Risiko- og sårbarhetsanalyse (ROS) 2004

Rapport om finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)

Kredittilsynet, 31. desember 2004

Innhold

1. Innledning

Den første ROS-analysen som ble utarbeidet av Kredittilsynet og offentliggjort i 2002, var primært en kartlegging av finansforetakenes bruk av IKT. Videre var hensikten å identifisere risikoelementer og kommunisere dette som et ledd i arbeidet med å sette fokus på nødvendigheten av å ha god oversikt og kontroll med IKT-systemer. Som i 2003 er det i 2004 valgt kun å fokusere på identifiserte risikoelementer og hva som kan være effektive tiltak. Likeledes er det arbeidet med å videreutvikle metodene og kildegrunnlaget for ROS-analysen.

2. Formålet med ROS-analysen

Det pågår fortsatt store forandringer i finansnæringen, og ikke minst skjer det fortsatt mye på teknologiområdet. Dette gjelder både infrastruktur og bruk av ny informasjonsteknologi som grunnlag for introduksjon av nye produkter og tjenester. Måten å distribuere produktene ut til kundene på gjennomgår endringer i takt med mulighetene som teknologien skaper. Utviklingen av Internett som en åpen infrastruktur gir grunnlag for lansering av en ny og mer effektiv distribusjon mellom tjenesteyter og kunde. I finansmarkedet er fortsatt bankene de mest aktive til å ta i bruk denne muligheten, særlig for distribusjon av nye tjenester. Som ledd i å øke effektiviteten i utvikling og drift av IT har foretakene i stor grad benyttet seg av utkontraktering til profesjonelle IT-leverandører. Hensikten med ROS-analysen er å identifisere risikoområder på de nevnte områdene og deretter å bidra til å rette foretakenes oppmerksomhet mot disse.

3. Strukturendringer – fellesløsninger

I finansnæringen har det skjedd og skjer stadig strukturelle endringer på IKT-området. Dette gjelder både for banker, i forsikringsforetak og i verdipapirsektoren. Alle de nevnte områder benytter i stor grad utkontraktering for å ivareta sin IKT-virksomhet.

Det er spesielt i 2004 at flere banker har flyttet, eller har besluttet å flytte, store deler av sin IT-virksomhet ut av Norge. I et nordisk perspektiv ser vi at IBM er i ferd med å få en svært sterk posisjon innen leveranser av IT-tjenester til foretak innen bank og finans. IBM har i inneværende år inngått flere strategiske avtaler, på området infrastruktur og IT-drift.

Danske Bank IT er en stor tjenesteleverandør til egne foretak, med leveranser til blant annet Danske Bank (Danmark), Östgöta Enskilda Bank (Sverige), Danske Bank Helsinki (Finland) og Fokus Bank (Norge). Sammen med danske Maersk Møller Gruppen eide Danske Bank 50 prosent hver av DM-Data AS i Danmark som ivaretok IT-driften for begge selskaper. IBM har nå kjøpt DM-Data og integrert denne i sin utkontrakteringsvirksomhet i Danmark.

Terra-Gruppen (TG) besluttet i første kvartal 2004 å avslutte sitt strategiske samarbeid med EDB Business Partner (EDB BP) for å etablere et nytt samarbeid med SDC Udvikling AS (SDC) i Danmark som eies av et holdingsselskap med utgangspunkt i medlemmer av foreningen Sparekassernes Datacenter. SDC utkontrakterte i 2003 egen IT-drift, inkludert aktuell bemanning til IBM Danmark.

Nordea Bank Norge ASA flyttet i andre kvartal 2004 store deler av sin IT-drift til selskapet Nordic Processor AB (NPAB) i Sverige. Dette selskapet oppsto som et joint venture selskap med Nordea og IBM som eiere. NPAB eies i dag med 60 prosent av IBM og 40 prosent av Nordea AB (publ). NPAB har tre datterselskaper, Nordic Processor Norge AS, Nordic Processor OY og Nordic Processor DK. Disse selskapene er i all vesentlighet bemannet med personell med Nordea-bakgrunn, mens personell fra IBM i stor grad utgjør ledelsen i NPAB. Organisasjonen har sterkt fokus på industriell tenkning.

EDB BP og IBM inngikk i tredje kvartal en avtale om strategisk samarbeid gjeldende for Norge som samtidig sikrer IBM langsiktige leveranser til EDB BP. Det var blant annet a. EDB BPs overtakelse av Telenors IT-drift som ga EDB BP slik samlet styrke. IBM blir gjennom EDB BP hovedleverandør til vår største og viktigste teleleverandør, vår største og viktigste IT-leverandør (EDB BP) og som dominerende leverandør av IT-tjenester til store foretak innen bank og finans på det nordiske markedet.

Dette er en utvikling som Kredittilsynet vil følge nøye da stor konsentrasjon ut fra en risikobetrakting kan være uheldig. IBM er allerede helt dominerende på salg av stormaskinløsninger med tilhørende programvare, og sammen med en offensiv internasjonal strategi på industrialisering av IT-driften kan dette bety store endringer på dette markedsområdet og følgekonsekvenser som påvirker risikobildet. Dette området er av stor betydning for framtidens IT-driftsløsninger og Kredittilsynet vil derfor lage en utredning rundt utkontraktering med spesiell oppmerksomhet på utkontraktering over landegrensene og gjennom dette arbeidet foreslå eventuelle tiltak.

4. Oppsummering og konklusjoner

4.1 Innledning

Kredittilsynet har med grunnlag i egne analyser og tilgjengelige datakilder identifisert noen særlig viktige risiko- og sårbarhetsområder hvor det er aktuelt med ulike risikoreduserende tiltak:

Nye områder:

- Prosjektstyring – store endringsprosjekter
- Organisert kriminalitet - bruk av Internett
- Endrede samarbeidsformer
- Utkontraktering over landegrenser
- Langsiktig svekking av norsk IT-kompetanse innen bank- og finans

Områder som også ble påpekt i fjorårets risikoanalyse:

- Katastrofeberedskap
- Endringsledelse
- Virus – organisering av beskyttelsestiltak

Gjennom arbeidet med risikoanalysen og med bakgrunn i Kredittilsynets siste års gjennomførte IT-tilsyn og intervjuer, synes de nevnte risikoområdene med få unntak å være relevante for de fleste virksomhetsområdene, enten det gjelder bank, forsikring eller verdipapirsektoren.

4.2 Prosjektledelse – store endringsprosjekter

Av ulike grunner er flere av de større finansinstitusjonene i Norge i prosess med strukturelle endringer for framtidig bruk av informasjonsteknologi. Det er ulike drivere til disse endringene, men de skjer i stor grad over den samme tidsperiode, 2004 til 2006. Dette kan samlet gi økt risiko. Hvordan de ulike endringsprosjektene blir etablert og gjennomført, vil avgjøre graden av risiko. Bruk av samme type begrensede kompetanseressurser kan være et gjennomgående område som kan påvirke risikobildet. I

tillegg til de store endringsprosjektene som er nevnt foran, gjelder dette for DnB NOR etter fusjonen mellom DnB og Gjensidige NOR og kan også gjelde for de banker som gjennom samarbeidsavtaler bruker DnB NORs IT-løsninger. Det vil også være aktuelt for BBS som har iverksatt endringer for å samle sin IT-virksomhet på færre teknologiske plattformer. Det pågår også endringer i bruk av informasjonsteknologi innenfor verdipapirsektoren, både når det gjelder bruk av nettverk og på IT-driftssiden.

Prosjektgjennomføring

Kredittilsynet har i 2004 gjennomført eller igangsatt egne IT-tilsyn på flere av de pågående endringsprosjekter som er omtalt ovenfor. Dette arbeidet blir videreført i 2005. Etter Kredittilsynets vurdering er det svært viktig at en i slike prosjekter vektlegger gjennomføring av grundige kravanalyser, risikoanalyser, fastlegging av kvalitetskrav samt fastlegging av prosedyrer prosjektene skal følge og sikring av at disse blir fulgt.

Kredittilsynet er av den formening at det er uheldig dersom disse forhold ikke blir tilstrekkelig ivaretatt i prosjektene, noe som kan medvirke til problemer i senere faser av prosjektgjennomføringen. Samlet kan dette bety høy risiko. Kredittilsynet har derfor besluttet å fortsette arbeidet med målrettede IT-tilsyn på de ulike endringsprosesser som pågår på IT-området i 2005.

4.3 Organisert kriminalitet – bruk av Internett

Microsofts ”monopolposisjon”

Utstrakt bruk av IT er helt sentralt i de fleste lands infrastruktur. Det være seg den finansielle infrastrukturen, sykehus, statsforvaltning, politi, forsvar mv. IT er helt sentralt for at disse områdene skal fungere. Over 90 prosent av de PC-er som er aktive i dag benytter seg av Microsofts operativsystemer. Dette medfører også at de samme PC-er er utsatt for de samme virus, ormer eller trojanere. Antall PC-er koblet opp mot Internett blir i følge beregninger doblet hver 10. måned. Samtidig dobles prosesseringskraften av PC-er tilkoblet Internett hver 9. måned. Når vi vet at hackere og organiserte kriminelle gjennom trojanere kan overta og styre PC-er tilkoblet Internett, kan den prosesseringskraften disse råder over være tilnærmet ubegrenset. Spørsmålet en må stille seg er om et foretaks kontinuitetsplaner bør være basert på ensartet teknologi, siden disse er sårbare overfor de samme trusler. Særlig er Microsofts nettleser Internet Explorer utsatt. Denne har samme utbredelse som operativsystemet. Det er hevdet at Microsoft har et stort antall sikkerhetshull i sine systemer. Det ser ut til at kompleksiteten i løsningene bidrar til at det ved feil som rettes har en tendens til å oppstå nye. Det er kjent at hackere og kriminelle har benyttet seg av hull i Internet Explorer og har utsatt store foretak som Citibank, NatWest og PayPal samt australske, engelske, amerikanske og flere brasilianske banker for angrep. Det finske samferdselsdepartementet og det svenske post- og teletilsynet har for kort tid siden offentlig gått ut og anbefalt overgang til andre nettlesere som Opera og Firefox for å bidra til å redusere denne typen risiko.

Nettbankangrep

Sikkerhetsnivået i nettbankene i Norge ligger generelt på et høyt nivå i internasjonal målestokk. Det kan likevel bli en utfordring å opprettholde denne posisjonen. Kredittilsynet er blitt oppmerksom på en økende trussel mot sikkerheten i nettbanker. Gjennom ulike kanaler har Kredittilsynet fått informasjon om potensielle svakheter i nettbanksikkerheten.

Norske nettbanker bruker i stor grad kontonummer, fødselsnummeret eller annen identitet som brukeridentifikasjon ved pålogging. Kontonummeret og fødselsnummeret anses ikke å være hemmelig. Dette er informasjon som er relativt enkelt å tilegne seg. Det som derimot er hemmelig, og bare kjent for brukeren, er PIN-koden (Personal Identification Number) eller annen form for passord. Dersom en bruker forsøker å logge seg på nettbanken med riktig brukeridentifikasjon, men med feil PIN med mer enn 3 – 5 forsøk, vil dette føre til at nettbanktjenesten stenges for den aktuelle bruker. Til forskjell fra kortsvindel har en på Internett betydelige ressurser som vil kunne settes inn for å prøve å trenge inn i systemer og til å forsøke å lamme systemene.

I Norge benyttes ulike løsninger og lengder på PIN. Det er også ulike måter å konstruere PIN-koden avhengig av valgt løsning. Lengden på PIN-koder har også betydning for hvor sikkerhetsmessig gode de oppfattes å være. Det er viktig at en benytter løsninger som genererer en unik PIN-kode for hver gang nettbanken åpnes samt eventuelt ved betaling av enkelttransaksjoner eller en samling av transaksjoner. Da er det ikke tilstrekkelig for kriminelle å få tak i en enkelt PIN-kode.

Phishing

«Phishing» begynte som en enkel form for ”lureri” der nettbrukere via e-post narres til å gå inn på en falsk nettside som ligner nettbanken de er kunde i eller nettbutikken de handler i.

Mottakeren blir bedt om å legge inn sine personlige opplysninger og kredittinformasjon på nytt. I e-posten bes det ofte om kontoinformasjon eller annen personlig informasjon, og en begrunner dette med at det har oppstått et problem med mottakerens nettbankkonto. Denne informasjonen kan så brukes til å svindle penger fra offeret.

En versjon, som nylig er oppdaget, går et skritt videre. I e-post som ser tilforlatelig ut, kan det ligge et program som søker på harddisken din etter bankinformasjon. Når slik informasjon er funnet, venter programmet til du logger deg inn på nettbanken. Så overskrives URL-adressen (www...osv) med en helt annen adresse, og leder deg til et annet nettsted med et utseende som nøyaktig ligner banken din. Vel inne på det falske nettstedet blir du bedt om å fylle inn et skjema med nøyaktige opplysninger om kontoen din, PIN-kode, kontonummer og lignende.

Den store forskjellen fra tidligere teknikker er at du ikke lenger aktivt må klikke på en nettadresse for å komme inn på den falske siden. Programmet lager selv en kopi av bankinformasjonen, komplett med nettside, adresse og annen relevant informasjon. Denne informasjonen overskrives på filnivå i stedet for på nettlesernivå.

I Storbritannia ble to av de største nettbankene stengt på grunn av utstrakt og til dels «vellykket» svindel som fortsatt er under etterforskning.

Det er ikke rapportert om at noen av svindelforsøkene overfor nordmenn har lykkes.

"Phisherne" blir mer og mer avanserte. Å finne måter som kan stoppe dem, er et prioritert område innen sikkerhetsarbeidet.

4.4 Nye samarbeidsformer

Kredittilsynet har gjennom inspeksjoner i verdipapirmarkedet erfart at de foretak som verdipapirinfrastrukturen består av ikke har et tilstrekkelig samarbeidsforum som sikrer at ende til ende-leveranser (test som blant annet involverer alle parter) varsles og testes i tilstrekkelig grad. Kredittilsynet anser at nødvendig samarbeidsform mellom Oslo Børs, VPS, NOS, børsmedlemmene og OM Technology ikke er etablert. Kredittilsynet har grunn til å tro at dette har medført en økning i nedetid i verdipapirinfrastrukturen. Det er noe uklart hva som kan være grunnen til dette, men det kan være grunn til å tro at endringen i foretakstrukturen i Oslo Børs og VPS kan ha hatt innvirkning på samarbeidet, selv om foretakene har sammenfallende interesser i å ha en stabil og sikker IT-leveranse.

Tilsvarende er det grunn til å se på samarbeidsformene til bankene når store banker og grupper får sine tjenester fra den samme IT-leverandøren. Denne konsentrasjonen har eksistert i EDB BP, men har vært tilfredsstillende da EDB BP-leveransene har blitt operert i adskilte miljøer. Denne risikoreduserende effekten reduseres når leverandøren iverksetter tiltak for å dra større nytte av volum og samordning. Ser vi på IBM er konsentrasjonen økende da de i stadig større grad ligger bak flere IT-leveranser til norske og nordiske finansforetak.

Det er også etablert ulike samarbeidskonstellasjoner mellom banker. Viktige eksempler på dette er: SpareBank 1 Gruppen, Terra Gruppen og allianseavtalen som en del banker har med DnB NOR. Dette gjør at bankene som deltar i slike samarbeidskonstellasjoner får del i stordriftsfordeler som følger av å være flere om en løsning. For mindre banker med lite IT-kompetanse er deltakelse i slike konstellasjoner viktig. Det betyr imidlertid også at de blir avhengige av IT-leveranser fra andre og at de i praksis får liten innflytelse på sine IT-leveranser, både når det gjelder nyutvikling, drift og forvaltning. De enkelte banker velger også å ivareta ulik grad av IT-oppgaver i egen regi. Alt dette skaper en risiko for manglende helhetsoversikt og liten reell kontroll over egen IT-virksomhet. Dette gjelder både med hensyn til organisasjon, ressurser, kompetanse og bruk av IT-leveransene i egen virksomhet. Bevissthet og klarhet for ansvarsforhold og dokumentasjon av dette er helt nødvendig. IKT-forskriften stiller klare krav til dette området og overholdelse av dette vil bli fulgt opp gjennom den løpende tilsynsvirksomheten.

4.5 Utkontraktering over landegrenser

Utkontraktering er et stort og veletablert område innen IT-tjenesteyting og området er i kraftig vekst. I følge eksterne analyser utgjorde leveranser av eksterne IT-tjenester i EMEA (Europa, Midt-Østen og Afrika) i 2003 et marked på ca. 194 milliarder USD. Foreløpige beregninger viser at markedet trolig vil øke med 6,3 prosent i snitt pr. år til 230 milliarder USD i 2007. I dette markedet er bank og finans det største kundesegmentet.

Etter hva vi har kunnet bringe på det rene er Norge et av de første land i verden hvor store deler av IT-virksomheten av den finansielle infrastruktur utkontrakteres ut over landegrensene. Oslo Børs, Fokus Bank, Nordea Bank Norge, S/E/B Kort, Enskilda Securities, Storebrand Liv og Terra Gruppen er alle eksempel på dette. Det å utkontraktere IT-tjenester til ikke norske nordiske IT-leverandører er allerede en realitet. Ser vi dette i et lengre perspektiv og i forhold til de aktuelle utviklingstrekk er det grunn til å tro at de store IT-leverandørene går fra en lokal til en globalisert leveransemodell. IT-leverandørene vil bygge opp færre, men større datasentraler og kompetansesentre og koble disse sammen slik at IT-leveransene kan gjennomføres der hvor det er tilgjengelige ressurser. Dette kan føre til at det blir en uoversiktlig og vanskelig oppgave for foretakene å følge opp IT-leveransene, og også for Kredittilsynet å føre tilsyn med foretakets IT-virksomhet.

Det vil også kunne by på store utfordringer dersom det oppstår kriser i land norske foretak har utkontraktert IT-tjenester til.

Tradisjonelt har de norske foretakene forholdt seg til én hovedleverandør som har hatt ansvar for underleveranser. En ser nå at foretakene i større grad kjøper sine IT-leveranser fra flere leverandører og tar dermed ansvaret for forvaltningen av kontraktene selv. Kredittilsynet ser at dette kan føre til ”gråsoner” mellom IT-leverandørene når det gjelder hvem som har ansvaret for å koordinere dersom feil oppstår eller når endringer skal gjennomføres. Endring fra å utkontraktere “vertikalt” (det vil si til én leverandør) til “horisontal” deling av tjenestene (flere leverandører), kan bety økt kompleksitet av styring og kontroll.

Foretakene har i stor grad selv bestemt sine retningslinjer når det gjelder utformingen og innholdet i utkontrakteringsavtalene. Dette har ført til at monopollignende situasjoner har oppstått (EDB BP). Vi ser at nye monopollignende konsentrasjoner etableres, som for eksempel OM Technologys posisjon i det nordiske verdipapirmarkedet. OM Technology kan ha en uheldig posisjon som både eier av leveransene (leverandøren) og børsene (kunden) som det leveres IT-tjenester til. Dette kan føre til et uklart forhold mellom kjøper og selger og til blanding av roller som på sikt kan gi negative konsekvenser.

IKT-forskriften innholder en egen bestemmelse som stiller krav til slike utkontrakteringsavtaler. Likeledes har Kredittilsynet iverksatt en utredning for å se nærmere på behovet for ytterligere regulering av IT-leverandørenes ansvar.

4.6 Norsk IT-kompetanse innen bank og finans i et langsiktig perspektiv

Norge har i stor grad vært foregangsland i bruken av IT innenfor de næringer der Kredittilsynet har tilsynsansvar. Den nærhet som har vært mellom foretak, samarbeidsorganisasjoner og IT-leverandør 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 områder. 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 endringer vi ser, med stadig større grad av utkontraktering over landegrensene, vil den norske andel av IT-leveranser avta og følgelig vil antall IT-ansatte avta. Sikkerhetsmessig og næringspolitisk er dette en bekymringsfull utvikling. Norsk finansnærings IT-virksomhet har ligget langt fremme og har hatt stor betydning for den totale IT-virksomheten i Norge. Samspillet mellom de ulike deler av foretakenes forretnings- og IT-utviklere vil bli svekket og kan redusere innovasjonen og nyskapningen på dette området over tid. Norge kan langt på vei komme til å bli et "filialland" når det gjelder finansforetakenes IT-virksomhet. Dette kan igjen svekke beredskapen og resultere i større risiko samlet sett.

4.7 Risikoanalyse

Fram til ikrafttredelsen av ny IKT-forskrift 1. august 2003 hadde Kredittilsynet ikke stilt krav til foretakene at egen risikoanalyse skal gjennomføres spesifikk for IT-virksomheten, annet enn de generelle krav til risikovurdering i intern kontroll forskriften. Kredittilsynet ser på risikoanalyser av IT-virksomheten som et sentralt hjelpemiddel for å sikre at foretakene har tilstrekkelig oversikt over den IT-risiko som foretakene er eksponerte for. Risikoanalyser bør regelmessig gjennomføres for å kunne vurdere relevant risiko med hensyn til oppnåelse av de mål som foretaket setter. Dette legger også grunnlaget for å bestemme hvordan risiko skal holdes innenfor det aksepterte nivå for risiko som foretaket har etablert. Kredittilsynet ser det som viktig at foretakene definerer akseptabel risiko for de enkelte risikoområder som ledd i sitt risikoarbeid. Gjennomføring av gode risikoanalyser vil også bidra til å forbedre sentrale prosesser som omhandler kontinuitet og katastrofe innenfor IT-virksomheten. Kredittilsynet ser det som en forutsetning at resultatet av en risikoanalyse dokumenteres.

Ut fra det materialet som Kredittilsynet bygger denne rapporten på, er det grunn til å påpeke at foretakenes arbeid rundt risikoanalyser og risikoarbeid i IT-virksomheten er i en tidlig fase. Områder som det kan pekes på, er foretakenes manglende fastlegging av akseptabelt risikonivå for egen

virksomhet. Få foretak har metoder og etablerte rutiner for gjennomføring av risikoanalyser for IT-virksomheten. For foretakene er det viktig å etablere en metode som understøtter arbeidet med risikostyring. Med bakgrunn i IKT-forskriftens § 3 Risikoanalyser, som stiller krav om at dette gjennomføres minst hvert år, vil dette bli fulgt opp videre gjennom den generelle tilsynsvirksomheten.

4.8 Katastrofeløsninger

For å holde høy tilgjengelighet på finansielle tjenester, og hindre at for eksempel betalingssystemene er utilgjengelige, er det nødvendig å ha velfungerende kontinuitets- og katastrofeløsninger. Løsningene må testes med jevne mellomrom for å få en bekreftelse på at både mennesker og utstyr er beredt når situasjonen krever det. Katastrofeplaner, -løsninger og tilstrekkelig testing av disse er hos enkelte foretak ikke prioritert og dette bidrar dermed til å øke den operasjonelle risikoen.

Det er en omfattende operasjon å etablere katastrofeløsningen. Videre er det også en omfattende operasjon å gå tilbake til normal drift etter at skaden er utbedret.

Noen forhold ved katastrofeløsninger foretakene i større grad bør fokusere på er:

- Foretakets krav og forventninger til tjenesteleverandør i en katastrofesituasjon
- Realismen i katastrofetesting

Kvaliteten på katastrofeløsningene hos foretak 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 en stor utfordring. Gjennomføring av katastrofetesting er ofte ikke en del av standardkontrakter. Dette kan medføre at katastrofetester vil kunne prises høyt og kan resultere i at færre tester gjennomføres og at beredskapen undergraves.

Kontinuitetsløsningene, som er del av det preventive arbeidet med å oppnå driftsstabilitet og for å unngå at det oppstår katastrofer eller lengre driftsstopp, bør regelmessig vurderes og testes.

Erfaringer har vist at hos flere foretak blir oppdatering av kontinuitetsløsningene ikke gjennomført parallelt med endringer i driftssystemene og som ledd i en systematisk, regelmessig og dokumentert prosess. Dette kan resultere i at det oppstår ulikheter mellom produksjonsløsningene og reserveløsningene.

4.9 Endringshåndtering

Den raske innføringstakten av nye tjenester fører til flere risikoelementer i betalingssystemene og kan derfor innebære økt operasjonell risiko. Gode endringsrutiner, oppfølging og etterlevelse av disse, er kritisk for foretakene. 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 og dokumenterte testresultater må forelegges ansvarlig før denne godkjenner gjennomføringen. Årsakene til driftsstans på grunn av endringer kan være mange; mangelfull utvikling og testing av programmer og tjenester, mangelfull etterlevelse av rutiner, vanskeligheter med å teste for en reell driftssituasjon. Endringskontroll er svært 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. Der samme IT-leverandør opererer samme løsning for mange foretak, og disse er integrert i samme fysiske systemløsning, øker også behovet for samordning mellom foretakene ved endringer som berører flere foretak.

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

Hovedårsaken til at avvik oppstår i IT-virksomheten er gjennomføring av endringer. De fleste foretak har etablerte endringshåndteringsprosedyrer, men den store utfordringen som foretakene står overfor er å sikre at de etablerte prosedyrene følges.

4.10 Ny teknologi

Kredittilsynet kjenner til at flere foretak vurderer å ta i bruk trådløse nettverk. Kredittilsynet er av den oppfatning at trådløse nettverk pr. i dag utgjør en så stor risiko at disse ikke bør kobles opp mot foretakets produksjonsnettverk. Trådløse nettverk er svært brukervennlige, noe som kan medføre at også uautoriserte personer relativt enkelt kan koble seg på foretakets nettverk.

4.11 BankID

Kredittilsynet følger utviklingen og implementeringen av BankID nøye. BankID er en elektronisk legitimasjon og signaturtjeneste som tilbys av bankene i Norge. BankID utstedes av bankene i Norge og kan benyttes til elektronisk identifisering og signering på Internett. Foreløpig brukes tjenesten til autentisering av kunder og signering av dokumenter. En nasjonal løsning for kontobetaling med BankID er under utvikling.

5. Kilder

Kredittilsynets arbeid med operasjonell risiko, i tillegg til den generelle IT-tilsynsvirksomheten, har vært rettet mot foretakenes bruk av informasjons- og kommunikasjonsteknologi.

Det er flere kilder og vinklinger som har vært benyttet i 2004:

5.1 Forrige ROS-analyse

Risiko- og sårbarhetsanalysen for 2003 har blitt benyttet som en avsjekkingskilde for den nye analysen.

5.2 IT-tilsyn

En viktig kilde ved denne analysen har vært resultatene fra gjennomførte IT-tilsyn i 18 ulike foretak i 2004. Dette har gitt en god måling av status i de aktuelle foretak, særlig når det gjelder hvordan IT-prosessene er etablert. Tilsynene er gjennomført som en kombinasjon av dokumentbasert og stedlige IT-tilsyn. Den risikoen som avdekkes i denne analysen skal brukes av Kredittilsynet for å se hvor innsatsen bør settes inn i forbindelse med nye tilsyn på IT-området.

5.3 Gjennomførte intervju

I 2004 ble det valgt ut 12 sentrale foretak hvor det ble gjennomført intervjuer med nøkkelpersonell. I samband med dette ble det også arbeidet med form og innhold av selve intervjuopplegget. I motsetning til tilsynsopplegget går dette i mindre grad på IT-prosessene, men mer direkte på utvalgte områder. Opplegget for gjennomføring av intervjuer vil bli videreutviklet og antall intervjuobjekter ytterligere økt i neste års ROS-analyse (2005).

Nedenfor vises eksempler på enkelte utvalgte områder som grunnlag for de gjennomførte intervju:

Personell, konfidensialitet, integritet og tilgjengelighet, IT-infrastruktur, interne misligheter, misligheter forårsaket av eksterne, transaksjonshåndtering og prosesstyring.

Et felles trekk er at de aktuelle foretak som er blitt intervjuet, mener å ha rimelig god kontroll over egen situasjon og er oppmerksom på viktige risikoområder. Et viktig forbedringsområde som er identifisert vil være å forbedre arbeidet med risikoanalyser i det enkelte foretak, som i neste omgang vil kunne bidra til å redusere risiko. Nettbank, bruk av Internett og beskyttelse mot virus og uønsket inntrenging er et annet område som har fått større oppmerksomhet.

5.4 Hendelser

Tilgjengelig informasjon om rapporterte hendelser fra enkelte foretak er analysert. Resultatet av dette viser at det fortsatt er grunn til å fokusere på endringshåndtering og ikke minst hvordan endringshåndteringen gjennomføres operasjonelt. Et annet forhold det er viktig å fokusere på er hvordan en hendelse/feil analyseres og behandles med tanke på gjenoppretting. Området hendelser er under vurdering for eventuelt å stille egne krav til registrering og rapportering. Dette ses også i samband med planlagt innføring av Basel II i 2007.

5.5 Internasjonale ROS-undersøkelser

Vi har også sett på ulike relevante internasjonale undersøkelser på IT-området. Disse er brukt som en sjekkliste mot situasjonen i Norge.

Resultatene fra de internasjonale undersøkelsene viser i stor grad samsvar med Kredittilsynets resultater. Det framgår at områdene virus/brannmur, endringsproblematikk og bruk av Internett som infrastruktur går igjen som potensielt sårbare og utsatte områder også i disse undersøkelsene. I tillegg viser disse større oppmerksomhet mot organisert kriminalitet og kriminalitet utført av tidligere eller nåværende, egne ansatte. Kredittilsynet har for øvrig etablert et bedre samarbeid med andre myndighetsorganer med tilgang til gradert informasjon både nasjonalt og internasjonalt. Dette har gitt nyttige impulser og viktig informasjon på et tidligere tidspunkt enn en normalt ville fått.

6. Hva vil Kredittilsynet gjøre?

6.1 IT-tilsynsopplegget

Kredittilsynet vil fortsette arbeidet med et IT-tilsynsopplegg som bygger på en internasjonal metodikk og som i stor grad er relatert til om relevante prosedyrer er på plass for alle områder av IT-virksomheten.

Nåværende tilsynsopplegg er i tråd med hvordan antatt nytt internasjonalt regime for operasjonell risiko vil bli utformet. Opplegget er foreløpig på et overordnet og prosessorientert nivå og dekker hele IT-virksomheten. Arbeidet med å videreutvikle dette til mer **hvordan** IT-virksomheten blir utført er imidlertid startet opp, og da på et mer detaljert nivå hvor områdene, virusbeskyttelse, katastrofeplan, "brannmur" og betalingstjenester allerede er utviklet. Nye områder som er valgt ut er:

- Nettbank
- Utkontraktering over landegrenser
- Hvitvasking

De nye modulene i tilsynsopplegget vil allerede i 2005 være i bruk under IT-tilsyn. Kredittilsynet regner derfor med allerede ved inngangen til 2006 å ha god innsikt i kvaliteten av IT-tjenestene innenfor de aktuelle områdene.

6.2 IKT-forskriften

Kredittilsynet vil fortsette det preventive arbeidet med å informere om IKT-forskriften samt følge opp at det enkelte foretak sørger for å tilpasse seg denne. Det er flere bestemmelser i forskriften som har en direkte preventiv effekt gjennom krav om å sikre seg effektivt på de aktuelle risikoområdene.

6.3 Lov om Betalingssystemer mv.

Lov om Betalingssystemer mv. i kapittel 3, § 3-2 pålegger bankene en meldeplikt når det innføres nye systemer for betalingstjenester. Ut fra en totalvurdering hvor risikoelementet på den ene siden, og forenkling på den andre siden, har hatt betydning, er det innført et nytt opplegg som er basert på en egenmelding med 19 ulike kontrollspørsmål, innført gjennom Kredittilsynets rundskriv nr. 17/2004. Dette opplegget antas å gi økt innsikt samt bidra preventivt til å redusere risiko ved etablering av nye systemer for betalingstjenester og ved gjennomføring av endringer i disse.

Dette opplegget vil bli fulgt opp i den ordinære tilsynsvirksomheten.

6.4 Risiko- og sårbarhetsanalyser (ROS)

Analysen som ble behandlet i Kredittilsynets styre høsten 2003 og senere offentliggjort, er blitt brukt aktivt som underlag for informasjonsmøter relatert til risiko. Også denne ROS-analysen vil bli benyttet aktivt som et hjelpemiddel i det forebyggende arbeidet.

Det er viktig til slutt å understreke at det er det enkelte foretak som fullt ut har ansvaret for egen IT-virksomhet. Kredittilsynets aktiviteter kan kun fungere som et bidrag til det viktige arbeidet det enkelte foretak selv må ivareta for å oppnå betryggende forhold i bruk av IT-løsninger.

6.5 Andre tiltak

Kredittilsynet har som et ledd i arbeidet med ROS-analysen etablert kontakter med flere organ for samarbeid. Dette gjelder både universitetsmiljøer og andre spesielle kompetansemiljøer på utvalgte områder. I tillegg vil det bli etablert et nærmere samarbeid med andre nasjonale og internasjonale myndighetsinstanser som også arbeider med sikkerhetsproblematikk som er relevant for finansnæringen. I samband med dette er Kredittilsynet også opptatt av ny teknologi som mangler tilstrekkelige sikkerhetsmekanismer. Vi ser på innføring av såkalt trådløs kommunikasjon som eksempler på slik teknologi med manglende sikkerhet, men er ikke kjent med at noen norske banker hittil har tatt dette i bruk. Det vil også bli gitt høyere prioritet til registrering og oppfølging av hendelser som ledd i preventive tiltak samt i relasjon til operasjonell risiko og innføring av Basel II.

Kredittilsynet vurderer at de tiltak som er iverksatt eller er under planlegging vil være tilstrekkelige for å sikre at en har nødvendig kompetanse for å behandle de risikoområder som er nevnt ovenfor.