FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Veiledning til IKT-forskriftens § 5 "Sikkerhet"

August 2013

Innhold

1 Innledning

Finansforetakene har brakt sine tjenester ut til kundene gjennom elektroniske systemer som nettportaler og nettbanker. Kundekommunikasjon går via Internett og mobilnett, og foretakene kan nås fra hele verden. Finansforetakene, spesielt bankene, har i tillegg elektronisk transaksjons- og informasjonsutveksling seg i mellom, mot offentlige myndigheter, og til eksterne tjenesteleverandører og datasentraler. Enkelte tjenesteleverandører befinner seg i utlandet, i større eller mindre grad under andre legale systemer og kulturer.

Den vesentligste delen av betalingsstrømmene i Norge går i elektroniske kanaler som må beskyttes på en betryggende måte. Også annen informasjon i foretakenes systemer representerer betydelige verdier for foretakene og kundene. Mengden dokumenter som utveksles elektronisk, øker stadig. Det er viktig at informasjonen oppbevares, behandles og utveksles på en betryggende måte, slik at den forblir riktig, er skjermet for uvedkommende og er tilgjengelig for foretaket og kunden.

Denne veiledningen er ment å være en hjelp for foretakene i hvordan de kan sikre at de etterlever kravene til informasjonssikkerhet som framgår av IKT-forskriftens § 5 [1]. Ordene sikkerhet og informasjonssikkerhet brukes i denne veiledningen om sikring av data/ informasjon og sikring av informasjonssystemer og utstyr som brukes i foretakets tjenesteproduksjon. Sikring av f.eks. utlån er ikke et tema for denne veiledningen.

2 Forskriftsmessige krav til sikkerhet i IKT-systemene

Den sentrale bestemmelsen i denne sammenheng er IKT-forskriftens § 5. Hele IKT-forskriften er imidlertid relevant, og en må også ta hensyn til andre paragrafer i forskriften ved utforming av sikkerhetsopplegg.

> ***§ 5.*** *Sikkerhet*
> *Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet, jf. § 1, mot skader, misbruk, uautorisert adgang og endring, samt hærverk. Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene. Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare. Oppfyllelse av kravene til informasjonssikkerhet for personopplysninger etter forskrift av 15. desember 2000 nr. 1265 til personopplysningsloven skal anses som oppfyllelse av kravene i paragrafen her.*

Andre viktige forskrifter angående informasjonssikkerhet er personopplysningsforskriften [3] og forskrift om risikostyring og internkontroll [2].

IKT-forskriften reflekterer anerkjent praksis, og er ikke strid med eller gjør standarder det er referert til i dette dokumentet overflødige.

3 Berørte områder av IKT-virksomheten

Bestemmelsene i IKT-forskriftens § 5 skal sikre at foretakene ivaretar tilstrekkelig sikkerhet for foretakets systemer, løsninger og data, og de gjelder systemer i eget foretak og eventuelt utkontrakterte systemer. I tillegg gjelder de for kommunikasjonsleddene som knytter systemene sammen. Dette omfatter også IKT-infrastruktur som deles av flere foretak. Sikringstiltakene skal omfatte retningslinjer, rutiner og organisering for å sikre konfidensialitet, integritet og tilgjengelighet. Det er også viktig at foretaket har rutiner som sikrer oppfølging av etterlevelse av egne retningslinjer og sikkerhetskrav.

IKT-forskriftens § 5 omfatter i tillegg krav om å beskytte utstyr mot skader og hærverk, krav til adgangskontroll og fysisk sikring av bygninger.

4 Etterlevelse

4.1 Styrets ansvar

I henhold til forskrift om risikostyring og internkontroll [2] er det styret som skal påse at foretaket har tilstrekkelig sikring. Styret skal fastsette mål og strategi for foretaket, samt overordnede retningslinjer for virksomheten. Utarbeidelse av sikkerhetspolicy og klar

organisatorisk forankring av sikkerhetsarbeidet, med oppfølging og rapportering, er viktig i denne sammenheng.

4.2 Sikkerhetspolicy

IKT-forskriften § 2 første ledd sier: *"Foretaket skal fastsette overordnede mål, strategier og sikkerhetskrav for IKT-virksomheten".* I IKT-forskriften § 5 vises det også til personopplysningsforskriften [3], som setter lignende krav: § 2-3 tredje ledd: *"Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi."*

Foretakene kan ha ulik begrepsbruk for, og oppdeling av, styrende dokumenter for sikkerhet. Begreper som strategi, policy, retningslinjer, prinsipper og kravdokumenter benyttes. Det er vesentlig at styrende dokumenter for sikkerhetsarbeidet finnes, ikke hva de benevnes. En bruker i denne veiledningen betegnelsen "sikkerhetspolicy".

Formålet med en sikkerhetspolicy er at foretakets styre gir retning og støtte for informasjonssikkerhet i samsvar med foretakets mål, forretningskrav og lover og forskrifter. I tråd med gode prinsipper for styring og kontroll med informasjonssikkerhet skal foretaket:

1. integrere sikkerhet i foretakets aktiviteter
2. påse at sikkerhetsnivå og sikkerhetstiltak er basert på risikovurderinger
3. påse at foretakets investeringer innenfor sikkerhet er basert på å oppnå foretakets mål og er i samsvar med sikkerhetskravene
4. sikre samsvar med interne og eksterne krav – herunder regulatoriske krav.
5. stimulere sikkerhetstenkning i foretaket
6. evaluere sikringstiltakene i forhold til foretakets mål og resultater

En sikkerhetspolicy skal godkjennes av styret, gjøres tilgjengelig og formidles til alle ansatte og andre, som eksterne parter og offentlige myndigheter, som trenger å kjenne til den. Policyen bør uttrykke styrets forpliktelse og stake ut retningen for sikkerhetsarbeidet. Dokumentet bør blant annet inneholde:

a) foretakets definisjon av informasjonssikkerhet, og betydningen av sikkerhet som en mekanisme for å dele informasjon på en forsvarlig måte
b) en bekreftelse fra styre/ledelse om at den støtter de oppførte målene og prinsippene for informasjonssikkerhet og at disse er i samsvar med foretakets mål og strategi
c) plassering av ansvar for informasjonssikkerhet generelt, og ansvar for avviks-håndtering spesielt, inkludert rapportering av hendelser
d) henvisninger til dokumenter som støtter opp om policyen, med mer detaljerte krav, retningslinjer, prosedyrer eller regler som styremedlemmer, ansatte, brukere og eksterne skal følge

Policyen skal revideres med jevne mellomrom, og når det inntreffer endringer eller behov for nye krav og økt eller endret oppmerksomhet for å sikre at den fremdeles er hensiktsmessig og effektiv. Styre/ledelse skal gjøres oppmerksom på vesentlige endringer innen lover, regler og kontrakter som får konsekvenser for sikkerhet i de ulike jurisdiksjonene der foretaket er etablert eller har utkontrakteringsavtaler.

Policyen må ha en eier som påtar seg ansvar for utvikling, evaluering og revidering, og den nye utgaven skal godkjennes av styret.

4.3 Dokumentasjon av roller og ansvar

Ansvar for informasjonssikkerhet skal være definert og tilordnet roller i foretaket.
Roller og ansvar må derfor avklares mellom avdelinger og i forhold til leverandører, og dette skal dokumenteres. Ledelsen må plassere ansvar for livsløpene til informasjon, data og transaksjoner.

Forskrift om risikostyring og internkontroll [2] fastslår at foretaket også har ansvaret for risikostyring og internkontroll i de deler av virksomheten som er utkontraktert, det samme gjør IKT-forskriften [1]. En må vite hvor ansvaret er når en arbeidsoperasjon utkontrakteres til en leverandør eller annen del av foretaket/konsernet i et annet land.

Definerte roller og ansvar er spesielt viktig ved alvorlige hendelser, hvor det er av vesentlig betydning at arbeidet blir koordinert på en effektiv måte. Det må jevnlig testes at samhandling virker.

Styret må se til at slik dokumentasjon foreligger og at den er oppdatert.

4.4 Administrasjonens ansvar

Administrasjonen har ansvar for å følge opp sikkerhetspolicyen gjennom løpende sikkerhetsarbeid, og må jevnlig vurdere om sikringstiltak er passende i forhold til foretakets risikovurdering. Dette gjelder også for utkontraktert virksomhet. Prosedyrer og rutiner må være utformet slik at endringer fanges opp og nye forhold som avdekkes, vurderes raskt.
Ved større endringer med betydning for informasjonssikkerheten, og ved hendelser i foretaket eller næringen, bør det foretas nye risikovurderinger. Det vises i denne sammenheng også til forskrift om risikostyring og internkontroll [2] og personopplysningsforskriften [3].

Administrasjonen må gi styret relevant og tidsriktig informasjon som er av betydning for foretakets risikostyring og internkontroll, herunder informasjon om nye risikoer og eventuelle brudd på regulatoriske bestemmelser. Rutiner og risiko skal være dokumentert.

Rapportering til ledelse og styre skal skje minst årlig. Det må i rapporteringen være mulig å følge en risiko over flere perioder, slik at utviklingen kommer fram (alvorlighet/ sannsynlighet).

Manglende sikkerhet kan føre til høy risiko og påføre foretaket kostnader og investeringer i tiltak. Resultatet av investeringene vises i hovedsak som fravær av uønskede hendelser. Derfor er det vesentlig at det jevnlig evalueres om sikkerhetstiltakene dekker de viktigste risikoområdene, og om de er effektive også etter økonomiske mål.

4.5 Krav om prosedyre for sikkerhet

Det viktigste kravet i IKT-forskriftens § 5 er kravet om at foretaket skal ha en prosedyre for å ta vare på sikkerheten i foretakets IKT-bruk: *"Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av* […]*."*. IKT-forskriften setter også krav til risikoanalyser, og prosedyren

skal basere seg på resultater fra disse analysene. Tiltakene skal skaleres etter de truslene som avdekkes. Kravet til sikkerhetsvurdering er at det skal gjennomføres regelmessig, minst årlig eller ved betydelige endringer, og det krever en syklisk prosess. Se vedlegg A.

4.6 Risikovurdering

IKT-forskriften § 3 stiller følgende krav til foretaket:

- *Foretaket skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene.*
- *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.*

De spesifikke sikkerhetskravene er angitt i § 5 i IKT-forskriften.

Her vises det også til personopplysningsforskriften [3]:

- § 2-4 andre ledd: *Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.*
- § 2-5 første ledd: *Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig*.

Også forskrift om risikostyring og internkontroll [2] stiller krav om gjennomføring av risikovurderinger.

- § 6 første ledd: *Foretaket skal løpende vurdere hvilke vesentlige risikoer som er knyttet til virksomheten. Ved endringer eller etablering av produkter og rutiner av vesentlig betydning skal en slik risikovurdering foreligge før virksomheten igangsettes.*

Her er det viktig å merke seg at risikovurderingen skal gjøres før endringer iverksettes, slik at en også kan iverksette tiltak for å avhjelpe eller redusere risiko som oppstår ved endringen.

Risiko- og sårbarhetsanalyser er nødvendige for å avdekke trusler (mulige uønskede hendelser) og sårbarheter, som kan få store konsekvenser for foretaket, og som det må sikres mot. Se beskrivelse av tiltak i Finanstilsynets veiledning for gjennomføring av risiko- og sårbarhetsanalyser [8]. Analysen skal avdekke trusler og identifisere tiltak for å avhjelpe disse truslene. Det bør vurderes om tiltakene vil medføre endringer i foretakets sikkerhetspolicy og sikkerhetssystem.

Etter gjennomføring av tiltakene vil det alltid være en viss restrisiko. Det bør framgå av dokumentasjonen at risikoeier aksepterer restrisikoen. Merk likevel at akseptanse av risiko skal ta hensyn til lover og forskrifter. Risikoer som kan føre til brudd på regulatoriske krav, kan ikke aksepteres.

IKT-forskriften bruker i enkelte sammenhenger generelle uttrykk som *"… av betydning for foretakets virksomhet …"*. Det vil derfor være nødvendig at den enkelte virksomhet selv avpasser nødvendig detaljeringsgrad til virksomhetens størrelse, behov og viktighet. Jo flere kunder som er avhengige av virksomhetens produkter og tjenester, jo viktigere er det også at virksomheten utfyller IKT-forskriften med egne krav til sin IKT-virksomhet.

4.7 Klassifisering av systemer og informasjon

Ikke alle systemer og data er like betydningsfulle for foretaket, av samme følsomhet for eksponering overfor utenforstående eller utsatt for samme trusler. Systemer og data kan derfor sikres på ulike måter og nivåer. IKT-forskriften gir ikke eksplisitt regler om ulik klassifisering, men i personopplysningsforskriften [3] heter det i § 2-1 *"Forholdsmessige krav om sikring av personopplysninger"*:

Reglene i dette kapittelet gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene.
Der slik fare er til stede skal de planlagte og systematiske tiltakene som treffes i medhold av forskriften, stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd.

Systemene bør derfor gjennomgås og klassifiseres ut fra krav til konfidensialitet, integritet og tilgjengelighet, og sikkerhetstiltakene bør avpasses tilsvarende. Hvor sensitiv og kritisk informasjonen er, vil variere. Dermed vil også sikringstiltakene variere, men må kunne optimaliseres i forhold til ressursbruk. Det vises i denne sammenheng til KOBI-rapporten [11], hvor klassifisering er gjennomgått.

Systemeier, som oftest er foretakets forretningsside, er ansvarlig for klassifiseringen av egne systemer og tilhørende data, og må ta eierskap til klassifiseringsarbeidet.

4.8 Informasjonssikkerhet i prosjekter

Informasjonssikkerhet bør være en del av alle IKT-prosjekter. Risikovurdering av prosjekt og leveranser (eksempelvis system som lages/kjøpes/videreutvikles) bør foretas i en tidlig fase for å identifisere og integrere relevante sikringstiltak og opplegg for målinger. Ansvarlige fra forretningssiden bør ta ansvaret for, eller involveres i, risikovurderingen. Ved system-utviklingsprosjekter bør krav til sikkerhetsopplegg, stabilitet og målinger være en del av kravspesifikasjonen.

4.9 Krav om beskyttelse

IKT-forskriftens § 5 "Sikkerhet" stiller krav både til fysisk sikring og tilgangskontroll for utstyr: "[…] *beskyttelse av utstyr, systemer og informasjon* […] *mot skader, misbruk, uautorisert adgang og endring, samt hærverk."*. Foretaket må vurdere disse kravene i forhold til sitt behov. Her gjelder foretakets vurderinger fra risikoanalysen og klassifiseringsarbeidet, jf. avsnitt 4.6 og 4.7. Et system som kun gir informasjon, og som ikke er koblet opp mot sensitive bakenforliggende systemer, krever ikke samme sikring som for eksempel en nettbank, se f.eks. FFIEC – Information Security – IT Examination Handbook [12].

I vedlegg B i denne veiledningen er det en "mapping" av kravene om beskyttelse i § 5 mot kontrolltiltak i annex A i ISO 27001. Det kan være nyttig å gå gjennom de refererte kapitlene i standarden og vurdere dem mot krav til beskyttelse av utstyr, systemer og informasjon i eget foretak.

Eksempel:
Bærbart utstyr kan ikke sikres på den samme fysiske måte som stasjonært utstyr. Mye ansvar blir her lagt på den enkelte bruker som må være godt informert om foretakets retningslinjer for bruk og oppbevaring/ transport av slikt utstyr. I tillegg må foretaket ha tiltak for sikring av systemer og informasjon på bærbart utstyr som PC-er, minnepinner, lesebrett og mobiler. Merking, bruk av passord og kryptering kan være stikkord i denne sammenheng.

Både hardware og software må vedlikeholdes og oppdateres slik at foretaket er sikret at best mulig støtte og service er tilgjengelig. Oppdatert basisprogramvare er også en sikring i seg selv.

4.10 Sikkerhet knyttet til ansatte og tillitsmenn

Sikkerhet i IKT-forskriftens betydning er knyttet både til IT-systemer og strategier, forvaltning, intern kontroll, rutiner og menneskelig samhandling. Ansatte, styremedlemmer og innleid personell vet mye om foretaket og dets kunder. De må forholde seg til etiske regler, prosedyrer og opplæring for ikke å avgi konfidensiell informasjon. Både ved ansettelser og besøk kan det være behov for signerte taushetsavtaler knyttet til sikkerhet. Styremedlemmer er ikke ansatt i foretaket. Informasjon til f.eks. styret sendes ofte elektronisk, og det må finnes beskyttelse også for slik informasjon.

Foretaket bør utvise ekstra omhu ved ansettelse i spesielle stillinger som f.eks. systemadministratorer, roller med tilgang til kryptografiske nøkler og kredittkortinformasjon eller ansatt som arbeider med tilgangskontroll og/eller sikkerhetsløsninger. Foretakene bør ha retningslinjer for slike vurderinger. Foretaket må ha rutiner for å deaktivere autorisasjon ved avslutning av et ansettelsesforhold/engasjement.

4.11 Systemforvaltning og tilgang

Tilgangskontroll til informasjon og data sikrer mot misbruk av informasjon og mot ulike typer av datakriminalitet.

Sikring mot uautoriserte endringer tas hånd om av et endringsregime og separasjon av drift og utviklingsmiljøene. Det bør tilstrebes et autorisasjonsregime som minimerer privilegier og skiller klart mellom roller.

Ved tildeling av tilgangsrettigheter må hensikten med systemer og informasjon ivaretas. Systemer og data skal være tilgjengelige for foretaket og dets brukere i henhold til behov og foretakets forpliktelser overfor kundene. Regulatoriske krav i denne sammenheng framgår av IKT-forskriftens §§ 8, 10 og 11. Disse områdene omhandles ikke videre i denne veiledningen.

4.12 Krav til autorisasjon

I § 5 heter det: *"Videre skal prosedyrene inneholde retningslinjer for tildeling, endring, sletting og kontroll med autorisasjon for tilgang til IKT-systemene."*
En slik prosedyre bør som minimum inneholde:

- En sikker registreringsprosess for nye brukere, eventuelt må det kreves legitimasjon.

- Prosess som autentiserer brukerne ved etterfølgende aktiviteter, innlogginger.
- Et autorisasjonssystem for å styre tilgang til de ulike ressursene.
- En overvåkingsprosess som følger opp tilgangsrettighetene tildelt den enkelte bruker, spesielt ved skifte av stilling eller arbeidsområde.
- Logging ved bruk av spesielle privilegier, samt endringer.
- Rapportering av bruk, statistikk, slik at avvik kan avdekkes.
- Periodiske lister over tildelte rettigheter som ledelsen skal kontrollere.

En god sjekkliste finnes i ISO 27001 – Annex A A.11

Merk at krav om logging av oppslag i kundedata blir tatt inn i lovverket fra 31. mars 2013.

4.13 Krav til målbarhet

I § 5 "Sikkerhet" vises det til at: *"Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare."*

Måling må i største mulig grad være integrert i systemene, slik at målinger blir mest mulig automatiske. Målene må være konkrete og kvantifiserbare, uttrykt i tall- og måleenheter, og målingene bør være reproduserbare.

Forventninger og mål for sikkerhetssystemet bør jevnlig sammenlignes med målingene for å avdekke mulige hull og mangler i opplegget. Det er også viktig å vurdere om tiltak identifisert ved risikoanalyser er riktige og tilstrekkelige, og om de virker etter hensikten. Også her kan målinger sammenlignes med forventningene, for å se om tiltakene er effektive. Boken *Security Metrics* [10] gir en god oversikt over sikkerhetsmålinger og anvendelse av disse. Eksempel på forhold som bør måles, kan være:

- Antall avvisninger i brannmurer
- Antall forsøk på uautorisert adgang
- Antall brukere med administrasjonsrettigheter
- Antall aksesser mot sikkerhetslogger
- Tilgjengelighet og pålitelighet, slik som:
  oppetider, planlagte nedetider, ikke planlagte nedetider, gjennomsnittlig tid mellom feil ("Mean Time Between Failures"), tid for oppstart etter en feilsituasjon, antall endringer

For applikasjoner:
Antall feil etter endringer, feil i forhold til størrelse (omfang) av applikasjoner.

Jevnlig oppfølging av målinger og sammenligning med historiske verdier for området, vil avdekke uregelmessigheter og avvik. Disse bør analyseres nærmere da det kan avdekke trusler (uønskede hendelser). For eksempel kan økende grad av avviste påloggingsforsøk indikere et systematisk forsøk på å bryte gjennom autorisasjonssystemet.

Trusselbildet er i stadig forandring, og det bør revideres både jevnlig og ved spesielle hendelser i næringen. Foretaket bør også sammenholde endringer i trusselbildet med målinger, for eventuelt å legge til målinger for nye områder. Sårbarheter bør også revideres ved endringer og oppgraderinger.

5 Nærmere beskrivelse av sikkerhetsprosedyren

5.1 Viktige kilder til krav

Krav til sikkerhetsopplegg kommer primært fra følgende kilder:

- Foretakets sikkerhetspolicy
  Foruten å beskrive områder som skal sikres, skal en her beskrive (målbare) mål for sikkerhetstiltakene og kriterier for aksept av (rest-)risiko.
- Foretakets sikkerhetspolicy skal avgrense område for sikring slik at det passer til foretakets forretningsområde og behov. Mindre aktører vil naturlig ha en annen vurdering av trusselnivået enn større. Sikringstiltakene bør skaleres tilsvarende så ikke kostnadene blir urimelige. Det bør begrunnes dersom områder utelates.
- Lovmessige og regulatoriske krav
- Kontraktsmessige forhold
- Sårbarheter avdekket i risiko og sårbarhetsanalysen
  De risikoreduserende tiltakene vil kunne inngå som nye krav til sikkerhetsopplegget.
- Varsler fra bransjeorganisasjoner og andre aktører i bransjen
- Eksternt trusselbilde beskrevet av for eksempel overvåkings- og tilsynsorganer
- Finanstilsynets årlige ROS-analyser [13]

5.2 Den operative prosessen

IKT-forskriften krever en syklisk prosess, og det legges også til grunn i anerkjente sikkerhetsstandarder. "Plan-Do-Check-Act"[1] (PDCA) er en vanlig metode for kvalitetsarbeid og er fyldigere beskrevet i ISO 27001-standarden [4]:

Planlegg:
Etabler sikkerhetspolicy, mål, prosess og prosedyrer som er relevante for å håndtere risiko og forbedre informasjonssikkerheten. Slik kan man levere resultater i samsvar med foretakets overordnede mål.

- Velg ut de truslene det skal sikres mot.
- Planlegg hvordan det skal sikres mot disse truslene. Planlegg organisasjon og dokumenter regler.
- Sørg for at ledelsen godkjenner planene.

Utfør:
Implementer og se til at sikkerhetssystemet virker iht. mål, kontroller, prosesser og prosedyrer.

- Definer hvordan sikringstiltakene skal måles og utarbeid detaljplaner.
- Iverksett sikringstiltakene fra planen.

[1] For bakgrunn, se for eksempel omtale av PDCA på Wikipedia: http://en.wikipedia.org/wiki/PDCA

- Etabler organisasjon og skaff eventuelt utstyr og systemer.
- Definer og sett i verk operative prosedyrer for overvåking av sikringstiltakene.
- Sikre at foretaket har tilstrekkelig kompetanse for å ivareta sikkerhetshendelser.

Kontroller:
Vurder og mål effektivitet og kvalitet av prosessene for sikkerhetssystemet opp mot målsettingen. Vurder og rapporter resultat til ledelsen.

- Overvåk systemet og bruk prosedyrene.
- Analyser sikkerhetshendelser og bruk av prosedyrer for avvikshåndtering.
- Saml målinger og måltall iht. plan.
- Følg med på statistikk og trender, og påse at kvalitet opprettholdes. Analyser eventuelle anomalier og finn utløsende faktorer og bakenforliggende årsaker til disse.
- Vurder effektiviteten i tiltakene etter planlagte intervaller og vurder også restrisiko.
- Gjennomfør interne gjennomganger av sikkerhetssystemet.
- Logg hendelser og forhold som kan påvirke effektiviteten i sikkerhetssystemet.

Beslutt:
Vurder korrigerende og forebyggende tiltak, basert på gjennomganger av sikkerhetssystemet og annen relevant informasjon. Slik kan man oppnå kontinuerlig forbedring.

- Avklar forbedringer til sikkerhetssystemprosessen, tilhørende prosedyrer, og kontroller.
- Sørg for korrektive tiltak for eventuelle avdekkede avvik.
- Vurder preventive tiltak for trusler for å minske konsekvenser av eventuelle uønskede hendelser/restrisiko.
- Vurder eventuelle interne og eksterne sikkerhetsanbefalinger.
- Følg opp overfor operatører med informasjon, opplæring og eventuelt andre personaltiltak.
- Sørg for god informasjon til alle relevante interessenter.
- Se til at forbedringer har fått tilsiktet virkning.
- Fjern eller minimaliser eventuelle effektivitetshindringer i systemet.
- Vurder kostnadsreduserende tiltak og prosessforbedringer.
- Sørg for at vedtatte forbedringer overføres til planleggingsprosessen!

5.3 Rapporter og dokumenter

Rapporter er informasjon til ledelsen, underlag for ajourføring av sikkerhetspolicy og arkiv for framtidige trendanalyser etc.

- Sørg for at relevante logger tas vare på.
- Dokumenter sikkerhetspolicy og målsetting.
- Dokumenter prosedyrer og kontrollaktiviteter.
- Dokumenter risiko- og sårbarhetsanalyser, avhjelpende tiltak og restrisiko.
- Rapporter sikkerhetssystemets ytelse målt mot målsettingene.

5.4 Komme i gang

For å håndtere informasjon og systemer på en sikker måte, må det etableres en sikkerhetskultur, hvor det systematisk avdekkes risikoer, mangler og muligheter for forbedringer, og med planmessig oppfølging av forbedringstiltakene.

Foretaket bør starte med å kartlegge og dokumentere hva som finnes av systemer og informasjon av betydning, og så utføre en risiko- og sårbarhetsanalyse.

Velg ut de viktigste områdene, avdekk gap og planlegg implementering av tiltakene. Det kan være hensiktsmessig å ta små områder av gangen, og færre tiltak. Det er bedre å komme i gang med de viktigste tiltakene, enn å planlegge for en ideell dekning som tar lang tid.

5.5 Stoppe uønskede hendelser

Hovedformålet med sikringstiltakene er å hindre uønskede hendelser, og i tillegg begrense skader og stoppe slike hendelser så raskt som mulig. I en krisesituasjon må foretaket derfor:

- Ha ajourført dokumentasjon på papir, eller i uavhengige elektroniske beredskapssystemer, eller frittstående PC-er.
- Ha avklarte ansvarsforhold internt og mot underleverandører.
- Ha gjennomført opplæring av relevant personell.
- Trent jevnlig på hva man skal gjøre.
- Vite hvor og hvordan nøkkelpersoner kan kontaktes.
- Teste at reserveløsninger virker for det som er viktigst gjennom hele verdikjeden.

Testing og trening/opplæring på disse områdene må derfor være en naturlig syklus i foretakets sikkerhetsarbeid.

6 Aktuelle standarder

6.1 ISO/IEC Sikkerhetsstandarder

Kort oversikt over sikkerhetsstandardene:

ISO/IEC 27000:2009 – Oversikt over sikkerhetsstandardene, og begrepsbruk
ISO/IEC 27001:2005 – Krav til sikkerhetssystemet
ISO/IEC 27002:2005 – Veiledning i styring av informasjonssikkerhet
ISO/IEC 27003:2010 – Implementasjonsveiledning for informasjonssikkerhetssystem
ISO/IEC 27004:2009 – Målinger
ISO/IEC 27005:2011 – Risikostyring i informasjonssystemer
ISO/IEC 27006 til 27009 omhandler revisjon av sikkerhetssystem.

6.2 Andre rammeverk og standarder

The Information Systems Audit and Control Association (ISACA)-Control Objectives for Information Technology (CobIT): www.isaca.org/cobit.htm.

Standard Online AS: http://www.standard.no/no/

7 Vedlegg A
Overordnet beskrivelse av sikkerhetsmodell

De regulatoriske kravene som er behandlet i kapittel 2, er i overensstemmelse med sikkerhetssystemet som er lagt til grunn for 27001-standarden i [4], og i samsvar med prosessen beskrevet i kapittel 5.2. Denne prosessen er også i overensstemmelse med OECD Guidelines [9]. I 27001-standarden gis en "mapping" av standarden mot OECDs Guidelines. Kapittel 4 i ISO/IEC 27001 trekker opp rammeverket for sikkerhetssystemet. For at foretakets sikkerhetssystem skal være i overensstemmelse med standarden, må følgende fem kapitler fra standarden være med:

- Kapittel 4 – Sikkerhetssystem
  Foretaket skal etablere et godt dokumentert ledelsessystem for informasjonssikkerhet. Systemet skal tilpasses foretakets forretningsområder og dekke de risikoer en står overfor. Foretaket skal bruke systemet aktivt, forvalte det som angitt nedenfor og vedlikeholde og forbedre systemet basert på erfaringer og ny kunnskap.

- Kapittel 5 – Ledelsens engasjement
  Ledelsen skal stille seg bak sikkerhetssystemet ved bl.a. å etablere en sikkerhetspolicy som skal kommuniseres til organisasjonen og samtidig påpeke viktigheten av å oppfylle sikkerhetsmålene. Ledelsen må sørge for informasjon og årvåkenhet i organisasjonen, og tilføre organisasjonen nødvendig kompetanse.

- Kapittel 6 – Interne sikkerhetssystem-revisjoner
  Det skal gjennomføres regelmessige planlagte revisjoner av systemet. Slik revisjon skal kontrollere at systemet oppfyller kravene i foretakets sikkerhetspolicy og lover og regler. En skal se etter at identifiserte sikkerhetskrav er dekket, at relevante tiltak er iverksatt på en effektiv måte, og at systemet gir beskyttelse som forventet. Sertifiserte foretak kan ha strengere krav til revisjon enn angitt her.

- Kapittel 7 – Forvaltning av sikkerhetssystemet
  Ledelsen skal sørge for regelmessige gjennomganger, minst en gang i året, for å påse at sikkerhetssystemet er effektivt og oppfyller kravene. Forbedringsbehov skal vurderes. Om nødvendig skal sikkerhetspolicy oppdateres.

- Kapittel 8 – Vedlikehold/forbedring av sikkerhetssystemet
  Foretaket skal kontinuerlig forbedre og effektivisere sikkerhetssystemet ved oppfølging av egen sikkerhetspolicy. En skal analysere uønskede hendelser og implementere korrektive tiltak for å hindre gjentagelser.

Hvis foretaket tar sikte på å bli autorisert etter ISO/IEC 27001-standarden, kan ingen av disse punktene utelates fra sikkerhetssystemet. Annex A i standarden har videre en rekke spesifikke områder for sikring. Ikke alle områder er relevante for alle foretak, og det er lov å utelate de som ikke er det. Men alle disse områdene må vurderes for sikring, og områder en ikke finner relevant å sikre, skal begrunnes og dokumenteres. Ansvarlig person for de enkelte områdene må godkjenne denne avgjørelsen. Dette omfatter også å akseptere de risikoene som det da ikke sikres mot.

8 Vedlegg B
Krav om beskyttelse – "Mapping" mot ISO 27001

I IKT-forskriftens § 5 "Sikkerhet" heter det: "[…] beskyttelse av utstyr, systemer og informasjon […] mot skader, misbruk, uautorisert adgang og endring, samt hærverk."

Her er det krav som treffer spesifikke områder i ISO 27001-standarden. Det er ikke mulig å gi en "en-til-en"-referanse mellom krav og standard, men som helhet er alle kravene godt dekket. I tabellen under finnes en grov "mapping" mellom kravene og sikringsområdene i Annex A i standarden [4], men "mappingen" er ikke utfyllende i alle detaljer. Flere andre områder kan komme til anvendelse for å oppfylle kravet.

BESKYTTE	UTSTYR	SYSTEMER	INFORMASJON
mot skader	A.9.1, A.9.2	A.9.1, A.10.4, A.10.5, A.11.6	A.9.1, A.10.1, A.11.5
mot misbruk	A.8.2, A.10.4, A.10.6	A.8, A.11	A.8, A.11, A.12.3, A.12.4
mot uautorisert adgang	A.9, A.8.2	A.10.4, A.10.6, A.11, A.13	A.8, A.11, A.12.3, A.12.4, A.13
mot uautorisert endring	A.9.2.4	A.8.2, A.10.1, A.10.4, A11, A.13	A.8, A.11, A.12.3, A.12.4, A.13
mot hærverk	A.9	A.8, A.10.10, A.11, A.12.6	A.8, A.11, A.12.4

9 Aktuelle referanser

9.1 Andre sikkerhetsrelevante paragrafer i IKT-forskriften.

IKT-forskriften har flere paragrafer som er relevante for sikkerhet. De mest sentrale er:
§ 8 – Drift
§ 9 – Avviks- og endringshåndtering
§ 10 – Krav til kontinuitet
§ 11 – Driftsavbrudd og katastrofeberedskap
§ 12 – Utkontraktering
Hele virkeområdet for disse er ikke dekket i denne veiledningen.

En må også vurdere § 3 – Risikoanalyse. Det er laget egen veiledning for denne [8]

9.2 Referanser

[1] - FOR-2003-05-21-630: Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) – http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20030521-0630.html
[2] - FOR 2008-09-22-1080: Forskrift om risikostyring og internkontroll http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20080922-1080.html
[3] - FOR-2000-12-15-1265: Personopplysningsforskriften. Behandling av personopplysninger – http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html
[4] - ISO/IEC 27001:2005 – Information technology—Security techniques—Information security management systems – Requirements
[5] - ISO/IEC 27002:2005 – Information technology—Security techniques—Code of practice for information security management
[6] - ISO/IEC 27014 Information technology—Security techniques—Governance of information security. N10019, 2011-5-20, 2nd CD
[7] - ISO/IEC 27015 Information technology — Security techniques — Information security management guidance for financial services (DRAFT)
[8] – Finanstilsynet: "Veiledning for gjennomføring av risiko- og sårbarhetsanalyser av IKT-systemer i finanssektoren": http://www.finanstilsynet.no/no/Artikkelarkiv/Rapporter/2008/Veiledning-for-gjennomforing-av-risiko--og-sarbarhetsanalyser-av-IKT-systemer-i-finanssektoren/
[9] – OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security
Internet economy - Organisation for Economic Co-operation and Development
[10] - Security Metrics. Replacing Fear, Uncertainty, and Doubt.
ISBN-13: 987-0-32-134998-9 Andrew Jaquith – Addison Wesley – 2007.
[11] – KOBI-rapporten – Kapittel 7 "Inndeling av informasjon i klasser": https://www.nsm.stat.no/Documents/KIS/Publikasjoner/KOBI%202008-04-30_Hoveddokument_1.1.pdf
[12] – FFIEC – Information Security – July 2006 – IT Examination Handbook
[13] – Finanstilsynets Risiko- og sårbarhetsanalyser: http://www.finanstilsynet.no/no/Venstremeny/Om-Finanstilsynet/Publikasjoner/Risiko--og-sarbarhetsanalyse/

FINANSTILSYNET
Postboks 1187 Sentrum
0107 Oslo
POST@FINANSTILSYNET.NO
WWW.FINANSTILSYNET.NO