring. Dette stiller ekstra strenge krav til at det er innebygde kontroller i løsningen som reduserer kundens mulighet for å gjøre feil. Høsten 2006 var det et større medieoppslag omkring en nettbanktransaksjon som havnet på feil konto. Finansdepartementet engasjerte seg i saken og ba Kredittilsynet om en utredning. Kredittilsynet har undersøkt hendelsen i samarbeid med bransjeforeningene. Finansnæringens Hovedorganisasjon (FNH) og Sparebankforeningen har utarbeidet en liste med 13 tiltak som bankene skal implementere i nettbankløsningene innen utgangen av første kvartal i 2007. Dette er tiltak som skal gjøre brukergrensesnittet i nettbanken sikrere slik at kunden vanskelig skal kunne gjøre utilsiktede feil. Kredittilsynet vil følge opp bankenes implementering av tiltakene og vurdere om ytterligere tiltak er nødvendige. Tiltakene er spesielt rettet mot funksjoner i regningsbetalingen for personkunder i

[7] Kilde: Årsrapport om betalingssystemer fra Norges Bank for 2005

nettbank. Funksjoner knyttet til andre tjenester enn regningsbetaling og til bedriftskunder i nettbank, kan også være aktuelle å vurdere for å gjøre løsningene mer robust mot brukerfeil.

5.1.2 Tilgjengelighet til nettbank

Flere og flere kunder baserer seg på å utføre egne banktjenester via nettbanken. Nettbanken er åpen 24 timer i døgnet og gjør det enkelt å tilpasse regningsbetaling til andre aktiviteter. Tjenestespekteret i nettbanken utvides stadig. I tillegg til regningsbetaling tilbys kjøp og endringer av forsikringsavtaler og pensjonsavtaler, handel med verdipapirer og til dels behandling av lånesøknader. Nettbank for bedriftskunder tilbyr også en rekke tjenester.

I 2006 var det eksempler på situasjoner der nettbanker var utilgjengelig over flere dager. Manglende tilgang til nettbanken kan i en del tilfeller kompenseres med betjening via telefon, men med den utbredelsen bruk av nettbank har i dag, er det vanskelig å mobilisere tilstrekkelig manuelle ressurser. Kontinuitets- og katastrofeløsninger på dette området er derfor spesielt viktige. Se for øvrig mer om dette i kapittel 5.3.

5.1.3 Sikkerhet ved bruk av nettbank

De alvorlige hendelsene på slutten av året 2006 der flere banker fikk sine nettbankløsninger kompromittert, var urovekkende. Måten disse angrepene ble utført på, kan representere et gjennombrudd for de kriminelle miljøene. Den ondsinnede koden (trojaner) er smart utformet og kan operere på baksiden av autentiseringsløsningene. Når nettbankbrukeren er pålogget, kan det genereres transaksjoner som kunden selv ikke ser. Den ondsinnede koden kan ha blitt overført til kundens pc i forbindelse med at en spam-mail blir åpnet, gjennom et phishing-angrep eller ved nedlasting av programvare, musikk, bilder eller annet fra nettet. Den ondsinnede koden er av relativt avansert karakter, og det er grunn til å tro at det er aktører utenfor Norge som står bak slike angrep. At det skjedde angrep i flere banker omtrent på samme tidspunkt, tyder på at dette er velregissert og at det er organiserte kriminelle miljøer som står bak.

Flere banker tilbyr sine kunder gratis nedlasting og bruk av antivirusprodukter. Kredittilsynet anser dette tiltaket som nyttig, og som et av mange tiltak for å høyne sikkerhetsnivået i de norske nettbankene. Samtidig kan ikke sikkerheten baseres på tiltak som skal ivaretas på den enkelte kundes pc. Det kan være behov for flere tekniske tiltak for å forhindre ondsinnet kode på brukerens lokale pc. Dette er et felles problem for alle bankene, og det kan være hensiktsmessig at tiltak blir utformet i form av felles krav til nettbankløsningene.

5.2 Ny teknologi og risikoanalyser

Bruk av ny teknologi kan introdusere nye risikoområder med ukjente sikkerhetshull som kan skape alvorlige feilsituasjoner. Eksempler på ny teknologi som vi har sett de siste årene, er nye former for autentiseringsmekanismer, bruk av mobile løsninger for betalingstjenester, nye løsninger for sikker e-handel, nye måter å utveksle data på og nye måter å konfigurere nettverk på. Samtidig ser vi også at

flere foretak tilpasser og flytter applikasjonene fra en velprøvd teknisk plattform til nye plattformer. Det er viktig at en i slike tilfeller også tar behørig hensyn til behovet for tilstrekkelig kapasitet i datasystemene for å kunne takle situasjoner med stor belastning på systemene.

Kredittilsynet gjorde i 2006 en kartlegging av bankenes tilbud om betalingstjenester og/eller handel med aksjer via mobiltelefon. Resultatet av undersøkelsen viste at noen banker allerede har lansert løsninger for dette, andre planlegger lansering i løpet av 2007, mens andre igjen, og da spesielt sparebankene, så langt ikke har planlagt å tilby slike tjenester. Bankene som har utviklet betalingsløsninger for mobiltelefon, svarer at de har gjennomført risikoanalyser av løsningene på like linje med slik de gjør ved lansering av andre nye produkter.

Uten tilstrekkelige risikoanalyser er det vanskelig å identifisere latente feil knyttet til Single Point of Failure i teknisk infrastruktur, dårlig skalering av ytelse og stabilitet ved volumøkning og ulike typer sikkerhetshull. Bruk av såkalt åpne løsninger som Internett, krever stadig større oppmerksomhet med bakgrunn i den innsatsen som organisert kriminalitet representerer og behovet for å ligge i forkant med preventive tiltak. Også på dette området er risikoanalyser svært viktige. Kredittilsynet har observert at mangelen på tilstrekkelige risikoanalyser ofte skyldes mangel på tilgang til nøkkelkompetanse. Dette gjelder både for aktørene i finansnæringen og de leverandørene som leverer IKT-tjenester til disse. Selv om risikoanalyser på dette nivået krever høyt kompetente ressurser og kan bety økte kostnader, er det etter Kredittilsynets vurdering en nødvendig investering. Konsekvensen av uforutsette hendelser kan i dag være større enn bare for noen år tilbake fordi forretningsdriften i foretakene nå i enda større grad er basert på IKT og ofte på internettbaserte tjenester som tilbyr en ubrutt åpningstid.

5.3 Endringshåndtering og katastrofeberedskap

Ulike drivere som samlet krever endringer, representerer en risiko og krever at det blir etablert gode prosedyrer for endringshåndtering og god kvalitet i gjennomføringen. Endringshåndtering er et område som er vektlagt i tidligere ROS-analyser. Kredittilsynets vurdering er at det de siste tre årene har vært en klar forbedring i finansnæringen på dette området. Foretakene har i stor grad implementert en prosess for endringshåndtering. Men fortsatt ser vi at det er i forbindelse med endringer problemer oftest oppstår. Det er viktig at endringshåndtering blir vektlagt i alle ledd som er involvert i en slik prosess, ikke minst gjelder det oppdatering av kontinuitets- og katastrofeløsninger.

Samlet sett kan summen av forretningsmessige krav og myndighetspålagte krav gi stort press på endringsbehovet. Organisasjonsmessige endringer, særlig når dette skjer over landegrenser, vurderes som en utfordring når det gjelder behovet for samordning og potensielle feilsituasjoner. Aktiviteter som medfører skifte av teknologisk plattform, vurderes av Kredittilsynet å gi høy risiko under endringsprosessen. Dette krever streng kontroll på endringshåndteringen. Internettbaserte tjenester som nettbank med 24 timeres ubrutt åpningstid, stiller store krav til kontinuitets- og katastrofeløsninger.

Intervju med utvalgte foretak viser at foretakene vurderer utilstrekkelige katastrofeløsninger som en av de største risikoene. Blant annet på grunn av det høye endringstempoet, er mange foretak usikre på om katastrofeløsningen er tilstrekkelig oppdatert til å fungere i en reell katastrofesituasjon.

God kontroll med endringshåndteringen og at denne inkluderer oppdatering av kontinuitets- og katastrofeprosessen, er derfor like aktuelt fortsatt.

5.4 Ufullstendig hendelsesrapportering

I ROS-analysen for 2005 var ufullstendig hendelsesrapportering identifisert som et risiko- og sårbarhetsområde, og beskrevet som et av de områdene Kredittilsynet ville arbeide videre med. I 2006 hadde Kredittilsynet på ulike måter fortsatt arbeidet med dette temaet. Hendelsesrapportering har blant annet blitt drøftet med FNH og Sparebankforeningen, og det vil bli lagt vekt på at tiltak på dette området blir utformet i samarbeid med næringen. Hensikten med en eventuell regulering på dette området er at det skal gi en gevinst i form av økt sikkerhet for det enkelte foretak samt for bransjen som helhet. Derfor er det viktig at foretakene ikke pålegges detaljregulering som øker byrden på foretakene, dersom dette ikke gir åpenbare gevinster tilbake.

Fortsatt er måten rapporteringen skjer på usystematisk og uten samordning. Mange av hendelsene har et hendelsesløp og en årsakssammenheng som kan være nyttig å kjenne til for flere enn foretaket der hendelsen har skjedd. Det har også vært eksempler på kjedevirkninger der en hendelse er med på å igangsette en serie påfølgende hendelser. Hendelser i foretakene blir i stor grad dokumentert, men det er ikke regulert hvordan dette skal gjøres.

Sentralt i en drøfting om rapportering av hendelser til en felles instans, er hvilke kriterier som skal legges til grunn for å avgjøre om en hendelse skal rapporteres. Hendelsene i 2006 er eksempler som viser at det er viktig å bruke flere ulike målestokker for å bestemme hvor alvorlig en hendelse er. Kartleggingen av foretakenes egen hendelsesregistrering – og kategorisering som Kredittilsynet gjennomførte høsten 2006 (se kapittel 4.4), viser at bankenes egne kategoriseringer ikke uten videre kan benyttes som grunnlag for å kvalifisere en hendelse for rapportering til en sentral instans.

5.5 Svindel med kort

5.5.1 Handel på Internett

Ved handel på Internett er få sikkerhetsmekanismer tatt i bruk. De fleste handelssteder på nettet tilbyr ingen spesiell sikkerhetsløsning. Kunden registrerer kortnummer og utløpsdato, og dette er all informasjon kunden blir avkrevd for å gjennomføre betalingen. Opplysninger om kortnummer og utløpsdato er trykket i klartekst på betalingskortene og er derfor informasjon som lett kan komme på

avveie. I tillegg har det vært eksempler på phishing-forsøk for å avlure kunder kortinformasjon og på tyveri av datafiler med kortinformasjon fra operatører knyttet til brukerstedene.

I 2006 innhentet Kredittilsynet informasjon fra APACS i London. I henhold til APACS er svindel med kort det området som bankene i Storbritannia taper penger mest på. Etter at Storbritannia i 2004 innførte betalingskort med chip og PIN, har tapstallene gått ned. Fortsatt utgjør svindel med kort de største tapstallene, men nå er denne svindelen av typen "Card Not Present" (CNP), det vil si ulike typer svindel der kundens opplysninger om kortnummer etc. er stjålet fra en annen. Handel på nettet, eller handel pr. telefon, er eksempler på tjenester som er utsatt for dette. Svindel med kort utgjør forholdsvis små tap i Norge i dag, og en del av tapene skyldes brukersteder som ikke gjør opp for seg, eller er involvert i svindelen. Men dette er et område som i større grad kan bli et mål for kriminelle operasjoner.

Det er utviklet ulike løsninger for å gjøre handel på Internett sikrere. Bankene vil i løpet av kort tid tilby en kontobasert betalingstjeneste for bruk på Internett (BankAxess) som er basert på at kundene autentiserer betalingen ved hjelp av BankID. For bruk av kredittkort kan autentisering av betalingen gjøres ved bruk av VISAs 3-D Secure og MasterCard SecureCode, som er de sikkerhetsløsningene som kortselskapene tilbyr på Internett. I noen tilfeller benyttes BankID i forbindelse med disse løsningene. Foreløpig er det mange handelssteder på nettet som ikke tilbyr kundene disse sikkerhetsløsningene.

Selskapene som har ansvar for innløsing av korttransaksjoner, bruker elektroniske overvåkningssystemer for å avdekke mistenkelige transaksjoner og kan dermed melde fra til kunden hvis det er unormale transaksjonsmønster. Men slike reaktive kontroller kan selvsagt ikke erstatte en sikkerhetsløsning i det betalingen skjer. Etter Kredittilsynets vurdering er det viktig at brukerstedene benytter tilgjengelige sikkerhetsløsninger slik at kundene gis en mulighet til å sikre sine betalinger med kort over nettet.

5.5.2 Betalingsterminaler

I 2006 installerte de fleste bankene utstyr på minibankene som hindrer skimming av betalingskortene. Ofte ser vi imidlertid at når en kanal tettes, finner de kriminelle miljøene nye kanaler å angripe. Angrep mot betalingsterminaler i butikkene og selvbetjente bensinpumper blir derfor nye mål for kriminell aktivitet. Også slike betalingsterminaler kan overvåkes av skjulte kameraer som fotograferer PIN-koder kombinert med organiserte tyverier av kort.

6 Hva kan Kredittilsynet gjøre?

I dette kapitlet vil vi forsøke å se nærmere på hvordan Kredittilsynet med sine virkemidler kan bidra til å bedre foretakenes håndtering av risiko knyttet til IKT. Det er det enkelte foretak som har ansvaret for å ivareta sikkerhet og håndtere risiko knyttet til bruk av IKT, på en akseptabel måte og i henhold til de rammebetingelser som foreligger. Dette vil gjelde offentlige regelverk, bransjeavtalte tiltak og internt fastsatte krav til bruk av IKT. Kredittilsynets bidrag vil i hovedsak skje gjennom tilsynsvirksomhet og gjennom å stille bestemte krav til bruk av IKT, men bidrag vil også skje ved å prioritere problemområder, veiledning og informasjonsvirksomhet.

6.1 Tilsynsopplegget

I 2001 startet Kredittilsynet arbeidet med å utvikle en ny tilsynsmetode for IT-tilsynet basert på den internasjonal metoden CobiT (Control Objectives for Information and Related Technology). Denne metoden er administrert og videreutviklet av den brukerstyrte internasjonale medlemsorganisasjonen ISACA (Information Systems Audit and Control Association) gjennom den heleide institusjonen IT Governance Institute. Denne organisasjonens hovedoppgave er knyttet til arbeid med styring, kvalitetssikring og revisjonsarbeid innenfor IKT-området. I 2006 ble CobiT videreutviklet slik at det nå dekker hele IT Governance-begrepet.

IT-tilsynsopplegget til Kredittilsynet har vært i bruk i om lag fem år, og resultatene av opplegget vurderes å være svært gode. Ved utgangen av 2006 var det gjennomført til sammen over 100 IT-tilsyn med bruk av egenevalueringsopplegget. Dagens tilsynsopplegg er modulinndelt og inneholder en hovedmodul som representerer det generelle opplegget for gjennomføring av IT-tilsyn. Dette er i stor grad rettet mot foretakets håndtering av IKT-prosesser og kan sammenlignes med en overordnet temperaturmåling av foretakets bruk av IKT. Basert på vår erfaring med bruk av dette opplegget, har vi videreutviklet egne tilleggsmoduler som adresserer egne risikoområder som kan benyttes alene eller i kombinasjon, avhengig av hvilken informasjon vi på forhånd har om det aktuelle tilsynsobjektet.

Det arbeides med å videreutvikle opplegget, både med vekting av risiko, men også for å tilpasse dette til en operasjonell risikomodul innenfor Basel II.

Med erfaring fra problemområder i 2006 har vi kommet til at neste hovedsteg i en videreutvikling vil være å legge vekt på transaksjonstest og sikring av integriteten av data i risikosensitive systemer. Dette kan bidra til å oppdage sårbare områder før det feiler.

Figur 3. Risikobasert IT-tilsynsopplegg

Bygge 3 hovedmoduler som adresserer, 1) IKT-prosesser, 2) risikosensitivitet og 3) ny test og verifikasjon. Samlet vil dette representere et mer komplett risikosensitivt tilsynsopplegg.

Tilnærming er: IKT-prosesser basert på Cobit's 34 IT-prosesser
Utviklet 170 kontrollspørsmål relatert til enkeltprosesser som kontrollmål.
Opplegget benyttes i et egenevalueringsopplegg med JA/NEI-svar.
Det er andre elementer i tillegg. Vi har nå femtegenerasjon kontrollspørsmål – CobiT 4.0. (Konsulentselskapet PWC kvalitetssikret førsteversjon). *Basert på hva du skal gjøre.*

Dette opplegget er i god gjenge.

Tilnærming er: Utvalgte IKT-temaer basert på en risikovurdering.
Utviklet kontrollspørsmål på utvalgte tema; virusbeskyttelse, brannmur, katastrofebackup, nettbank, betalingstjenester, hvitvasking, krav til interne målemetoder / IRB-modeller og meldeplikten (lov om betalingssystemer). Vi har benyttet spesielle kompetansemiljøer for hvert av temaene som ledd i å kvalitetssikre kontrollspørsmålene. Tilsynsmodulene benyttes i et egenevalueringsopplegg med JA/NEI-svar.
Er mer fokusert på hvordan ulike forhold skal ivaretas.

Kan ITIL gi en bedre referanse for å utvikle kontrollspørsmål og valg av kontrolltema?

Tilnærming er: Transaksjonstest på utvalgte IKT-deler basert på en risikovurdering (ende til ende-test) og verifikasjon.
Planlagt som den siste modulen i et risikosensitivt tilsynsopplegg.

Dette er et tema som det er gjort enkelte forberedelser til, men arbeidet med dette er foreløpig ikke iverksatt.

Det pågår en betydelig profesjonalisering internasjonalt med hensyn til identifisering, måling og styring av operasjonell risiko. Skal Kredittilsynet evne å følge med i denne utviklingen, blir det viktig at vi finner frem til rasjonelle tilsynsopplegg som har basis i beste praksis-løsninger internasjonalt, eventuelt tilleggsutviklet og tilpasset våre forhold. Fra gjennomførte IT-tilsyn har vi gode erfaringer med bruk av forhåndsutsendte kontrollspørsmål for egenevaluering. Dette ligger til grunn for vår videreutvikling.

6.2 Regelverksutvikling

En tradisjonell angrepsvinkel for tilsynsmyndigheter for å møte observerte trender til økt operasjonell risiko, er en fortsatt aktiv videreutvikling og bruk av regelverket som preventivt virkemiddel og for standardsetting. Økt bruk av regelverk på denne måten kan føre til større belastninger for finansnæringen. Det er derfor viktig at regelverket og vår håndheving ikke er for detaljorientert, samtidig som det bør være et mål at kravene spiller sammen med internasjonale trender for standardsetting og beste praksis. Eksempler her er tenkningen som ligger bak Corporate Governance, IT Governance, ISO-standarder og andre industristandarder og opplegg av type balansert målstyring. Med basis i prosesser som Basel II og Solvens II, vil omfanget av regler knyttet til internkontroll øke.

Det blir derfor viktig at vi evner å se de ulike lovene og forskriftene i sammenheng og ikke bare øke "bruttobyrden" ved kun å lage nye regelverk basert på nye behov (bruttometoden). Dette blir en utfordring i den rollen som Kredittilsynet ivaretar. Vi antar uansett at Internkontrollforskriften, IKT-forskriften, lov om betalingssystemer og Basel II-regelverket, og senere Solvens II-regelverket blir viktige verktøy for vårt videre arbeid med operasjonell risiko, samtidig som det vi må legge vekt på å samordne og forenkle regelverket.

6.2.1 Veiledning i etterlevelse av IKT-forskriften for mindre foretak

Kredittilsynet vil fortsette arbeidet med å informere om IKT-forskriften, samt følge opp at det enkelte foretak etterlever denne. Mange mindre foretak har gitt uttrykk for at de synes det er vanskelig å etterleve IKT-forskriften. Forskriften virker omfattende når foretaket har en begrenset IKT-virksomhet. Som en hjelp til de mindre foretakene utabeidet Kredittilsynet i 2006 en veiledning i etterlevelse av IKT-forskriften spesielt rettet mot eiendomsmeglingsforetak. Dette arbeidet vil bli videreført, og det arbeides også med å lage en lignende veiledning rettet mot mindre sparebanker i 2007. ISACA Norge har etter samarbeid med Kredittilsynet utarbeidet et eget temahefte for etterlevelse av IKT-forskriften. Denne type samarbeid ser vi på som positive bidrag som kan gjøre det lettere for det enkelte foretak å sørge for å ivareta kravene i forskriften.

6.3 Videreutvikling av opplegget for meldeplikt for systemer for betalingstjenester

Arbeidet med opplegget for meldeplikten vil bli videreført i 2007. Samtidig vil vi vurdere å videreføre opplegget med målrettede spørreundersøkelser på spesifikke områder for dermed å identifisere mulige sårbare områder. Dette vil særlig relatere seg til autentisering, autorisasjon og sikkerhet, samt til gjennomgang av kundeopererte løsninger i ulike kanaler.

Det er planlagt en samlet gjennomgang og analyse av hele infrastrukturen på betalingssystemområdet, inkludert teknisk nettverk, samhandling, applikasjoner, driftsansvar, reserveløsninger og ansvarsforhold for å identifisere mulige sårbare områder, uklare ansvarsforhold eller manglende/utilstrekkelige reserveløsninger.

6.4 Risiko- og sårbarhetsanalyser (ROS)

Det er viktig å understreke at det er det enkelte foretak som fullt ut har ansvaret for egen IKT-virksomhet og håndtering av risiko. Kredittilsynets aktiviteter er et bidrag til det viktige arbeidet det enkelte foretak selv må gjennomføre for å oppnå betryggende forhold i bruk av IKT-løsninger.

Vi vil videreføre påbegynt arbeid med å sikre mer kvantitative data som underlag for ROS-analysen, i hovedsak relatert til hendelser og feil. Fortsatt vil likevel hovedtyngden av informasjon være kvalitativ. Fordelen med å få mer kvantitative data, er å få frem utviklingstrender.

Et annet utviklingsområde vil være metodeforbedring for gjennomføring av ROS-analyser. I 2006 pågikk det et nært samarbeid med myndighetenes BAS 5-prosjekt (Beredskap av Samfunnet), hvor nr. 5 er relatert til å få frem bedre metodegrunnlag for å gjøre ROS-analyser. Det er Forsvarets Forskningsinstitutt (FFI) som har ledet prosjektet, og Kredittilsynet bidro til testgjennomføring av en ROS-analyse i VPS. Sluttrapporten fra dette arbeidet skal foreligge i 2007, og vil bli vurdert nærmere som grunnlag for en metodeforbedring av vår ROS-analyse. Likeledes vil dette kunne gi grunnlag for å utvikle en veiledning relatert til etterlevelse av § 3 Risiko, i IKT-forskriften.

Det er også planlagt å se nærmere på bruk av problemindikatorer som hjelpemiddel både ved gjennomføring av ROS-analyser, men også knyttet til tilsynsvirksomheten. Eksempler på slike indikatorer er:

- Høye, faste IKT-kostnader
- Store budsjettoverskridelser i IT-prosjekter
- Mange skrinlagte eller forsinkede IT-prosjekter
- Høy turnover og manglende rekruttering
- Manglende kompetanseutvikling
- Stor avhengighet av nøkkelpersonell
- Stor hyppighet på hardware- og software-feil
- Omfattende avviks-/hendelsesrapporter
- Manglende oppfølging av avviks-/hendelsesrapporter

6.5 Hendelsesregistrering og rapportering

6.5.1 Felles retningslinjer for kategorisering av hendelser

Undersøkelsen Kredittilsynet gjennomførte i 2006, viser at det er stor variasjon i hvordan foretakene vurderer og kategoriserer hendelser på. Det kommer tydelig frem at det er store ulikheter bankene imellom når det gjelder antall kritiske hendelser registrert i perioden. Selv om konsekvensen av en og samme hendelsestype kan variere fra foretak til foretak og fra system til system, er ulikhetene neppe så store som resultatet av denne undersøkelsen indikerer.

Dersom en sentral regulering av hendelsesregistrering og rapportering skal kunne fungere hensiktsmessig, må denne baseres på at foretakene har en felles oppfatning av hva som skal rapporteres. Det mangler i dag felles retningslinjer for kategorisering av hendelser, og ett tiltak kan være å etablere en gruppe med representanter fra Kredittilsynet, bransjeorganisasjonene, banker og andre sentrale aktører for å definere slike retningslinjer. Det bør også avklares om dette skal være en frivillig eller obligatorisk kategorisering internt i det enkelte foretak. Det finnes for øvrig standarder som langt på vei definerer og klassifiserer hendelser.

6.5.2 Bruk av ITIL i IT-organisasjonen

Mange av foretakene som Kredittilsynet fører tilsyn med, har tatt i bruk eller i ferd med å ta i bruk rammeverket ITIL[8] i IT-organisasjonen. ITIL definerer en hendelse som: "Alle hendelser som ikke er en del av den normale driftssituasjon og som medfører eller kan medføre et avbrudd eller reduksjon av kvaliteten til aktuelle tjenester." ITIL deler mellom håndtering av hendelser på den ene siden og håndtering av problemer på den andre siden, og beskriver rutiner for eskalering av hendelser. Innføring av ITIL i IT-organisasjonen kan bidra til mer likeartet avviksbehandling foretakene imellom og en enklere tilnærming til felles retningslinjer for kategorisering av hendelser.

6.6 Informasjon og kommunikasjon

Som ledd i vårt arbeid med å legge vekt på styring og kontroll med operasjonell risiko, bør vi bli bedre til å informere om hvilke risikoscenarier som identifiseres og hvilke tiltak som Kredittilsynet gjennomfører, blant annet ved å vise til eksempler på beste praksis fra andre land og lignende. Informasjon kan formidles gjennom seminarer, møter og publikasjoner. Informasjonsarbeidet på dette risikoområdet vil være en del av Kredittilsynets kommunikasjonsarbeid fremover.

6.6.1 Bransjemessige tiltak som vektlegger operasjonell risiko

- FNH og Sparebankforeningen: Gjennom finansnæringens organisasjoner har det i en rekke år vært jobbet med saksområder med stor relevans til operasjonell risiko – gjennom utvikling av standarder, metoder og styringsverktøy, utredninger, kurs osv. Sikringsfondet har hatt sin egen tilsynsaktivitet, blant annet ved stedlige inspeksjoner og rapporter. Kredittilsynet vil arbeide videre for å utvikle dette samarbeid med bransjeorganisasjonene og dermed ivareta en mer systematisk informasjonsutveksling til gjensidig nytte.

- Allianser, samarbeidsgrupper: Det er en rekke eksempler på at bankene gjennom sine forretningsmessige allianser (SpareBank 1 Gruppen, Terra-Gruppen) søker å utvikle en felles metodikk for bedre håndtering av operasjonell risiko. Tilsvarende har også vært gjort på regional basis (virksomhetsstyring i sparebanker – Midt-Norsk Sparebankgruppe). Lignende initiativ er tatt av samarbeidsorganene for kommunale og private pensjonskasser. I

[8] Information Technology Infrastructure Library (ITIL) er et internasjonalt rammeverk for best practice på de operative områder av IT-virksomheten

forbindelse med IKT-forskriften § 3 vil Kredittilsynet i 2007 utarbeide en veiledning for etterlevelse av kravene.

- Foreninger (Den norske Revisorforening – DnR, Norges Interne Revisorers Forening – NIRF, ISACA m.fl.): Disse samler profesjonsutøvere som enkeltvis står sentralt i kontrollmiljøene i de enkelte foretak, eller er engasjert som rådgivere/leverandører av kontroll- og revisjonstjenester. Gjennom slike fora for standardutvikling og opplæring kan Kredittilsynet delta både for egen kompetanseutvikling og som foredragsholdere. At tilsynsmyndigheten er representert i slike fora, gir både nyttig informasjonsutveksling og viser at Kredittilsynet ser på slike fora og disse profesjonene som viktige aktører i samarbeidet med næringene.

6.7 Det enkelte finansforetak

6.7.1 Operasjonell risiko

Når det gjelder banker og deler av verdipapirsektoren, er arbeidet knyttet til Basel II en viktig pådriver for håndteringen av operasjonell risiko. På samme måte vil krav i forbindelse innføring av Solvens II-regelverket bidra til mer fokus på arbeidet med operasjonell risiko i forsikringssektoren. Den internasjonale tendensen vi ser nå med å gi mer oppmerksomhet til styring og kontroll og mer oppmerksomhet på internasjonale og nasjonale standarder, virker også positivt inn i arbeidet med operasjonell risiko.

Noen av de større bankene har lagt spesielle ressurser i å arbeide frem metoder og modeller for håndtering av operasjonell risiko. Kredittilsynets rolle i forhold til disse kan være som dialogpartner til de initiativene som dukker opp fra enkeltinstitusjoner eller fra samarbeidsorganer (se foregående punkt). Det er likevel i det enkelte foretak arbeidet primært må foregå for at vi totalt skal lykkes.

6.7.2 Bestillerkompetanse i det enkelte finansforetak

Som påpekt i kapittel 3.6, er det en viktig forutsetning for å kunne lykkes med en utkontraktering av IKT at foretaket beholder nok kapasitet og kompetanse til å være i stand til å forvalte avtalene og kontrollere og følge opp leveransene. Kredittilsynet har erfart gjennom IT-tilsynene at det kan være vanskelig for foretakene å håndtere avtalene med IKT-leverandørene. Det kan være en utfordring for foretakene å sikre tilstrekkelig kompetanse på IKT-siden over tid når egen IKT-virksomhet bygges ned. Bestillerkompetanse kjennetegnes ved generelt god kompetanse på IKT samt god forståelse av forretningsområdet. Gjennom IT-tilsynene har Kredittilsynet sett at der foretakene har investert spesielt i å tilføre eller beholde slik kompetanse, er dette en investering som har vist seg kostnadseffektiv. Det gjør foretaket bedre rustet til å sikre styring og kontroll med IKT-leveransene, samt å følge opp at innhold og kvalitet er i henhold til foretakets behov og spesifikasjoner. Etter Kredittilsynets vurdering er bestillerkompetanse i det enkelte foretak helt avgjørende for å beholde tilstrekkelig kontroll og styring med egne IKT-tjenester.