Risiko- og sårbarhetsanalyse

(ROS) 2003 – knyttet til

finansforetakenes bruk av

Informasjons- og

Kommunikasjonsteknologi (IKT)

Kredittilsynet, 20. november 2003

Risiko- og sårbarhetsanalyse (ROS) 2003 – knyttet til finansforetakenes bruk av Informasjons- og kommunikasjonsteknologi (IKT)

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 Kredittilsynets preventive tiltak. Erfaringene fra dette arbeidet vurderes å ha vært positive. Denne gang har Kredittilsynet imidlertid valgt å utelate kartleggingsdelen fra dokumentet og kun fokusere på identifiserte risikoelementer og hva som kan være effektive tiltak. Likeledes har Kredittilsynet arbeidet med å finne fram til hvilke typer kilder som bør benyttes for ROS-analysen, samt effektive måter å få informasjonen fram på.

2. Formålet med ROS-analysen

Det har skjedd og pågår fortsatt store forandringer i finansnæringen. Ikke minst har det skjedd mye på teknologiområdet, noe som har gitt grunnlag for introduksjon av nye produkter og tjenester. Endringer i måten å distribuere produktene ut til kundene på har vært et av områdene med store forandringer og Internett-teknologien har medført et generasjonsskifte med høy endringshastighet. Oppbyggingen av Internett som en åpen ny infrastruktur har gitt grunnlag for lansering av en ny og mer effektiv distribusjon mellom tjenesteyter og kunde. I finansmarkedet har bankene vært de mest aktive til å ta i bruk denne nye muligheten, særlig for distribusjon av nye tjenester. Som ledd i å øke effektiviteten i utvikling og drift av IKT har foretakene i stor grad benyttet seg av utkontraktering til profesjonelle IKT-leverandører. I Norge har dette gjort seg sterkt gjeldende. Hensikten med ROS-analysen er å identifisere risikoområder på IKT-området, for deretter å fokusere på disse overfor foretakene.

3. Strukturendringer - fellesskapsløsninger

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 foretakstyper benytter i stor grad utkontraktering for å ivareta sin IKT-virksomhet.

Spesielt for sparebanksiden er at tidligere Fellesdata AS, som var sparebankenes felles datasentral, er solgt til EDB Business Partner ASA og der organisert som et eget datterselskap, EDB Fellesdata AS. Driften tas imidlertid hånd om av EDB Teamco AS. Dette har store konsekvenser for arbeidsoppgaver og ansvarsdeling både hos EDB Fellesdata AS og hos berørte banker. I realiteten betyr dette at det er blitt et mer rendyrket kunde leverandørforhold, i motsetning til tidligere da IKT-leverandøren fungerte mer som en intern IKT-avdeling. Særlig mindre banker må nå ta et sterkere ansvar for kontraktsinngåelse, oppfølging og egne IKT-løsninger. Dette skjer samtidig som andre deler av norsk banknæring går over på felles nordiske løsninger slik som i Fokus Bank og senest beslutningen i Nordea om samordning av IKT-driften. Samlet sett gir dette store endringsprosesser på både kort og lang sikt. Sammen med de øvrige teknologiske endringer som også skjer, gir det en situasjon med mange endringer, og derav høy risiko og muligheter

for feil i beslutninger og gjennomføring. Det er en utfordring for de berørte foretakene å håndtere denne endringsprosess og tilknyttet risiko på en akseptabel måte.

4. Konklusjoner

Basert på Kredittilsynets analyser og de datakilder Kredittilsynet har hatt tilgang til er følgende risiko- og problemområder identifisert som særlig viktige, og hvor det er aktuelt med ulike risikoreduserende tiltak:

- Risikoanalyse
- Personalledelse
- Katastrofeberedskap
- Endringsledelse
- Utkontraktering
- Kvalitet
- Virus

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

Vurdering av risikoelementer:

4.1 Risikoanalyse

Fram til ikrafttredelsen av ny IKT-forskrift 1. august 2003 har Kredittilsynet ikke stilt krav til foretakene om at egen risikoanalyse skal gjennomføres for IKT-virksomheten. Kredittilsynet ser på risikoanalyser av IKT-virksomheten som et sentralt hjelpemiddel for å sikre at foretakene har tilstrekkelig oversikt over den IKT-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 risikoer 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 IKT-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 IKT-virksomheten er i en tidlig fase. Områder som kan pekes på er foretakenes manglende fastlegging av akseptabelt risikonivå for egen virksomhet, og at få foretak har metoder og etablerte rutiner for gjennomføring av risikoanalyser for IKT-virksomheten. For foretakene er det viktig å etablere en metode som understøtter arbeidet med risikostyring.

4.2 Personalledelse

Styring av ressurser er viktig for å bidra til å sikre at den operasjonelle risiko holdes på et forsvarlig nivå. Noen områder har spesielt pekt seg ut.

Når et foretak utkontrakterer hele eller deler av sitt IKT-område til en tjenesteleverandør, vil det være faglig utfordrende å opprettholde egen kompetanse og erfaring på dette området. Foretaket taper erfaring, med det resultat at det kan være vanskelig å samhandle med tjenesteleverandør. Det er derfor viktig at foretaket har et aktivt forhold til egen og tjenesteleverandørs kompetanseprofil. Foretaket bør være sikker på at foretaket selv og tjenesteleverandør har tilgang til den kompetansen som er nødvendig for å utføre inngåtte avtaler. Foretaket bør med jevne mellomrom gjennomgå nødvendige opplæringsprosesser for å se at disse fungerer og sikrer at eventuelle mangler innen kompetanse avdekkes. Opplæringsprosessen bør også sikre at foretaket og tjenesteleverandør ikke gjør seg for avhengige av enkeltpersoner for å kunne innfri de krav avtalene stiller.

Det å sikre tilstrekkelig og riktig kompetanse på områder som er under oppbygging eller nedtrapping er viktig for å kunne sikre avtalt kvalitet. Det er derfor viktig å ha et aktivt forhold til hvordan behovet for kompetanse på nye og endrede områder skal ivaretas. Tilsvarende viktig er det å ha planer for å sikre kompetanse på teknologiområder som er på vei ut, men hvor det fortsatt benyttes løsninger som er basert på denne.

Vurderingen er at dette området innebærer store utfordringer for IKT-virksomheten i foretakene, og kan resultere i alvorlige problemer om de ikke ivaretas i tilstrekkelig grad. Særlig har mindre foretak problemer med å ivareta dette på en tilfredsstillende måte.

4.3 Katastrofeløsninger

For å holde høy tilgjengelighet på finansielle tjenester, og hindre at f.eks. 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 og -løsninger er hos foretak i noen grad ikke prioritert, og dette bidrar dermed til å øke den operasjonelle risiko.

Det er en omfattende operasjon å etablere en katastrofeløsning. Videre er det er 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.

Realisme i katastrofetestingen er et område det knyttes usikkerhet til. Kredittilsynets erfaring er at katastrofetesting i IKT-virksomheten gjennomføres i et for begrenset omfang.

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.

Erfaringen 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.

4.4 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 pga endringer kan være mange; mangelfull utvikling og testing av programmer og tjenester, mangelfull etterlevelse av rutiner, vanskeligheter med å teste for en reell driftssituasjon, mv. Endringskontroll er særs 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 IKT-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 gjennomføres på tvers av 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

En av hovedårsakene til at avvik oppstår i IKT-virksomheten er gjennomføring av endringer i gjeldende driftsversjoner. De fleste foretak har etablerte endringshåndteringsprosedyrer.

Den store utfordringen som foretakene står overfor er å sikre at de etablerte prosedyrene følges. Det er Kredittilsynets erfaring at de alvorlige driftsavbrudd som har skjedd i de senere år er forårsaket av at prosedyrene rundt endringshåndtering ikke ble fulgt eller var utilstrekkelige.

4.5 Utkontraktering

Utkontraktering av IKT-virksomheten kan bidra til øking av operasjonell risiko dersom prosessen ikke håndteres tilfredsstillende. Mange krevende og ofte nye problemstillinger dukker opp når utkontraktering av IKT-virksomheten vurderes. Kredittilsynet har i sitt tilsynsarbeid avdekket stor grad av manglende kompetanse for å kunne forvalte de utkontrakteringsavtalene som foreligger. Dette gjelder spesielt små og mellomstore foretak. For sparebankene som benyttet Fellesdata AS siden 1970-tallet, ble Fellesdata betraktet som en del av bankenes egen interne IKT-virksomhet. Etter at foretakene solgte sin andel av

Fellesdata AS til EDB Business Partner ASA har kravene til inntjening og effektivitet økt, samtidig som foretakenes kunnskap rundt de utkontrakterte tjenestene ikke lenger naturlig er i foretakenes organisasjon.

Kredittilsynet vurderer at foretakene har en stor utfordring i å få oversikt og kunnskap om egne utkontrakterte oppgaver. En slik situasjon over tid innebærer høy risiko.

4.6 Kvalitet

Kredittilsynet ser det som viktig at foretak som har IKT-systemer av betydning for virksomheten har etablert kvalitetsmål for IKT-virksomheten. Disse bør samsvare med de overordnede mål foretaket styrer sin virksomhet etter. Kvalitetsmålene bør være målbare og av et omfang som sikrer at de tjenester som IKT-virksomheten leverer, er av tilstrekkelig kvalitet for å underbygge foretakets overordnede mål. Det er viktig at overordnede kvalitetsmål utformes på en slik måte at det er mulig å følge opp om målsettingen oppnås.

Kredittilsynet finner at foretakenes overordnede kvalitetsmål i liten grad er brutt ned i kvalitetsmål for IKT-virksomheten. IKT-virksomheten bruker i utstrakt grad Service Level Agreements (SLA) for å følge opp de leveransekrav som stilles til de ulike tjenester, men det er vanskelig å se sammenhengen mellom leveransekravene til tjenestene og de kvalitetskrav som stilles til de som skal utføre leveransen.

4.7 Virus

Det har vært stor aktivitet i spredning av datavirus internasjonalt. Det er særlig økningen i bruk av Internett som har gjort det mulig å skape det store omfang av virusangrep og forsøk på inntrenging som foretakene erfarer. Likeledes har standardiseringen med bruk av Microsoft produkter som en felles industristandard i stor grad også bidratt til å øke skadepotensialet, samt gjøre det enklere for forfattere av virusprogram å påføre andre skade eller utføre kriminelle handlinger.

De logger og rapporteringer som IKT-systemer og -utstyr genererer mht. virusangrep og forsøk på inntrenging, er for de fleste foretak så store og omfangsrike at de i praksis er uhåndterlige. Dette medfører at foretakene i stor grad baserer sine rutiner rundt virus og datainnbruddsforsøk på virusbeskyttelsen som antivirusleverandørene tilbyr. Dette har i den senere tid vist seg å ikke være tilstrekkelig for flere av foretakene som er under tilsyn. Kredittilsynet vurderer risikoen som svært høy, dersom funksjoner av betydning for foretaket har direkte tilgang til Internett. I tillegg anser Kredittilsynet det nødvendig at det etableres egne rutiner for bruk av bærbare PC'er, medbragte disketter og andre lagringsmedia. Det er også viktig at innføring av antivirusprogram kombineres med prosedyrer som omfatter oppdateringsrutiner, supportorganisasjon, opplæring av ansatte, prosedyrer knyttet til bruk av løsningen og hvordan dette er knyttet opp i foretakenes sikkerhetspolicy, prosedyrer for IKT-sikkerhet generelt og hvordan dette blir fulgt opp og kontrollert.

Kredittilsynets erfaring viser at det er ulik status hos foretakene og at potensialet for at det kan oppstå store problemer på IKT-området er til stede, slik at ytterligere tiltak for enkelte foretak på dette området er helt nødvendig.

5. Kilder

5.1 Forrige ROS-analyse

Risiko- og sårbarhetsanalysen for 2001 var den første analysen som ble foretatt av Kredittilsynet med utgangspunkt i foretakenes bruk av IKT. Resultatene fra denne har vært benyttet som en avsjekkingskilde for den nye analysen.

5.2 IT-tilsyn

En viktig kilde denne gang har vært resultatene fra gjennomførte IT-tilsyn i 14 ulike foretak i 2002 og 15 i 1. halvår 2003. Dette har gitt Kredittilsynet en god måling av status i de aktuelle 29 ulike foretak, særlig når det gjelder hvordan IKT-prosessene er etablert. Tilsynene er gjennomført som en kombinasjon av dokumentbasert og stedlige IT-tilsyn. Den risiko som avdekkes i denne analysen skal brukes av Kredittilsynet for å vektlegge innsatsen hver prosess skal få under gjennomføringen av nye tilsyn på IKT-området.

5.3 Gjennomførte intervju

Gjennomføring av intervjuer med enkelte sentrale aktører i finansnæringen. Denne gang er det valgt ut et lite antall foretak hvor det er gjort intervjuer med sentrale personer. I samband med dette er det arbeidet videre med form og innhold av selve intervjuopplegget. I motsetning til tilsynsopplegget går dette i mindre grad på IKT-prosessene men mer direkte på utvalgte områder. Pga det smale grunnlaget denne gang er dette vektet svært forsiktig. Opplegget vil imidlertid kunne gi et godt grunnlag for å utvide antall intervjuer i neste ROS-analyse.

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

> Nettbank, Minibank, Telefonbank, Virus, Brannmur, Endringshåndtering, Problemhåndtering, Konfidensialitet, Integritet og Autentifikasjon.

Spørsmålsformen var i hovedsak følgende:

1) Har dere oversikt over problemer som oppsto på området X i 2002/2003? Hvis JA
2) Hva besto problemet/ene i?
3) Hvor viktig for foretaket er funksjonen/objektet på en skala fra 1 til 10?
4) Hvor sårbar/eksponert vurderes denne funksjonene/objektet å være på en skala fra 1 til 10?
5) Hvis over 5, hva er gjort av tiltak for å redusere risiko?

Denne gang har antall personer som har blitt intervjuet vært såpass begrenset, at Kredittilsynet ikke har funnet det hensiktsmessig å presentere resultatene direkte. Fellestrekk er vel at de aktuelle foretak som har blitt intervjuet mener å ha rimelig god kontroll over egen situasjon og er oppmerksom på viktige risikoområder. Et identifisert viktig forbedringsområde vil være å forbedre arbeidet med risikoanalyser, som i neste omgang vil kunne bidra til å redusere risiko.

5.4 Hendelser

Kredittilsynet har analysert tilgjengelig informasjon om rapporterte hendelser fra enkelte foretak. Resultatet av dette viser at det fortsatt er all grunn til å fokusere på endringshåndtering og ikke minst hvordan endringshåndteringen blir gjennomført operasjonelt. Et annet forhold det er viktig å fokusere på er hvordan en hendelse/feil skal

analyseres og behandles for gjenoppretting. Her ligger også en kilde til alvorlige feilsituasjoner.

5.5 Internasjonale ROS-undersøkelser

Kredittilsynet har også sett på ulike relevante internasjonale undersøkelser på IKT-området, mer brukt som en sjekkliste mot situasjonen i Norge.

Resultatene fra de internasjonale undersøkelsene viser i stor grad samsvar med Kredittilsynets resultater. Det framgår at det er områdene virus/brannmur, endringsproblematikk og bruk av Internett som infrastruktur, som går igjen som potensielle sårbare og utsatte områder også i disse undersøkelsene. I tillegg viser disse økt fokus på organisert kriminalitet og kriminalitet utført av tidligere eller egne ansatte.

6. Hva vil Kredittilsynet gjøre?

Følgende områder er relevante:

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 IKT-virksomheten.

Kredittilsynets tilsynsopplegg er foreløpig på et overordnet og prosessorientert nivå og dekker hele IKT-virksomheten. Kredittilsynet har imidlertid startet arbeidet med å videreutvikle dette til mer **hvordan** IKT-virksomheten blir utført, da på et detaljert nivå. De områdene vi har valgt ut er:

- betalingssystemer
- virus/brannmur
- kontinuitets- og katastrofeløsninger

Kredittilsynet har kommet forholdsvis langt med opplegg for betalingssystemer, og har startet arbeidet med virus/brannmur og kontinuitets-/og katastrofeløsninger. Dette antas å ville bidra preventivt til at foretak under tilsyn vil gi større oppmerksomhet og prioritet til disse viktige områdene.

6.2 IKT-forskriften

Det preventive arbeidet med å informere om IKT-forskriften skal fortsette og en vil 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 risikoområder.

6.3 Risiko- og sårbarhetsanalyser (ROS)

Analysen som ble behandlet i Kredittilsynets styre våren 2002 og senere offentliggjort har blitt brukt aktivt som underlag for informasjonsmøter relatert til risiko. Kredittilsynet har planlagt at også nåværende ROS-analyse vil bli benyttet aktivt som et hjelpemiddel i Kredittilsynet arbeid.

Det er viktig til slutt å understreke at det er det enkelte foretak som fullt ut har ansvaret for egen IKT-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 IKT-løsninger.