KREDITTILSYNET
The Financial Supervisory Authority of Norway

Veiledning for gjennomføring av risiko- og sårbarhetsanalyser

Ref. IKT-forskriften § 3

Innhold

[Red. anm. 17.07.2008: I avsnitt 2.2
på side 9 er kulepunkt 2 og 5 rettet.]

1 Innledning

1.1 Regelverk

Gjennomføring av risikoanalyser er viktig for å kunne kjenne til foretakets risikonivå og for å kunne iversette tiltak for å oppnå et akseptabelt risikonivå. Foretak i finanssektoren som er underlagt IKT-forskriften er gjennom forskriftens § 3 Risiko pålagt å gjennomføre risikoanalyser av foretakets bruk av IKT.

Aktuelle foretaksområder pr. 31.3.2008:

§ 1 Virkeområde

Forskriften gjelder for norske:
1. *Forretningsbanker*
2. *Sparebanker*
3. *Finansieringsforetak*
4. *Forsikringsselskaper*
5. *Private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond*
6. *Børser og autoriserte markedsplasser*
7. *Verdipapirforetak*
8. *Forvaltningsselskaper for verdipapirfond*
9. *Oppgjørssentraler*
10. *Verdipapirregistre*
11. *Inkassoforetak*
12. *Eiendomsmeglerforetak*
13. *E-pengeforetak*
14. *Systemer for betalingstjenester*

IKT-forskriftens krav til gjennomføring av risikoanalyser er uttrykt slik i forskriftens ***§ 3***

Risikoanalyse:

Foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene. Foretaket skal ha en dokumentert prosess for gjennomføring av risikoanalyser av IKT-virksomheten. Prosessen skal blant annet definere klare ansvarsforhold og omfatte oppfølging av tiltak som iverksettes som et resultat av den gjennomførte risikoanalysen.

Foretaket skal minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten, gjennomføre risikoanalyser for å påse at risiko styres innenfor akseptable grenser i forhold til foretakets virksomhet. Resultatet av risikoanalysen skal dokumenteres.

Dersom flere foretak inngår i en samlet gruppe eller har inngått et forpliktende samarbeidsopplegg og benytter samme IKT-systemer, kan gruppen gjøre en felles risikoanalyse for de deler av IKT-løsningene som inngår i ”fellesskapet” og benytte dette som grunnlag i foretakenes egne risikoanalyser.

Risikoanalyse har i økende grad blitt et hjelpemiddel for foretakene for å avdekke sårbarheter i IT-systemene og ved bruken av IKT. Risikoanalyser og tiltak som følge av disse, kan gjøre foretaket i stand til å herde IT-systemene, dvs. gjøre systemene mer robuste, noe som vil bidra til å redusere sannsynligheten for at uønskede hendelser inntreffer. Hovedhensikten med risikoanalyse er først og fremst å bli klar over egen risikosituasjon og basert på denne kunnskap, iverksette risikoreduserende tiltak eller på annen måte sikre en forsvarlig håndtering av egen risiko. Det er viktig for foretaket å klargjøre hva som er et akseptabelt risikonivå med utgangspunkt i foretakets forretningsstrategi og virksomhetens omfang og viktighet.

En ønsket effekt er at risikoanalysen "beskytter" mot tap og skade på renommé. Risikoanalysen gir *løpende* avkastning for virksomheten. Risikoanalysene er et viktig verktøy for å sikre at virksomhetsmålene nås og skal være en integrert del av den *daglige driften*. En forutsetning for å sikre kvaliteten på risikoanalysen er at den må være utarbeidet av fagpersonell som har forutsetning for å vurdere risikoen på et tilstrekkelig detaljert nivå.

Erfaringen viser at mange uønskede hendelser sannsynligvis kunne vært unngått dersom foretaket hadde gjennomført risikoanalyse med tilstrekkelig kvalitet. Risikoanalyse er derfor et viktig tiltak når det gjelder skadeforebygging.

1.2 Basel II

En risikoanalyse som beskrevet i dette dokumentet, vil utgjøre en viktig del av grunnlaget for måling innenfor områdene som Basel II dekker: *"Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk."*

Elektroniske systemer og manuelle systemer og rutiner faller inn under rammen for analysen. I Basel II regelverket inngår operasjonell risiko i beregning av kravet til kapital. Basel II angir tre alternative måter å måle operasjonell risiko på.

Innenfor Basel II-regelverket opereres det med en standardisering av de kategorier eller hendelser som faller inn under begrepet operasjonell risiko. Registrering av tap og hendelser relatert til operasjonell risiko vil være et av kravene til de institusjoner som ønsker å beregne kapitalkravet her etter avanserte metoder (AMA). Selv om en ikke forventer at anvendelse av AMA blir aktuelt for mange norske banker, vil et av kravene også for å benytte sjablongmetoden (TSA) være at foretakene bygger opp en taps- og hendelsesdatabase etter en slik inndeling av operasjonell risiko, som da naturlig bygges over samme lest som etter AMA-kravene.

De 3 ulike alternative valg for operasjonell risiko er:

Basic Indicator Approach (BIA)	Basismetoden	For mindre foretak med relativt enkelt produktspekter.
The Standardized Approach (TSA)	Sjablongmetoden	For mellomstore foretak hvor risiko inndeles i forretningsområder (business lines).

Advanced Measurement Approach (AMA)	AMA-metoden (Avanserte metoder)	Større komplekse konsern som etter godkjennelse fra tilsynsmyndigheten (Kredittilsynet) kan ta i bruk AMA-modeller for risikostyring

1.3 Hensikt

Denne veiledningen er ment å være en enkel momentliste over viktige deler som bør medtas når risikoanalyser gjennomføres. For en utdypende veiledning i valg av metode, se BAS 5 - Evaluering av ulike metoder.[1]

Alle eksemplene i veiledningen her er hentet fra virkeligheten og er ment å illustrere spennvidden i de sårbarheter som foretaket bør se på. Veiledningen krever ingen forkunnskaper. Kvaliteten på foretakets risikoanalyse derimot, står og faller med erfaring og kunnskap hos dem som utarbeider den. Vi vil forvente at disse har kjennskap til konsepter, modeller, prosesser og terminologi slik de fremkommer i ISO/IEC 27001, ISO/IEC 27002 og ISO/IEC 27005.

Risikoanalyse foretatt for et gitt system er ikke en engangsforeteelse, men må gjentas regelmessig eller ved større endringer.

- Systemenes sårbarhet endrer seg over tid. Det å utnytte svakheter i systemer var tidligere forbeholdt noen få eksperter. I dag finnes det verktøy tilgjengelig på Internett som gjør at det er ”plug and play” å utnytte svakheter i systemene.
- Systemendringer kan medføre at risiko endrer seg.
- Gjentagende risikovurderinger med tilhørende tiltak gjør at systemet blir gradvis mer robust (”herding”).
- Uønskede hendelser som skjer fortløpende, kaster nytt lys over systemets svake sider.
- Gjentagelse gjør at analyseteamet får et nærmere og mer presist forhold til hvilke uønskede hendelser som kan skje, skaden som oppstår, og hvilke hendelser som sannsynligvis ikke vil skje. Ressursene som benyttes til skadeforebygging, kan dermed utnyttes mer effektivt.
- Erfarte feil, mangler og nestenulykker er viktige kilder i analyseprosessen. En oversikt over slike gir verdifulle assosiasjoner og koplinger til mulige likeartede feil.

Risikoanalysen kan inndeles i klart adskilte faser:

1. ***R***amme inn systemet eller området som er gjenstand for risikovurderingen, dvs. å avgrense området som undergis risikovurdering
2. ***I***dégenerering rundt temaet ”Hva kan gå galt?”
3. ***S***kalere, dvs. å rangere de uønskede hendelsene
4. ***I***nnkapsle, dvs. å innføre tiltak som reduserer sannsynlighetene for at uønskede hendelser inntreffer eller som reduserer følgen av de uønskede hendelsen.
5. ***K***ontrollere at tiltakene virker som forutsatt.

[1] http://www.proactima.no/pa/publicfile/download/Filer/Vedlegg%202%20-%20Metodeevaluering%20ver7.pdf

6. ***O***ppsummere områdene som er risikovurdert til en total for foretaket og dokumentere analysen

2 Risikoanalysens faser

2.1 Ramme inn systemet som skal risikovurderes

Utfordringen her er å finne grensene for området som skal risikovurderes. Ofte vil datasystemer være definert i forhold til foretakets forretningsområder slik som utlånssystemet, remburssystemet, reskontrosystemet, cash management-systemet, økonomisystemet osv. Risikoanalysen skal ha utgangspunkt i de enkelte forretningsområdene og IKT som inngår i disse. For IKT-systemer som er felles for flere forretningsområder, slik som tilgangskontrollsystemet, web-publisering, databasesystemer osv., kan foretaket velge å gjøre en (1) risikoanalyse for hver av disse, og stille dem til disposisjon for forretningsområdene.

Det er viktig å notere seg at foretaket er pålagt å gjennomføre en risikoanalyse av hele IKT-virksomheten, minimum årlig.

I tillegg til IKT-forskriften § 3, finnes det andre bestemmelser[2] som stiller krav til at foretaket skal gjennomføre risikoanalyse. Enkelte foretak kan være underlagt flere av disse bestemmelsene. Risikoanalysen som beskrevet i veiledningen her, tar utgangspunkt i foretakets forretningsområder, og kan derfor være et vesentlig bidrag til også å dekke kravene i andre bestemmelser.

Ledelsen for forretningsområdet er ansvarlig for å identifisere IKT-systemer innenfor forretningsområdet, og for å prioritere systemene etter deres behov for analyse og beskyttelse. I denne vurderingen må ledelsen vurdere blant annet:

- hvor alvorlig virksomheten i forretningsområdet kan rammes
- hvor mange kunder som berøres
- hvor hardt kunden rammes
- om kunnskap om skaden holdes internt i foretaket inntil skaden er reparert, eller om skaden er umiddelbart ”synlig”
- om skaden er et resultat av, eller om den innebærer at lovbestemmelser ikke overholdes
- om foretaket risikerer at sensitiv personinformasjon kommer på avveie
- om skaden innebærer at avtaler ikke overholdes

Konkurranseforhold i bransjen, foretakets strategi/mål, kundelojalitet, foretakets størrelse/og forhandlingsstyrke, etterspørsel etter foretakets tjenester etc. er faktorer som virker inn på vurderingen av disse forhold.

Systemet som understøtter forretningsområdet bør beskrives med setninger som sier noe om:

[2] Finansieringsvirksomhetsloven (LOV-1988-06-10-40),
jf. § 2-9 første og andre ledd. Kapitalkravforskriften (FOR-2006-12-14-1506).
Internkontrollforskriften (FOR-1997-06-20-1057),
§ 3-2. Gjennomgang av risiko og sikring

- Eierskap, ansvar, oppgaver og roller
- Hvilke hensikt skal systemet tjene?
- Hvilke entiteter/maskiner eller grupper av mennesker er det som benytter systemet?
- Hva slags data behandles i systemet?
- Hvilken informasjon vil bli overført mellom entiteter?
- Hvilke deler av systemet må beskyttes (data, maskinvare, programvare, prosedyrer, autorisasjon og mennesker)?
- Hvor lenge er det akseptabelt at systemet ikke virker etter målsettingen, for eksempel når det gjelder manglende tilgang til informasjon, ukorrekt informasjon, tilgang for uautoriserte brukere eller systemer?

Erfaringer viser at det er viktig å dele opp det området som er gjenstand for risikovurdering i mindre enheter. Mindre, avgrensete enheter gjør det praktisk å planlegge og å utføre analysen. Dette vil f. eks. være til hjelp i arbeidet med å identifisere den kompetansen som trengs for å gjøre en kvalitetsmessig analyse. Videre blir det mulig å rangere systemene for eksempel slik at man lister systemer som bør risikovurderes oftere enn andre. Eksempel: For tjenester som tilbys via Internet, kan det være praktisk å analysere de delene av tjenesten som ligger ”nær” Internett isolert fra andre (”back-end”) deler av tjenesten. Dette bør gjøres blant annet fordi trusselbildet på Internett er svært dynamisk. For øvrig viser vi til KOBI-rapporten, se *Vedlegg 4. Verdivurdering og klassifisering*.

Det er ledelsen i foretaket som er ansvarlig for gjennomføringen av risikoanalysene som gjennomføres i foretaket. Ledelsen må følge opp og etterspørre resultater av risikoanalysen. Ledelsen må skape et miljø som gjør at medarbeidere tør å flagge sårbarheter. Medarbeidere og andre som peker på sårbarheter og på den måten gir uttrykk for at de bryr seg om foretaket, bør honoreres. I mange foretak vil det være påkrevet med kraftige tak fra ledelsens side for å skape dette kontrollmiljøet.

En vanlig organisering av arbeidet knyttet til risikoanalyse er at lederen for forretningsområdet utpeker en person, som rapporterer direkte til lederen. Vedkommende har ansvar for å tilrettlegge, koordinere og gjennomføre forretningsområdets risikoanalyser. I dette arbeidet får hun bistand av ansatte med kunnskap om forretningsområdet og tilhørende prosesser, systemer og risikofaktorer. Innenfor forretningsområdene er det ikke uvanlig at det eksisterer ”superbrukere”. Dette er brukere som fungerer som bindeledd til IT-avdelingen. Disse medarbeiderne er egnet til å delta og bistå den som er ansvarlig for gjennomføring av risikoanalysen. I tillegg bistår IT- teknikere direkte med informasjon om eksisterende automatiske kontroller og identifisering av mulige nye kontroller. Omfanget av bistand bør bestemmes og ressurser allokeres og avtalefestes.

Under idegenereringsfasen (se nedenfor) vil systemets forhold til andre systemer (hardware, kommunikasjon og software) og funksjoner (drift, tilgangskontroll mv) bli avdekket. De som gjennomfører risikoanalysen må ta stilling til hvilke uønskede hendelser og uønskede situasjoner som kan oppstå som en følge av svakheter i omkringliggende systemer. Videre må det innhentes informasjon som belyser risikoen knyttet til disse systemer, og tas stilling til i hvilken grad en kan bygge på sikkerhet i disse systemene. Se mer om dette i kapittel 2.3.

Endringer i systemene skal inngå i risikovurderingen – hvilke uønskede hendelser kan endringen medføre? Identiske, repeterende endringer undergis en enkel risikovurdering der det blir vurdert om eventuelle kritiske terskelverdier overskrides som følge av endringen, for eksempel allokert datalagringsplass, antall samtidige brukere osv.

2.2 Idégenerering

Resultatet av forrige fase er en liste over systemer prioritert etter systemenes betydning for forretningsområdet og en overordnet beskrivelse av systemet.

I denne fasen begynner vi med det viktigste systemet og lister opp svakheter (sårbarheter), uønskede hendelser (trusler) som utnytter svakhetene og en verbal beskrivelse av uønskede situasjoner (skaden) som oppstår.

Eksempel:

Sårbarhet	Trussel	Skade
Svak innlogging	Uvedkommende utnytter svakhetene og utgir seg for å være andre	Renommé, må vi stenge tjenesten?
Vi har ingen rutiner for systematisk gjennomgang av web-applikasjoner med tanke på hvor sårbare disse er for Cross Site Scripting, HTML header poisoning, SQL injection etc.	Uvedkommende utvikler et SQL script som eksponerer sensitive kundedata	Kunder og betingelser blir kjent for konkurrenter og vi taper marked

Den ansvarlige for denne fasen bør være en person med erfaring fra arbeid med risikoanalyser, og som følgelig gjør henne i stand til å stille de rette ledende, åpne spørsmålene.

Ved første gangs gjennomgang er det viktig at man tenker fritt og ukritisk. Det viktige er å få alle potensielle skader og skadeårsaker opp på bordet. Ingen skade skal utelukkes fordi "… vi har jo kontroller som hindrer denne skaden". Det er altså systemets iboende risiko vi er ute etter her. Eventuelle kontroller vurderes i en senere fase, der spørsmålet blir stilt om kontrollene har vært testet, er de egnet til å avverge trusselen, hvor "sterke" er de osv.

I idégenereringsfasen bør foretakets styre, ledere, saksbehandlere og systemutviklere delta. Ledelsen bør ha oversikt over hvilke uønskete hendelser som vil skade foretaket og andre interessenter, som kunder eller samfunn. Deltagere med utviklingsbakgrunn vil kunne beskrive sårbarheter og trusler som kan utløse skaden. Det er en gylden mulighet til å forklare ledere hvilket ansvar de har og for systemutviklere til å forstå hva som er vesentlig for virksomheten.

Feil, mangler og nestenulykker som man har erfart selv eller som man for øvrig kjenner til, er viktige kilder i analyseprosessen. En oversikt over slike gir verdifulle assosiasjoner og koplinger til mulige likeartede feil. Likeledes er funn fra tidligere utførte risikoanalyser viktig input. Det å lese logger og belastningsanalyser gir ofte gode indikasjoner og assosiasjoner. Søk på leverandørenes sider på Internett gir ofte verdifull informasjon om sårbarheter i programvare, applikasjoner og tjenester.

Eksemplene nedenfor er hentet fra virkeligheten og er ment å illustrere spennet i vurderingene som gjøres i forbindelse med en risikoanalyse:

- Internettjenesten stopper opp fordi ”noen” har glemt å fornye digitale sertifikater som prosesser/ systemer benytter for å autentisere seg (dersom autentiseringen feiler, vil ikke prosessen kjøre).

- I perioder med ekstremt mye nedbør renner vann som er fraktet fra de høyere deler av byen ut (!) av kummer og sluk i de lavere deler, og oversvømmer datamaskiner som er plassert i kjellere i bygninger her, og tjenester som går på disse maskinene stopper opp.

- Foretaket har utkontraktert drift av systemene. Avtalen dekker ikke katastrofeberedskap på en tilfredsstillende måte, og det er uklart hvem som har hvilke oppgaver når noe går galt.

- Foretaket ”trodde” at nettverket bestod av kabler som aldri krysset hverandre, slik at den ene kunne ta over for den andre dersom denne falt ned. I virkeligheten går kablene delvis i samme grøft.

- Gebyret som kunden betaler for bruk av minibank varierer, alt avhengig av om uttaket skjer på dagtid eller nattetid/helg. Det viser seg at bankens IT-program ikke tolker tidsangivelsen fra minibankene på rett måte, og gebyr blir ikke beregnet og belastet. Feilen har pågått over lang tid, og banken har tapt betydelig inntekter.

Som eksemplene viser, vil deltakernes utsagn typisk beskrive en uønsket hendelse som inntreffer og en uønsket situasjon som oppstår som følge av dette.

2.3 Skalere

Forrige fase resulterte i en liste av sårbarheter, mulige trusler og skaden som kan oppstå som et resultat av disse.

I denne fasen tar vi utgangspunkt i listen. Vi identifiserer de kontrolltiltakene som foretaket har implementert for å avverge trusselen, og vurderer hvor effektive disse er for å avverge trusselen. Dette gjør oss i stand til å sette en indikator for sannsynligheten for at det skal skje skade. Vi setter også en indikator som gir uttrykk for konsekvensene dersom skaden skulle inntreffe. Resultatet av fasen er en liste som viser sårbarhet, trussel og skade. Det er foretatt en totalvurdering av sårbarhet, trussel og skade. Totalvurderingen kan uttrykkes som en risikoscore.

Når en uønsket hendelse (trussel) treffer en sårbarhet inntrer en skade. Høy sannsynlighet for stor skade innebærer høy risiko for foretaket. Har foretaket mange, kjente sårbarheter, er det stor sannsynlighet for at det finnes kjente angrep (trusler), og foretaket er svært utsatt (høy risiko).

Kunnskap om hvilke kontroller som er relevante, varierer fra foretak til foretak. Enkelte foretak har etablert en sikkerhetspolicy som beskriver kontroller som skal være implementert i foretaket. Disse kontrollene inngår i vurderingen av risikoen for at en uønsket hendelse skjer.

Utelukkende kontroller som er virksomme på analysetidspunktet skal være med i vurderingen. Kontroller som antas å være virksomme, teller ikke med i denne sammenheng – kontrollene må være testet og verifisert virksomme. Foretaket skal blant vurdere kontrollmiljøet og i denne forbindelse legge vekt på kompetanse, oppfølging, rapportering, varsling, overvåking.

Det første spørsmålet å stille seg er: Har personell innenfor området tilstrekkelige forutsetninger (kompetanse og erfaring) til å identifisere sårbarhetene og relevante kontroller? Er man kjent med det aktuelle trusselbildet – har det dukket opp nye trusler siden sist vurdering?

Alle systemendringer skal risikovurderes. Systemendringer kan ha utilsiktede negative konsekvenser for andre systemer eller for foretaket totalt sett. Eksempel: For å unngå at en transaksjon ikke lar seg gjennomføre innenfor tildelt tid, så vurderes det å øke time-out parametre, dvs. den maksimale tiden applikasjonen tillates å vente på svar fra en sentral prosess. Dersom mange applikasjoner deler ressurser, kan denne endringen medføre at andre applikasjoner får problemer. I denne fasen er det viktig at det er kompetanse til stede som kan kontrollere at slik sektortenking ikke blir dominerende, og at konsekvenser for foretaket totalt sett blir belyst og vurdert, samt at nødvendige beslutninger i denne forbindelse blir tatt.

I denne fasen er det viktig at det ikke uten videre tas forutsetninger med hensyn til kvaliteten i områder utenfor analysen – for eksempel systemer som systemet under analyse er avhengig av. Slike systemer er gjerne fellessystemer som for eksempel tilgangskontrollsystem, mail-system, web-portalsystem osv.

Eksempel 1: Ved en analyse av utlånssystemet skal analyseteamet ikke ta for gitt at tilgangskontrollsystemet fungerer som forutsatt. Teamet skal gjøre en selvstendig vurdering av sannsynlighetene for uautorisert tilgang til utlånssystemet (uautorisert tilgang kan føre til at uvedkommende kan gjøre uautoriserte endringer på rentesatsen på visse lån for eksempel). I vurderingene kan teamet bygge på opplysninger fra andre, herunder risikoanalyser gjennomført for tilgangskontrollsystemet.

Eksempel 2: I vurderingen av ”Hvor stort er skadeomfanget?” vil teamet måtte ta stilling til hvor lenge den uønskede situasjonen ventelig vil vare. Teamet skal i denne sammenheng ikke uten videre forutsette at en eventuell reserveløsning eller katastrofeplan fungerer som forutsatt. Teamet skal gjøre en selvstendig vurdering av dette. Det skal foreligge konkrete bevis for at katastrofeløsninger fungerer som forutsatt, før teamet kan ta katastrofeløsningen i betraktning når det skal settes score for ”Hvor stort er skadeomfanget?”.

Gitt kontrolltiltakene som er implementert, vurderes hvert sett av sårbarheter og tilhørende trusler etter disse kriterier:

1. Hvor vanskelig er det å oppdage sårbarheten?
2. Hvor vanskelig er det å utløse hendelsen?
3. Hvilken kompetanse kreves for å utløse hendelsen?
4. Hvor stort er skadeomfanget?
5. Hvor mange brukere blir berørt av skaden?

I vurderingen kan det benyttes en skala fra 0 til 10, der 0 trekker i retning av lav sårbarhet mens 10 trekker i retning av høy sårbarhet.

Foretakets risiko, fremkommer ved å ta det aritmetiske gjennomsnitt av ”karakteren” for de fem kriteriene.

Graderingen gir en grov indikasjon av risikonivået. Det kan argumenteres for at en uønsket hendelse med mindre varians innenfor de tre første kriteriene, er farligere enn en uønsket

situasjon der en karakter nær 0 på en av kriteriene indikerer at hendelsen nærmest er forhindret fra å kunne skje. For å fange opp dette må modellen utvides med en beregning av varians.

Denne fasen forutsetter at det er systemkompetanse tilgjengelig. Systemets eier vil være ansvarlig for aktiviteten.

Eksempler på gradering fra 0 – 10:

1. **Hvor vanskelig er det å oppdage sårbarheten som la grunnlaget for de(n) uønskede hendelsen(e)?**

0 = Svakhet som kan utnyttes til ondsinnet angrep og det er veldig vanskelig eller umulig å finne svakheten. 0= Krever kildekode eller administrativ tilgang.	5 = Kan oppdages ved å gjette eller spore nettverkstrafikk 5 = En kritisk software lisens ”sier fra” på konsollet og i loggen om at den er i ferd med å gå ut på tid, men rutinene for å følge opp loggen og konsollet er mangelfulle.	8 = Svakheten er ”usynlig” (tikkende bombe), for eksempel et digitalt sertifikat løper ut på tid – ingen oppfølging av utløpstid. 9 = Detaljer om svakhetene er allerede offentlig kjent, og kan lett søkes opp på Internet. 10 = Svakheten er synlig i URL linjen eller i et skjema eller brukere kan uforvarende utløse skaden. 8 = ”Snikende fare” - allokert mengde diskplass ”sprekker” eller en database går full.

2. **Hvor vanskelig er det å utløse de(n) uønskede hendelsen(e)?**

0 = Svært vanskelig eller umulig, selv for administrator	5 = krever 1 eller 2 tiltak, kan kreve administratorrettigheter	10 = bare WEB browser og adresselinjen kreves, ingen autentisering. 10= Skaden er selvutløsende, jf. sertifikater som automatisk går ut på tid. Eller at en disk renner full.

Her er det et spørsmål om hvor vanskelig det er å utnytte svakhetene slik at de(n) uønskede hendelsen(e) skjer.

Dersom det for eksempel kreves at mange usannsynlige hendelser skjer samtidig, vil poengberegningen bli lav.

Likeså kan det bli få poeng dersom det kreves godt koordinerte og organiserte tiltak i tillegg til at det kreves høy autorisasjon. Det å utløse hver hendelse behøver ikke være komplisert, men koordinering mv. gjør det hele vanskelig gjennomførbart og dermed mindre sannsynlig. Det blir som å sette opp et korthus: hver ”hus” isolert sett er enkel å sette opp, men å fullføre huset er vanskelig. Det kreves ikke spesialkompetanse for å utløse de skadeutløsende

hendelser, men kompleksiteten kan gjøre gjennomføringen vanskelig hvis det er lite som kan gjøres for å redusere kompleksiteten.

3. Hvilken kompetanse kreves for å utløse de(n) uønskede hendelsen(e)?

0 = Grundig kjennskap til programmering/nettverk, spesialbygde/avanserte angrep	5 = Ondsinnet kode finnes på nettet, eller angrep er lett å utføre med tilgjengelige midler	10 = Gjennomsnittsbruker

Her tenkes det på krav til kunnskap, kompetanse og ressurser.

4. Hvor stort er skadeomfanget?

0 = ingen	5 = brukerdata er kompromittert eller berørt	9 = Systemet blir utilgjengelig for en lengre periode. 10 = Flere/alle systemer blir utilgjengelig for en lengre periode. 10 = En sentral utvikler har kopiert og solgt foretakets unike programmer. 10= Tilgangskontrollsystemet blir kompromittert og uvedkommende tildeler seg selv administrasjonsrettigheter i systemet og ødelegger systemer og sikkerhetskopier av systemer

Skadeomfanget må ta med direktekostnader ved en potensiell skade, kostnader knyttet til å reparere skader, til å få systemet opp i god stand, kostnader ved å ta i bruk vernetiltak og kontroller, kostnader ved tap av tillit og kostnader ved ikke å gjøre noe, dvs. opprettholde en høy risiko.

5. Hvor mange brukere blir berørt av skaden?

0 = Ingen	5 = Noen, ikke alle	10 = Alle brukere

Vurderingen skal ta hensyn til flere forhold; hvor mange er berørt og i hvilken grad rammes brukerne. At nettbanken er nede øyeblikket, berører i mindre grad en kunde som skal betale en regning som forfaller om 1 uke. En daytrader av aksjer som ønsker umiddelbart å komme ut av en aksjeposisjon, rammes i betydelig grad.

2.4 Innkapsle

Resultatet av forrige fase er en liste som viser sårbarhet, trussel og skade. Det er foretatt en totalvurdering av sårbarhet, trussel og skade. Totalvurderingen er uttrykt som en risikoscore. Listen er sortert synkende etter risikoscore.

Denne fasen består i å ta stilling til risiko, og eventuelt definere og utarbeide planer for å redusere risikoen.

Flere kategorier av risikoreduserende tiltak skal vurderes:

1. Dublering av systemer i produksjon (”speilsystemer”) og/eller personell, ut i fra tanken om at to identiske svakheter sannsynligvis ikke utløses samtidig
2. Etablere en reserveløsning
3. Redusere sannsynligheten for at de(n) uønskede hendelsen(e) skjer ved å herde systemet
4. Redusere skaden som oppstår dersom svakheten utløses
    a. Gjøre seg mindre avhengig av systemet
    b. Forsikre seg bort fra skaden som inntreffer
5. Akseptere risikoen, og eventuelt å gjøre regnskapsmessige avsetninger for å dekke en eventuell skade

Dersom ansvarlig velger å akseptere risikoen, skal hun skrive en erklæring som begrunner hvorfor risikoen aksepteres. Erklæringen skal signeres av eier av forretningsområdet. Erklæringen sendes så til gjennomgang og godkjenning i foretakets sentrale risikofunksjon, internrevisjonen og eventuelt andre interesserte.

Foretakets sentrale risikofunksjon godkjenner erklæringen bare dersom den ikke kan medføre skade på andre forretningsområder. I motsatt fall eskaleres beslutningen. Ofte godkjennes erklæringen, men med visse kompenserende kontroller som reduserer risikoen. Erklæringen er typisk gyldig i 6 til 12 måneder, avhengig av omstendighetene.

Nedenfor er listet noen eksempler på sårbarheter, trusler og uønskede hendelser som er hentet fra virkeligheten i senere tid. Vurderingene og tiltakene er imidlertid oppdiktet og er tatt med for illustrasjonsformål.

Eksempel 1: Vi har erfart at visse endringer utvider datamengden betydelig, og vi har hatt sprekk i en database som satte en tjeneste ut av drift. I og med at vi ikke var forberedt på denne situasjonen, tok det lengre tid enn nødvendig for å få nødvendig kapasitet på plass. Vi har undersøkt og vet at vi har en rekke andre datasett og vi har ikke oversikt over eventuelle konsekvenser for disse ved endringer i systemet.

Risikovurdering: Deltakerne i risikoteamet har forespurt dataavdelingen om endringene kan gi kapasitetsproblemer andre steder. Ingen i dataavdelingen har oversikt eller er i stand til å gi noe fyllestgjørende svar. Den ansvarlig føler det hele som en tikkende bombe og føler sterkt ubehag. Hun er særskilt betenkt over at det ikke synes å eksistere gode nok rutiner for ende til ende test av endringer av denne type. Vi antar at slik test ville avdekket problemene.

Oversikt og overvåking av datasett og fyllingsgraden av disse mangler. Det er derfor vanskelig å vite når datasettene vil ”sprekke”. Skaden er selvutløsende, det kreves ingen spesielle tilgang eller kompetanse. Skaden vil ramme systemet som basen betjener og vil ramme kunder i en begrenset periode. Riskoscore blir som vist nedenfor.

Oppdage	Utløse	Kompetanse	Skade	Kunder	Total
8	10	10	4	4	7,2

Eksempel 2: Vi har utviklet og produksjonssatt en kundetjeneste på WEB. Tjenesten var forsinket i forhold til plan. Testing ble det så som så med. Men ansvarlige på utviklingssiden mener å vite at all sluttbrukerfunksjonalitet ble testet. På grunn av dårlig tid er ikke testingen dokumentert enda. Tjenestene virker, ledelsen er svært fornøyd med produktet og anser produktet for å være en suksess. Kostnadene har vært i henhold til budsjett. Ledelsen anser tjenesten som ferdig og har nå fokus på lansering av en ny tjeneste.

Risikovurdering: Ansvarlig frykter at utviklerne bare har rukket å utvikle brukerfunksjonaliteten. Logging, feilmeldinger, sporingsdata osv. er ikke utviklet i tilstrekkelig grad. Deltakerne i risikoteamet har videre fortalt ansvarlige at en ”web-applikasjon” er ikke en ”web-applikasjon” – like viktig som å kode sluttbrukerfunksjonaliteten er det å ”herde” tjenesten, det vil si kode på en slik måte at tjenesten er beskyttet mot angrep. Ord som ”Cross Site Scripting”, SQL injection, og HTML Header Poisoning ble nevnt. Ansvarlig frykter at det ikke ble tid til å ”herde” tjenesten i tilstrekkelig grad. Det er behov for å gå gjennom koden og teste for angrep. Dette arbeidet må gjøres av ”kostbare” spesialister. Den ansvarlige er usikker på hvordan dette vil bli mottatt av ledelsen.

En gjennomsnitts-”hacker” vil fort teste seg frem til at koden nok ikke er vanntett. Blant annet vil hun fort oppdage at brukerinput blir ikke renset før svar sendes tilbake til brukeren, html blir returnert som kode ikke som literaler. Disse svakhetene gjør at ondartet kode kan returneres brukeren og gjøre skade der. Det er ikke vanskelig å lage ondartet kode og utgi denne for å komme fra web-tjenesten vår. Systemet vårt vil komme i et uheldig lys og brukerens PC kunne bli kompromittert. Risikoscore blir som vist nedenfor.

Oppdage	Utløse	Kompetanse	Skade	Kunder	Total
7	10	6	6	7	7,2

Eksempel 3: Ny innloggingsfunksjonalitet for en web-tjeneste er produksjonssatt. Leverandører av produkter og tjenester innen IT-sikkerhet hevder at det er utviklet ”Man in the Middle” angrep som gjør at angripere kan overta sesjonen mot tjenesten etter at rette bruker har logget seg inn.

Risikovurdering: Den ansvarlige har oppfordret leverandørene til å vise trusselen. En av leverandørene har demonstrert et tilsynelatende vellykket angrep. Ingen kunder har rapportert at de har vært utsatt for angrep. Den ansvarlige frykter for situasjonen som oppstår dersom det inntreffer et massivt angrep som gjør at tjenesten må stenges ned i en lengre periode. Tjenesten er basert på at kunden betjener seg selv. Etter hvert vil svært mange kunder benytte tjenesten. Dersom tjenesten måtte stenges ned, vil kundene forvente at de kan henvende seg til foretaket og få utført tjenesten der, noe foretaket ikke på noen måte har kapasitet til. Ansvarlige vurderer situasjonen slik at før volumet blir stort, må det utarbeides planer for kontinuitet og beredskap.

Nærmere undersøkelser viser at det er lett å styre til hvilken IP-adresse forespørsel og svar går. Det krever nok en viss kompetanse å utvikle et script som styrer IP-pakkene og som

forteller når rette bruker er innlogget og angriperen kan ta over sesjonen. Skaden på tjenesten antas å ville være betydelig og i verste fall vil tjenesten måtte stenges ned for en periode og omprogrammeres.

Oppdage	Utløse	Kompetanse	Skade	Kunder	Total
4	6	4	7	6	5,4

Eksempel 4: Den ansvarlige har lest i avisen om en Internettjeneste som ble angrepet. Angrepene kom fra en rekke ulike adresser og i et omfang som gjorde at tjenesten ble overbelastet og gikk ned. Dataavdelingen instruerte brannmuren til å avslå trafikk fra angripernes adresse, men det kan se ut som angriperen bytter adresse hele tiden. Angrepet har vart i tre uker nå og foretaket har store problemer med å betjene kundene.

Risikovurdering: Den ansvarlig frykter at tilsvarende angrep kan ramme dem. Foretaket har ikke reserveløsninger som kan håndtere en situasjon der internettjenesten er nede i lengre tid. Dataavdelingen forteller at kundene oppgir en kundeidentifikasjon ved pålogging. Virksomheten kontrollerer kundeidentifikasjonen som kunden oppgir. Kontrollen innebærer ganske mye prosessering. Blant annet hentes en god del kundeinformasjon inn i ”front end”, klar til å presenteres for kunden. Dette med tanke på at svarstiden overfor kunden skal være så kort som mulig. Dersom kunden ikke passerer kontrollene, blir kunden avvist. Den ansvarlige frykter for hva som vil skje dersom et automatisert script ”bomber” tjenesten med påloggingsforsøk. Hun lurer på om kontrollene kunne vært kodet bedre, for eksempel slik at prosesseringen i første omgang var begrenset til å identifisere kunden. Da vil ikke et ugyldig innloggingsforsøk okkupere maskinressurser i samme grad som i dag, og tjenesten vil være mindre sårbar for overbelastning. Den ansvarlige prioriterer høyt å få utført en analyse av dette og eventuell endre systemdesignet. Risikoscore blir som følger:

Oppdage	Utløse	Kompetanse	Skade	Kunder	Total
9	7	6	8	7	7,4

Eksempel 5: IT-organisasjonen varsler om at den versjonen av programvare (database) som foretaket benytter, må oppgraderes innen en gitt tidsfrist grunnet manglende støtte fra leverandøren etter denne dato. Oppgraderingen er omfattende og krever planlegging for testing og produksjonssetting og vil legge beslag på ressurser. For hvert år foretaket utsetter å ta kostnadene ved denne oppgraderingen, øker risikoen. Årsaken til dette er at kompetanse og støtte fra leverandøren gradvis trappes ned og at annen programvare ikke lenger leveres med støtte for integrering mot denne versjonen av programvaren.

Oppdage	Utløse	Kompetanse	Skade	Kunder	Total
8	5	6	7	7	6,6

2.5 Kontrollere

Det finnes utallige eksempler på foretak som har levd med en illusjon om at kontroller er på plass, men når tiltakene er blitt satt på prøve, så fungerer de ikke som forutsatt.

Nedenfor beskrives noen få virkelige hendelser fra den senere tid (sommer/høst 2007).

- Sikkerhetskopier viser seg å inneholde tomme datasett. Det har aldri vært noen reell test av tilbakeleggingsprosedyrer.

- Beredskapslister, herunder lister med navn på kontaktpersoner hos leverandører, er utdatert, med den følge at det i forbindelse med en unntakssituasjon tapes verdifull tid og oppstår dårlig samarbeidsklima.

- Viruskontroll på servere fungerer ikke som forutsatt.

- Deler av nettverket faller ned, reserve linjer fungerer ikke som forutsatt.

Fasen innebærer at det lages en plan og et opplegg for regelmessig testing av at kontrollene fungerer som forutsatt til enhver tid, og formidling av problemstillinger/resultater til de ansvarlige i foretaket.

Selv om foretaket har kontroller og har testet disse, kan foretaket rammes av trusler som setter IT ut av spill for kortere eller lengre perioder. I følge IKT-forskriften § 10 skal foretaket ha planer for hvordan virksomheten skal drives videre i tiden inntil IT-funksjonene er reetablert. Bestemmelsen sier blant annet at ”Det skal gjennomføres opplæring, øvelse og testing av reserveløsningene i et omfang som gir trygghet for at reserveløsningene fungerer tilfredsstillende. Testene skal dokumenteres slik at gjennomføring og resultat kan vurderes i ettertid”.

2.6 Oppsummere og kommunisere

Risikoprosessen og resultatet av denne skal dokumenteres. For foretak underlagt IKT-forskriften er kravet oppstilt i § 3.

Dokumentasjonen skal lagres, og

- dokumenterer ledelsens tolkning av sitt ansvar for risikoanalyse
- er et startpunkt for senere risikoanalyser
- er informasjon for nye ledere/ansatte
- gjør at andre enheter, for eksempel internrevisjonen, kan kontroller at foretakets policy blir fulgt.

I utgangspunktet står foretaket fritt i å bestemme dokumentasjonsformen. Men foretaket må sørge for at formen er slik at den tilfredsstiller eventuelle krav til ekstern revisjon, tilsyn og kontroll foretaket er underlagt. Foretaket må ha tilstrekkelig dokumentasjon av risikoanalysen til at interne og eksterne tilsynsorganer kan vurdere om lovbestemte krav til gjennomføring av risikoanalysen er oppfylt. En risikoanalyse som inneholder alle fasene ovenfor, og som dokumenterer viktige vurderinger som er gjort samt resultatet av fasene, antas å være tilstrekkelig.

Dersom analysene dokumenteres mange ulike steder i foretaket, kan det være hensiktsmessig å følge mye brukte, anerkjente standard verktøy for analyse og dokumentering.

BAS 5 - Evaluering av ulike metoder [3] inneholder en liste over slike, og en vurdering av hvilke type foretak verktøyet passer for.

For alle innenfor finanssektoren fremgår dokumentasjonskravet av Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT), § 3. Foretak underlagt bestemmelsen skal "… ha dokumentert en prosess for gjennomføring av risikoanalyser av IKT virksomheten".

De som gjennomfører risikoanalyser må kommunisere resultater fra analysen med foretakets ledelse, eventuelt med kunder og andre interessenter.

[3] http://www.proactima.no/pa/publicfile/download/Filer/Vedlegg%202%20-%20Metodeevaluering%20ver7.pdf

Vedlegg 1. Veiledninger

Beskyttelse av samfunnet 5 (BAS5) – Sårbarhet i kritiske IKT-systemer[4]
ISO 27005, Information technology -- Security techniques -- Information security risk management
ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements
ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management

Vedlegg 2. Valg av metode

BAS 5 - Evaluering av ulike metoder[5]

Vedlegg 3. Aktuell litteratur

Aven T. (2007) A unified framework for risk and vulnerability analysis and management covering both safety and security. Reliability Engineering and System Safety, 92, 745-754

Aven, T. (2006) Expressing risk in a security context. ESREL 2006. pp. 2577-2582

Wiencke, HS, Aven, T. Hagen, J. (2006) A framework for selection of methodology for risk and vulnerability assessments of infrastructures depending on ICT. ESREL 2006, pp. 2297-2304

Aven, T. og Wiencke, H. (2006). Rammeverk for gjennomføring av risiko- og sårbarhetsanalyser av samfunnskritisk infrastruktur. I NoU 2006:6, vedlegg 9. s 262-267

Vedlegg 4. Verdivurdering og klassifisering

Utdrag fra KOBI-rapporten:

8 INNDELING AV INFORMASJON I KLASSER

8. 1 Om verdivurdering og behovet for beskyttelse av informasjon

Dagens samfunn karakteriseres ofte som et informasjonssamfunn. Vi informerer hverandre i en nesten endeløs strøm, og selv om vi ikke anser all den informasjonen vi mottar som like interessant, er det å utveksle informasjon sett på som verdifullt. Informasjonsutveksling er en viktig forutsetning for at vårt samfunn skal fungere, og er derfor positivt. Dette er også en grunn til at vi tilstreber mest mulig åpenhet i informasjonsbildet. I den offentlige forvaltning er dette prinsippet gitt lovs form ved Lov om offentlighet i forvaltningen.

[4] http://rapporter.ffi.no/rapporter/2007/01204.pdf
[5] http://www.proactima.no/pa/publicfile/download/Filer/Vedlegg%202%20-%20Metodeevaluering%20ver7.pdf

Informasjon kan også misbrukes. Vårt behov for å beskytte informasjon springer ut av det forholdet at den har en verdi som kan gå tapt for oss eller føre til et tap av verdier dersom den blir misbrukt, ødelagt eller endret. Vi kan finne eksempler på slik type informasjon på alle nivåer i samfunnet.

Informasjon om hvor vi har gjemt reservenøkkel til huset deles ikke med andre enn akkurat de som har behov. Det samme gjelder koden til sykkellåsen. Vi forutsetter at ingen urettmessig kan endre opplysningene på et gjeldsbrev. En virksomhet passer godt på den informasjonen som er viktig for at akkurat de skal gjøre det godt i markedet, og vil sikre at nødvendige opplysninger er tilgjengelige når beslutninger skal tas. Landets myndigheter har et ansvar for at ikke informasjon som kan misbrukes mot innbyggerne kommer uvedkommende i hende, for ikke å snakke om slik informasjon som kan skade landets sikkerhet.

På alle nivåer finnes det informasjon som det er et behov for å beskytte i ulik grad. Det er ikke sikkert at de som ”eier” informasjon er like bevisste på hvilken verdi informasjonen kan ha, også med tanke på misbruk. Verdivurdering av informasjon dreier seg om å analysere informasjon med tanke på hvilke konsekvenser det kan få dersom denne informasjonen går tapt, endres eller kan bli misbrukt av noen med ondsinnede hensikter.

Det faktum at man anser informasjon for å ha en verdi, innebærer at det eksisterer et skadepotensial dersom informasjonen blir kjent for uvedkommende. Informasjonen kan eksempelvis inneholde opplysninger om sårbarheter eller handlingsmønstre i en krisesituasjon. Målsettingen med informasjonsbeskyttelsen er nettopp å hindre at uvedkommende utnytter våre sårbarheter til å påføre oss skade. Slik skade kan komme til uttrykk gjennom krenkelse av individers integritet og private sfære, gjennom kriminelle handlinger, spionasje, sabotasje eller i verste fall terror- eller krigshandlinger. Forebygging av disse truslene avhenger av at vi evner å verdivurdere informasjon, og å gi kritisk informasjon den nødvendige beskyttelse.

Det kan være en stor utfordring å beskytte informasjon på en tilfredsstillende måte. I mange tilfeller vil det kunne føre til mer kompliserte arbeidsformer, og det kan også gjøre det nødvendig å sette i verk tiltak som krever både økonomiske og andre ressurser. Verdivurderingen vil i stor grad virke dimensjonerende på hvilke beskyttelsestiltak som settes i verk. Av den grunn er det derfor nødvendig å ha et nyansert register av tiltak som kan benyttes. Men det er også viktig at selve verdivurderingen gjennomføres på en grundig måte, slik at de tiltakene som til slutt velges står i et rimelig forhold til de verdiene som skal beskyttes.

Det finnes noen enkle spørsmål som kan gi grunnlag for en nærmere vurdering av informasjonens verdi:

- Hvordan kan informasjonen misbrukes?
- Hvem kan misbruke informasjonen?
- Hva blir konsekvensen dersom informasjonen blir tilgjengelig for uvedkommende?
- Kan informasjonen påføre skade for andre?
- I hvilket tidsrom har informasjonen verdi?

Hvilken informasjon som til en hver tid vil ha et beskyttelsesbehov, vil aldri være helt statisk over tid. Det vil alltid være et tilsig av ny informasjon som bør beskyttes, samtidig som behovet for beskyttelse av tidligere ansette verdier kan falle fra eller bli redusert. Det finnes informasjon som bare trenger beskyttelse ”over natten”, mens annen informasjon kanskje må beskyttes i mange tiår.

En utfordring ved verdivurderingen er at elementer av informasjon som hver for seg kan virke harmløs vil kunne endre karakter når de sammenstilles med andre elementer som også virker harmløse og er åpent tilgjengelige. Likeså kan informasjon som for en part er ufarlig utgjøre en trussel for tredjeparts virksomhet, hvis den kommer på avveie. Dilemmaet ligger i at det kan være en fare for at for stor del av den informasjonen vi omgir oss med og som vi faktisk trenger, blir vurdert som kritisk. Dette kan dreie seg om informasjon som, dersom den ikke er tilgjengelig når vi trenger den, kan føre til skade eller tap av verdier. Det vil derfor være viktig at den som setter sammen og forvalter slik informasjon gjør en kritisk vurdering om informasjonen for eksempel bør skjermes iht. Sikkerhetsloven eller på annen måte.

8.2 Inndeling i klasser

I en verdivurdering er det opp til virksomhetene selv å vurdere kritikalitet til informasjonen. ref. kap. 8.1. For å dele informasjonen inn i klasser med tilhørende krav til beskyttelse, har KOBI valgt en inndeling i fire klasser. Dette er begrunnet i internasjonale standarder og beste praksis fra flere områder. En inndeling med tre klasser vil etter gruppens vurdering ikke gi tilstrekkelig differensiering og faren for overgradering vil øke. En inndeling i flere enn fire klasser har gruppen vurdert til å gi en vanskeligere brukersituasjon samt en uoversiktlig differensiering.

De fire klassene gis følgende betegnelser etter hvor store krav som stilles til hhv konfidensialitet, integritet eller tilgjengelighet:

1 – Lav

2 – Middels

3 – Høy

4 – Svært høy

Gruppens vurdering er at krav til konfidensialitet, integritet eller tilgjengelighet sjelden vil være sammenfallende og komme i samme beskyttelsesklasse. Det kan for eksempel være at informasjon med meget store krav til integritet ikke har tilsvarende krav til konfidensialitet eller tilgjengelighet. Vi har derfor valgt å beskrive krav til konfidensialitet, integritet og tilgjengelighet i hver av klassene separat i tabellen.

Tabell 1: Inndeling i klasser

Klasser /Område	Konfidensialitet	Integritet	Tilgjengelighet
Lav	Informasjon som ikke kan skade noe eller noen basert på virksomhetens bedømmelse, relevant lovverk eller reguleringer. Informasjon som alle kan få se, og som ikke har noen krav til skjerming. Eier kan gi egne bestemmelser for publisering som for eksempel tilgjengeliggjøring eller skjerming for søkemotorer på Internett. I utgangspunktet vil denne klassen gjøres tilgjengelig for anonyme brukere.	Informasjon der feil ikke påvirker beslutningsprosesser. Eier kan gi egne bestemmelser for kvalitetssikring av opplysningene.	Informasjon der utilgjengelighet har liten betydning for virksomheten.
Middels	Informasjon som kan gi moderate skader for virksomhetens interesser eller enkeltparter hvis den kommer uautoriserte i hende. Informasjon hvor tilgang er begrenset til organisasjonen, samt andre virksomheten har autorisert Informasjon skal gis / underlegges kontrollert distribusjon.	Informasjon som i noen grad påvirker beslutningsprosesser. Dersom feil oppstår, kan det gi moderat skade eller verditap og medføre svekket omdømme for bruker eller andre. Kan føre til merarbeid å gjøre oppretting etter feilen.	Informasjon der utilgjengelighet kan føre til noe etterslep og redusert servicenivå.

Klasser /Område	Konfidensialitet	Integritet	Tilgjengelighet
Høy	Informasjon som kan føre til alvorlig skade for virksomhetens interesser, samarbeidspartnere, enkeltpersoner og samfunnet om den kommer uautoriserte i hende. Informasjon der innsyn må begrenses til autoriserte brukere med tjenstlig behov. Virksomheter må stille krav om en taushetserklæring ved utveksling av slik informasjon ut over virksomhetens interne distribusjon.	Informasjon som direkte påvirker beslutninger og der feil kan føre til betydelig skade eller verditap for virksomheten, tredjepart eller samfunnet.	Informasjon der utilgjengelighet vil føre til store etterslep eller stans i vesentlige tjenesteleveranser.
Svært høy	Informasjon som kan gjøre katastrofal skade på virksomhetens interesser, samarbeidspartnere, enkeltpersoner og samfunnet om den kommer uautoriserte i hende. Informasjon som er kritisk for virksomheten og som må begrenses til et fåtall nøkkelpersoner. Informasjon som kun skal gis til autoriserte brukere etter kontrollert vurdering. Virksomheter må stille krav om en taushetserklæring ved utveksling av slik informasjon ut over virksomhetens interne distribusjon.	Informasjon der feil i beslutningsgrunnlaget vil kunne føre til feilvurderinger med fatale konsekvenser.	Informasjon der utilgjengelighet er katastrofalt dvs. selv korte avbrudd vil føre til kritiske situasjoner.

Merk at fordi kravet til beskyttelse kan være på forskjellig nivå for de forskjellige sikkerhetsegenskapene så kan dette påvirke beskyttelsestiltakene. For eksempel kan vi ha informasjon med lav konfidensialitet, høy integritet og middels tilgjenglighet. Selv ved lesing av denne informasjonen vil det være krav om autentisering av informasjonen. Dette kan medføre at brukeren må benytte autentisering, til tross for at konfidensialitetsnivået tilsier at autentisering ikke bør brukes.