Risiko- og sårbarhetsanalyse (ROS) 2005

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

Kredittilsynet, 24. mai 2006

Innhold

1. Innledning

Kredittilsynets ROS-analyse for 2004 var i stor grad retningsgivende i forhold til de områder som ble lagt vekt på i tilsynet med finansnæringens behandling og styring av teknologiske løsninger i 2005. Kredittilsynet anser det som både viktig og nyttig å gjennomføre en slik årlig gjennomgang av finansforetakenes bruk av IKT. Det å publisere resultatet av ROS-analysen for 2004 viste seg å ha positiv virkning på finansforetakenes arbeid på området. Tilbakemeldingen viser at resultatet av Kredittilsynets ROS-analyse blir brukt i arbeidet med å sikre foretakenes oppfølging av de områder som analysen påpeker som sårbare.

2. Bakgrunn og formål

I 2005 ble det gjennomført store endringer på IKT-området hos flere sentrale foretak innen finanssektoren. Dette gjelder både områder innenfor infrastruktur og bruk av ny informasjonsteknologi som grunnlag for introduksjon av nye produkter og tjenester. Kredittilsynet ser det som viktig å gjennomføre ROS-analysen blant annet for å kunne peke på de områder som er særlig utsatte. I finanssektoren har foretakene i stor grad utkontraktert IT-tjenesten til eksterne IT-leverandører. Utkontraktering av IT-tjenester til store internasjonale aktører blir mer vanlig. Dette skaper en ny situasjon i foretakenes arbeid med kontroll og oppfølging av IT-leveransene, da den tradisjonelle nærheten mellom foretak og leverandør i større grad enn tidligere baseres på rene forretningsmessige prinsipper.

Formålet med Kredittilsynets ROS-analyse er å identifisere om det er felles tendenser som har med risikoeksponering og sårbarhet å gjøre, og - gjennom informasjon om og fokus på problemområdene - å bidra til at nødvendige tiltak settes i verk.

3. Utviklingstrekk

3.1 Operasjonell risiko

Undersøkelser som er gjennomført i store internasjonale banker, konstaterer at institusjonene gir den operasjonelle risikoen betydelig vekt i sin interne kapitalallokering. En stor del av den operasjonelle risikoen er knyttet til funksjonalitet og driftsstabilitet i IT-systemene. Operasjonell risiko har i de siste årene fått større oppmerksomhet, bl.a. med grunnlag i det arbeidet som Baselkomiteen har gjennomført. Dette arbeidet har resultert i fastsetting av nytt regelverk for hvordan operasjonell risiko skal håndteres. Kredittilsynet ser på foretakenes behandling av operasjonell risiko som en sentral del av virksomhetsstyringen. Derfor tas dette opp spesielt i denne rapporten.

Baselkomiteen har utarbeidet en definisjon for operasjonell risiko. Denne har vi også lagt til grunn for vår forståelse:
"Med operasjonell risiko menes risiko for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelig feil eller eksterne hendelser".

Operasjonell risiko er i utgangspunktet vanskelig å identifisere, og det er ikke utviklet objektive kriterier eller tilfredsstillende metoder for kvantifisering av denne risikotypen. Det er dermed vanskelig å vurdere den operasjonelle risikoen som en relativ faktor i forhold til andre risikotyper og behovet for tilfredsstillende kapitaldekning. Det er imidlertid allmenn enighet om at det er mulig å karakterisere den operasjonelle risikoen som ”høy”, ”lav” eller ”middels” i forhold til sannsynlighet og økonomisk konsekvens.

En rekke faktorer har betydning for den operasjonelle risikoen, og det er institusjonens evne til å styre og kontrollere disse faktorene som avgjør om den operasjonelle risikoen er høy eller lav, og/eller er i samsvar med det som institusjonen selv finner forsvarlig. Det er dermed institusjonens evne til egen risikostyring på dette området som er det primære i forhold til den tilsynsmessige vurderingen. Viktige elementer i foretakets operasjonelle risikostyring er:

- identifikasjon og vurdering av faktorer som påvirker den operasjonelle risiko
- evne og vilje til å etablere kontrolltiltak slik at den gjenværende risikoen blir forsvarlig håndtert
- evne til forsvarlig å gjennomføre etablerte kontrolltiltak
- logg og evaluering av uønskete hendelser i forhold til den aksepterte risikoen

Faktorer som kan påvirke den operasjonelle risiko er eksempelvis:

- form på forankring i organisasjonens ledelse
- organisering og ansvarsdeling
- ledelse
- turnover blant medarbeidere
- etikk blant ledere og medarbeidere
- kompetanse
- teknologiske løsninger med manglende funksjonalitet
- oppfølging av kunder og engasjementer
- kontroll- og avstemmingsrutiner
- systemer og rutiner for rapportering
- kvalitet på beredskapsplaner

Dette er faktorer som, om de ikke er håndtert på forsvarlig vis, innebærer at den operasjonelle risikoen kan være høy, og at uønskede hendelser vil kunne påføre institusjonen betydelige tap.

For å kunne ta stilling til nivået på den operasjonelle risikoen, er det nødvendig å vurdere hvordan foretaket styrer og kontrollerer de aktuelle faktorene. Hvis foretaket har innført et tilfredsstillende system for risikostyring og kontroll og det kan konstateres at systemet blir etterlevd, kan den operasjonelle risikoen anses som forsvarlig.

3.2 Endringer i bruk av IKT i finansnæringen

Operasjonell risiko kan ha sammenheng med strukturelle endringer i finansmarkedene, for eksempel fusjoner, oppkjøp eller bytte av IT-leverandør. Dette medfører som oftest omorganiseringer, nedbemanning og skifte eller endringer av IT-systemer og tjenesteleverandører. Slike forhold har det siste året vært et kjennetegn for norsk finansnæring. Denne typen operasjonell risiko er knyttet til foretakenes bruk av informasjons- og kommunikasjonsteknologi (IKT). Det har gjennom 2005 vist seg at de store forandringene som pågår på IKT-området i finansnæringen i Norge, og som vi skrev om i ROS-analysen for 2004, har medført driftsforstyrrelser.

Terra-Gruppen besluttet 1. kvartal 2004 å avslutte sitt strategiske samarbeid med EDB Business Partner ASA for å etablere et nytt samarbeid med SDC Udvikling AS (SDC). SDC holder til i Danmark og eies av et holdingsselskap med utgangspunkt i medlemmer av foreningen Sparekassernes Datacenter. Bankene tilknyttet Terra-Gruppen startet konverteringen til ny løsning sommeren 2005. Konverteringen ble avsluttet i november 2005. Den nye løsningen har medført til dels store problemer for både kunder og ansatte i bankene. For kundene har selvbetjeningsløsningene hatt stor ustabilitet med til dels alvorlige feil. Dette gjelder både for privat- og bedriftskunder. For bankenes ansatte har endringene i regnskapssystemene medført en stor økning i manuelle operasjoner for å kunne

gjennomføre regnskapsmessige årsavslutninger. Dette har ført til tildels stor belastning og høyt sykefravær på de regnskapsansvarlige i bankene.

DnB NOR hadde som følge av fusjonen mellom DnB og Gjensidige NOR store endringsprosjekter under gjennomføring i 2005. Omfanget og kompleksiteten av prosjektene har ført til en omfattende endringstakt, som igjen har medført noe ustabilitet i foretakets IT-løsninger.

De store endringene har både direkte og indirekte redusert tilgjengeligheten for kundene. Summen av endringsprosessene utgjør i seg selv en risiko som må håndteres. De tiltakene som har vært iverksatt på dette området har ikke fungert tilfredsstillende, og det er grunn til å gi større oppmerksomhet til styring og kontroll ved gjennomføring av slike prosesser. Det er viktig at gode målsettinger ikke fortrenger krav til nødvendig styring og kontroll. Kredittilsynet fortsetter å gi høy prioritet til oppfølging av denne type endringsprosjekter gjennom målrettede tilsyn.

Kredittilsynet har i 2005 gjennomført eller igangsatt egne IT-tilsyn med flere av de pågående endringsprosjektene som er omtalt ovenfor. Dette arbeidet blir videreført i 2006. Etter Kredittilsynets vurdering er det svært viktig at man i slike prosjekter gjennomfører grundige kravanalyser, risikoanalyser, fastlegging av kvalitetskrav og prosedyrer som prosjektene skal følge, samt sikring av at disse blir fulgt.

Kredittilsynet mener det vil være uheldig dersom disse forholdene 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 av de ulike endringsprosessene som pågår på IT-området i 2006.

4. Kredittilsynets vurderinger

Kredittilsynet har med bakgrunn i egne analyser og tilgjengelige data identifisert noen særlig viktige risiko- og sårbarhetsområder:

Nye områder:

1. Organisert kriminalitet
2. Ufullstendig hendelsesrapportering
3. Manglende etterlevelse av eksterne krav

Områder som også ble pekt på i fjorårets risikoanalyse:

1. Kontinuerlig service og katastrofeplaner
2. Planlegging og gjennomføring av store prosjekt
3. Endringshåndtering

4.1 Organisert kriminalitet

Med bakgrunn i Kredittilsynets materiale er det grunn til å anta at målrettede data- og identitetstyverier økte betraktelig i 2005. Angrepene rettes mot utvalgte organisasjoner, bedrifter eller enkeltpersoner med sikte på å få fatt i data som kan gi angriperne økonomisk gevinst. Mens man i tidligere år har sett at ondsinnet kode, som for eksempel virus, ormer og spam, hovedsakelig ble laget og distribuert for å overbelaste og lamme IKT-systemer, ser vi nå en økende tendens til målrettede angrep utført med vinnings hensikt, og med store økonomiske tap, eller tap av tillit og anseelse som resultat for dem som rammes.

Flere banker og finansinstitusjoner, spesielt i engelsktalende land, men i 2005 også i Norge, er blitt utsatt for såkalt phishing. Dette er en form for svindel på Internett der kundene blir lurt til å oppgi fortrolig informasjon til hackere. Bankkunder har mottatt e-post eller blitt kontaktet per telefon og blitt bedt om å oppgi passord til nettbank, kortnummer og PIN-kode. Denne måten å få tak i informasjon på er også blitt gjennomført mot kunder i en norsk bank. I dette tilfellet var det e-post som ble brukt som distribusjonskanal, men på grunn av årvåkenhet og godt sikkerhetsarbeid i banken ble skadene begrenset. Det finnes også eksempler på identitetstyveri i 2005. Dette er en del av samme

problemstilling, å skaffe seg uautorisert tilgang til informasjon, for i neste omgang å forsøke å benytte dette i vinnings hensikt.

Det er viktig at foretakene fokuserer på å informere egne kunder om at de aldri skal oppgi passord eller PIN-kode til andre, og at de skal være varsomme med hvem de gir annen fortrolig informasjon til, som for eksempel kredittkortopplysninger.

4.2 Ufullstendig hendelsesrapportering

I foretakene som Kredittilsynet fører tilsyn med har det i 2005 oppstått flere alvorlige hendelser knyttet til IKT som har medført svikt i tjenestene til kundene. Dette kan som konsekvens medføre svekket tillit og tiltro til de etablerte løsningene. Årsaken til hendelsene har vært driftsavvik i IKT-virksomheten, ondsinnede angrep, brudd i sentral infrastruktur som strøm eller nettverk, eller fysiske skader som brann eller flom.

Foretakene i finansnæringen har ingen lov- eller forskriftsmessig plikt til å registrere eller rapportere om hendelser til Kredittilsynet. I IKT-forskriftens § 9 Avviks- og endringshåndtering er det stilt krav om at avvikshåndteringen skal omfatte alle avvik som oppstår i driften av IKT-systemene, både for å gjenopprette normal drift samt å benytte informasjonen i et preventivt arbeid som å gjennomføre tiltak for at samme problem ikke oppstår på nytt.

Det er i dag ingen krav om rapportering til en felles instans eller til Kredittilsynet. Gjennom ulike kilder blir Kredittilsynet likevel gjort kjent med alvorlige hendelser i IKT-virksomheten. Kilder til informasjonen kan være foretaket selv, media, publikum eller andre. Det er heller ikke andre myndighetsorgan som mottar denne typen rapportering rutinemessig. Samlet oversikt over alle hendelser kan være en effektiv måte å ”måle” stabiliteten i finansnæringen på og kan gi indikasjoner på en uønsket utvikling som det enkelte foretak selv ikke ser. Kredittilsynet vurderer derfor å etablere et krav til foretakene om registrering og rapportering av hendelser som berører IKT-virksomheten.

Kredittilsynet mener et slikt krav vil bidra til at foretakene i større grad organiserer IKT-virksomheten slik at sikkerheten øker og risikoen reduseres, og setter av mer tid og ressurser til å vurdere forebyggende og preventive tiltak. Krav om registrering og rapportering kan dermed gi foretakene en gevinst i form av bedre styring av den operasjonelle risikoen. Dette samsvarer også med krav i Basel II-regelverket. Tilsynsmyndighetene på sin side vil sikres oppdatert informasjon om, og oversikt over, kvaliteten på IKT-virksomheten i finansnæringen, og på bakgrunn av dette kunne sette inn tiltak på et tidligst mulig tidspunkt.

4.3 Manglende etterlevelse av eksterne krav

Oppfølging av lovkrav og andre myndighetskrav er et ledelsesmessig ansvar, og det forventes derfor at oppfølging av myndighetskrav forankres i styrene og følges opp av linjeledelsen i foretakene som ledd i arbeidet med styring og kontroll. I Kredittilsynets tilsynsmetodikk er det konkrete spørsmål som stilles om etterlevelse av lovkrav og andre myndighetskrav. Med bakgrunn i de svarene som er mottatt gjennom spørsmålsskjemaene våre, kan det se ut som at alle foretak har etablerte prosesser på dette området. Kredittilsynet har imidlertid grunn til å anta at flere foretak ikke bruker, eller har prosesser, for å sikre etterlevelse av lovkrav og andre myndighetskrav.

I en spørreundersøkelse til 623 eiendomsmeglere angående etterlevelse av IKT-forskriften var det hele 125 som ikke svarte på henvendelsen. Videre var det 100 som svarte at de hadde hørt om forskriften, men at de ikke overholdt den.

I lov om betalingssystemer pålegges alle som etablerer nye løsninger eller gjennomfører store endringer på betalingstjenester å melde fra til Kredittilsynet, den såkalte meldeplikten. I rundskriv nr 17/2004 har Kredittilsynet fastsatt retningslinjer for gjennomføringen av denne meldeplikten. Kontroller vi har foretatt i forbindelse med gjennomførte tilsyn i 2005 viser at dette ikke alltid etterleves. Kredittilsynet har derfor grunn til å tro at foretakenes etablerte prosesser ikke er tilstrekkelige for å sikre etterlevelse av lovpålagte- og andre myndighetskrav.

4.4 Kontinuitet og katastrofeplaner

Kredittilsynet satte gjennom innføringen av IKT-forskriften fokus på kontinuitet og katastrofeplaner. Det er egne paragrafer i forskriften som omhandler det å sikre kontinuerlig service og katastrofeberedskap. Hensikten med en kontinuitetsplan er å ha en samlet oversikt over de løsningene foretaket har for å sikre konfidensialitet, integritet og tilgjengelighet til IKT-systemer i en regulær driftssituasjon.

Med utgangspunkt i tilgjengelig dokumentasjon og gjennomførte tilsyn, er det grunn til å anta at det i prosessen med å lage for eksempel nettbankløsninger, ikke rettes tilstrekkelig oppmerksomhet mot å etablere robuste løsninger for tjenestene som tilbys. Man ser i økende grad at portalløsninger eller nettbankløsninger er inngangen til flere tjenester i nettbankene. Særlig de kundene som benytter nettbanken som inngang til løsninger i verdipapirmarkedet, for eksempel kjøp og salg av aksjer, stiller store krav til tilgjengelighet. Kredittilsynet vurderer det slik at prosessen med å etablere robuste løsninger med sikte på å oppnå høy tilgjengelighet må forbedres.

Med 'katastrofe' menes hendelser som forårsaker driftsavbrudd, slik at foretakets IKT-drift ikke kan fortsette med normalt tilgjengelige ressurser. Dersom foretakets IKT-drift må flyttes til en annen

lokasjon enn normalt driftssted, vil en katastrofeplan med tilhørende katastrofeløsning normalt bli iverksatt. Gjennom Kredittilsynets tilsynsaktivitet i 2005 finner vi at de fleste har etablert en katastrofeplan. Vi har likevel sett flere eksempler på at det planverket som foretakene har utarbeidet ikke er tilstrekkelig og/eller ikke er realistisk testet. Det er også en utfordring å holde katastrofeløsningene tilstrekkelig oppdatert i en periode med mange og omfattende endringer.

4.5 Planlegging og gjennomføring av større IKT-prosjekter

I Kredittilsynets ROS-analyse for 2004 ble det fokusert på de strukturelle endringene for fremtidig bruk av informasjonsteknologi. Ulike drivere som fusjoner, oppkjøp, kostnadsbesparinger, konkurranse, ny teknologi, nye tjenester osv., påvirker endringene. I den finansielle sektoren i 2005 var det samlet sett en høy endringstakt. Dette så vi i mange og store IKT-prosjekter. Kredittilsynets materiale om store IKT-prosjekter viser at planleggingsfasen i prosjektene har stor betydning for graden av risiko som følger senere i prosjektet.

Den høye endringstakten i finansnæringen i 2005 medførte flere uønskede hendelser enn det vi har sett tidligere år. Hendelsene resulterte i utilgjengelige nettjenester både for person- og bedriftskunder. Kredittilsynet ser alvorlig på dette da det er grunn til å anta at bakgrunnen for det økte antallet feil er mangelfulle prosesser rundt prosjektstyring generelt og spesielt området som berører testing og endringshåndtering i prosjektene.

4.6 Endringshåndtering

På grunn av endringer i bruk av teknologi, fusjoner, omorganisering, utkontraktering osv. har det i 2005, som nevnt ovenfor, vært et høyt endringstempo. En samlet vurdering av alle foretakene som har gjennomført store endringer i bruk av IKT, viser at risikoen for at det oppstår feil ved gjennomføring av endringer er stor.

Kredittilsynets materiale gir grunn til å anta at omlag 70 prosent av alle feil som inntreffer oppstår i planlagte endringer. Kompleksiteten i løsningene innen finansnæringen er ofte høy. Dette medfører at det stilles stadig større krav til nødvendig kompetanse for å planlegge, teste, implementere og godkjenne endringer.

Kredittilsynet har gjennom sitt tilsynsarbeid i flere år påpekt overfor foretakene viktigheten av å ha en god endringshåndteringsprosess. Dette området er også regulert i IKT-forskriften.
Likevel er det Kredittilsynets vurdering at det i 2005 forekom for mange feilsituasjoner som ga ustabilitet og manglende tilgjengelighet. Særlig berørte dette bankenes nettbanker som har høye krav til oppetider og tilgjengelighet. I endringshåndteringsprosessen er det særlig to områder som er sentrale: Risikovurdering og testing. Kredittilsynet ser i sitt tilsynsarbeid at når endringer skal

gjennomføres og når disse får mindre tid enn beregnet til utføring, blir risikovurdering og testing ofte skadelidende.

5. Kilder

Kredittilsynets arbeid med operasjonell risiko, i tillegg til den generelle IT-tilsynsvirksomheten, har vært rettet mot foretakenes bruk av informasjons- og kommunikasjonsteknologi. ROS-analysen for 2005 bygger på flere kilder, der de viktigste er IT-tilsynsvirksomheten og intervjuer med nøkkelpersoner knyttet til utvalgte områder.

5.1 IT-tilsyn

Kredittilsynet gjennomførte 31 IT-tilsyn i 2005 fordelt på tilsynsområdene bank, forsikring, finansieringsselskaper, verdipapirinstitusjoner, inkassovirksomhet, eiendomsmeglerforetak og regnskapsførerforetak. IT-tilsynene omfattet også gjennomføring av IT-tilsyn hos leverandører av IT-tjenester med hjemmel i IKT-forskriftens § 12 om utkontraktering av IKT-virksomhet. Det ble også gjennomført IT-tilsyn av filialer av utenlandskeide banker.

Når det gjelder IT-tilsynsopplegget er det utarbeidet en oppdatert utgave av kontrollspørsmålene i egenevalueringsopplegget. Vi har også utviklet nye moduler som spesielt adresserer IT-leverandører, IT-prosjekter, hvitvasking, nettbank, katastrofeberedskap, virusbeskyttelse, brannmur og betalingstjenester. IT-tilsynsopplegget følger utviklingen av risikobasert tilsyn og innføring av Basel II. Meldeplikten for betalingstjenester har ikke fått den ønskede virkningen og vil bli fulgt opp videre i 2006. Når det gjelder oppfølging av IKT-forskriften har vi arbeidet videre med:

- etterlevelse
- vurdering av utvidelse av tilsynsområdet
- bedre veiledning

Resultatene fra 31 IT-tilsyn gjennomført i 2005 har gitt oss en god indikasjon på status i de aktuelle foretakene, særlig med hensyn til hvordan IT-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 IT-området i tiden fremover.

5.2 Gjennomførte intervju

Vi valgte 12 sentrale foretak der vi gjennomførte intervjuer med nøkkelpersonell. I forbindelse med dette har vi arbeidet med form og innhold på selve intervjuopplegget. I motsetning til tilsynsopplegget går intervjuene i mindre grad på IT-prosessene, men mer direkte på utvalgte områder. Opplegget vi har kommet frem til for gjennomføring av intervjuer, vil bli videreutviklet, og antall intervjuobjekter ytterligere økt i neste års ROS-analyse.

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

- personell
- konfidensialitet
- integritet
- tilgjengelighet
- IT-infrastruktur
- interne misligheter
- misligheter forårsaket av eksterne
- transaksjonshåndtering
- prosesstyring.

Et felles trekk ved de foretakene som er intervjuet, er at de vurderer å ha rimelig god kontroll over egen situasjon og er oppmerksomme på viktige risikoområder. Et viktig forbedringsområde vil likevel være å arbeide mer med risikoanalyser, 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 stor oppmerksomhet i foretakene.

5.3 Hendelser

Vi har vurdert tilgjengelig informasjon om rapporterte hendelser fra 2005 fra enkelte foretak. Resultatet av dette viser at det fortsatt er grunn til å fokusere på endringshåndteringsprosessen, og, ikke minst, hvordan endringshåndtering gjennomføres operasjonelt. Ikke uventet er frekvensen av hendelser størst i foretak hvor det gjennomføres mange endringer. Et annet forhold som bør vektlegges er hvordan hendelser analyseres og behandles for gjenoppretting og for å hindre gjentagelse. Informasjon om hendelser er en viktig kilde til ROS-analysen. Dette sees også i forbindelse med operasjonell risiko og planlagt innføring av Basel II i 2007.

5.4 Internasjonale ROS-undersøkelser

Relevante internasjonale rapporter[1] og undersøkelser på IT-området, har under arbeidet blitt brukt som sjekklister mot situasjonen i Norge. Resultatene fra de internasjonale undersøkelsene viser i stor grad samsvar med våre resultater. Det fremgår 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 vies det økt oppmerksomhet på organisert kriminalitet, og kriminalitet utført av tidligere eller egne ansatte. Kredittilsynet har etablert samarbeid med andre myndighetsorganer med tilgang til gradert informasjon både nasjonalt og internasjonalt. Dette har gitt oss nyttige impulser, og viktig informasjon på et tidligere tidspunkt enn vi normalt ville fått.

[1] McKinsey Quarterly Reports for 2005
Rapport 1. halvår 2005 Symantec
Garner Group Updates 2005

6. Hva kan 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 fokuserer på at relevante prosesser er på plass for alle områder innen IT-virksomheten.

Nåværende tilsynsmetode er i tråd med hvordan nytt internasjonalt regime for operasjonell risiko vil bli utformet. Vårt opplegg er foreløpig på et overordnet og prosessorientert nivå og dekker hele IT-virksomheten.

For å få mer detaljerte gjennomganger av særlig utsatte områder, som ikke er dekket tilstrekkelig, er det utviklet flere tilleggsmoduler med prosessbasert tilnærming som skal favne alle IKT-prosesser for å komplettere tilsynsmetodikken innenfor IKT-området. Disse modulene ble benyttet ved IT-tilsyn i 2005, og erfaringene er så langt svært positive. Det samlede tilfanget av informasjon som Kredittilsynet får gjennom tilsynsopplegget gir en god innsikt i kvaliteten på foretakenes IKT-virksomhet.

6.2 IKT-forskriften

Kredittilsynet vil fortsette arbeidet med å informere om IKT-forskriften, samt følge opp at de enkelte foretakene tilpasser seg denne. Det er flere bestemmelser i forskriften som har en direkte preventiv effekt gjennom krav om å sikre seg effektivt på aktuelle risikoområder.

6.3 Lov om Betalingssystemer mv

Kredittilsynet er opptatt av at foretakene overholder lov om betalingssystemer, og vil særlig referere til innholdet i Rundskriv 17/2004, som peker på meldeplikt for systemer for betalingstjenester. Systemer for betalingstjenester blir regulerte av kapittel 3 i loven, og § 3-2 pålegger banker og

finansieringsforetak meldeplikt til Kredittilsynet for etablering og drift av systemer for betalingstjenester.

Følgende forhold utløser meldeplikt:

- innføring av nytt system for betalingstjeneste
- ny versjon som i vesentlig grad påvirker andre berørte parter som inngår i løsningen
- ny versjon med endret eller ny funksjonalitet som er vesentlig for systemet for betalingstjenesten

Når meldeplikten blir utløst, skal foretaket svare på en egenmelding ved å krysse av for "Ja/Nei/Ikke relevant" på kontrollspørsmålene nummerert fra 1 til 19.

6.4 Risiko- og sårbarhetsanalyser (ROS)

Analysen for 2004, som ble behandlet i Kredittilsynets styre våren 2005 og senere offentliggjort, er blitt brukt aktivt som underlag for informasjonsmøter relatert til risiko. Vi har også planlagt å bruke denne ROS-analysen som et hjelpemiddel i vårt arbeid fremover.

Kredittilsynet understreker at det er det enkelte foretaket selv som fullt ut har ansvaret for egen IT-virksomhet. Kredittilsynets aktiviteter er et bidrag til det viktige arbeidet det enkelte foretaket må ivareta for å oppnå betryggende forhold i bruken av IT-løsninger.

6.5 Hendelsesregistrering- og rapportering

Som nevnt i kap. 4.3 vurderer Kredittilsynet å innføre et regelverk for registrering og rapportering av hendelser som påvirker IKT-virksomheten. Dette kan skjerpe foretakenes arbeid med å organisere IKT-virksomheten slik at sikkerheten øker og risikoen reduseres. Dette vil kunne bidra til bedre styring med den operasjonelle risikoen, og vil være i tråd med krav som ellers følger av det nye kapitaldekningsregelverket knyttet til operasjonell risiko.

Et standardisert format for registrering av hendelser vil legge til rette for utveksling av informasjon mellom tilsynsmyndighet og foretak, men også for utveksling av informasjon mellom foretakene. Hendelsesrapporter utformet i henhold til standardiserte formater kan danne grunnlag for ”benchmarking” foretakene imellom. Man kan videre tenke seg muligheten for å opparbeide en felles database over hendelser i IKT-virksomheten i finansnæringen.

Andre myndighetsorganer og organisasjoner har forsøkt å få til innrapportering av hendelser som berører IKT-virksomheten på frivillig basis, men har i liten grad lyktes med dette. Fellestrekk for de rapporteringskanalene som er etablert, er at rapporteringen baseres på frivillighet, går på tvers av sektorer og fokuserer mest på tilsiktede (ondsinnede) hendelser. Det finnes få eksempler på

rapportering av driftsrelaterte hendelser, og det finnes også lite litteratur rundt dette. Kredittilsynet ønsker å prioritere arbeidet med rapportering av hendelser i IKT-virksomheten i finansnæringen, og at rapporteringen skal omfatte både tilsiktede og utilsiktede hendelser. Med dette følger at Kredittilsynet vil utforme krav til måten registreringen og rapporteringen skal gjennomføres på. Kredittilsynet har mulighet for å etablere et krav med hjemmel i forskrift, og stiller slik med et virkemiddel som gjør at dette kan lykkes. Temaet er aktuelt også i andre land. Både Finland og Sverige iverksatte i 2005 regelverk med krav om rapportering av hendelser.