FFI RAPPORT

TILSYNSMETODIKK OG MÅLING AV INFORMASJONSSIKKERHET I FINANS- OG KRAFTSEKTOREN

HAGEN Janne Merete, NORDØEN Lisa Maria, HALVORSEN Elin Espeland

FFI/RAPPORT-2007/00880

TILSYNSMETODIKK OG MÅLING AV INFORMASJONSSIKKERHET I FINANS- OG KRAFTSEKTOREN

HAGEN Janne Merete, NORDØEN Lisa Maria,
HALVORSEN Elin Espeland

FFI/RAPPORT-2007/00880

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2007/00880	UNCLASSIFIED	61
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
1014	-	

4) TITLE

TILSYNSMETODIKK OG MÅLING AV INFORMASJONSSIKKERHET I FINANS- OG KRAFTSEKTOREN

MEASURING COMPLIANCE TO INFORMATION SECURITY LAW - A CASE STUDY OF THE FINANCE AND ELECTRICITY SECTOR

5) NAMES OF AUTHOR(S) IN FULL (surname first)

HAGEN Janne Merete, NORDØEN Lisa Maria, HALVORSEN Elin Espeland

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Informasjonssikkerhet	a) Information security
b) Finans	b) Finance
c) Kraftforsyning	c) Electric Power Supply
d) Regulering	d) Regulation
e) Tilsyn	e) Supervision

THESAURUS REFERENCE:

8) ABSTRACT

This report presents a comparative study of the regulatory authorities within the Norwegian, Danish, Swedish and British finance and energy sector. The study is part of the ”Critical Information Infrastructure Protection Project” (BAS5), and it has been conducted to provide an overview of the supervisory process carried out by the proper authorities in the finance and energy sector, as well as experiences related to supervisory controls. Furthermore, this study provides an identification of the coarse features of legal acts, methodology used in regulatory and supervisory activities, and the use of performance measuring such as metrics and indicators in relations to research needs.

The research, based on interviews and literary searches, revealed that the statutory framework concerning information security and supervisory methodology employed by the proper authorities varies both between sectors and countries. Compared to UK, Sweden, Finland and Denmark; it seems like Norway has put more emphasis on strong regulation of information security compared to the other countries. Furthermore, the study reveals that quantitative indicators or metrics are not applied, however there seems to be a potential for developing metrics to follow up compliance to law trends.

9) DATE	AUTHORIZED BY This page only	POSITION
2007-03-30	Jan Erik Torp	Director

ISBN 978-82-464-1151-4

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

TILSYNSMETODIKK OG MÅLING AV INFORMASJONSSIKKERHET I FINANS- OG KRAFTSEKTOREN

1 INNLEDNING

Denne rapporten inngår i BAS5-prosjektet ved FFI og inneholder en beskrivelse av gjeldende praksis innen offentlig tilsyn med informasjonssikkerhet. Gjennom tilsynsprosessen avdekker tilsynsmyndighetene svakheter i forhold til de krav til informasjonssikkerhet som er gitt i de lover og forskrifter som danner basis for tilsynet. Hvis myndigheten oppdager avvik, må avvikene lukkes innen avtalte frister. Vi har imidlertid lite kjennskap til tilsynsmetodikken og målingene som gjøres i de ulike sektorene. Vårt hovedmål har derfor vært å studere målepraksis hos tilsynsmyndigheten for to sektorer; kraftforsyning og finans. Disse to sektorene er valgt fordi de begge er svært avhengige av pålitelige og sikre IT-systemer, mens de har ulik lovmessig forankring og tradisjon innen informasjonssikkerhet.

BAS5-prosjektet har valgt å se nærmere på målepraksis blant annet fordi det er påpekt en mangel på nasjonal koordinering av informasjonssikkerhet (28). Tilsynsmyndighetene utgjør en ”utøvende makt” i forhold til å måle sikkerhetsstatus i forhold til legale krav og følge opp informasjonssikkerhet. Utvikling og bruk av gode, relevante måleindikatorer for informasjonssikkerhet kan gi rom for sammenligning på tvers av sektorer og muligheter for en mer helhetlig oppfølging av informasjonssikkerhet på nasjonalt nivå. Slike måleindikatorer må imidlertid være i overensstemmelse med lovene og forskriftene som regulerer informasjonssikkerhet i den enkelte sektor. Denne rapporten utgjør et grunnlagsarbeid i forhold til videre utvikling av måleindikatorer eller metrikker.

Vi antar at ulike sektorer har felles utfordringer i henhold til oppfølging av informasjonssikkerhet innenfor sitt område, men at det er stor forskjell i hvordan tilsyn med informasjonssikkerhet blir gjennomført og hvordan informasjonssikkerhet blir målt og avvik fulgt opp. Rapporten har hovedfokus på tilsynsmetodikker og måleverktøy hos norske tilsynsmyndigheter, men har også en overordnet sammenligning med tilsynspraksis i Sverige, Danmark, Finland og Storbritannia.

Lover som regulerer informasjonssikkerhet er utgangspunktet for studien. De viktigste norske lovene er framstilt i boken *Informasjonssikkerhet – Rettslige krav til sikker bruk av IKT (27).* Boken er den første og eneste samlede fremstillingen av regelverk om informasjonssikkerhet i Norge.

Rapporten bygger delvis på et arbeid av sommerstudentene Lisa Maria Nordøen og Elin

Espeland Halvorsen, som ble gjennomført sommeren 2006[1].

2 PROBLEMSTILLING, AVGRENSNINGER OG METODE

2.1 Formål

Formålet med rapporten er å skaffe innsikt i tilsynsmetodikk og måling av informasjonssikkerhet. Dette gjøres ved å se på praksis i Norge, hovedsaklig hos Norges vassdrags- og energidirektorat (NVE) og Kredittilsynet. I tillegg er også Datatilsynet og Nasjonal Sikkerhetsmyndighet inkludert, siden disse er tverrsektorielle tilsynsmyndigheter. Rapporten ser også den norske praksisen opp mot praksis i Sverige, Danmark, Finland og Storbritannia.

Følgende problemstillinger danner grunnlag for rapporten:

1. Hvilke krav stiller sektorrelevant lovverk til informasjonssikkerhet?
   Vi vil undersøke hvilke krav lovverket stiller til sikring av IT-systemer og beskyttelse av informasjon og til dokumenterte risikoanalyser og beredskapsplaner, samt hvilke lovhjemler de ulike tilsynsmyndighetene opererer ut i fra.
2. Hvilke metoder, prosesser, verktøy og måleindikatorer brukes av tilsynsmyndighetene?
   Dette innebærer å beskrive tilsynsprosessen og anvendte metoder/verktøy i de sektorene studien omfatter, inklusive reaksjonsmuligheter som tilsynsmyndigheten kan benytte.
3. Hvilke erfaringer har ulike aktører gjort seg med hensyn til måling og tilsyn av informasjonssikkerhet?
   Spørsmålet belyses både fra myndighetenes og bedrifters side med primærdata fra noen få respondenter hos utvalgte myndigheter og virksomheter.
4. Hvilken tilsynspraksis har utenlandske myndigheter, og i hvilken grad gjøres det måling av informasjonssikkerhet?
   Spørsmålet besvares kun av utenlandske myndigheter og ikke virksomheter det er ført tilsyn med. Primærdata er samlet inn gjennom skriftlig eller muntlig kommunikasjon med vedkommende myndigheter.
5. Hvilket forbedringspotensial er det i forhold til norsk tilsynspraksis?
   Vi sammenligner tilsynspraksisen i de to sektorene, både nasjonalt og internasjonalt, og drøfter på dette grunnlaget forbedringsmuligheter.

2.2 Metode

Vi har gjennomført en utforskende studie, og problemstillingen er behandlet gjennom datainnsamling på to måter:

[1] Arbeidet omfattet bl.a. innhenting og systematisering av informasjon, både gjennom intervjuer og via søk i aktuelle databaser.

- **Primærdata:** Samtaler med myndigheter og virksomheter, samt andre ressurspersoner på området i perioden sommeren 2006 til januar 2007
- **Sekundærdata:** Søk i databaser og på internett etter litteratur

For å kvalitetssikre funnene i studien har all informasjon gjengitt i rapporten blitt tilsendt de studerte objekter for validering. Rapporten er også sendt til høring til berørte norske og nordiske informanter[2].

En begrensning med vår metode er at den primære informasjonsinnsamlingen baserer seg på oppfatninger fra individer som er intervjuet i de ulike virksomhetene. Det må derfor tas høyde for en viss grad av subjektive vurderinger, avhengig av individenes syn på problemstillingen.

2.3 Avgrensninger

Rapporten tar hovedsaklig for seg tilsynsføring innen finans- og kraftforsyningen. Disse to sektorene er valgt fordi de begge er svært avhengige av pålitelige og sikre IT-systemer, mens de har ulik lovmessig forankring og tradisjon innen informasjonssikkerhet.

Sverige, Danmark, Finland og Storbritannia er valgt ut som case for studier av tilsynspraksis i utlandet. Sverige, Danmark og Finland er valgt på bakgrunn av at både NVE og Kredittilsynet, samt flere energi- og finansvirksomheter, har et formalisert nordisk samarbeid. Ettersom det allerede eksisterer nære samarbeid i sektorene, er det naturlig å se nærmere på vedkommende lands praksis. Samtidig er det også interessant å gjennomføre en komparativ studie av de land som samsvarer med norske forhold og kultur. Storbritannia er valgt fordi de spiller en sentral rolle i EU og underliggende arbeidsgrupper, som bl.a. ENISA[3].

2.4 Rapportens oppbygging

Etter de innledende kapitlene (1 og 2) presenteres resultatet av litteratursøket (kapittel 3). Kapittel 4 og 5 tar for seg tilsynsføring i henholdsvis finans- og energisektoren med utgangspunkt i gjeldende særlover, både nasjonalt og internasjonalt. Det blir gitt en trinnvis beskrivelse av tilsynsprosessen i de ulike sektorer, som går fra lovhjemmel til praksis.

I kapittel 6 blir tilsynsprosessen til to andre norske tilsynsmyndigheter, som opererer på tvers av sektorene beskrevet og drøftet. Deretter gir kapittel 7 en sammenstilling av studiens funn og resultatene drøftes i henhold til problemstillingen.

[2] Kvalitetssikring av beskrivelsen av praksisen fra Storbritannia er gjort ved at de har lest og kommentert referatet.
[3] ENISA - the European Network and Information Security Agency – er en myndighet nedført av EU som arbeider for å oppnå et høyt og effektivt nivå at IT- og informasjonssikkerhet innen EU – http://www.enisa.eu.int/, 10. august 2006

3 LITTERATURSØK

Kapittelet beskriver resultatet etter et litteratursøk innen temaene informasjonssikkerhet, sikkerhetsmetrikker, tilsynsmetodikk og effekten av lovverk.

Kort oppsummert synes det å være begrenset med relevant forskning på temaene. Litteratur som vi fant beskriver behovet for både økt fokus og forskning innenfor disse temaene, samt ideer, konsepter og rammeverk.

3.1 Definisjoner

ISO/IEC17799 (40) definerer *informasjon* som en annen forretningsmessig verdi som er helt fundamental for organisasjonens virksomhet og dermed har krav på beskyttelse. *Informasjonssikkerhet* defineres som beskyttelse av informasjon fra et vidt spekter av trusler for å sikre virksomhetens kontinuitet, minimere risiko og maksimere avkastning på kapital og forretningsmuligheter.

The National Institute for Standards and Technology definerer *metrikker* som beslutningsstøtteverktøy og et instrument for å øke ytelsen gjennom å samle inn, analysere og rapportere relevante ytelsesdata.

FFI skiller mellom *infrastrukturer* og *samfunnsfunksjoner*, og har beskrevet kritisk infrastruktur som ”de nettverk som er grunnlaget for all annen samfunnsvirksomhet, mens samfunnsfunksjoner er tjenester som benytter de kritiske infrastrukturene for å dekke behovene til befolkningene, virksomheter og aktører i samfunnet” (38).

Statlig tilsyn er ett av flere virkemidler for å følge opp intensjonene i lovverket. Statlig tilsyn innebærer at representanter fra tilsynsmyndigheten gjennom tilsynsprosessen skal kontrollere samsvar mellom praksis og de krav lovverket stiller. Tilsynsmyndighetens påfølgende krav om utbedring av eventuelle avvik, samt rådgivning, skal medvirke til at tjenestene blir drevet på en faglig forsvarlig måte, at svikt i tjenesteytingen forebygges og at ressursbruken er effektiv. Slik vil til slutt befolkningens behov for tjenester blir ivaretatt.

3.2 Søkestrategi

For å finne relevant litteratur ble det i tidsrommet 19. juni – 21. juli 2006 gjort søk i utvalgte databaser (jf A.2) etter PhD-avhandlinger, masteroppgaver, rapporter, artikler og bøker som omhandler informasjonssikkerhet, sikkerhetsmetrikker og/eller beskriver måleindikatorer. Søkeresultatet inneholder litteratur om metrikker; hva de er, hvordan de utvikles og ledes, anvendelsesområder og teorier/rammeverk, økonomisk avkastning, samt behovet for gode, relevante metrikker.

Av alle treff ble en beskjeden mengde funnet relevant i forhold til følgende kriterier;

- Tittel – Stikkord og tilsynelatende relevans

- Abstrakt/Abstract – Stikkord og tilsynelatende relevans

Resultatet av litteratursøket er gjengitt under. Som det fremgår er det ikke store mengder relevant litteratur som kom frem i løpet av søkeprosessen.

3.3 Sikkerhetsmetrikker – hva er det?

The National Institute for Standards and Technology (NIST) definerer metrikker som beslutningsstøtteverktøy og et redskap for å øke ytelsen gjennom å samle inn, analysere og rapportere relevante ytelsesdata. Målinger forteller noe om omfang, dimensjoner, kapasitet, størrelse, antall eller en annen kvantitativ karakteristikk av programvare eller system. De er diskrete og objektive verdier, og det er kun når vi relaterer dem til en felles term eller rammeverk at de blir metrikker. Det er viktig å skille mellom en indikator og en metrikk, da begrepene brukes ofte om hverandre. En metrikk kjennetegnes av en fast struktur og oppbygning, mens en indikator opererer på et mer generelt grunnlag. Gode metrikker kjennetegnes av at (8):

- rekkevidde/omfang er klart definert
- de er basert på en godt definert modell av det problemet de beskriver
- de har en godt definert måleprosess som inkluderer kvalifikasjoner til den som utfører evalueringen, identifikasjon av nødvendig informasjon, instruksjoner på hvordan spesielle faktorer kan bli målt, algoritmer for å beregne sluttverdier, og forklaring på kilder til usikkerhet.
- de er repeterbare
- de er relevante for beslutningstakere
- de er effektive, dvs. at det er mulig å få et raskt svar med lave nok kostnader, slik at beslutningstakere faktisk vil bruke metrikkene

I en tid da trusselen fra Internett øker (9) påpekes det at gode metrikker er nødvendige. Gode metrikker bør kunne måle systemets motstandsdyktighet eller evne til å stå imot ulike typer angrep, evne til å gjenkjenne og oppdage angrep når de oppstår, evne til å vedlikeholde grunnleggende tjenester, begrense skaden av angrep og gjenskape fulle tjenester etter angrepet. Gode metrikker blir brukt fordi de kan bidra til å (14):

- etablere en grunnlinje for overvåkning eller forbedring
- rettferdiggjøre budsjett og oppnå tilleggsbevilgninger
- oversette detaljerte tekniske saker til ledelses- og beslutningsnivå
- forbedre eksisterende sikkerhetspraksis og integrere sikkerhet inn i eksisterende forretningsprosesser

Et beslektet område til informasjonssikkerhet er ”Information assurance”, som betyr å beskytte verdifull informasjon mot ødeleggelse, degradering, manipulering og utnytting (9). I praksis kan det være vanskelig å skille begrepene fra hverandre. Begge handler om å beskytte informasjon. Klassifisering av Information assurance (IA) metrics er gjengitt i (9). I (8) beskrives en taksonomi for IA-metrikker, som inkluderer metrikker for organisasjonssikkerhet og metrikker for tekniske system/produkt/objekter.

Metrikker som måler innsatsen til sikkerhetspersonell og verktøyene de bruker, er av begrenset verdi for å vurdere effektiviteten av investeringer i informasjonssikkerhetstiltak. Da er det bedre å kombinere sikkerhetsmetrikker med andre ytelsesindikatorer, som for eksempel effekten sikkerhetsproblemer har på interne forretningsprosesser. Måler man for eksempel nedetid som følge av virus/dataorm-angrep, har man mulighet til å kople hvordan angrep mot deler av IT-infrastrukturen påvirker forretningsprosessene (1).

3.4 Anvendelsesområder og betydning av måling

Teknologiledere prøver å rettferdiggjøre og prioritere investeringer i sikkerhet, men de mangler verktøy til dette. Trenden er at sikkerhetsbudsjettet har økt, og man spør seg hva får jeg igjen for dette? Hvis svaret er: Du får bedre sikkerhet, er neste spørsmål: Hvordan vet jeg at sikkerheten er blitt bedre (2)? Systematiske målinger kan gi bedre svar på slike spørsmål.

De fleste organisasjoner kaller sikkerhet et prioriteringsområde for toppledelsen, og i én studie rangerer toppledere sikkerhet som 7,5 på en skala fra 1-10. Den påståtte betydningen stemmer imidlertid dårlig med virkeligheten der bedrifter i gjennomsnitt bruker kun 0,047 % av inntekten på sikkerhet. Det at toppledelsen ikke prioriterer å investere i sikkerhetsteknologi og heller ikke i å utvikle sikkerhetspolicy, leder til treghet i organisasjonen og medfører sårbarhet. Den lave prioriteten er sannsynligvis et resultat av følgende faktorer: Mangel på bevissthet rundt problemet sammen med en antakelse om at sikkerheten blir tatt hånd om av ansatte i IT-avdelingen, og at forretningsprosjekter har høyere avkastning enn sikkerhetsinvesteringer (22).

Til tross for manglende ledelsesfokus på informasjonssikkerhet, blir det hevdet at informasjonssikkerhet ikke bare er et teknisk anliggende, men også et strategisk og legalt anliggende. Informasjonssikkerhet bør derfor integreres inn i ledelsesfunksjonene. Det kan gjøres gjennom å utvikle et rammeverk for informasjonssikkerhetsledelse (25). IT-ledere ved NASA og noen få private selskaper har erfart at frekvente, formelle, metrikkdrevne revisjoner er en god måte å relatere sikkerhetsmålingene til forretningsprosessene på. Suksessfaktoren ligger i å involvere linjeledere på alle nivå og definere gode sikkerhetsmål (6). Dette kan bidra til å overvinne problemet ved at en stor andel toppledere (59 %) ser sikkerhet som et teknologiproblem, og ikke som et forretningsanliggende. For eksempel har en bank oppnådd et klarere bilde av IT-sikkerheten ved å klassifisere alle viktige informasjonssystemer på en skala; høy, medium og lav, basert på betydningen for driften og tapene som ville oppstått dersom feil eller svikt oppstod i systemene. Det samme er gjort for trusler og sårbarheter. Sannsynligheten for at truslene utnytter sårbarhetene er også anslått. Denne tilnærmingen har gitt banken et klarere bilde av IT-risikoen, og har også vist seg nyttig når nye sikkerhetstiltak skulle innføres (4).

3.5 Måle mot hva?

Litteraturen presenterer ofte sikkerhetsmetrikker som målinger mot en aller annen referanselinje. To alternative tilnærminger er sentrale; tvang (legale virkemidler) eller normativ tilnærming

(benchmarking og læring).

En casestudie analyserer disse to tilnærmingene. Studien viser at regulerende krefter (tvang), slik som Sarbanes Oxley (SOX)[4], er en sterkere drivkraft for organisasjonsendring og bevissthetsbygging hos toppledere når det kommer til sikkerhetsteknologi og politikk enn normativ innflytelse, som i hovedsak påvirker IT-personell (23). En annen studie viser også at SOX har innvirkning på informasjonssikkerheten, særlig fremheves integritet. Gode retningslinjer er en nøkkelfaktor for å kunne oppnå kravene i SOX (24).

Standarder, som er et eksempel på normativ tilnærming, er imidlertid i følge litteraturen mye brukt som referanselinje. COBIT og ISO/IEC 17799 er to kjente standarder. Disse to er komplementære, og det finnes en kopling mellom ISO/IEC 17799 og COBIT der hver prosess som er beskrevet i COBIT koples mot kontroller i ISO-standarden (7).

3.6 Ledelse av sikkerhetsmetrikker

Det er viktig for en organisasjon å ha indikatorer for å få informasjon om effektiviteten til tiltakene og sikkerhetskontrollene. Effektiviteten i hele ledelsessystemet er direkte betinget av effektiviteten i de implementerte informasjonssikkerhetskontrollene. I (10) skilles det mellom metrikker og indikatorer, der metrikker er kvantitative data av ulike aspekter som kan være nyttige for å evaluere effektiviteten av sikkerhetskontrollene. Indikatorene er på et høyere nivå, en aggregering/kombinasjon av data laget av metrikkene, slik at de gir nyttig informasjon til organisasjonen. Indikatorene og metrikkene deles inn i følgende grupper:

- Generelle – for eksempel antall ansatte eller PCer i organisasjonen
- Ledelse - antall ansatte med sikkerhetsansvar
- Operasjonelle - antall hendelser rapportert av ansatte
- Tekniske - gjennomsnittlig tilgjengelig bredbåndskapasitet
- Miljømessige - antall virus på internett forrige uke
- Personellopplæring - kunnskapsnivå hos personell

En nøkkelsuksessfaktor er å definere grenseverdier for hver indikator.

Ikke alle mener at metrikker må omgjøres til indikatorer før de kan brukes som verktøy til å informere ledelsen. I (13) gis en presentasjon av hvordan man kan bruke metrikker direkte for å orientere ledelsen, rettferdiggjøre budsjettet og bruke trendanalyser for å utvikle mer effektive informasjonssikkerhetsprogram. Det understrekes at det er viktig å etablere en prosess som sikrer at man kan hente inn data. Antall systemer og antall brukere er sentrale drivere for arbeidsbelastningen knyttet til informasjonssikkerhet, og er relevante metrikker. De øvrige metrikkene som presenteres viser trender over tid for ulike forhold som vedrører

[4] SOX, Sarbanes-Oxley Act ble innført i USA i juli 2002. Formålet er at selskap som operer på New York børsen og Nasdac-børsene skal innføre et regelsystem for internkontroll for å gjenskape fortroligheten etter rekken av finansskandaler som har inntruffet i USA. Regelverket skal forhindre juks i bokføringen og sikre at årsrapporten er pålitelig.

informasjonssikkerhet; f.eks. antall dager det tar å godkjenne et system for behandling av fortrolig informasjon.

En finsk studie viser at å måle informasjonssikkerhet er viktig, men fordelene er avhengig av at metrikkene blir brukt som en *prosess*, mens erfaringene hentes fra historiske data (16). Prosesstankeganger er også støttet og beskrevet i mer detalj i (21), der forfatterne gjennom å bruke et fiktivt selskap som eksempel, går igjennom hvordan man kan lage metrikker og drifte dem. Metrikkene som presenteres måler bruk av sikkerhetskontroller og -verktøy.

Et forslag til prosess for måling av informasjonssikkerhetsnivå kopler målinger opp mot rapportering til ledelse og evaluering/læring (19). Studien kartlegger videre i hvilken utstrekning informasjonssikkerhet måles gjennom en spørreundersøkelse til 78 store virksomheter i Norden. Ett resultat av studien er at de som bruker balansert målstyring også er de som måler mest. Tekniske metrikker og risikovurderingsmetrikker er utbredt i bruk, men de fleste organisasjonene bruker ikke metrikkene som en prosess. Studien påpeker behov for å måle individuell erfaring, samt å automatisere målingene (16).

3.7 Eksempler på sikkerhetsmetrikker

Holdning og bevissthet til ansatte antas å ha stor betydning for sikkerheten. Derfor arbeider mange virksomheter nettopp med å heve bevissthet til sikkerhet, gjennom f.eks. kampanjer, opplæringsprogram etc. Enkelte bedrifter forsøker å måle resultatet av kampanjene, men ingen bruker målingene systematisk for å oppnå kontinuerlig forbedring. Ett prosjekt har utviklet ni metrikker rundt bevissthet. Metrikkene dekker ulike aspekter av sikkerhetsbevissthet; for eksempel trening, sikkerhetshendelser, papirmakulering, svake passord og kundetilfredshet (20).

Eksempler på metrikker som måler ulike aspekter av hendelseshåndtering er vist i (17) mens tekniske metrikker for Peer to Peer-applikasjoner er utviklet og testet i (18). Eksempler på metrikker er antall linjekoder som igjen brukes til å beregne potensielle sikkerhetshull, antall spyware og adware-komponenter som installeres, risiko for at brukere gjennom uhell deler data m.fl. I (22) nevnes andre eksempler på metrikker; antall knekte passord ved bruk av automatiske verktøy, inntrengninger og forsøk på inntrengning, kostnaden til mangel på sikkerhet mm. Metrikker for måling av oppfyllelse av krav innen personvernlovgivningen er utviklet i (41). Verktøyet tilbyr et grensesnitt mellom myndigheter og teknisk IT-personell. Verktøyet er testet på ulike typer brukere; ledelse, superbrukere og vanlige sluttbrukere. I (30) er det utviklet et sett av sikkerhetsmetrikker til bruk i måling av informasjonssikkerhet i kraftforsyningens driftskontrollsentraler.

3.8 Status for forskning på og kommersialisering av sikkerhetsmetrikker

En artikkel skrevet i 2004 tar for seg temaet trender og utvikling i information assurance metrics (11). Artikkelen påpeker at det har vært et antall industri- og forskningsinitiativ for å utvikle en standardisert rating som kan reflektere informasjonssikkerhet forbundet med et produkt eller et

system. Det henvises her til Common Criteria, som definerer ratingsnivå EAL 1-7[5]. National Institute for Standards and Technology (NIST) har utviklet en guide for sikkerhetsmetrikker. Også Nislab ved Høyskolen på Gjøvik nevnes som aktør i dette arbeidet.

I 2005 (12) ble det annonsert at en ny gruppe planla å lage standardmål for å måle, vurdere og sammenligne ytelsen til informasjonssikkerheten. Slik artikkelen kan tolkes, er det mulig det vil ligge noe forskning i dette initiativet. Gruppen ser for seg å møte flere utfordringer; det som er bra for noen er ikke nødvendigvis bra for andre, og virksomheter og andre aktører er generelt uvillige til å gi fra seg sikkerhetsinformasjon.

3.9 Økonomisk avkastning

Sikkerhetsinvesteringer er rettferdiggjort ved kostnaden ved å gjøre forretninger og beskyttelsen av firmaets verdier. Ofte blir sikkerhetsinvesteringer sett på som en forsikringspremie; de blir brukt for å håndtere en risiko, men man forventer ikke avkastning. En tredje grunn til å investere i sikkerhet er legale krav som må tilfredsstilles (26).

Returns of investment (RoI) er en metodisk tilnærming hvor nettonytte beregnes, og i (26) drøftes en prosessmodell og analysekriterier for kostnader og nytte. Kriteriene omfatter kostnadsfaktorer knyttet til planlegging, implementasjon og operasjon av sikkerhetstiltak. Nytten er inndelt i operasjonell nytte (kostnadsbesparelser, profitt, beslutningsstøtte, forretningsfunksjon), og strategisk nytte (redusert trussel og bedre kunde og leverandørrelasjoner).

Det er hevdet at RoI ikke er en egnet metrikk for å evaluere investeringsbeslutninger (3), fordi det må være klarhet i hvilken avkastning man snakker om. Internrenten er til sammenligning et økonomisk anvendbart mål for å sammenligne investeringer, men det finnes ingen enkel prosedyre for å omforme RoI til internrente. Samtidig er målet ofte å maksimere nettonytten av sikkerhetsinvesteringer, og da er nåverdibetraktninger mer relevante enn å maksimere internrenten. I (3) illustreres dette gjennom et eksempel der både nåverdi og internrente beregnes. De gjør også et poeng av at både nåverdi- og internrenteberegninger er ex-ante beregninger der man gjør beregningene på forhånd før investeringen blir gjennomført. Skal man beregne effektiviteten, bør man foreta ex-post beregninger basert på historiske data (3).

3.10 Utfordringer ved utvikling av gode sikkerhetsmetrikker

Gode metrikker trenger gode og pålitelige data å lage statistikk av. Gode og pålitelige data er imidlertid en mangelvare, spesielt knyttet til angrep mot IKT-systemer. Grunnene til det er at bedrifter og organisasjoner har sterke motiver for å holde tilbake informasjon om; frykt for påvirkning på finansmarkedet, skade på omdømmet, risiko for rettstvister i etterkant, risiko for forsikringsansvar ift kunder, risiko for at hackere informeres om at bedriftens systemer er svake og til sist at IT-personell kan frykte for jobben etter en hendelse (5). Også risiko for å miste

[5] Common Criteria er en standard for produkt/system sikkerhetssertifisering. Det er mulig å sertifisere i syv nivåer, der EAL 1 representerer laveste nivå og EAL7 det høyseste

kunder nevnes i (22). Uten at toppledelsen har fokus på dette, er det grunn til å tro at det blir vanskelig å finne ressurser til å samle inn og bearbeide statistikk i forbindelse med målinger (22). Det er verdt å merke seg at harde tall ikke alltid forteller den fulle sannheten, fordi det er for mange variabler og avhengigheter involvert. På sitt beste kan det utvikles trendindikatorer som sier noe om utviklingen (2).

Å måle kostnader er ikke enkelt og rett fram. Angrep produserer mange typer kostnader, og ikke alle kan bli kvantifisert enkelt, hvis i det hele tatt. Kostnader forbundet med angrep fra Internett kan deles inn i direkte og indirekte kostnader. Direkte kostnader inkluderer utgifter for å tilbakeføre systemet til opprinnelig tilstand, kostnader forbundet med driftsavbrudd, tapt salg i nedeperioden eller effekter på lang sikt. Å måle produktivitetstap er ikke alltid like entydig. Verdien på informasjon kan endres over tid, og er svært avhengig av hvem som eier informasjonen. Immaterielle verdier er vanskelig å tallfeste. Angrep har også indirekte kostnader som tap av eller skade på omdømme og merkevare. Inkludert i indirekte kostnader er også skade på individer og organisasjoner som indirekte berøres av angrepet, men som ikke var målet ved angrepet. Undersøkelser om f.eks. kostnader ved angrep fra kjente dataormer/virus viser store variasjoner (5).

4 TILSYN OG MÅLING AV INFORMASJONSSIKKERHET I FINANSSEKTOREN

Kapittelet beskriver hvordan tilsyn og måling av informasjonssikkerhet skjer i den norske finanssektoren. I tillegg er noen erfaringer fra utlandet inkludert.

4.1 Lovverk og forskrifter innen emnet informasjonssikkerhet

EØS-avtalen setter rammer for reguleringen av finansinstitusjonene i Norge, og avtalen er implementert i norsk rett gjennom en rekke lover og forskrifter. Kredittilsynsloven, Verdipapirhandelloven, Verdipapirregisterloven, Betalingssystemloven, Bokføringsloven og Personopplysningsloven med tilhørende forskrifter er de mest sentrale lovene for finansmarkedet. Siden vårt fokus er på informasjonssikkerhet, omtaler vi IKT-forskriften som har sin hjemmel i Kredittilsynsloven

Kredittilsynsloven[6] kommer til anvendelse på tilsynsmyndighet, tilsyn og tilsynets virksomhet, meldeplikt, samt sikring av konsesjonerte finansforetaks trygge og stabile drift. Loven skal sikre at dette foregår på en samfunnsmessig rasjonell måte. Lovens § 3 gir hjemmel for tilsynsføring både på generelt grunnlag, og med informasjonssikkerhet; ” *Tilsynet skal se til at de institusjoner det har tilsyn med, virker på hensiktsmessig og betryggende måte i samsvar med lov og bestemmelser gitt i medhold av lov samt med den hensikt som ligger til grunn for institusjonens opprettelse, dens formål og vedtekter. Tilsynet skal granske regnskaper og andre oppgaver fra institusjonene og skal ellers gjøre de undersøkelser om deres stilling og virksomhet som tilsynet finner nødvendig*”. Loven trådde i kraft 7. desember 1956.

[6] LOV 1956-12-07: Lov om tilsynet for kredittinstitusjoner, forsikringsselskaper, og verdipapirhandel mv.

IKT-forskriften[7] kommer til anvendelse ved planlegging, organisering, utvikling og anskaffelse av IKT-systemer og ved IKT-sikkerhet. Forskriftens § 1 utdyper dens virkeområde: *"Forskriften gjelder for norske forretningsbanker, sparebanker, finansieringsforetak, forsikringsselskaper, private, kommunale og fylkeskommunale pensjonskasser og pensjonsfond, børser og autoriserte markedsplasser, verdipapirforetak, forvaltningsselskaper for verdipapirfond, oppgjørssentraler, verdipapirregistre, inkassoforetak, eiendomsmeglerforetak, e-pengeforetak, samt systemer for betalingstjenester. Forskriften omfatter IKT-systemer som er av betydning for foretakets virksomhet. For eksterne brukere av foretakets IKT-systemer skal det foreligge avtaler som sikrer at forskriftens krav til sikkerhet og dokumentasjon ivaretas*". Det er noe variasjon i hvilke virksomheter som er omfattet i IKT-Forskriften og hvilke som er omfattet i Kredittilsynsloven.

Forskriften stiller krav til at alle finansvirksomheter skal gjennomføre dokumenterte risikoanalyser minst en gang årlig, eller ved endringer som har betydning for IKT-sikkerheten. Det er opp til virksomheter selv å etablere og utføre ROS-analysene.

Forskriftens § 5 setter krav til sikkerhet; *" Foretaket skal utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet 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*". Det vises også til personvernloven: *"Oppfyllelse av kravene til informasjonssikkerhet for personopplysninger etter forskrift av 15. desember 2000 nr. 1256 til personopplysningsloven*[8] *skal anses som oppfyllelse av kravene i paragrafen her*". Man skal hindre at uvedkommende får tilgang til sensitive opplysninger om kunder eller drift, samt sørge for kontinuitet i systemer som ivaretar viktige funksjoner.

Forskriftens § 11 stiller videre krav ved driftsavbrudd og katastrofeberedskap; *"Foretaket skal ha en dokumentert katastrofeplan som skal iverksettes dersom IKT-driften ikke kan opprettholdes som følge av en katastrofe. Med katastrofe menes hendelser som forårsaker driftsavbrudd slik at foretakets IKT-drift ikke kan fortsette med normalt tilgjengelige ressurser*".

Kredittilsynet kan i følge § 12 i IKT-forskriften føre tilsyn med norske og utenlandske IT-leverandører som et ledd i IT-tilsynet med et foretak som er underlagt IKT-forskriften.

Avslutningsvis stiller Forskriftens § 13 strenge krav til dokumentasjon; *"Det skal foreligge en samlet oppdatert oversikt over organisasjon, utstyr, IKT-systemer og vesentlige forhold i IKT-virksomheten. Det skal foreligge oppdatert dokumentasjon av det enkelte IKT-system som er av betydning for foretakets virksomhet og som dokumenterer at forskriftens krav er oppfylt til enhver tid*".

Forskriften trådde i kraft 1. august 2003.

---

[7] FOR 2003-05-21-630: Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)
[8] LOV 2000-04-14-3: Lov om behandling av personopplysninger (personopplysningsloven).

4.2 Tilsynsprosessen i finanssektoren

Kredittilsynets IT-tilsynsgruppe fører tilsyn med hjemmel i Kredittilsynsloven og IKT-forskriften. Tilsynets hovedmål er å kontrollere at forskriften samt relevante lover blir etterlevd hos tilsynsobjektet, og at sikkerhetstiltak er godkjente. Kredittilsynets seksjon for IT-tilsyn består av fire personer, alle med ulik IT-faglig bakgrunn. Normalt blir det gjennomført ca 20-25 stedlige IT-tilsyn i året. I 2005 ble det gjennomført tilsyn med fire IT-leverandører med hjemmel i Forskriftens §12.

Som ledd i arbeidet med påfølgende års virksomhetsplan, lager IT-tilsynsgruppen en liste med 20-25 foretak som det skal føres tilsyn med. Til grunn for utvelgelsen av foretak ligger innspill fra de ulike fagavdelingene i Kredittilsynet. Størrelsen og rollen til virksomheten, varigheten siden siste tilsyn, om det er behov for et oppfølgende tilsyn, om det gjennomføres store prosjekter i foretaket og hensynet til representativitet i utvalget bestemmer hvilke virksomheter det skal føres tilsyn med.

Etter at tilsynsobjekt er valgt ut, sender Kredittilsynet et skriftlig varsel til foretaket hvor de ber om spesifisert dokumentasjon av IT-virksomheten. I tillegg blir foretaket bedt om å fylle ut egenevalueringsskjema med ca 180 kontrollspørsmål med ja/nei-svar. Dette skjemaet er basert på COBIT, en internasjonal standard for IT-kontroll og -revisjon[9]. COBIT har definert 34 prosesser som dekker alle aspekter ved IT-virksomheten i et foretak. Egenevalueringsskjemaet Kredittilsynet bruker er delt inn i de 34 COBIT-prosessene, med kontrollspørsmål knyttet til hver prosess. Når Kredittilsynet mottar dokumentasjonen og det utfylte egenevalueringsskjemaet, blir dette gjennomgått som en del av tilsynsforarbeidet.

Tilsynsmøtet finner sted hos tilsynsobjektet. Kredittilsynets IT-tilsyn stiller med minimum to deltakere. Fra virksomhetens side pleier foretakets IT-ansvarlig, ansvarlig for internkontroll, sikkerhetsansvarlig, eventuelle andre med IT kompetanse og ofte representant fra foretakets ledelse å delta på tilsynsmøtet. Et stedlig IT-tilsyn varer gjerne en dag, typisk 09:00 – 14:00. Møtet begynner ofte med en innledning fra Kredittilsynet hvor de forteller om sin oppgave og hensikt med tilsynsføringen. Gjennomgang av prosessene i egenevalueringsskjemaet brukes ofte som agenda på tilsynsmøtet.

Det finnes også en forenklet versjon av egenevalueringsskjemaet som dekker 12 av de 34 COBIT-prosessene med ca 75 kontrollspørsmål. Som ledd i ordinære tilsyn med finansforetak gjennomført av andre seksjoner i Kredittilsynet, blir foretaket bedt om å svare på det forenklede egenevalueringsskjemaet om foretakets IT-virksomhet. IT-tilsynsgruppen får de ferdig utfylte skjemaene til vurdering og kan gi tilbakemeldinger til fagavdelingene som tar dette med i sin rapport. Dette kalles forenklet IT-tilsyn. IT-tilsynsgruppen analyserer informasjonen fra de forenklede egenevalueringsskjemaene før det blir vurdert om det skal gjøres et IT-tilsyn med den aktuelle bedriften førstkommende år.

[9] Mer informasjon om COBIT finnes her: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981

Kredittilsynets IT-tilsynsgruppe har også utarbeidet en rekke andre temabaserte egenevalueringsskjemaer basert på COBIT-metodikken, som benyttes i spesifikke tematilsyn eller som supplement til ordinære IT-tilsyn. Temaer det er laget spørreskjemaer til er virus, brannmur, katastrofehåndtering, IT-leverandører, prosjekt, hvitvasking og nettbank.

Grad av viktighet			**DS12**	Kontroll rutiner		Sårbarhet		
H	M	L	IT-Prosesser	Ja	Nei	H	M	L
			Styring av fasiliteter					
			1. Er lokaliseringen av IT-virksomheten i henhold til egne og lovpålagte krav?					
			2. Foreligger det prosedyrer for adgangskontroll for ansatte, leverandører, kunder og vedlikeholdspersonell?					
			3. Foreligger det prosedyre som sikrer håndtering av innbrudd?					
			4. Foreligger det prosedyrer som sikrer jevnlig vurdering og oppdatering av sikkerhetssystemene?					
Kommentarer:								

Figur 4.1 Eksempel på spørsmål fra COBIT-prosess DS12 om "Styring av Fasiliteter", plassert i undergruppen "Leveranse og Støtte (DSx)"

I egenevalueringsskjemaet skal virksomheter svare på spørsmålene knyttet til hver COBIT-prosess, og hver prosess skal ROS-analyseres så virksomheten kan svare på om sårbarheten i den utvalgte prosessen (se for eksempel figur 4.1 og prosessen 'Styring av fasiliteter') er ansett til å være høy, middels eller lav. Alle kontrollspørsmål som er besvart med nei er i utgangspunktet å anse for avvik, og betyr ofte at bedriften må iverksette forbedringstiltak.

Svarene registreres i en database og analyseres ved hjelp av verktøyet ISAP. Selv om dette gir kvantitative mål på resultatet av egenevalueringen, diskuterer IT-tilsynet nytten av denne informasjonen. Ofte viser det seg (gjennom det stedlige tilsynsmøtet) at det foretaket svarer på egenevalueringsskjemaet, fremstår med annen sikkerhet enn det som virkelig gjelder. Årsaken til denne uoverensstemmelsen kan være misforståelser og ulik oppfatning av hvordan spørsmålene skal tolkes. Egenevalueringsskjemaet er uansett viktig, fordi det krever svar fra foretaket på alle deler av IKT-virksomheten, og det er utgangspunkt for diskusjon om temaene på tilsynsmøtet.

Etter at tilsynsmøtet er holdt, blir det utarbeidet en foreløpig rapport med oversikt over hvor tilsynet fant sted, hvem som deltok og en situasjonsbeskrivelse inklusive hvilke avvik som ble funnet. Den foreløpige rapporten blir oversendt styret i foretaket det er ført tilsyn med ca fire uker etter at tilsynet har funnet sted. Denne er unntatt offentlighet. Foretaket får ca fire ukers frist på å svare Kredittilsynet, med kommenterer til de påpekte avvikene og beskrive planlagte tiltak. Omlag tre uker etter at Kredittilsynet har mottatt virksomhetens (styrets) svar på den foreløpige rapporten, utarbeider Kredittilsynet endelige merknader som også går til styret. Disse er offentlige. Avvik som ble påpekt i den foreløpige rapporten, men som foretaket i sine kommentarer beskriver tilfredsstillende rutiner for å håndtere, blir kun beskrevet som tatt til etterretning i de endelige merknadene.

Virksomheten er pålagt å rette seg etter vedtak, men har en fire ukers klagefrist etter at vedtaket er mottatt. Videre har de en tidsfrist på ca tre måneder til å iverksette og dokumentere nødvendige forbedringstiltak eller lukke avvik. Det er mulighet for å be om utsettelse, og det blir normalt innvilget for ytterligere tre måneder. Hvis et pålegg med hjemmel lov ikke blir etterkommet, kan vedkommende departement *(*Finansdepartementet i dette tilfellet*)*, i følge § 10 i Kredittilsynsloven, bestemme at *"de personer eller den institusjon, institusjonenes morsselskap eller morsselskapet i det konsern som institusjonen er en del av, som skal oppfylle pålegget, skal betale en daglig løpende mulkt til forholdet er rettet*".

Offentliggjøring av endelige merknader er i seg selv et virkemiddel som kan medvirke til at foretakene i all hovedsak retter seg etter tilsynets påpekninger.

Ved siden av de stedlige IT-tilsynene, gjør Kredittilsynets IT-tilsynsgruppe veiledningsarbeid i forhold til informasjonssikkerhet og forbedring av dette. Om det er nødvendig kan bedrifter kalles inn til møte for å diskutere ustabilitet i driften og forslag til forbedringstiltak. Utover dette har ikke Kredittilsynets IT-tilsynsgruppe spesielle rutiner for å summere opp erfaringer i etterkant av et tilsyn, men samlet gir de stedlige IT-tilsynene tilgang til informasjon som gjør at IT-tilsynsgruppen har en oppdatert oversikt over de viktige aktørenes status og planer for IKT-virksomheten.

4.3 Erfaringer og forbedringspotensial innenfor tilsynsvirksomhet

Oppmerksomheten rundt informasjonssikkerhet i finanssektoren har vært generelt god, mye på grunn av sektorens utsatte posisjon som kapitalforvalter og sektorens avhengighet av kundenes tillit. Kredittilsynets IT-tilsynsgruppe har arbeidet med å forbedre informasjonssikkerheten hos virksomhetene, spesielt via IKT-forskriften og tilsynet med etterlevelse av denne. Kredittilsynets IT-tilsyn har også ført til en modning i finansforetakene i forhold til å etablere sterke prosedyrer for IT-sikkerhet, forbedre ryddigheten, samt skape en "prosesstenkning" i sektorens IT-virksomhet.

Utvalgte finansforetaks erfaring med eksterne tilsyn er også generelt god, men mange små virksomheter oppfatter kravene i IKT-forskriftens som omfattende og vanskelige å etterleve. Kredittilsynet har laget en veiledning spesielt rettet mot mindre foretak, der man eksemplifiserer

hvordan man kan etterleve IKT-forskriftens krav gjennom ”livet” til et lite foretak.

Basert på samtaler vi har gjort med to foretak om deres erfaringer med tilsynsprosessen, får Kredittilsynets IT-tilsyn ros for arbeidet de gjør, men det er også usikkerhet om hvor betydningsfullt tilsynsføring er. Hos en virksomhet var betydningen av eksterne IT-tilsyn antatt å være stor. Eksterne IT-tilsyn økte bevisstheten i forhold til lovverk og trusler mot IT-systemene. IT-sikkerhet er ansett som et ”ressurstap”, ettersom det ikke er noe man aktivt profiterer av, og eksterne IT-tilsyn kan bidra til å øke viktigheten og dermed gjøre det lettere å få ressurser til å drive essensielt sikkerhetsarbeid. Eksterne IT-tilsyn etablerer fokusområder innenfor bedriften og bidrar dermed til at feil, som normalt ville forblitt uoppdaget, blir bemerket og utbedret. I en annen virksomhet ble det derimot betvilt om mangel på IT-tilsyn fra myndigheten hadde ført til lavere informasjonssikkerhet. Dette ble begrunnet med at man i finanssektoren selger et renommé der sikkerhetstroverdighet er essensielt for den daglige driften. Det var imidlertid en enighet om at et åpent og ryddig forhold mellom tilsynsmyndighet og tilsynsobjekt ga gode resultater og økt sikkerhet.

4.4 Utenlandsk praksis

4.4.1 Danmark

Danmarks ”Lov om finansiel virksomhed”[10] (FiL) har som formål å sikre at landets finansielle virksomhet tilrettelegges og gjennomføres i overensstemmelse med hensynet til forbrukerbeskyttelse, tjenesteleveringssikkerhet, samt beskyttelse ved tilsiktede eller utilsiktede feil.

De overordnede rammene for IT-sikkerhetstilsyn er beskrevet i FiL § 70, § 71, stk. 1, nr. 4, samt § 117 – 123 (Kapitel 9):

FiL § 70 *Bestyrelsen skal for den finansielle virksomheds væsentligste aktivitetsområder udfærdige skriftlige retningslinier, hvori arbejdsdelingen mellem bestyrelse og direktion fastlægges.*

FiL § 71, stk. 1, nr. 4 *En finansiel virksomhed skal have betryggende kontrol- og sikringsforanstaltninger på IT-området.* Danske finansforetak er pålagt å ha og teste beredskapsplaner og foreta risikoanalyser. Finansforetaks ledelse har ansvaret for IT-sikkerhet selv ved utkontraktering.

FiL § 117 – 123 (Kapitel 9) omhandler behandling av fortrolige opplysninger (taushetsbestemmelser).

Danmark har også en *’Vejledning om kontrol- og sikringsforanstaltninger på it-området i henhold til lov om finansiel virksomhed §71, stk. 1, nr. 4’* [11]. Innholdet i veiledningen kan

[10] LBK 286 af 04/04/2006
[11] Vejledning nr. 9074 af 23/01/2004

sidestilles med den norske IKT-forskriften, men det er en vesentlig forskjell; en veiledning i Danmark er et uttrykk for myndighetenes forståelse og tolkning av lovgivningen, mens en forskrift i Norge er en rettsregel. Den danske veiledningen gjelder for alle finansielle virksomheter uavhengig av størrelse, og er utformet på et overordnet nivå slik at hvert enkelt foretak står fritt til å utforme og velge praktiske løsninger. Dette gir den enkelte finansvirksomhet mulighet til å iverksette sikkerhetstiltak i henhold til eget behov.

Tilsyn med den danske finanssektoren besørges av det danske Finanstilsynet, som er et direktorat. Finanstilsynet står ansvarlig ovenfor sentrale ministere og råd i Danmark. Finanstilsynet er også sekretariat for tre råd; Det Finansielle Virksomhedsråd, Fondsrådet og Pensionsmarkedsrådet.

Tilsyn med informasjonssikkerhet i den danske finanssektoren svarer til de prosedyrer Kredittilsynets IT-tilsyn benytter seg av. Basert på en virksomhetsplan sendes et skriftlig varsel med forespørsel om informasjon til de foretak hvor Finanstilsynet annonserer tilsynet. Senere mottar Finanstilsynet rekvirert materiale. Dette gjennomgås før et stedlig tilsyn finner sted. Et stedlig tilsyn begynner med et felles orienteringsmøte, hvorpå det holdes individuelle møter og intervjuer med relevant personale. Tilsynet avsluttes med rekvirering av supplerende materiale.

I etterkant av et stedlig tilsyn går Finanstilsynet gjennom tilsynsresultater og deres observasjoner sammen med foretaket og avslutter tilsynsprosessen med en formell rapportering til foretaket. Ved avviksfunn har Finanstilsynet fire reaksjonsmuligheter:

- Risikoopplysning
- Påtale/Påbud
- Politianmeldelse
- Inndragelse av tillatelse

Det danske Finanstilsynet benytter ikke måleindikatorer eller metrikker i forbindelse med tilsynsaktiviteter. Finansforetak blir vurdert på grunnlag av lovgivning, risiko og vesentlighet, individuelle sikkerhetsmessige behov og hvordan sikkerhetstiltak utføres praktisk.

4.4.2 Sverige

Finansielle virksomheter i Sverige reguleres i henhold til lover og forskrifter som regulerer finansvirksomheten, men det finnes ingen spesifikk lov eller forskrift som omhandler informasjonssikkerhet tilsvarende IKT-forskriften i Norge.

Finansinspektionen (FI) er tilsynsmyndighet. FIs virksomhet styres av Regjeringens Reguleringsbrev. Der angir Regjeringen hvilke mål FI skal ha for sin virksomhet, samt hvilke oppdrag Regjeringen vil at FI skal utføre. FIs virksomhet reguleres også i en forskrift som beskriver myndighetenes spesifikke mål, oppgaver og ansvar.

FIs tilsynsansvar er organisert på en annen måte enn Kredittilsynets. Innen FI arbeider seks personer med operative risikoer, hvorav 2-3 har en IT-orientert bakgrunn. Innen

Sikkerhetsenheten finnes det tre personer med denne kompetansen. Sikkerhetsenheten støtter tilsynsarbeidet som FI utfører, men arbeider først og fremst med myndighetssamordning, bl.a. gjennom Krisberedskapsmyndigheten. Generelt arbeider FI ut i fra sitt "Allmänna Råd om styrning och kontroll av Finansiella Företag". FI har laget et overordnet rammeverk for den planleggingen som en virksomhet bør ha for å være beredt til å håndtere eventuelle kriser som måtte oppstå i finanssektoren i dokumentet "Vägledning för kontinutetsplanering (mars 2005)". I 2006 gjennomførte FI en undersøkelse som kun fokuserte på IT- og informasjonssikkerhet, og frem til nå har 13 virksomheter blitt gransket iht. Basel IIs sjablongmetode[12], hvor bl.a. kontinuitetsplanlegging og backup granskes på samme linje som håndteringen av operative risikoer. Ytterligere en tilsynsaktivitet pågår hos FI; en kartlegging av den omfattende utkontrakteringen av svenske IT-tjenester. Utover dette inngår også IT og informasjonssikkerhet i mer generelle tilsynsaktiviteter.

Stedlige tilsyn gjennomføres på en generell basis. Rene IT-tilsyn blir normalt inkludert på andre måter, gjerne gjennom oppfølgingsmøter som fokuserer kun på IT og informasjonssikkerhet, eller gjennom spørreundersøkelser. FI annonserer tilsyn via et skriftlig varsel ca fire uker i forkant. Det forekommer også at FI holder forberedende planmøter eller introduksjonsmøter. I forbindelse med et tilsyn blir virksomheter bedt om å forberede presentasjoner, sende inn rekvirert dokumentasjon, og eventuelt forberede produktdemonstrasjoner. Normalt finner tilsynsmøter sted hos FI, og et stedlig tilsynsmøte varer gjerne 2-3 dager om det er en større virksomhet. FI stiller med et tilsynsteam som alltid består av to personer, hvorav en er oppdragsansvarlig. Virksomheten vil normalt stille med en kontaktperson, noen fra ledelsen, samt virksomhetsrepresentanter og spesialister ved behov.

Ved eventuelle avvik oppfordres det til frivillig iverksetting av forbedringstiltak. Dersom dette ikke skjer, kan FI pålegge virksomheter bøter.

Internt i FI dokumenteres tilsyn i en undersøkelsesrapport, og FIs interne risikosystem oppdateres med risikobedømning på bakgrunn av funn. Eksternt sendes først en uttalelse til virksomheten med den samlede bedømmingen, og eventuelle forslag til forbedringstiltak. Tilsynet avsluttes med en kort rapport. Ingen av de ovenfor nevnte rapporter er offentlige.

4.4.3 Finland

I Finland er det Finansinspektionen som fører tilsyn med finansforetak. Finansinspektionen er administrativt sammenkoplet med Finlands Bank. Utover loven om Finansinspektionen anvendes også loven om Finlands Bank og andre bestemmelser om Finlands Bank på forvaltningen. Det bemerkes at det er Försäkringsinspektionen som fører tilsyn med forsikringsselskapene, så her er det altså to tilsynsmyndigheter som er involvert der man i Norge kun har en; Kredittilsynet. Det etterfølgende avsnittet baserer seg på opplysninger gitt fra Finansinspektionen.

[12] Metode som bankene bruker for å sikre at kapital-allokeringen er risiko sensitiv,separere operasjonell risiko fra kredittrisisko og kvantifisere begge to. Basel II bygger på tre pillarer: Minimum kapitaldekning, tilsynsprosess og markedsdisiplin. Mer informasjon finnes: http://www.bis.org/publ/bcbsca.htm

Finland har en lov om beskyttelse av data som er allmenn og som ikke kun gjelder finansielle foretak. Lovens formål er å beskytte konfidensialitet og integritet[13]. Finansinspektionen har imidlertid gitt en forskrift (Standard 4.4b Hantering av operativa risker) hvor punkt 6.6 berører informationssikkerhet[14](42). Det er ingen eksplisitte krav til risikoanalyser i lovteksten, men standarden berører håndtering av operative risker, herunder også risikovurdering.

Krav til beredskapsplanering finnes både i Kreditinstitutslagen (§6a), i Lagen om utländska kreditinstituts verksamhet i Finland (§13a), i Lagen om placeringsfonder (§4a) og i Lagen om värdeandelssystemet (§13a). Utover disse lover har den Försvarsekonomiska planeringskommissionen gitt et allment råd om beredskapsplanlegging i finansbransjen, og Finansinspektionen jobber med å inkludere det i sin standard om håndtering av operativ risiko. De antar at standarden kan ferdigstilles våren 2007.

Informasjonssikkerhet overvåkes gjennom inspeksjoner hos tilsynsobjektene og innrapportering fra tilsynsobjektene. Finansinspektionens tillsyn er risikoorientert. Det betyr at tilsynene rettes inn mot de mest risikofølsomme virksomhetene. Finansinspektionen forsøker å identifisere risiko og forandringer som kan true den finansielle stabiliteten. Man har ingen standardisert tilsynsmetode slik som COBIT-metodikken hos Kredittilsynet. Finansinspektionen foretar ikke målinger av informasjonssikkerhet, men kredittinstitusjonene følger selv opp ved å bruke indikatorer. Ved avvik har Finansinspektionen flere sanksjonsmuligheter, blant annet anmerkninger, advarsler, politianmeldelse og inndragning av konsesjonen.

4.4.4 Storbritannia

Den britiske finanssektoren er en sentral del av det globale finansielle system, og spiller en viktig rolle i å sikre de fordelene et større og mer integrert marked tilbyr. Storbritannia har tre finansmyndigheter, *HM Treasury*, *The Bank of England, samt The Financial Services Authority (FSA)*, men hovedansvaret for å bevare og utvikle det britiske finansmarkedets posisjon ligger hos sektoren selv. Britiske virksomheter som er kritiske for landets infrastruktur plikter å ha beredskapsplaner på plass, noe som krever tilgjengelighet og tilsvarende sikring av driftsdata, men det blir ikke formelt ført tilsyn med informasjonssikkerhet[15].

De primære lovbestemmelsene brukt til å validere eventuelle IT-reguleringer i finanssektoren er The Financial Services and Markets Act 2000 (FSMA) og The Data Protection Act 1998 (DPA).

FSMA danner et rammeverk for opprettelsen av en regulerende myndighet for den finansielle sektoren. Loven uttruster myndigheten med et bredt spekter av lovfestet makt. Denne loven trådde i kraft 1. desember 2001.

---

13 http://www.finlex.fi/sv/laki/ajantasa/2004/20040516?search%5Btype%5D=pika&search%5Bpika%5D=dataskydd

14 Se www.finansinspektionen.fi

15 Mailkorrespondanse med Mr. M. Davis NISCC - Finance Sector Outreach

Financial Services Authority (FSA) ble opprettet i desember 2001 under FSMA, og er eneste regulerende myndighet for den britiske finanssektoren. I henhold til britisk lov er de fleste britiske finansvirksomheter avhengige av autorisasjon fra FSA. Når de er autorisert, blir de innført i FSAs registre og må følge FSAs regler. Etter at en virksomhet er blitt autorisert av FSA blir de jevnlig kontrollert, og FSA fører tilsyn med virksomhetens administrering, finansielle ressurser og interne systemer. Om nødvendig vil FSA undersøke, straffe eller straffeforfølge enhver virksomhet eller individ som bryter FSAs regler.

Informasjonssikkerhet blir ivaretatt gjennom The National Infrastructure Security Co-ordination Centre (NISCC). NISCC er et tverrsektorielt, statlig senter som tilbyr beskyttelse av essensiell infrastruktur, og er ansvarlig for å beskytte Storbritannias kritiske nasjonale infrastruktur mot elektroniske angrep. NISCC er ikke en rettskraftig organisasjon, og den har ingen myndighet for å føre tilsyn eller utvikle regelverk for finanssektoren eller andre sektorer. NISCC har ikke regulerende myndighet, og deres arbeid er basert på etablering av tillitsforhold mellom deltakerne/medlemmene i organisasjonen. Senteret ble etablert i 1999. NISCC søker å oppnå sine mål gjennom fire brede fokusområder;

- Trusselvurdering
- Samarbeid
- Rådgivning
- Forskning og Utvikling

En fundamental del av NISCCs ansvarsområde er å gi periodiske forsikringer til innenriksministeren at Storbritannias kritiske nasjonale infrastruktur er tilstrekkelig beskyttet mot elektroniske angrep. I forbindelse med det benytter NISCC seg av indikatorer i produseringen av Assurance Reports (rapporter som beskriver sikkerhetsnivået på landets kritiske nasjonale infrastruktur), men disse indikatorene røper ingen informasjon bedrifter ikke frivillig har delt med NISCC, og det antas at det er lite informasjon ettersom Assurance Reports blir offentliggjort.

4.5 Oppsummering

Noe av hensikten med å sammenligne norsk praksis med utenlandske praksis var å søke etter mulige forbedringer med særlig fokus på bruk av måleindikatorer og metrikker. Vår begrensede informasjon fra utenlandske tilsynsmyndigheter gjør det vanskelig å gjennomføre en rettferdig sammenligning av de ulike lands tilsynsmyndigheter. Det generelle inntrykket er at man i norsk finanssektor har kommet langt i forhold til å ha en strukturert og etterprøvbar tilsynsprosess innen informasjonssikkerhet, gjennom bruk av evalueringsskjema basert på COBIT. Selv om målingene er basert på kvalitative vurderinger og ja/nei-svar, finner vi ikke mer kvantitative løsninger hos de andre landene vi har sammenlignet norsk praksis med.

Det er nasjonale forskjeller i hvordan fokus rettes mot informasjonssikkerhet fra myndighetenes side. I Storbritannia er sektoren selv pålagt mye ansvar for informasjonssikkerhet, mens Norge har IKT-forskriften og Danmark har tolket og konkretisert lovverket i retningslinjer. Sverige har ikke tilsvarende lovverk som i Norge, men basere tilsyn på generelt regelverk om finansforetak.

Finland har utviklet en forskrift som bankene skal følge. Innenfor Norden er det tett samarbeid mellom de ulike tilsynsmyndighetene og det arbeides med å harmonisere lovverket og språklige definisjoner.

I tabell 4.1 har vi laget en kortfattet oppsummering av tilsynspraksis i de ulike landene.

	Norge	**Danmark**	**Sverige**	**Finland**	**Storbritannia**
Lovverk	Kredittilsyns-loven IKT-Forskriften	Lov om finansiel virksomhed Vejledning om kontrol- og sikrings-foranstaltninger på it-området	Ingenting som omhandler informasjons-sikkerhet	Lov for bank virksomhter (forsikring er underlagt egen lov) Lov om databeskyttelse Standard/ retningsliner	 Financial Services and Markets Act 2000 (Data Protection Act 1998)
Tilsyns-myndighet	Kredittilsynet (KT)	Finanstilsynet	Finans-Inspektionen (FI)	Finans-Inspektionen	The Financial Services Authority (FSA)
Tilsynsmåte	Stedlig Dokument-basert	Stedlig Dokumentbasert	Stedlig Dokumentbasert	Stedlig tilsyn	Fører ikke tilsyn med informasjonssik kerhet
Beredskaps-planer	Pålagt av lov	Pålagt av lov	BASEL II stiller krav til dette, men regelverket er frivillig å følge	Inngår i Standarden	Plikter å ha dette
ROS – analyser	Pålagt av lov	Pålagt av lov	Ikke pålagt av lov, men anbefalt a ha generelle ROS-analyser (ikke IT-spesifikke)	Inngår i Standarden	Ikke pålagt av lov, men har Assurance Reports
Måle-indikator metrikker brukt i tilsyns-prosessen	Ingen Egenutviklet skjema basert på COBIT	Ingen	Ingen	Ingen	Ingen
Fokus fra myndigheter på informasjon s-sikkerhet	Lov og IKT-forskrift Statlig tilsyn innen IS	Lov og veiledning Statlig tilsyn som i Norge	IT inngår i generelle tilsynsaktiviteter Oppfølgingsmøte for spesielle IT-tilsyn	Allmenngyldig lov om databeskyttelse	Generelt tilsyn NISCC er en viktig aktør innen informasjonssik kerhet i kritisk infrastruktur

Tabell 4.1 Tilsyn av finanssektoren i Norge, Danmark, Sverige og Storbritannia

5 TILSYN OG MÅLING AV INFORMASJONSSIKKERHET I ENERGISEKTOREN

Kapittelet beskriver hvordan tilsyn og måling av informasjonssikkerhet skjer i den norske

finanssektoren. I tillegg er noen erfaringer fra utlandet inkludert.

5.1 Lovverk og forskrifter innen emnet informasjonssikkerhet

Energiloven[16] kommer til anvendelse på all produksjon, omforming, overføring, omsetning og fordeling av energi, og skal sikre at dette foregår på en samfunnsmessig rasjonell måte. Kapittel 6 i loven omhandler beredskap i kraftsektoren, og definerer Kraftforsyningens beredskapsorganisasjons (KBO) rolle som ansvarlig for kraftforsyningen under beredskap og i krig. Lovens § 6-2 gir departementet (OED) rett til å "*treffe vedtak om sikring av kraftforsyningsanlegg mot skade som skyldes naturgitte forhold, teknisk svikt eller tilsiktede ødeleggelser i fred, under beredskap og krig*". Loven trådde i kraft 1. januar 1991.

Energilovforskriften[17] kommer til anvendelse ved planlegging, bygging og drift av anlegg for produksjon, omforming, overføring og fordeling av elektrisk energi, varmeenergi produsert i fjernvarme- og fjernkjøleanlegg, samt ved omsetning av elektrisk energi. Forskriften skal sikre at dette foregår på en samfunnsmessig rasjonell måte. Kapittel 6 i forskriften omhandler beredskap. I henhold til § 6-1 er formålet med beredskap i kraftforsyningen å forebygge og begrense skade på liv og eiendom forårsaket av naturgitte forhold, teknisk svikt, terror- og sabotasjeaksjoner eller ved rasjonering i fred, under beredskap og i krig. § 6-2 beskriver hvordan enheter i KBO skal etablere tilfredsstillende beredskap. Videre stiller § 6-4 krav til forebyggende sikkerhetstiltak hos KBO-enhetene. Blant annet stilles det krav til "*beskyttelse av viktige informasjonssystemer og sensitiv eller sikkerhetsgradert informasjon*". I henhold til § 6-7 pålegges enheter i KBO å etablere internkontroll for kraftforsyningsberedskap. § 6-7 stiller også krav til dokumentasjon av tiltak for å påse at de krav som finnes i forskriften overholdes. Forskriften trådde i kraft 1. januar 1991.

Forskrift om beredskap i kraftforsyningen (Beredskapsforskriften)[18] gjelder alle enheter i KBO. Forskriften stiller krav til at enhetene skal ha et kvalitetssystem som dokumenterer at kravene i forskriften er oppfylt, oppdaterte risiko- og sårbarhetsanalyser, oppdatert og funksjonell beredskapsplan og at de skal gjennomføre beredskapsøvelser. Kapittel 2 beskriver KBOs oppgaver, organisering, ansvar og plikter. I henhold til forskriftens § 4-3 om anskaffelser i kraftforsyningen, skal det inngås sikkerhetsavtale mellom leverandør og NVE eller vedkommende enhet i KBO dersom leverandøren kan få tilgang til sensitiv informasjon gjennom sitt oppdrag. Forskriftens kapittel 6 omhandler informasjonssikkerhet. Forskriften setter følgende krav til informasjonssikkerheten hos enheter i KBO:

- § 6-1 sier generelt at enhetene skal "*foreta en løpende helhetlig vurdering av informasjonssikkerheten*". KBO – enheter pålegges i tillegg å utpeke en datakyndig IT-sikkerhetsleder.
- § 6-2 påpeker at *sensitiv informasjon om kraftforsyningen ikke skal offentliggjøres*, samt definerer områder hvor sensitiv informasjon skal avskjermes for uvedkommende til

[16] LOV 1990-06-29 nr 50: Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.
[17] FOR 1990-12-07-959: Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.
[18] FOR 2002-12-16 nr 1606

enhver tid.

- § 6-3 *pålegger enheter å til enhver tid ha oppdaterte sikkerhetskopier av informasjon og programvare som er av betydning for kraftforsyningens drift og sikkerhet.*
- § 6-4 stiller *særlige krav til driftskontrollsystemer*.
- § 6-5 *pålegger enheter i KBO å ha tilgang til et mobilt sambandssystem* dersom enheten er avhengig av pålitelig mobilkommunikasjon for drift, sikkerhet eller gjenoppretting av funksjon.
- § 6-6 *pålegger kommunikasjonsbaserte vernsystemer i sentral- og regionalnett å ha pålitelige og sikre samband som fungerer upåvirket av feiltilstander i kraftsystemet.*
- I henhold til forskriftens § 7-1 plikter alle enheter i KBO å *innrapportere ekstraordinære situasjoner til NVE*. Dette gjelder også situasjoner innen feltet informasjonssikkerhet.

NVE har ikke hjemmel i noe lovverk til å føre direkte tilsyn med virksomheters leverandører, men lovverket stiller krav til at sikkerhetsavtale skal inngås mellom leverandør og NVE eller enhet i KBO dersom leverandøren kan få tilgang til sensitiv informasjon (jf Beredskapsforskriftens § 4-3). NVE kan imidlertid vedta at virksomheter som leverer varer, utfører tjenester eller andre som kan ha betydning for kraftforsyningens drift og sikkerhet skal inngå i KBO (Beredskapsforskriftens §2-2).

I forskrift om beredskap i kraftforsyningen omfatter begrepet informasjonssikkerhet alle typer beredskapsmessig relevant informasjon og informasjonshåndtering, samt driftskontrollfunksjoner og mobil kommunikasjon (29). Av særskilt viktighet vil det være å hindre at uvedkommende får tilgang til sensitive opplysninger om kraftforsyningen i landet, samt sørge for oppetid for systemer som ivaretar viktige driftskontrollfunksjoner. Sensitiv informasjon om kraftforsyningen vil være informasjon som, i de gale hender, kan brukes til å skade eller hindre funksjoner i kraftforsyningen. Noe av denne informasjonen vil være sikkerhetsgradert og må behandles i henhold til Sikkerhetsloven[19].

Beredskapsforskriften trådde i kraft 1. januar 2003. NVE har utarbeidet en veiledning til beredskapsforskriften for å gi anvisninger til virksomhetene om hvordan de kan forstå og oppfylle de krav denne stiller. Denne veiledningen blir revidert med jevne mellomrom, og i arbeidet med dette blir innspill fra virksomheter i sektoren vektlagt.

5.2 Tilsynsprosessen i kraftsektoren

Når NVE Seksjon for beredskap fører tilsyn med sikkerhet og beredskap, er det med utgangspunkt i beredskapsforskriftens krav. Reglene som omhandler informasjonssikkerhet i forskriften og forskriften som helhet er av funksjonell karakter. NVE utarbeider spørsmål som kan danne utgangspunkt for revisjonen. Her er flere spørsmål (de fleste ja/nei) koplet mot forskriftens ulike paragrafer. NVE lager både omfattende revisjonsskjemaer og enklere spørsmålslister.

NVE baserer sin revisjonsmetodikk blant annet på standarden NS-EN ISO 19011 Retningslinjer

[19] LOV 1998-03-20-10: Lov om forebyggende sikkerhetstjeneste, se også kapittel 6.2

for revisjon av kvalitet- og/eller miljøstyringssystemer. Standarden beskriver metodikk og stiller krav til revisorer. Når NVE fører tilsyn må de forholde seg til Offentlighetsloven[20] og Forvaltningsloven[21]. Avvik hos tilsynsobjektene er å anse som brudd på norsk lov, og tilsynsobjektene er pliktige til å lukke disse avvikene.

NVE utfører stedlig tilsyn og spørreundersøkelser. I november 2005 sendte NVE ut en spørreundersøkelse til alle enheter i KBO. Spørsmålene i undersøkelsen omhandlet sentrale deler av beredskapsforskriften. KBO-enhetene var pålagt å svare på undersøkelsen, og svarene NVE fikk, ble brukt til å fatte vedtak mot virksomhetene. Avdekket svarene avvik, ble virksomhetene pålagt å lukke disse. I de siste årene har NVEs beredskapsseksjon holdt stedlig tilsyn med omtrent 20 virksomheter i året.

Før *stedlig tilsyn* finner sted, utarbeider NVE en tilsynsplan. I arbeidet med denne blir det foretatt en vurdering av hvilke virksomheter det skal føres tilsyn med og tema for tilsynet. Tilsynsobjektene blir valgt ut blant annet på grunnlag av tidligere gjennomførte tilsyn. Da har det vært ønske om å se på de virksomheter som kom dårligst ut samt den/de som kom best ut. I tillegg føres det oftere tilsyn med sektorens viktigste aktører. Det blir så laget relevante revisjonsspørsmål med utgangspunkt i forskriftstekst og i henhold til tema som skal være gjenstand for revisjonen. Disse spørsmålene skal helst gi ja/nei-svar. Tidligere tilsyn har blant annet hatt som tema risiko- og sårbarhetsanalyser. Høsten 2006 ble det utført tilsyn med spesiell fokus på temaet informasjonssikkerhet.

Det utarbeides en plan over hvem hos NVE som skal besøke hvilke enheter og når. Deretter tar NVE kontakt med de aktuelle tilsynsobjekter. Dette skjer som oftest to måneder før tilsynsbesøket skal skje. NVE har også hjemmel for å føre uanmeldte tilsyn, men dette benyttes ikke ofte.

NVE vil ofte kreve å få oversendt aktuell dokumentasjon fra tilsynsobjektet før tilsynsmøtet finner sted. Dette vil være dokumentasjon som går spesielt på temaet for tilsynet, og kan for eksempel være risiko- og sårbarhetsanalyser, virksomhetens beredskapsplan og IT-sikkerhetsinstruks. Når slik dokumentasjon er oversendt, vil NVE gå gjennom denne som en del av forarbeidet før tilsynsmøtet finner sted.

Tilsynsmøtet finner som regel sted hos tilsynsobjektet. NVEs revisjonsteam stiller som oftest med to deltakere. I dette teamet vil det være en revisjonsleder og en revisjonsmedarbeider. Det forekommer at en tredje fagrevisor også deltar. Fra virksomhetens side ønsker NVE typisk å snakke med administrerende direktør, beredskapsleder, beredskapskoordinator og ledere innen eventuelle andre felt som er tema for tilsynet.

Under tilsynsmøtet stiller representantene fra NVE spørsmål og kan kreve at virksomheten fremlegger aktuell dokumentasjon for å understøtte svarene som blir gitt. Spørsmålene er av

[20] LOV 1970-06-19-69: Lov om offentlighet i forvaltningen
[21] LOV 1967-02-10: Lov om behandlingsmåten i forvaltningssaker

overordnet karakter, og NVE har derfor sjelden behov for å intervjue ansatte på lavere nivå i virksomheten. Tilsynsførerne fra NVE bruker også stikkprøver ol, og observerer forhold når de besøker virksomheten. Eventuelle observerte synlige avvik blir påpekt. Dette kan for eksempel være om det er tilstrekkelig adgangskontroll. NVE benytter seg ikke av noen måleindikatorer eller metrikker for å måle informasjonssikkerhet eller annet hos tilsynsobjektet.

Etter at tilsynsmøtet er holdt, kommenterer tilsynsførerne fra NVE muntlig for bedriften hvilke avvik de har oppdaget og hvilke observasjoner som er gjort. Det blir så utarbeidet en revisjonsrapport med oversikt over hvor tilsynet fant sted, hvem som deltok, hvor lenge møtet varte og hvilke avvik som ble funnet. Revisjonsrapporten blir oversendt til tilsynsobjektet sammen med tidsfrister for å lukke avvikene. Blir ikke avvikene lukket, oversendes enkeltvedtak i henhold til forvaltningslovens bestemmelser. Virksomheten er pålagt å rette seg etter vedtak, men har tre ukers klagefrist etter at vedtaket er sendt ut. Dersom ikke vedtak blir fulgt opp av virksomheten, og en eventuell klage ikke blir tatt til følge, vil virksomheten bli ilagt en daglig tvangsmulkt av NVE inntil forholdet er rettet.

I etterkant av et tilsyn vil NVE ofte gjøre mye veiledningsarbeid. Virksomhetene vil ringe og ha spørsmål om hva som vil være tilfredsstillende oppfølging av vedtak. Ofte møter NVE på et problem under sitt tilsynsvirke ved at virksomheter ønsker en slags godkjennelse av de tiltak de har satt inn og metoder de bruker for å etterleve beredskapsforskriftens krav. En slik godkjenning skal ikke NVE gi, og virksomhetene må selv vurdere risiko og sette inn de tiltak de mener er nødvendige. Beredskapsforskriften setter funksjonskrav, og ut fra disse må virksomhetene som er omfattet av forskriften, selv velge metode og ambisjonsnivå for å oppfylle kravene. I NVEs veiledning til beredskapsforskriften er enkelte metoder for å oppfylle disse kravene beskrevet. Om virksomheten velger å benytte seg av disse metodene, trengs ikke ytterligere dokumentasjon. Virksomheten står fritt til å bruke andre metoder, men de må dokumenteres.

I dag er det liten bruk av måleindikatorer for informasjonssikkerhet i kraftsektoren. NVEs spørreundersøkelse danner grunnlag for måleindikatorer som %-andel ja-svar på virksomhetsnivå og %-andel ja-svar på type spørsmål. Dette gir NVE muligheter til å rangere virksomhet og fagområde etter avvik. En større aktør i sektoren har i skrivende stund på gang et prosjekt for å finne slike måleindikatorer de kan bruke. Hovedårsaken for mangelen på bruk av måleindikatorer i bransjen er at det er vanskelig å se nytten av indikatorer som måler sikkerhetsnivået, og at det heller ikke finnes gode indikatorer. Selv om det ikke er noen utstrakt bruk av måleindikatorer i den norske kraftsektoren, er det blitt gjort arbeid på området.

5.3 Erfaringer og forbedringspotensial innenfor tilsynsvirksomhet

Eksterne tilsyn med informasjonssikkerhet i kraftbransjen har en positiv effekt ved at det stilles formelle krav til virksomheten, i stedet for at man kun har meninger internt om hvordan ting burde gjøres. Det kan også gjøre det enklere å få gjennomslag for sikkerhetstiltak hos ledelsen. Tilsyn kan synliggjøre problemstillingene og øke motivasjon og innsats.

Tilsyn med informasjonssikkerhet i kraftsektoren er også med på å bevisstgjøre virksomheter på de bestemmelser som finnes på området. Dette er illustrert ved at noen mindre aktører ikke var klar over de krav beredskapsforskriften stilte på området. Det medførte at i etterkant av spørreundersøkelsen som NVE sendte ut høsten 2005, var det flere virksomheter som kontaktet NVE og mente at de var for små eller for spesielle til at dette regelverket kunne omfatte dem.

De fleste virksomheter er positive til NVE og deres tilsynsarbeid. NVEs representanter opplever en høy grad av åpenhet og ærlighet ute hos virksomhetene, og har ikke inntrykk av at tilsynsobjekter prøver å skjule mangler og avvik fra dem. Etter at NVE har utført tilsyn innen et tema, får ofte temaet økt fokus i bransjen. Dette skjedde etter stedlige tilsyn av risiko- og sårbarhetsanalyser, som ble etterfulgt av innlegg og artikler i tidskrifter ol. Det bidrar til å heve oppmerksomheten i bransjen. 2006 arrangerte NVE egne seminarer om informasjons- og IKT-sikkerhet for bransjen i etterkant av det dokumentbaserte tilsynet de hadde, som blant annet omhandlet disse temaene hos virksomhetene. NVE avholder årlig en beredskapsøvelse i samarbeid med Statnett og OED, hvor man tar for seg konsekvenser av uønskede ekstraordinære hendelser. IKT-sikkerhet har vært blant temaene her.

Det krever stor grad av flerfaglighet både innenfor teknologi, juss og kraftsystem for å utføre tilsyn innen informasjonssikkerhet. NVE og andre som har dette som virke, har derfor store utfordringer på området når IKT-systemene er i stadig utvikling. Virksomheter innen kraftsektoren vil være utsatt for mange forskjelligartede trusler, og det må tas utgangspunkt i alle disse når sikkerhetstiltak skal iverksettes.

5.4 Utenlandsk praksis

5.4.1 Danmark

Danmarks ”Lov om elforsyning”[22] har i henhold til § 1 som formål å sikre at landets elforsyning tilrettelegges og gjennomføres i overensstemmelse med hensynet til forsyningssikkerhet, samfunnsøkonomi, miljø og forbrukerbeskyttelse. Lovens § 85b pålegger virksomheter innen elforsyningen å gjennomføre nødvendig planlegging og tiltak for å sikre elforsyningen i beredskapssituasjoner og andre ekstraordinære situasjoner. Videre har Danmark nylig vedtatt ”Lov om beredskab for elsektoren”[23] som trådde i kraft 1. februar 2005. Denne er tydelig inspirert av den norske beredskapsforskriften for kraftforsyningen. Loven pålegger virksomheter å utarbeide sårbarhetsvurderinger og beredskapsplaner. § 19 pålegger virksomhetene å registrere gitte hendelser av relevans for beredskapssituasjoner. Loven stiller imidlertid få krav til informasjonssikkerhet, kun to paragrafer omhandler emnet;

- § 11 pålegger at anlegg klassifisert som klasse 1 eller 2 (anlegg av vesentlig betydning for å opprettholde elektrisitetsforsyningen for henholdsvis et sammenhengende forsyningssystem eller på regionalt nivå) skal ha lav sårbarhet ovenfor funksjonssvikt av vesentlige IT-systemer.

[22] LBK nr 286 af 20/04/2005
[23] BEK nr 58 af 17/01/2005

- § 25 krever at sårbarhetsvurderinger og beredskapsplaner samt annet materiale av vesentlig relevans skal behandles fortrolig og ikke komme uvedkommende i hende. Paragrafen stiller videre krav til oppbevaring av slikt materiale, og påpeker at forsendelse av dette skal skje via brev og ikke må foregå elektronisk.

I henhold til lovens § 21, er det den systemansvarlige virksomhet som skal føre tilsyn med virksomhetenes beredskapsarbeid, og sørge for at reglene i loven er oppfylt.

Systemansvarlig virksomhet, Energinet.dk, ble opprettet etter fusjon mellom selskapene Elkraft, Eltra og Gastra, 1. januar 2005. Tilsynsarbeidet Energinet.dk har i henhold til den ovenfor nevnte loven om beredskap har derfor nylig startet. I kraft av loven måtte alle selskapene den omfattet sende inn en beredskapsplan til Energinet.dk for godkjennelse innen 1. mai 2006. I juni 2006 utførte Energinet.dk et pilotprosjekt hvor enkelte tilsyn ble utført med fokus på om selskapenes godkjente beredskapsplaner var implementert i praksis. Informasjonssikkerhet har ikke vært noe tema ved utførte tilsyn. Innen den danske elektrisitetsforsyningen er det i utgangspunktet ikke vurdert at et brudd i informasjonssystemer kan medføre forsyningssvikt.

Tilsyn med beredskap innen den danske elektrisitetssektoren er planlagt over en treårig periode, hvor alle virksomheter omfattet av loven er inkludert. Tilsynene vil bli varslet, planlagt og avtalt med virksomhetene i rimelig tid på forhånd for å sikre at de personer Energinet.dk ønsker å snakke med er tilstede og har tid til å delta. Et tilsyn vil vare i 1-3 dager avhengig av virksomhetens størrelse og om denne eier viktige anlegg i den danske elforsyningen. I etterkant av tilsynet vil Energinet.dk utarbeide en tilsynsrapport som virksomheten og tilsynsførerne blir enige om. Denne rapporten kan inneholde anbefalinger og gode råd til forberedelse, samt påpeke avvik som virksomheten må lukke innen en avtalt tidsperiode. Rapporten vil ikke bli offentliggjort. Energinet.dk har ikke mulighet til å pålegge virksomheter tvangsmulkt eller annen form for straff. Om det skulle oppstå uenigheter mellom en virksomhet og Energinet.dk, vil uenighet kunne avgjøres av den danske Energistyrelsen[24]. Skulle forholdet ikke bli avklart ved dette, kan saken bringes inn for retten.

Energinet.dk vil med henhold til tilsynsmetodikk legge seg opp mot ISO-serien, da spesielt ISO 9001 om kvalitetsstyring og ISO 14001 om miljøledelsessystemer. Dette gjøres på grunnlag av at mange av de involverte virksomheter er sertifisert etter disse standardene, og dermed gjør det naturlig å benytte seg av de metoder og begreper som brukes i disse.

Energinet.dk har ikke utviklet noen form for indikatorer eller metrikker for å måle nivå av informasjonssikkerhet eller annet hos tilsynsobjektene.

Den danske Energistyrelsen har tilsynsansvar for Energinet.dks beredskapsarbeid, og da også Energinet.dks tilsynsvirksomhet med øvrige virksomheter. Det er per i dag ikke fullstendig

[24] Den danske Energistyrelsen er underlagt Transport og Energiministeriet, og skal være rådgiver om energispørsmål for ministeren samt ivareta administrasjonen av den danske energilovgivning (http://www.ens.dk/sw11490.asp, 10. august).

fastlagt hvordan dette tilsynet skal organiseres. Energinet.dk er forpliktet til å utarbeide blant annet beredskapsplaner og sårbarhetsvurderinger som skal oversendes Energistyrelsen. I tillegg holdes det jevnlige møter mellom de to virksomhetene.

I Danmark har Beredskapsstyrelsen[25] utarbeidet en modell for risiko- og sårbarhetsanalyser (ROS-analyser) av samfunnets kritiske funksjoner. Energinet.dk og Energistyrelsen har i samarbeid med Beredskapsstyrelsen tilpasset denne ROS-modellen til el- og gassektoren.[26] I modellen er det definert seks scenarier som virksomhetene omfattet av "Lov om beredskab for elsektoren" skal vurdere. I tillegg må virksomhetene vurdere om det er behov for supplerende scenarier. Scenario nr. 6 omhandler et internt IT-brudd. I scenariet inntreffer IT-bruddet på en hverdag etter arbeidstid, og IT-systemene vil ikke være fullstendig tilgjengelige før etter syv dager. Virksomhetene er pålagt å gjennomføre disse ROS-analysene i henhold til lovens § 6.

5.4.2 Sverige

Den svenske Ellag[27] gir generelle retningslinjer for produksjon, overføring og forbruk av elektrisitet, samt handel med elektrisitet. I tillegg finnes det en Elberedskapslag[28] som inneholder bestemmelser om beredskap vedrørende produksjon og overføring av elektrisitet samt handel med elektrisitet. Förordning om krisberedskap och höjd beredskap[29] omfatter statlige myndigheter som gjennom sin virksomhet skal minske sårbarheten i samfunnet og utvikle en god måte å håndtere sine oppgaver på under krisesituasjoner i fredstid og høy beredskap (§ 1). Informasjonssikkerhet i kraftsektoren er ikke et tema i noe av dette lovverket, men det er derimot nevnt i Säkerhetsskyddslag (1996:627) § 9: *Vid utformningen av informationssäkerheten skall behovet av skydd vid automatisk informationsbehandling beaktas särskilt.* Säkerhetsskyddsförordningen (1996:633) gir nærmere spesifikasjoner mht hemmelighold av informasjon vedrørende rikets sikkerhet. Dette tilsvarer den norske sikkerhetslovens med forskrift som NSM fører tilsyn med.

I Sverige er det utnevnt en Elberedskapsmyndighet som blant annet har tilsynsansvar iht Elberedskapslagen og Säkerhetsskyddslagen overfor kraftselskaper. Denne myndighetsfunksjonen innehar Svenska Kraftnät. Som Elberedskapsmyndighet må Svenska Kraftnät forholde seg til regelverket i "Förordning om krisberedskap och höjd beredskap", og plikter i henhold til dette å gjennomføre årlige ROS-analyser som omhandler deres ansvarsområde innen beredskap. Disse analysene skal oversendes det svenske regjeringskontoret. Den svenske regjeringen, via riksrevisjonen, fører tilsyn med at Svenska Kraftnät etterlever sine forpliktelser som Elberedskapsmyndighet, og Svenska Kraftnät informerer årlig regjeringen om sitt beredskapsarbeid og annet virke. Nettselskap i den svenske

[25] Beredskapsstyrelsen er underlagt det danske Forsvarsministeriet, og leder det statlige redningsberedskap samt tar seg av koordineringen av den sivile sektors beredskap (http://www.brs.dk/praesentation/index.htm, 10. august).
[26] Den fullstendige ROS-modellen kan finnes på http://www.energinet.dk/da/menu/Sikkerhed+og+beredskab/Beredskabsplanl%c3%a6gning/Risiko+og+s%c3%a5rbarhedsanalyser/Risiko+og+s%c3%a5rbarhedsanalyser.htm (10. august 2006)
[27] SFS nr 1997:857: Ellag
[28] SFS nr 1997:288: Elberedskapslag
[29] SFS nr 2006:942: Förordning om krisberedskap och höjd beredskap

kraftforsyningen plikter også å gjennomføre ROS-analyser, men per i dag er det ikke klarlagt hvilken myndighet deres analyser skal leveres til. For andre aktører i kraftmarkedet er det ingen myndighet som fører tilsyn med at ROS-analyser blir gjennomført. Svenska Kraftnät har utarbeidet veileder for risikoanalyse[30].

Svenska Kraftnät krevde tidligere å få tilsendt beredskapsplaner fra aktører i den svenske kraftsektoren, og de har fortsatt myndighet til å kreve inn dette, men de har ikke benyttet seg av dette de siste to år.

Det føres ikke tilsyn med beredskap eller informasjonssikkerhet i den svenske kraftsektoren på samme måte som det gjøres i Norge. I Sverige blir det hvert år tildelt midler (260 millioner SEK) fra staten som skal brukes til beredskapstiltak hos virksomheter i sektoren. Det er opp til Elberedskapsmyndigheten å fordele disse midlene til virksomhetene, og den tilsynsaktivitet som blir utført i forbindelse med beredskap i den svenske kraftsektoren vil omhandle å vurdere hvem som skal tildeles midler. Beredskapstiltakene skal sikre landets kraftforsyning i tilfelle av krig, samt i ekstreme situasjoner. Andre tiltak for å sikre mot mindre alvorlige situasjoner, må aktørene i sektoren selv vurdere nødvendigheten av og sette av midler til. Beredskapstiltak det bevilges midler til kan omhandle informasjonssikkerhet, for eksempel ved sikring av driftssentral og dublering av datautstyr.

5.4.3 Finland

Energisektoren i Finland sorterer under Energi och Handelsministeriet[31]. Energimarknadsverket er ett ”sakkunnigämbetsverk”, som startet sin virksomhet som Elmarknadscentralen da den finske Elmarknadslagen trådde i kraft i august 1995. Elmarknadscentralen ble omdannet til Energimarknadsverket den 1. august 2000, og utvidet virksomheten til også å dekke naturgassmarkedet[32]. Energimarknadsverkets hovedoppgave er å overvåke at lovgivningen følges og fremme konkurranse innen el- og naturgassmarkedet. Tilsynsoppgavene realiseres i samarbeid med Handels- och industriministeriet, Konkurrensverket og visse andre myndigheter.

Forsyningsberedskap er å trygge samfunnets økonomiske funksjoner av ulike slag. Næringsliv og offentlig forvaltning samvirker for å oppnå målsettingene om beredskap. Försörjningsberedskapscentralen er underlagt Energi och Handelsministeriet og har blant flere oppgaver, oppgaven med å sikre at nødvendige tekniske system fungerer og trygge kritisk vare- og tjenesteproduksjon.

”Lag om dataskydd vid elektronisk kommunikation” gjelder her som i finanssektoren. Försörjningsberedskapscentralen har i samarbeid med næringsliv og industri utarbeidet instruksjoner og anbefalinger for hvordan informasjonssikkerhet skal ivaretas i krisesituasjoner. Försörjningsberedskapscentralen bistår bedrifter og myndigheter med å utarbeide en beredskapsplan der for eksempel sikkerhet til informasjonssystem og databasenes planlegges.

[30] http://www.svk.se/upload/4190/Sakerhetsanalys.pdf
[31] http://www.ktm.fi/index.phtml?l=sv&s=196
[32] http://www.ktm.fi/index.phtml?l=sv&s=1445

Det finnes metoder for å overvåke beredskapsnivået og redundansen innen ulike bransjer, og benchmarking og øvelser kan kartlegge mangler i bedriftenes og myndighetenes beredskapsnivå. Det finnes ikke indikatorer for informasjonssikkerhet, men det finnes et nylig lansert system som baserer seg på beredskapsindikatorer innen ulike bransjer. Tilstanden illustreres gjennom fargekoder.

5.4.4 Storbritannia

Energy Act 2004 og Electricity Act 1989 omhandler ikke informasjonssikkerhet eksplisitt. Alle aktører i elsektoren må ha lisens for å drive sin virksomhet. Som lisensinnehaver finnes det flere Standard Conditions de må forholde seg til.

I Storbritannia er Department of Trade and Industry (DTI) det departement som tar seg av energirelaterte saker, fra produksjon til forsyning. Departementet skal sørge for konkurransedyktige energimarkeder som samtidig sikrer en trygg, sikker og bærekraftig energiforsyning for Storbritannia. Videre er Office of Gas and Electricity Markets (Ofgem) regulatoren i Storbritannias gass- og elektrisitetsindustri. Deres hovedprioritet er å beskytte forbrukere og sikre Storbritannias energiforsyning, noe de gjør gjennom å fremme effektive konkurransedyktige markeder. DTI har sammen med Ofgem ansvar for å overvåke energiforsyningssikkerheten i de britiske gass- og elektrisitetsmarkedene. Dette gjøres gjennom Joint Energy Security of Supply Working Group (JESS). JESS utgir en halvårlig rapport med oversikt over sikkerheten i forsyningen av energi i Storbritannia. JESS arbeider også med å utvikle indikatorer for forsyningssikkerheten i landet, men disse indikatorene sier noe om utviklingen i markedet, og det er ingen indikatorer eller metrikker til bruk i måling av informasjonssikkerhet eller annet hos virksomheter (31)(32)(33)(34).

Det er også etablert en Energy Emergencies Executive (E3) som skal overvåke hvordan beredskapsplanleggingen i energisektoren er strukturert og praktisert. E3 er ledet av DTI, og inkluderer Ofgem, National Grid samt alle store aktører i sektoren (32). I tillegg til energimyndighetene, har NISCC en undergruppe som tar for seg energisektoren (for mer informasjon om NISCC, se kapittel 4.6.3).

Reguleringsmyndighetene i Storbritannia innehar en veldig ulik rolle fra den i Norge. Det drives ikke med den form for stedlig tilsyn som her i Norge, men overvåkning og oppfølging av at virksomheter legger til rette for et konkurransedyktig marked samt opprettholder de krav som stilles i den lisensavtalen de har. Det vil sjelden forekomme at myndighetene pålegger virksomheter å rette eventuelle avvik de måtte oppdage. Men dersom det har oppstått en sikkerhetshendelse som resulterte i at virksomheten ikke kunne opprettholde noen av sine forpliktelser, vil myndighetene (i form av Ofgem) foreta en undersøkelse av årsaken til hendelsen. Dersom de da skulle oppdage at årsaken var manglende informasjonssikkerhet (eller annen mangel hos virksomheten), vil de sannsynligvis reagere med tiltak motvirksomheten. Med andre ord, virksomheter får ikke pålegg eller straff av myndighetene så lenge sikkerhetsbrudd ikke blir oppdaget.

5.4.5 Oppsummering

Tabell 5.1 oppsummerer funnene fra den internasjonales sammenligningen.

	Norge	**Danmark**	**Sverige**	**Finland**	**Storbritannia**
Lovverk	Energiloven, Energilov-forskriften, Beredskaps-forskriften med krav til informasjons-sikkerhet Veiledning til forskrift	Lov om elforsyning, Lov om beredskab for elsektoren inklusive krav til informasjons-sikkerhet	Elberedskaps -lag, og Ellag Säkerhetsskydds-lagen Ikke noe i lovverket som omhandler informasjons-sikkerhet	Energilov Forsynings-beredskapslov Lov om databeskyttelse	Ikke noe spesifikt lovverk som omhandler informasjonssik kerhet i sektoren Energy Act og Electricity Act
Tilsyns-myndighet	NVE	Energinet.dk	Svenska Kraftnät	Försörjningsber edskaps-centralen	Ofgem/NISSCI
Tilsynsmåte	Stedlig/doku mentbasert	Stedlig	Føres ikke tilsyn	Føres ikke eget tilsyn med informasjons-sikkerhet	Føres ikke tilsyn Uønskede hendelser følges opp
Beredskaps-planer	Pålagt av lov	Pålagt av lov	Svenska Kraftnät kan kreve at virksomheter oversender dette til dem, men dette benytter de seg ikke lenger av	Pålagt ved lov, Försörjningsber edskaps-centralen organiserer øvelser og fører tilsyn ut fra hensyn til forsyning	Plikter å ha dette
ROS – analyser	Pålagt av lov	Pålagt av lov	Nettselskaper samt Svenska Kraftnät plikter å ha dette, men ikke andre aktører	Øvelser gjennomføres innen forsynings-beredskap	Ikke pålagt av lov, men har Assurance Reports
Bruk av måle-indikatorer/ -metrikker	Egenutvikled e basert på tilsyn	Ingen	Ingen	Nei, men noen brukes innen forsynings-beredskap	Ingen
Fokus fra myndigheter på informasjon -sikkerhet	Mye, via lovverk mm og andre virkemidler som samarbeidsgr upper etc.	Ikke ansett som kritisk for dansk elforsyning.	Lite konkret og lovpålagt	Lov om databeskyttelse gjelder alle	Lite konkret og lovpålagt, Informasjonsdel ing via f.eks. NISCC.

Tabell 5.1. Tilsyn av kraftsektoren i Norge, Danmark, Sverige, Finland og Storbritannia

Innen lovverk og tilsynsføring er det store forskjeller mellom landene. Norge har lovverk, forskriftstekst og veiledning relatert til informasjonssikkerhet som danne grunnlag for tilsyn med informasjonssikkerhet i kraftsektoren. Danmark har nettopp startet sitt arbeid på feltet, og lovverket mht informasjonssikkerhet er mindre omfattende sammenlignet med Norge. I

Storbritannia og Sverige føres det ikke stedlige tilsyn med informasjonssikkerhet som man er kjent med i Norge. I Finland har man ivaretatt forsyningsberedskapen med egen lovgivning og ansvarlig myndighet. En generell lov om datasikkerhet gjelder alle. Konklusjonen er at det synes å være begrenset læring å hente for norske myndigheter med hensyn til tilsynsføring av informasjonssikkerhet.

6 ANDRE TILSYNSMYNDIGHETER

I dette kapittelet er tilsynspraksisen for de to tverrsektorielle tilsynsmyndigheter Nasjonal sikkerhetsmyndighet (NSM) og Datatilsynet oppsummert. Begrunnelsen for dette er at lovverket som disse myndighetene forvalter og fører tilsyn med, har grenseflater mot kraft- og finanssektoren. Sikkerhetsloven gjelder for forvaltningsorganer (stat og kommune) og deres leverandører, men Infrastrukturutvalget har diskutert om sikkerhetsloven også bør gjøres gjeldende for private virksomheter innen nasjonal kritisk infrastruktur. Slik er sikkerhetslovens relevans vurdert opp mot finans- og kraftsektoren. Personvernloven gjelder for alle som oppbevarer personopplysninger, dvs for eksempel alle som har opplysninger om ansatte eller personlige kunder. IKT-forskriften som anvendes på finanssektoren har inkludert kapittel 2 i Personopplysningsforskriften, mens en tilsvarende harmonisering ikke er gjort innenfor kraftsektoren.

6.1 Datatilsynet

Datatilsynet er et tverrsektorielt tilsyn med hovedfokus på personvern i både offentlig og privat sektor. Tilsynet jobber for bevaring av privatlivets fred - personvern, blant annet med hensyn til kameraovervåkning, sikring av helseopplysninger, rettsforfølging av individer, samt hvordan personopplysninger skal lagres som data. De er administrativt underlagt Fornyings- og administrasjonsdepartementet, men er faglig uavhengige på grunnlag av et EU-direktiv som pålegger Datatilsynet å være et fritt og uavhengig organ fordi de fører tilsyn også med de oppgaver staten selv organiserer. Klageinstansen på Datatilsynet er Personvernnemda, og eventuelt domstolene.

Siden Datatilsynet er en tverrsektoriell tilsynsmyndighet, vil de i lovverket ha mye overlappende tilsynsansvar med andre tilsynsmyndigheter, men i praksis er det lite reell overlapping. Slik overlapping vil føre til redusert tilsynsinnsats fra Datatilsynets side, eventuelt samarbeid, felles tilsynsføring eller oppfordring fra en myndighet til en annen om at tilsyn bør føres. Datatilsynet har i lengre tid ikke ført tilsyn innen oljesektoren, siden man i denne sektoren har generelt mye tilsynsaktivitet og fokus fra andre myndigheter. Datatilsynet var også i dialog med Kredittilsynet da disse utarbeidet IKT-forskriften[33], og regelverket i denne forskriften er harmonisert med kapittel 2 i personopplysningsforskriften.

Datatilsynet forvalter og fører tilsyn etter en rekke lover og forskrifter. Her følger en kort

[33] FOR 2003-05-21-630: Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)

oversikt over lovverket om personvern. Dette er et tverrsektorielt lovverk, og omhandler alle virksomheter som behandler personopplysninger. For en fullstendig liste over de lovverk Datatilsynet forvalter, se appendiks A.4.

Personopplysningslovens[34] formål er å beskytte personer mot at personvernet blir krenket gjennom behandling av personopplysninger, og den gjelder for "*behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler og annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister*" (jf lovens § 3). § 13 i loven handler om informasjonssikkerhet, og pålegger den behandlingsansvarlige og databehandleren å "*gjennom planlagte og systematiserte tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger*". Videre pålegger paragrafen at disse skal "*dokumentere informasjonssikkerhet og sikkerhetstiltakene*". § 42 beskriver Datatilsynets organisering og oppgaver, hvor en av oppgavene er "*kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet*". I henhold til § 44 kan Datatilsynet og Personvernnemda "*kreve de opplysninger som trengs for at de kan gjennomføre sine oppgaver*". Videre gir paragrafen Datatilsynet lov til å "*kreve adgang til steder hvor det finnes personregistre, overvåkningsutstyr og billedopptak (..), personopplysninger som behandles elektronisk og hjelpemidler for slik behandling*". Loven trådte i kraft 1. januar 2001.

Kapittel 2 i *Personopplysningsforskriften*[35] omhandler emnet informasjonssikkerhet, og stiller blant annet krav til risikovurderinger og sikkerhetsrevisjoner. Den stiller krav til fysisk sikring av utstyr som brukes for å behandle personopplysninger, samt sikring av konfidensialitet, tilgjengelighet og integritet. Forskriften trådde i kraft 1. januar 2001.

Datatilsynet bruker primært *stedlig tilsyn*, men har også testet ut tilsyn via brev. Sistnevnte har vært best egnet til kartlegging. Datatilsynets tilsynsmetodikk baserer seg på NS-ISO/IEC 17799 standarden.

Tilsynsmyndigheten fører normalt 130-150 tilsyn i året fordelt likt på to tilsynsperioder; vår og høst. De fører tilsyn med alle virksomheter som behandler personopplysninger. Objekter for tilsyn velges med utgangspunkt i de prioriteringer som foretas i Datatilsynets virksomhetsplan. Hvor mange tilsyn som føres innen en bransje kan variere fra 3-5 per år og opp til ca. 30. Datatilsynet fører en liste med risikovurdering i de ulike bransjene, og tilsynsintensiteten i en bransje vil være avhengig av denne risikovurderingen. Også innspill fra etatens eksperter innen ulike fagfelt vil bli tatt i betraktning ved utvelgelse av tilsynsobjekter. Etter at tilsyn er ført innen en bransje, utarbeider tilsynet en tendensrapport som gir en pekepinn på hvordan bransjen ligger an.

Rundt 80 % av tilsynene blir varslet på forhånd, normalt minst tre uker før tilsynet skal finne

[34] LOV 2000-04-14-31: Lov om behandling av personopplysninger
[35] FOR 2000-12-15-1265: Forskrift om behandling av personopplysninger

sted. De resterende 20 % er uanmeldte tilsyn. Uanmeldte tilsyn benyttes ofte ved tilsyn med virksomheter som benytter kameraovervåkning eller etter tips der fare for bevisforspillelse er til stede. Ved varslede tilsyn vil Datatilsynet kreve oversendelse av styrende dokumenter for internkontroll. Det forutsettes at virksomheten har dette, siden det er en plikt i følge regelverket.

Før et stedlig tilsyn finner sted, vil saksbehandlerne hos Datatilsynet forberede seg hovedsakelig bransjevis. Forberedelsene vil bestå av å gjennomgå oversendt dokumentasjon fra tilsynsobjektet samt eventuelle tidligere saker mot tilsynsobjektet.

Selve tilsynsmøtet kan vare fra en halv dag til tre dager. Dette vil være avhengig av blant annet virksomhetens størrelse. Majoriteten av tilsynene varer 4-6 timer. På tilsynsmøtet vil som oftest to representanter fra Datatilsynet delta; en jurist og en teknolog. I enkelte tilfeller kan Datatilsynet være representert med opp til fire personer, dette gjelder spesielt for større virksomheter eller ved tyngre tilsyn. Fra virksomheten vil ledelsen være representert, samt relevante linjeledere.

Datatilsynet fører i hovedsak tilsyn med hvordan personopplysninger blir behandlet i virksomheten. Dette gjelder blant annet hvordan disse opplysningene blir innhentet, behandlingsgrunnlaget, kvalitetssikring, informasjon til registre, innsyn, retting og sletting, og informasjonssikkerhet. Informasjonssikkerhet er dermed kun en liten del av hva Datatilsynet fører tilsyn med. Når det gjelder informasjonssikkerhet, er det kapittel 2 i personopplysningsforskriften det føres tilsyn etter. Datatilsynet velger ut et tema for tilsynet innen en aktuell bransje basert på antatte problemstillinger.

Under et tilsyn utfører Datatilsynet systemrevisjon og systemrettet verifikasjon. Førstnevnte består av å kontrollere dokumenter hos virksomheten som beskriver dennes internkontroll innen valgte tema for tilsyn, mens sistnevnte går ut på å kontrollere om det er samsvar mellom dokumentasjonen av systemet og hva man i praksis etterlever i virksomheten. Denne systemrettede verifikasjonen utføres gjennom stikkontroller av rutiner som virksomheten har beskrevet. Slik verifikasjon går som oftest på øvrige ansatte hos tilsynsobjektet, og ikke ledelsen.

Datatilsynet har definert fire kategorier av tilsyn. Disse kategoriene er (36):

- Systemrevisjon med verifikasjon: Tyngste form for tilsyn. Omfatter total gjennomgang av virksomhetens internkontrollsystem, og herunder dokumentasjon av informasjonssikkerhet. Kontrollen omfatter videre verifikasjon på de punkter som er valgt som tema for tilsynet
- Systemrevisjon med påpeking av plikter: Kontroll av dokumentasjon er som under ”Systemrevisjon med verifikasjon”, men verifikasjon er noe tonet ned. Når denne form for tilsyn benyttes, vil plikter virksomheten ikke synes å ha ivaretatt påpekes, men det vil ikke bli gitt noen formelle varsel eller pålegg.
- Systemrettet verifikasjon: Denne typen tilsyn starter med verifikasjoner og ender opp med dokumentasjonskontroll. Dokumentgjennomgang legges mindre vekt på.

- Lett verifikasjon: I denne tilsynsformen utgjør praktisk kontroll hovedtyngden. Den tar sikte på å kontrollere virksomhetens internkontrollsystem, og avvik vil bli relatert til dette.

Datatilsynet benytter seg ikke av måleindikatorer eller metrikker for måling av informasjonssikkerhet eller annet hos virksomheten under sine tilsyn.

I etterkant av et tilsyn dokumenteres det ved protokoll og tilsynsrapport. I noen få saker sikres det bevis dersom Datatilsynet føler det nødvendig å gå til anmeldelse av virksomheten. Ca 15 – 20 % av tilsynene vil bli fulgt opp av etterkontroller.

Eventuelle avvik Datatilsynet måtte finne hos virksomheten håndteres ved at det fattes vedtak mot denne. Saken lukkes ikke før de eventuelle avvik er lukket. Virksomheten har anledning til å klage på vedtak, og en klage kan føre til at Datatilsynet må omgjøre vedtak. Om ikke vedtak følges opp fra virksomhetens side, og klage ikke er sendt eller har fått gjennomslag, vil virksomheten bli pålagt tvangsmulkt. Datatilsynet må sjelden gå til det skritt å pålegge tvangsmulkt.

Datatilsynet sørger for at loven blir overholdt. De gjør også annet arbeid enn tilsyn, blant annet ved å avholde en ”råd og veiledningsuke” som et gratis og frivillig tilbud til virksomheter ca hver femte uke. Datatilsynet har også utarbeidet veiledningsdokumenter innen emnet informasjonssikkerhet som virksomheter kan benytte seg av. Høsten 2006 er det planlagt utarbeidet dokumenter som omhandler IKT-sikkerhet for små og mellomstore bedrifter.

I 2005 ble det utført en undersøkelse av norske virksomheters behandling av personopplysninger av Transportøkonomisk institutt (37). Undersøkelsen baserte seg på svar fra 424 virksomheter. Den påviste at det var en grunnleggende positiv holdning til personvern blant virksomheter, men kunnskapen om personopplysningslovverket og de plikter som følger av dette var lav. Mange virksomheter mente at krav i lovverket ikke gjaldt dem selv om de behandlet personopplysninger og således var underlagt lovverket, og et fåtall etterlevde de konkrete kravene lovverket stiller. Dette gjaldt blant annet krav til informasjonssikkerhet. Datatilsynet har dermed store utfordringer foran seg for å informere norske virksomheter om lovverk og følge opp at lovverket etterleves.

6.2 Nasjonal sikkerhetsmyndighet (NSM)

NSM er underlagt Forsvarsdepartementet og driver forebyggende, defensiv sikkerhetstjeneste, noe som i Norge omfatter alle tiltak for å sikre skjermingsverdig informasjon og skjermingsverdige objekter mot sikkerhetstruende virksomhet som spionasje, sabotasje og terrorhandlinger. Direktoratet rapporterer om sikkerhetstilstanden i militær sektor til Forsvarsdepartementet, og om sikkerhetstilstanden i sivil sektor til Justis- og Politidepartementet. Som tilsynsmyndighet er NSM tverrsektorielt, men forholder seg kun til de aktører som er underlagt Sikkerhetsloven. Sikkerhetsarbeid i NSM har historisk dreid seg rundt begrepet konfidensialitet, og det er først i de senere år at begreper som tilgjengelighet og

integritet er blitt inkludert.

Det er i hovedsak Sikkerhetsloven med aktuelle forskrifter som angår NSMs virksomhet. I tillegg inneholder Lov om Forsvarshemmeligheter[36] enkelte bestemmelser av betydning for den forebyggende sikkerhetstjeneste. Av forskrifter med hjemmel i Sikkerhetsloven finnes forskrifter om personellsikkerhet, sikkerhetsadministrasjon, informasjonssikkerhet og sikkerhetsgraderte anskaffelser. I tillegg er det utarbeidet en rekke veiledninger til regelverket.

Sikkerhetslovens[37] formål er å "*legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, ivareta den enkeltes rettssikkerhet, og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste*" (jf § 1). Den er gjeldende for forvaltningsorganer og for leverandører av varer eller tjenester til et forvaltningsorgan i forbindelse med en sikkerhetsgradert anskaffelse. Kapittel 4 i loven omhandler informasjonssikkerhet. Kapittelet inneholder paragrafer om plikter til å beskytte sikkerhetsgradert informasjon, pålegge sikkerhetsmessig godkjenning av informasjonssystemer, stille krav til kryptosikkerhet og adgang for NSM til å drive overvåkning av informasjonssystemer og foreta tekniske sikkerhetsundersøkelser. Videre omhandler lovens kapittel 5 objektsikkerhet, kapittel 6 personellsikkerhet og kapittel 7 omhandler sikkerhetsgraderte anskaffelser. Loven trådde i kraft 1. juli 2001.

Formål og virkeområde til *Forskrift om informasjonssikkerhet*[38] er likelydene med sikkerhetsloven, og gjelder også for informasjon som er sikkerhetsgradert i samsvar med NATOs bestemmelser. Forskriften omhandler områdene sikkerhetsgradering, tilgang til sikkerhetsgradert informasjon, dokumentsikkerhet, informasjonssystemsikkerhet, fysisk sikring mot ulovlig inntrenging, administrativ kryptosikkerhet, kurerposttjeneste, sikring av konferanserom, tekniske sikkerhetsundersøkelser og overvåkning av og inntrengning i informasjonssystemer. Forskriften trådde i kraft 1. juli 2001.

Alt NSM fører tilsyn med favner temaet informasjonssikkerhet, enten det er snakk om informasjonssystemer, personellsikkerhet eller annet. NSM driver koordinerte tilsyn, fagtilsyn og systemtilsyn i virksomhetsdivisjonen. Et fagtilsyn oppstår når en av faggruppene hos NSM fører tilsyn med et objekt. I et systemtilsyn sjekker NSM et system flere av virksomhetene benytter seg av. I et koordinert tilsyn holder flere av faggruppene et felles tilsyn hos en virksomhet.

NSM har ingen standardmetodikk for hvordan de fører tilsyn, men baserer mye av sitt arbeid på tidligere tilsynserfaring. De har blant annet en "spørsmålsbank", hvor spørsmål til bruk under tilsyn er listet opp sammen med en henvisning til lovhjemmel, samt hva som vil være godkjente svar. NSM fører tilsyn basert på en blanding av observasjon, intervjuer og dokumentsjekking.

[36] LOV 1914-08-18-03
[37] LOV 1998-03-20 nr 10: Lov om forebyggende sikkerhetstjeneste
[38] FOR 2001-07-01

De benytter seg ikke av noen måleindikatorer eller metrikker i forbindelse med sin tilsynsaktivitet.

Ved slutten av hvert år utvelges objekter til tilsyn, blant annet på bakgrunn av forutgående risikovurderinger eller tips/hendelser. Utvelgelsen koordineres mellom de ulike faggruppene, og en plan settes opp. Det kan forekomme endringer i tilsynsplanen på grunn av uforutsette hendelser eller sikkerhetsbrudd som vil kreve et snarlig tilsyn med objektet hvor hendelsen har inntruffet. Innbrudd eller interne sikkerhetsbrudd innen NSMs tilsynsområde skal rapporteres direkte til NSM, og ved behov føres da tilsyn kort tid i etterkant.

Ved større koordinerte tilsyn gjøres det et omfattende forarbeid hos NSM. Etter at plan over tilsynsobjekter er satt opp, ringer NSM de ønskede objektene omtrent en måned før tilsynet skal finne sted, og avtaler et tidspunkt det passer for objektet å ha tilsynsmøte på. Deretter sendes et varselbrev til tilsynsobjektet. I varselbrevet er NSMs hjemmelsgrunnlag for tilsyn beskrevet, det inneholder en anmodning om at spesifikt personell er til stede under tilsynet, det bes om at spesifikk dokumentasjon oversendes NSM, samt inneholder en beskrivelse av hvem som skal delta i tilsynet fra NSMs side, herunder hvilken klarering de har og hvem som er kontaktperson for tilsynet. Utover dette informeres det om at NSM ønsker å holde en møteinnledning hvor ledelse eller virksomhetsleder bes være til stede.

Etter at varselbrev er sendt og ønsket dokumentasjon er mottatt fra tilsynsobjektet, gjennomgås den aktuelle dokumentasjon av faggruppene hos NSM. Det avholdes fagmøter blant faggruppene, og settes opp tidsskjema for møter hos tilsynsobjektet dersom flere faggrupper ønsker å ha møte med samme person.

Ved stedlig tilsyn åpner NSM med en innledning hvor virksomhetsleder, sikkerhetspersonell og eventuelt annet relevant personell er til stede. Under innledningen informeres tilsynsobjektet om NSM og deres virke, videre snakkes det om tilsynsobjektet og dets virke, samt litt generelt om sikkerhet. NSM pålegger tilsynsobjektet å ha gjennomgått det lokale instruksverket før et stedlig tilsyn, så eventuelle spørsmål om forbedringer eller usikkerheter rundt dette kan stilles til NSM under innledningen. Så gjennomgås møteplanen NSM har satt opp, før representantene fra NSM deler seg opp i de individuelle faggruppene, og gjennomfører de aktiviteter de måtte ha på agendaen.

Et stedlig tilsyn avsluttes med en utbrief hvor alle NSMs inspektører deltar sammen med representanter fra tilsynsobjektet, og hvor det blir foretatt en gjennomgang av positive og negative utfall fra tilsynsaktiviteten. Det skal ikke forekomme overraskelser i den endelige rapporten, og derfor blir alle avvik funnet tatt opp på denne utbriefen.

Et tilsynsmøte vil ha en varighet på fra en halv dag til en uke. NSM avholder et åpningsmøte (innbrief) og et avslutningsmøte (utbrief). Tiden mellom disse møtene er selve tilsynsgjennomføringen. I forbindelse med NSMs tilsyn ytes det råd og veiledning overfor de virksomhetene det føres tilsyn med. Det er samtidig viktig at råd- og veiledningsaktiviteten ikke

blandes med den kontrollbasert tilsynsaktiviteten, slik at det oppstår tvil om hvilken rolle NSM har i det forebyggende sikkerhetsarbeidet.

NSM kan måle avvik på to ulike måter:

1. Måle opp mot sikkerhetsloven med dens forskrifter og betrakte alle mangler på oppfølging og etterlevelse av loven som avvik.
2. Undersøke om tilsynsobjektet etterlever sine strategiske mål, og om ikke dette er tilfelle evaluere om det er loven eller tilsynsobjektet som er utilstrekkelig.

Det må presiseres at sikkerhetsloven er bygget opp for å angi et minimumsnivå av sikringstiltak. I tillegg kan NSM utøve skjønn der lov- eller forskriftsteksten åpner for dette, og dermed tilpasse kravene etter forholdene. Det er imidlertid en rekke krav i sikkerhetsloven med forskrifter som ikke åpner for en slik mulighet. Når NSM undersøker om tilsynsobjektet er i stand til å etterleve sine forpliktelser, gjøres en vurdering av verdien av objektet/informasjonen og risiko og sårbarhet ved objektet. Vurderingen benyttes for å fastslå om det er behov for sikringstiltak utover det minimum som er satt i lov og forskrift.

Et stedlig tilsyn blir avsluttet med en gradert rapport. Rapportskriving koordineres mellom de ulike faggruppene hos NSM, og teamleder innhenter faggruppenes bidrag og setter sammen endelig rapport som sjekkes av faggruppene før den oversendes tilsynsobjektet. Etter at rapport er sendt ut, har tilsynsobjektene en tremåneders frist fra de har mottatt rapporten til å sende skriftlig tilbakemelding til NSM om hvilke forbedringstiltak de skal iverksette, og når. Ved manglende tilbakemelding følger NSM opp ved å kontakte tilsynsobjektet.

Enkelte funn blir anonymisert og publisert i NSMs årlig utgitte risikovurdering, som kommer både i gradert og ugradert form.

NSM har et reaksjonsforum som skal reagere på alvorlige avvik både under og i etterkant av et tilsyn. Alvorlige hendelser som er eller nærmer seg sikkerhetsbrudd, samt gjentatte avvik, blir slått ned på av reaksjonsforumet. Dersom inspektører fra NSM skulle oppdage alvorlige avvik hos et tilsynsobjekt, holdes det en løpende kontakt med reaksjonsforumet, hvor det eventuelt kan bli nødvendig for inspektørene å gjøre inndragninger ol på stedet. For å kunne iverksette tiltak må reaksjonsforumet ha objektiv informasjon og klare beviser på sikkerhetsbrudd. Reaksjonsforumet har mange virkemidler, fra tilbaketrekking av sikkerhetsklarering eller godkjenning, ev. anmeldelse.

7 OPPSUMMERING AV RESULTATER

7.1 Sammenligning av tilsynsmyndigheter

Tabell 7.1 viser en sammenstilling av hovedfunnene i denne studien.

	NVE	KT	DT	NSM
Sektor	Energi Vassdrag	Finans	Tverrsektoriell	Tverrsektoriell, begrenset til stats-, fylkes- og kommuneforvaltningen samt leverandører
Lovverk	Energiloven, Energilov-forskriften, Beredskaps-forskriften Vannressursloven	Kredittilsynsloven, IKT-forskriften	Personopplysningloven, Personopplysnings-forskriften, SIS-loven (m/forskrift), Helseregisterloven, esignaturloven	Sikkerhetsloven m/forskrifter
Del av tilsyn som omhandler informasjons-sikkerhet	Informasjons-sikkerhet en del av tilsynet med beredskap	Har eget IKT-tilsyn	Informasjons-sikkerhet en mindre del av personverntilsynet	Alt av tilsyn omhandler informasjonssikkerhet i større eller mindre grad.
Bruk av standarder/ metodikk i tilsynsføring	ISO 19011 Egenutviklet spørreskjema	Egenutviklet skjema basert på COBIT	Har utviklet egen prosedyre basert på ISO 17799	Spørsmålbank og erfaringer fra tidligere tilsyn
Tilsynsmåter	Stedlig og dokumentbasert tilsyn	Stedlig og dokumentbasert tilsyn	Stedlig og dokumentbasert tilsyn	Stedlig tilsyn
Utvelgelse av tilsynsobjekter	Kritikalitet og risiko	Kritiske virksomheter, hyppighet, interne innspill	Kritiske virksomheter, hyppighet, hendelser, tips	Kritiske virksomheter, hyppighet, hendelsesbasert
Dokumentering av tilsyn	Rapport unntatt offentlighet	Offentlig rapport	Offentlig rapport	Gradert rapport, offentlig og gradert risikovurdering
Måleindikatorer /metrikker brukt i tilsynsprosessen	Enkle egenutviklede	Ingen COBIT	Ingen	Ingen
Tiltak/ virkemidler	Vedtak, tvangsmulkt	Vedtak, offentlig rapport	Vedtak, tvangsmulkt, bruk av media	Vedtak, mange reaksjonsformer

Tabell 7.1 Sammenstilling av fire norske tilsynsmyndighetene

De norske tilsynsmyndighetene har noen fellestrekk i sin praksis å drive tilsyn på. I grovt foregår tilsynsføring på følgende måte: I forkant gjøres det en vurdering av selskapene ut i fra kriterier som risiko, viktighet og status. Myndigheten varsler tilsynsobjektet, ber om informasjon og avtaler møte, gjennomfører møtet og innhenter mer informasjon, analyserer og dokumenterer avvik som det gis en frist på å lukke.

Det er klare ulikheter mellom de ulike tilsynsmyndighetenes praksis. De ulike myndighetene har ulik tilsynsmetodikk. NVE baserer sitt tilsyn på NS-EN ISO 19011 som beskriver en revisjonsmetodikk og stiller krav til revisorer. Kredittilsynet har videreutviklet et skjemabasert verktøy basert på COBIT. Datatilsynet har utarbeidet en egen strategi og metodikk for føring av operativt tilsyn med behandling av personopplysninger basert på NS-ISO/IEC 17799, mens

NSM benytter seg av erfaringsbasert tilsyn og en egenutviklet spørsmålbank med klar kopling mot forskriftsteksten.

Dokumentasjon av tilsyn og virkemidler varierer. Mye av det NVE oppdager under tilsynsbesøk er opplysninger som er kraftsensitive og skal beskyttes mot uvedkommendes innsyn. Det NSM oppdager under sine tilsyn, vil være opplysninger av betydning for rikets sikkerhet og dermed gradert informasjon. Datatilsynet og Kredittilsynet offentliggjør sine funn i rapport som virkemiddel for å få virksomheter til å lukke sine avvik.

For noen av tilsynsmyndighetene vil informasjonssikkerhet kun være en del av et større tilsyn, slik som i kraftforsyningen, mens Kredittilsynet og NSM fører tilsyn med kun informasjonssikkerhet på agendaen. I dag er det ingen av tilsynsmyndighetene som benytter seg av noen måleindikatorer eller metrikker ved tilsynsføring av informasjonssikkerhet som beskrevet i teorikapittelet her. Det nærmeste vi kommer er NVEs måleindikatorer for å rangere virksomheter og fagområder etter avvik. Kredittilsynet vurderer å ta i bruk en mer spesifikk måleindikator i tilsynsprosessen, ved å etablere en skala fra 1-4 som hver COBIT-prosess måles mot eller graderes etter. Det er opplyst at det er gjort noe arbeid med å utvikle metrikker til slik bruk i kraftbransjen. Begrunnelsen for at det ikke er noen utstrakt bruk av disse ligger hovedsakelig i mangel på tilgjengelige og relevante måleindikatorer/metrikker og nytten av dem.

Eksterne tilsyn er med på å sette informasjonssikkerhet på agendaen. Samtidig savnes det mer spesifikt og tilpasset lovverk og veiledninger innen informasjonssikkerhet. Flere av tilsynsmyndighetene i denne studien var på tidspunktet for intervjuet i gang med å utarbeide flere spesialtilpassede veiledninger til lovverket.

7.2 Utenlandsk tilsynspraksis

Tilsynspraksisen i landene som har vært en del av studien er i stor grad ulik fra den norske. Selv om de skandinaviske landene har mye samarbeid både innen elberedskap (39) og i finans, har de ulike tilnærmingsmåter for tilsynsføring.

I Danmark finnes regelverk som tilsvarer den norske IKT-forskriften i finanssektoren og den norske beredskapsforskriften for kraftsektoren. Innen finanssektoren har Finanstilsynet tilsynsmyndighet, og de fører tilsyn med informasjonssikkerhet som ligner mye på hva IT-seksjonen hos det norske Kredittilsynet gjør. Den danske beredskapsloven omhandler derimot ikke informasjonssikkerhet i like stor grad som den norske. I energisektoren er tilsynsprosessen med beredskap i Danmark i en tidlig fase. Informasjonssikkerhet er per i dag ikke ansett å være kritisk for den danske elforsyningen, og tilsyn med informasjonssikkerhet vil kun bli en liten del av det generelle tilsynet med beredskap.

I Sverige er det ikke noe lovverk som omhandler informasjonssikkerhet i finans- eller kraftsektoren spesielt, men sikkerhetsloven kan gjøres gjeldende for kritisk infrastruktur. I den svenske finanssektoren fører Finansinspektionen tilsyn med informasjonssikkerhet hos

virksomhetene. Svenska Kraftnät er tilsynsmyndighet og forvalter også et årlig beløp som skal brukes på beredskapstiltak hos el-virksomhetene. Disse beredskapstiltakene kan omhandle informasjonssikkerhet i form av for eksempel sikring av driftskontrollsentraler.

I Finland har man en generell lov som gjelder for datasikkerhet i alle sektorer. Innen Finanssektoren har Finansinspektionen gitt en forskrift som bankvirksomhetene skal følge. En tilsvarende standard finnes ikke for kraftforsyningen. Finland skiller seg litt ut med fokuset på og organiseringen av forsyningsberedskap i forhold til de andre landene.

Storbritannia skiller seg mest ut fra det norske systemet. I Storbritannia utføres det ikke stedlige tilsyn som det gjøres i Norge. De har en egen organisasjon for å bistå med kunnskap for å sikre den kritiske infrastrukturen i landet mot elektroniske angrep (NISCC), men det er ikke støttet opp av noe lovverk og har ingen reguleringsrolle. Det finnes ikke sektorspesifikke lover innenfor informasjonssikkerhet i finans- og elektrisitetssektoren i landet. Den tverrsektorielle ”Data Protection Act 1998” tilsvarer det norske lovverket om personvern. For finanssektoren har ”The Financial Services Authority” (FSA) tilsynsmyndighet, men de fører ikke tilsyn med informasjonssikkerhet. For energisektoren har ”Office of Gas and Electricity Markets” (Ofgem) reguleringsansvar, og de fører tilsyn med at virksomhetene i sektoren opprettholder de krav som stilles i henhold til lisensavtaler og annet regelverk. Ofgem fører ikke stedlig tilsyn slik NVE gjør i Norge, men fører tilsyn gjennom å innhente og analysere diverse informasjon fra virksomheter, kunder og andre.

7.3 Avsluttende betraktninger

Vi har studert tilsynspraksis i norsk finans- og kraftsektor og sett den norske praksisen opp mot praksis i Sverige, Danmark og UK. Vi har også men i mindre grad studert tilsynspraksisen innenfor NSM og Datatilsynet siden disse har grenseflater mot de sektorene vi har valgt som studieobjekt.

For å føre offentlig tilsyn, kreves det lovhjemler. Uten lovhjemler blir det heller ikke noe tilsynsprosess, og uten relevante lovhjemler blir det heller ikke et myndighetsfokus på relevante forhold. Vi har observert at ulikheter i lovverket også gjenspeiles i ulik tilsynspraksis mellom de ulike landene i studien. Vår studie viser at Norge bruker offentlig tilsyn med informasjonssikkerhet som virkemiddel i større grad enn de andre landene i denne studien. IKT-forskriften innen finanssektoren er i en særstilling, ved at den alene fokuserer på informasjonssikkerhet. Vanlig praksis ellers er at informasjonssikkerhet er inkludert i andre forskrifter.

En suksessfaktor for at lovverket skal bli fulgt, er klare retningslinjer (24). Både NVE og Kredittilsynet utarbeidet retningslinjer. I tillegg drives opplæring og rådgivning overfor de virksomheter som er underlagt tilsynsmyndigheten. Tilsynsmyndighetene har også sanksjonsmuligheter overfor virksomheter som ikke følger loven. Selv om disse varierer i karakter mellom ulike tilsynsmyndigheter, så har alle myndighetene sterke sanksjonsmuligheter. Klare retningslinjer, opplæring og sanksjonsmuligheter vil sammen bidra til at myndighetene

oppnår effekt av loven.

Vi har observert at tilsynsprosessen stort sett følger samme mal på tvers av myndigheter og land: Varsling (som kan utelates), innhenting av skriftlig informasjon, tilsynsmøte, supplering med mer informasjon, rapport til virksomheten, tilsvar fra virksomheten, og endelig rapport med pålegg/tiltak. I etterkant følger gjerne opplæring.

Verktøyene tilsynsmyndigheten bruker er stort sett spørreskjema med ja/nei svar der nei betyr avvik. Det er altså klare grenser for hva som er akseptert og hva som ikke er akseptert. Måleverktøyene varierer imidlertid. Kredittilsynet bruker egenutviklede COBIT-skjemaer. Datatilsynet baserer sitt opplegg på NS-ISO/IEC 17799. NVE har egenutviklede spørsmål med forankring i lovteksten, og NSM har en spørsmålsbank der tilsynsmyndigheten utøver stor grad av skjønn og bruker loven som baseline for sikkerhetsnivået. Med referanse til vårt litteratursøk i kapittel 3 og teorien om metrikker og indikatorer, synes det som om det kan være et potensial for å utvikle måleindikatorer innenfor tilsynsmyndighetenes virkeområde. NVE har på en måte tatt ett steg i denne retning med å beregne %-andel nei-svar sortert på virksomhet og tema. Selv om dette er enkle indikatorer, kan de dersom de blir registrert i et felles rammeverk og over tid, gi informasjon om trender når det gjelder hvor flinke virksomhetene er til å følge loven. Kredittilsynets COBIT-skjema ville også kunne være et grunnlag for måleindikatorer eller metrikker etter modell av NVE; % nei-svar fordelt på prosess og tema og % nei-svar fordelt på virksomheter over tid. Styrken med Kredittilsynets COBIT-metodikk er bredden og den standardiserte metoden som gjelder for alle virksomheter. Det ligger imidlertid ikke innenfor denne rapportens mandat å utvikle slike indikatorer, bare å påpeke forbedringsmuligheter.

Avslutningsvis påpeker vi at vi ikke har vurdert effekt av offentlig tilsyn opp mot effekt av andre mekanismer, for eksempel markedets makt som regulator, der sikkerhet er en premiss for tillit mellom kunde og virksomhet. Vi kan derfor ikke uttale oss om den norske modellen er bedre enn de modellene som er anvendt i andre land. Særlig er forskjellen stor i forhold til Storbritannia, som det også er eksemplifisert i (35) når det gjelder reguleringsregime for forsyningssikkerhet.

I henhold til (15) har dagens regulerende miljø innen informasjonssikkerhet ført til at sikkerhetspersonell ikke bare må forstå de tekniske utfordringene, men også forretningsmodellen og de legale kravene som skal følges. Basert på norske erfaringer er det klart at lovverk og offentlig tilsyn tvinger toppledelsen til å følge opp informasjonssikkerheten blant annet ved at representanter fra ledelsen er med på tilsynsmøtene og må svare på spørsmål. I tillegg sendes tilsynsrapportene til styret i finansforetakene, noe som signaliserer at informasjonssikkerhet er et styreansvar. Sett i lys av toppledelsens ”distansering” i forhold til informasjonssikkerhet (22)(23), er dette positivt.

APPENDIKS

A FORKORTELSER

AFIN	-	Avdeling for Forvaltningsinformatikk
BAS	-	Beskyttelse av Samfunnet
BAS3	-	Beskyttelse av Samfunnet 3 – En Sårbar Kraftforsyning
BAS5	-	Beskyttelse av Samfunnet 5 – Critical Information Infrastructure Protection
BBS	-	Bankenes Betalingssentral AS
CC	-	Common Criteria
DPA	-	The Data Protection Act 1998
DT	-	Datatilsynet
DTI	-	Department of Trade and Industry
E3	-	Energy Emergencies Executive
ENISA	-	The European Network and Information Security Agency
EU	-	Den Europeiske Union
EØS	-	Det Europeiske Økonomiske Samarbeidsområde
FFI	-	Forsvarets Forskningsinstitutt
FI	-	Finansinspektionen (Sverige)
FIH	-	FinansieringsInstituttet for Industri og Håndværk A/S
FIL	-	Bekendtgørelse af lov om finansiel virksomhed
FSA	-	The Financial Services Authority
FSMA	-	The Financial Services and Markets Act 2000
FT	-	Finanstilsynet (Danmark)
IA	-	Information Assurance
ICT	-	Information- and Communication Technology
IT	-	Informasjonsteknologi
IKT	-	Informasjons- og Kommunikasjonsteknologi
JESS	-	Joint Energy Security of Supply Working Group
KBO	-	Kraftforsyningens Beredskapsorganisasjon
KIS	-	Koordineringsutvalget for informasjonssikkerhet
MW	-	Måleenhet for installert effekt/overføringskapasitet
NASA	-	National Aeronautics and Space Administration
NATO	-	North Atlantic Treaty Organisation
NISCC	-	National Infrastructure Security Co-ordination Centre
NIST	-	The National Institute for Standards and Technology
NSM	-	Nasjonal Sikkerhetsmyndighet
NVE	-	Norges vassdrags- og energidirektorat
OD	-	Oljedirektoratet
OECD	-	Organisation for Economic Co-operation and Development
OED	-	Olje- og energidepartementet
Ofgem	-	Office of Gas and Electricity Markets
PST	-	Politiets sikkerhetstjeneste
RoI	-	Return of Investment
ROS	-	Risiko- og Sårbarhet

SIS	-	Schengen informasjonssystem
SOX	-	Sarbanes Oxley
TWh	-	Måleenhet for elektrisitetsforbruk
TØI	-	Transportøkonomisk Institutt
UiO	-	Universitet i Oslo
VDI	-	Varslingssystem for Digital Infrastruktur
VPS	-	Verdipapirsentralen ASA

B SØKESTRATEGI

For å finne relevant litteratur ble det i tidsrommet 19. juni – 21. juli gjort søk med følgende søkeord:

- Information Security or Information Assurance or Computer Security AND Security Metrics
- Information Security or Information Assurance or Computer Security AND Audit
- Information Security or Information Assurance or Computer Security AND External Control
- Information Security or Information Assurance or Computer Security AND Performance Measuring
- Information Security or Information Assurance or Computer Security AND Effectiveness
- Information Security or Information Assurance or Computer Security AND Cost Benefit Analysis
- Information Security or Information Assurance or Computer Security AND Return of Investment
- Information Security or Information Assurance or Computer Security AND Quality Management
- Information Security or Information Assurance or Computer Security AND Measurement
- Information Security or Information Assurance or Computer Security AND Law
- Information Security or Information Assurance or Computer Security AND Legislation
- Information Security or Information Assurance or Computer Security AND Legal Acts
- Security Knowledge Management
- Informasjonssikkerhet or Informasjonsassuranse or Datasikkerhet AND Sikkerhetsmetrikker
- Informasjonssikkerhet or Informasjonsassuranse or Datasikkerhet AND Revisjon
- Informasjonssikkerhet or Informasjonsassuranse or Datasikkerhet AND Effektivitet
- Informasjonssikkerhet or Informasjonsassuranse or Datasikkerhet AND Måleindikatorer
- Sikkerhetsadministrering

Litteratursøket ble foretatt i følgende databaser, de fleste tilgjengelige ved FFI.
Kvalitet på databasene, rangert etter synkende relevans:

- Bibsys http://www.bibsys.no/
- IEEE XPLORE http://ieeexplore.ieee.org/
- EBSCO Host http://search.epnet.com/

- Web of Science http://isiknowledge.com/
- First Search http://firstsearch.oclc.org/
- SCOPUS http://www.scopus.com/
- LexisNexis http://www.lexisnexis.com/
- JStor http://www.jstor.org/
- Jane's http://www.janes.com/
- SwetsWise http://www.swetswise.com/
- CIAO http://www.ciaonet.org/

I de tre første databasene var det gode resultater, de fire neste var det noe varierende og i de fire siste fantes lite eller ingenting av relevans for studien. Som det fremgår i Kapittel 3 er det generelt ikke store mengder relevant litteratur som kom frem i løpet av søkeprosessen.

Av alle treff ble en beskjeden mengde plukket ut etter følgende kriterier;

- Tittel – Stikkord og tilsynelatende relevans
- Abstrakt/Abstract – Stikkord og tilsynelatende relevans

Søkeresultatet inneholder lovverk, forskrifter, veiledninger, Phd-avhandlinger, Masteroppgaver, rapporter, artikler og bøker. Lovverket er hovedsaklig norsk og nordisk, mens artiklene skrevet av både norske og utenlandske, spesielt amerikanske, forfattere, mens bøkene er både norske og utenlandske. Innholdet i søket dreier seg typisk om metrikker, hva de er, hvordan de utvikles og ledes, anvendelsesområder og rammeverk for metrikker, økonomisk avkastning, samt behovet for gode, relevante metrikker.

For å oppsummere søket synes det å være begrenset med relevant forskning på temaene informasjonssikkerhet, sikkerhetsmetrikker, tilsynsmetodikker og effekten av lovverk. Litteraturen vi fant beskriver behovet for både økt fokus og forskning innefor disse temaene, videre tar den for seg ideer, konsepter og rammeverk.

C GENERELT INFORMASJONSGRUNNLAG

C.1 Litteratur

(1) Vijayan, Jaikumar, 2005: Metrics Fall Short of Mark on Security, Computerworld; 9/26/2005, Vol. 39 Issue 39, p1-16, 2p, Article

(2) Vijayan, Jaikumar, 2003: IT Managers See Need for Risk Metrics, Computerworld, 6/9/2003, Vol 37 Issue 23, p1, 2p, Article

(3) Gordon Lawrence A and Loeb, Martin, 2002: Return of Information Security Investments; Myths vs Realities (cover story), Strategic Finance, Nov 2002, Vol 84 Issue 5, p26, 6 p, Article

(4) Vijayan, Jaikumar, 2006: Security Exec Push for Broader Use of Metrics, Say measuring risks and evaluating controls helps prioritize spending, Computerworld, 2/20/2006, Vol. 40 Issue 8, p1, 2p, Article

(5) Cashell, Brian, Jackson William D., Jickling Mark, Webel, Baird, 2004: The economic impact of Cyberattacks: RL32331, Congressional Reserach Service Report; 4/1/2004, p1,45p, CRS Report for Congress

(6) Hicks, Matt, 2001: Security: How do you rate? (cover story), eWeek, 12/12/2001, Vol. 18 Issue 49, p37, 3p. Article.

(7) Von Solms, Basie, 2005: Information Security Governance: COBIT or ISO 17799 or both? Computers and security, 2005 24, 99-100. Article.

(8) Vaughn Rayford B., Henning Ronda and Siraj Ambareen, 2002: Information Assurance Measures and Metrics – State of Practce and Proposed Taxonomy, Proceedings of the 36th Hawai International Conference on System Sciences (HICSS'03), 0-7695-1874-5/03, 2002 IEEE.

(9) Reznic Leon, 2003: Which Models should Be Applied To Measure Computer Security and Information Assurance, The IEEE International Conference on Fuzzy Systems 0-7803-7810-5/03 2003 IEEE.

(10) Herrera, Sven Olof Sandström, 2005: Information Security Management Metrics Development, Applus+SIT, 0-7803-9245-0/05 2005 IEEE.

(11) Seddigh, Nabil, Pieda, Peter, Matrawy, Ashraf, Nandy, Biswayit, Lambadaris, John, Hafield, Adam, 2004: Current Trends and Advances in Information Assurance Metrics, Second Annual Conference on Privacy, Security and Trust; October 2004

(12) Vijayan, Jaikumar, 2005: New Group Plans Security Metrics; 9/5/2005, Vol. 39 Issue 36, p10-10, 3/5p, Article.

(13) Kovacich, Gerald, 1997: Information Systems Security Metrics Management, Computers & Security, 16 (1997) 610-618, Article.

(14) Netsec, 2004: Using metrics to improve Security, Netsec, Security Brief, September 2004.

(15) Lobree, Bruce A., 2002: Impact of Legislation on Information Security Management, Information Systems Security, Nov/Dec 2002, Vol 11 issue 5, p 41, 8p, Article

(16) Sademies Anni, 2004: Process appriach to Information security Metrics in Finnish Industry and State Institutions, VTT Technical Research Center of Finland, VTT Publication 544.

(17) Orderuløkken, Tore, 2005: Security incident handling and eporting – a study of the difference between theory and practice, Nislab, Department of Technology, Gjøvik University College, June 22nd, Master of Science Thesis.

(18) Botnen Ståle, 2005: Metrics for Measuring Security in Peer-to-Peer Software, Nislab, Department of Computer Science and Media Technology, Gjøvik University College, Master of Science Thesis.

(19) Bakås, Tone, 2005: God Praksis for måling av informasjonssikkerhet, Department of Computer Science and Media Technology, Gjøvik University College, Master of Science Thesis.

(20) Mathisen, Johnny, 2004: Measuring Information Security Awareness – A survey showing the Norwegian way to do it. Examensarbete 20 pöeng i data- och systemvetenskap inom magisterprogrammet i informations- och kommunikations säkerhet, Kungl Tekniska Högskolan, Stockholm.

(21) Kovacich, Gerald L., Halibozek, Edward P., 2006: Security Metrics Management. How to Manage the Cost of an Asset Protection Program, Elsevier Inc, New York, pp 1-319

(22) Geer, Daniel Jr, Hoo, Kevin Soo and Jaquit, Andrew, 2003: Information Security, Why the Future Belongs to the Quants, IEEE Security & Privacy, 1540-7933/03.

(23) Hu, Quing, Hart, Paul and Cooke, Donna, 2006: The Role of external Influences on Organizational Information Security Practices: An Institutional Perspective, Proceedings at the 39th Hawaii International Conference on System Sciences – 2006, 0-7695-2507-5/06, IEEE

(24) Spears, Janine L., Cole, Robert J., 2006: A preliminary Investigation of the Impact of the Sarbanes-Oxley Act on Information Security, Proceedings at the 39th Hawaii International Conference on System Sciences – 2006, 0-7695-2507-5/06 IEEE.

(25) Posthumus, Shaun, von Solms Rossouw, 2004: A framework for the governance of information security, Computers & Security, (2004) 23, 638-646.

(26) Kim, Sangkyun, and Lee, Hong Joo, 2005: Cost-Benefit Analysis of Security Investments: Methodology and Case Study, Gervasi et al (Eds.): ICCSA 2005, LNCS 3842, pp 1239-1248. Springer-Verlag Berlin Heidelberg.

(27) Jansen (red.), Schartum (red.), et al, 2005: Informasjonssikkerhet – Rettslige krav til sikker bruk av IKT, Fagbokforlaget Vigmostad & Bjørke AS (2005)

(28) Bogen, Mørkestøl, 2006: Håndtering av IKT-Kriser – Aktører og roller, FFI/RAPPORT-2005/03536

(29) NVE, 2006: Veiledning til forskrift om beredskap i kraftforsyningen, http://www.nve.no/FileArchive/97/Veiledning%20BfK_29062006.pdf

(30) Nygård, Arne Roar, 2004: Risk management in SCADA-system, Gjøvik University College, Master of Science Thesis.

(31) DTI, 2006: The Energy Challenge, http://www.dti.gov.uk/files/file31890.pdf

(32) DTI, 2006: Secretary of State's Second Report to Parliament on Security of Gas and Electricity Supply in Great Britain, http://www.dti.gov.uk/files/file31630.pdf

(33) DTI, 2006: Joint Energy Security of Supply Working Group (JESS) Sixth Report, http://www.dti.gov.uk/files/file28800.pdf

(34) Ofgem, 2006: Ofgem Annual Report 2005-2006, http://www.ofgem.gov.uk/temp/ofgem/cache/cmsattach/15887_128_06.pdf

(35) OECD, 2002: Security of supply in electricity markets – Evidence and policy issues, http://www.iea.org/textbase/nppdf/free/2000/security2002.pdf

(36) Datatilsynet, 2002: Strategi og metodikk for operativt tilsyn med behandling av personopplysninger

(37) Ravlum, Inger-Anne, 2005: Behandling av personopplysninger i norske virksomheter, TØI rapport 800/2005

(38) Hagen J, Fridheim H (2005): Hva er kritisk infrastruktur?, FFI/NOTAT-2005/00363, Forsvarets forskningsinstitutt

(39) The Nordic Forum for Emergency Matters regarding the Power Sector (2005): Nordic Contingency Planning and Crisis Management

(40) Norsk Standard: NS-ISO/IEC 17799, 2.utgave juni 2005. Informasjonsteknologi. Sikkerhetsteknikk. Administrasjon av informasjonssikkerhet (ISO/IEC 17799)

(41) Målbakken, Ole Kristian, 2002: Towards Measuring Legal Compliance. A case study on EU Directive 95/46, Article 17: Security in Processing, Examensarbete, Kungliga Tekniska Högskolan, Høgskolen i Gjøvik, NISlab.

(42) Finansinspektionen, Standard 4.4b Management of operational risk. Regulation and guidelines. Issued on 25 May 2004. Valid from 1.January 2005 until further notice, J. No. 3/120/2004.

C.2 Lovverk

C.2.1 Norske Lover

LOV 1956-12-07-1: Lov om tilsynet for kredittinstitusjoner, forsikringsselskaper og verdipapirhandel m.v.
Kredittilsynsloven
http://www.lovdata.no/all/hl-19561207-001.html

FOR 2003-05-21-630: Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)
IKT-Forskriften
http://www.lovdata.no/for/sf/fd/xd-20030521-0630.html

LOV 1990-06-29-50: Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.
Energiloven
http://www.lovdata.no/all/hl-19900629-050.html

FOR 1990-12-07-959: Forskrift om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.
Energilovforskriften
http://www.lovdata.no/for/sf/oe/xe-19901207-0959.html

FOR 2002-12-16 nr 1606: Forskrift om beredskap i kraftforsyningen
Beredskapsforskriften
http://www.lovdata.no/for/sf/oe/xe-20021216-1606.html

LOV 2000-04-14-31: Lov om behandling av personopplysninger
Personopplysningsloven
http://www.lovdata.no/all/hl-20000414-031.html

FOR 2000-12-15-1265: Forskrift om behandling av personopplysninger
Personopplysningsforskriften
http://www.lovdata.no/for/sf/fa/xa-20001215-1265.html

LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger
Helseregisterloven
http://www.lovdata.no/all/hl-20010518-024.html

LOV 1999-07-16 nr 66: Lov om Schengen informasjonssystem (SIS)
SIS - loven
http://www.lovdata.no/all/hl-19990716-066.html

FOR 2000-12-21 nr 1365: Forskrift til lov om Schengen informasjonssystem
SIS - forskriften
http://www.lovdata.no/for/sf/jd/xd-20001221-1365.html

LOV 2001-06-15 nr 81: Lov om elektronisk signatur
E-signaturloven
http://www.lovdata.no/all/hl-20010615-081.html

LOV 1998-03-20 nr 10: Lov om forebyggende sikkerhetstjeneste
Sikkerhetsloven
http://www.lovdata.no/all/hl-19980320-010.html

LOV 1914-08-18-03: Lov om Forsvarshemmeligheter
http://www.lovdata.no/all/hl-19140818-003.html

FOR 2001-07-01 Forskrift om informasjonssikkerhet
http://www.lovdata.no/for/sf/fo/xo-20010701-0744.html

C.2.2 Danske Lover

LBK nr 286 af 04/04/2006: Bekendtgørelse af lov om finansiel virksomhed
http://147.29.40.90/_SHOWF_A361330810/715&A20060028629REGL&0001&000040

VEJ nr 9074 af 23/01/2004: Vejledning om kontrol- og sikringsforanstaltninger på it-området § 71, stk. 1, nr. 4
http://147.29.40.90/_SHOWF_A377503377/1489&C20040907460REGL&0002&000016

LBK nr 286 af 20/04/2005: Bekjendtgjørelse av Lov om elforsyning
http://147.29.40.90/_SHOWF_A361330810/715&A20050028629REGL&0002&000015

BEK nr 58 af 17/01/2005: Bekjendtgjørelse om beredskab for elsektoren
http://147.29.40.90/_SHOWF_A361330810/715&B20050005805REGL&0007&000001

C.2.3 Svenske Lover

SFS nr 1997:857: Ellag
http://www.notisum.se/index2.asp?iParentMenuID=236&iMenuID=314&iMiddleID=285&top=2&sTemplate=/template/sok.asp?DokTyp=1

SFS nr 1997:288: Elberedskapslag
http://www.notisum.se/index2.asp?iParentMenuID=236&iMenuID=314&iMiddleID=285&top=2&sTemplate=/template/sok.asp?DokTyp=1

SFS nr 2006:942: Förordning om krisberedskap och höjd beredskap
http://www.notisum.se/rnp/sls/lag/20060942.HTM

C.2.4 Finske lover

Loven om databeskyttelse gjelder for informasjonssikkerhet hos alle
Lag om dataskydd vid elektronisk kommunikation (16.6.2004/516)

Kredittlovgivningen (eksklusive Forsikring)
Kreditinstitutslag (9.2.2007/121)
Lag om placeringsfonder (29.1.1999/48)
Lag om affärsbanker och andra kreditinstitut i aktiebolagsform (28.12.2001/1501)
Sparbankslag (28.12.2001/1502)
Lag om andelsbanker och andra kreditinstitut i andelslagsform (28.12.2001/1504)
Lag om utländska kreditinstituts och finansiella instituts verksamhet i Finland (30.12.1993/1608)
Lag om värdeandelssystemet (17.5.1991/826)
Lag om tillsyn över finans- och försäkringskonglomerat (30.7.2004/699)
Lag om hypoteksbanker (23.12.1999/1240)

Den finske energilovgivingingen med vekt på forsyningsberedskap
Elmarknadsförordning (7.4.1995/518)

Forsyningsberedskap, se:
Lag om tryggande av försörjningsberedskapen (18.12.1992/1390, ändr. 2.9.2005/688)
Förordning om Försörjningsberedskapscentralen (18.12.1992/1391)
Kommunikationsmarknadslag (23.5.2003/393)

Enskilda stadganden om krav på beredskapsplanering:
Kreditinstitutslag (121/2007) 123-124 §§
Lag om placeringsfonder (48/1999) 4 a §
Lag om värdeandelssystemet (826/1991) 13 a §
Lag om utländska kreditinstituts och finansiella instituts verksamhet i Finland (1608/1993) 13 a §
Lag om försäkringsbolag (1062/1979) 7 §
Lag om försäkringsföreningar (1250/1987) 8 §
Lag om utländska försäkringsbolag (398/1995) 63 a §
Lag om pensionsstiftelser (1774/1995) 4 a §
Lag om försäkringskassor (1164/1992) 7 a §
Lag om sjömanspensioner (72/1956) 64 e §
Lag om pension för lantbruksföretagare (467/1969) 17 h §
Lag om Pensionsskyddscentralen (397/2006) 15 §

Se www.finlex.fi/en/ eller www.finlex.fi/sv/

C.2.5 Britiske Lover

The Financial Services and Markets Act 2000
2000 Chapter c.8
http://www.opsi.gov.uk/acts/acts2000/20000008.htm

The Data Protection Act 1998
1998 Chapter 29
http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm

The Energy Act

2004 Chapter 20
http://www.opsi.gov.uk/ACTS/acts2004/20040020.htm

The Electricity Act 1989
1989 c. 29
http://www.opsi.gov.uk/ACTS/acts1989/Ukpga_19890029_en_1.htm

C.3 Intervjuer

Finans	Energi
Norske Aktører	
Kredittilsynet, 6. juli 2006 Anonym finansvirksomhet, 11. juli 2006 Anonym bankvirksomhet, 17. juli 2006	Statnett, 5. juli 2006 Norges vassdrags- og energidirektorat, 17. juli 2006 Lite kraftselskap, 18. juli 2006 Lite kraftselskap, 21. juli 2006
Utenlandske Aktører	
Danmark Finanstilsynet Henrik Kjølberg It-konsulent, CISA (mailkorrespondanse – 24. juli 2006) *Sverige* Finansinspektionen Kerstin af Jochnick Avdelingssjef (mailkorrespondanse/telefon – 19. juli 2006) Anders Broman Kredit og Operative Risker (mailkorrespondanse/telefon – 10. august 2006) *Finland* Arto Sundström (mailkorrespondanse januar 2007) *Storbritannia* FSA Mr. S. Katte Consumer Contact Centre (mailkorrespondanse – 28. juli 2006) NISCC	*Danmark* Energinet.dk Hans Åge Nielsen (mailkorrespondanse – 20. til 26. juli 2006) Energistyrelsen Uffe Strandkjær (mailkorrespondanse – i perioden 17. til 20. juli 2006) *Sverige* Svenska Kraftnät Peter Helsing (telefon – 7. og 8. august 2006) *Finland* NESA Matti Jauhiainen (mailkorrespondanse januar 2007) *Storbritannia* Ofgem Keith Smith (mailkorrespondanse – i perioden 26. juli til 4. august 2006) Central Networks Jonathan Ashcroft

Mr. Martin Davis Finance Sector Outreach (mailkorrespondanse – i perioden 27. juli til 3. august 2006)	(mailkorrespondanse – i perioden 31. juli til 4. august 2006) NISCC Ciaran Osborn (mailkorrespondanse – 7. august 2006)

Andre myndigheter og ressurspersoner

Herbjørn Andresen,
Stipendiat ved Avdeling for Forvaltningsinformatikk, UiO
6. juli 2006

Datatilsynet, 12. juli 2006

Nasjonal Sikkerhetsmyndighet, 20. juli 2006

Dag Wiese Schartum, AFIN, UiO, mailkorrespondanse

D LOVVERK SOM OMHANDLER DATATILSYNET (VEDLEGG TIL KAPITTEL 6)

LOV 2000-04-14-31: Lov om behandling av personopplysninger
Personopplysningsloven
Lovens formål er å beskytte personer mot at personvernet blir krenket gjennom behandling av personopplysninger, og den gjelder for *"behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler og annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister*" (jf lovens § 3).
http://www.lovdata.no/all/hl-20000414-031.html

FOR 2000-12-15-1265: Forskrift om behandling av personopplysninger
Personopplysningsforskriften
Kapittel 2 i forskriften omhandler emnet informasjonssikkerhet, og stiller blant annet krav til risikovurderinger og sikkerhetsrevisjoner. Den stiller krav til fysisk sikring til utstyr som brukes for å behandle personopplysninger, samt sikring av konfidensialitet, tilgjengelighet og integritet. Forskriften trådde i kraft 1. januar 2001.
http://www.lovdata.no/for/sf/fa/xa-20001215-1265.html

LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger
Helseregisterloven
Formålet med loven er i henhold til § 1 *"å bidra til å gi helsetjenesten og helseforvaltningen informasjon og kunnskap uten å krenke personvernet, slik at helsehjelp kan gis på en forsvarlig og effektiv måte*". Lovens § 16 pålegger den databehandlingsansvarlige og databehandleren å sørge for tilfredsstillende informasjonssikkerhet. Informasjonssystemet og sikkerhetstiltakene skal dokumenteres. Loven trådde i kraft 1. januar 2002.
http://www.lovdata.no/all/hl-20010518-024.html

LOV 1999-07-16 nr 66: Lov om Schengen informasjonssystem (SIS)
SIS - loven
Lovens formål er i henhold til § 1 å *"regulere behandlingen i Norge av opplysninger innenfor Schengen informasjonssystem (SIS), herunder å ivareta hensynet til personvern*". § 3 omhandler informasjonssikkerhet, og pålegger den registeransvarlige og databehandleren å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i SIS. Informasjonssystemet og sikkerhetstiltakene skal dokumenteres. Loven trådde i kraft 1. januar 2001.
http://www.lovdata.no/all/hl-19990716-066.html

FOR 2000-12-21 nr 1365: Forskrift til lov om Schengen informasjonssystem
SIS - forskriften
Kapittel 7 i forskriften tar for seg internkontroll og informasjonssikkerhet, og pålegger blant annet at risikovurdering skal gjennomføres ved endringer av betydning for informasjonssikkerheten, og at sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Samtidig skal konfidensialitet, tilgjengelighet og integritet sikres. Forskriften trådde i kraft 1. januar 2001.
http://www.lovdata.no/for/sf/jd/xd-20001221-1365.html

LOV 2001-06-15 nr 81: Lov om elektronisk signatur
E-signaturloven
I henhold til lovens § 1 er formålet med loven *"å legge til rette for en sikker og effektiv bruk av elektronisk signatur ved å fastsette krav til kvalifiserte sertifikater, til utstederne av disse sertifikatene og til sikre signaturfremstillingssystemer*". Loven trådde i kraft fra 1. juli 2001.
http://www.lovdata.no/all/hl-20010615-081.html