KUNGL
TEKNISKA
HÖGSKOLAN

Risk management of information systems in dynamic environments

-A case study of the Norwegian Defence and the process of approving classified information systems.

Ola Holm

Institutionen för
Data- och Systemvetenskap

Examensarbete
Nr 2004-x-164
2002

Examensarbete 20 poäng
i data- och systemvetenskap
inom magisterprogrammet i informations- och kommunikations säkerhet,
Kungl Tekniska Högskolan

Sammendrag

Det er ingen selvfølge at forutsetningene som er lagt til grunn for et sikkerhetsnivå i et informasjonssystem fortsatt er gyldige når omgivelsene endres kontinuerlig. Denne MSc rapporten beskriver et risikohåndteringskonsept som går ut på å gi en kort opplæring i risikohåndtering og dokumentering av sikkerhetstiltak for å øke kompetansen hos lokale sikkerhetsorganisasjoner. Opplæringen skal gi nødvendig forståelse for sammenhengen mellom kritisk informasjon, trusler og sårbarheter slik at personellet får et aktivt forhold til dokumenterte sikkerhetstiltak. Etter endt opplæring kan medarbeiderne bidra til å opprettholde de forutsetningene som ligger til grunn for et sikkerhetsnivå, og avdekke avvik som medfører en vesentlig endring i det vedtatte sikkerhetsnivået.

Det er gjennomført en kvalitativ studie av Forsvarets informasjonssystemer og prosessen for å oppnå en sikkerhetmessig godkjenning i henhold til Sikkerhetsloven. Et kurs i risikohåndtering av informasjonssystemer er gjennomført som et eksperiment for å demonstrere hvordan en kan imøtekomme et stort kompetansebehov som er avdekket innen dette området. Kurset ble evaluert av en gruppe med variert erfaringsbakgrunn, fra nybegynnere til ekspertnivå. Rapporten foreslår en struktur for å organisere alle dokumenterte sikkerhetstiltak, slik at det skal bli lettere å forholde seg til dem og gjøre forløpende oppdateringer i takt med skiftende omgivelser.

Abstract

The validity of preconditions for an information system’s security level can’t be taken for granted when the environment for that system is constantly changing. This MSc report describes a risk management concept that is based on a brief education in risk management procedures and documentation of security measures in order to strengthen local security organization competence. The purpose is to give key personnel necessary understanding about the connection between critical information, threats and vulnerabilities in such a manner that they will achieve an active relationship to the documented security measures. After completing the course, the coworkers can contribute to uphold the preconditions which a given security level is based on and reveal deviations which represent a significant change of that security level.

A qualitative study of the Norwegian Defences information systems and the process of achieving a security certification according to national legislation have been conducted. A course in risk management of information systems is carried out as an experiment in order to demonstrate how a revealed need for competence in this area can be addressed. The course was evaluated by a group of people with varied experience background, from beginners to experts. This report suggests a structure to organize all documented security measures, in order to make it easier to relate to them and make continuously updates as the environment changes.

Forord

Denne rapporten er avsluttende del av mitt MSc studie ved HIG og KTH. Parallelt med studiene har jeg arbeidet som seniorinstruktør i Forsvaret ved Utdannings og kompetansesenter for Hærens Samband. Oppgaven har på mange måter vært sammenfallende med de arbeidsoppgavene jeg har utført i Forsvaret, noe som har gitt meg mulighet til å bruke egne erfaringer og kontaktnett til oppgavearbeidet.

Problemstillingen er formulert ut fra erfaringer med å veilede sikkerhetspersonell og dokumentere sikkerhetstiltak for informasjonssystemer som skal sikkerhetsgodkjennes. I løpet av perioden jeg har arbeidet med denne oppgaven, har prosjektet blitt kjent blant sentrale aktører i godkjenningsarbeid av informasjonssystemer i Forsvaret. Derfor har jeg blitt kontaktet av flere militære avdelinger som ønsker støtte til å organisere sikkerhetstiltak og dokumentere dem slik det foreslås i denne rapporten.

Dersom denne oppgaven kan bidra til å forbedre sikkerhetsdokumentasjon generelt og gi ideer til hvordan risikohåndtering av sikkerhetsgraderte informasjonssystemer kan utføres, vil hensikten min med å velge denne problemstillingen være oppnådd.

En stor takk rettes til kollegaer og venner i informasjonssikkerhetsmiljøene i Forsvaret og Nasjonal Sikkerhetsmyndighet for bidrag til denne oppgaven. Dere har gitt verdifulle innspill gjennom samtaler, diskusjoner, intervjuer og skriftlig korrespondanse. Det må også sies at denne oppgaven hadde ikke vært mulig å gjennomføre uten den støtten og forståelsen som min nærmeste familie har utvist i oppgavearbeidsperioden.

Tusen takk!

Lillehammer 30. juni 2004

Ola Holm

> ”*Mange tror at de utarbeider dokumentasjon for å tilfredstille NSM. Da blir jeg litt provosert. Hensikten med dokumentasjonen er å sørge for at systemet er sikkert, ikke å tilfredstille NSM.”*
>
> Sikkerhetsekspert ansatt hos
> Nasjonal Sikkerhetsmyndighet

Figur 1: Hensikt med sikkerhetsdokumentasjon

Innhold

Figurliste

Kapittel

1 Innledning

Dette kapitlet beskriver problemstillingen som er valgt for oppgaven og utdyper hvorfor den er relevant for kontrollmyndigheter, systemeiere og sikkerhetsledere. Problemstillingen konkretiseres i forskningsspørsmål som skal søkes besvart i denne oppgaven. Kapitlet avsluttes med avgrensninger og disposisjon for det videre arbeidet.

1.1 Tema

Denne MSc rapporten vil drøfte et sikkerhetskonsept for informasjonssystemer med dynamiske omgivelser. Med *sikkerhetskonsept* menes en ide og skisse til løsning for å opprettholde informasjonssikkerheten i en organisasjon. Med *dynamiske omgivelser* forstås i denne sammenhengen alle former for endringer i miljøet rundt et informasjonssystem som kan få betydning for informasjonssikkerheten. Ideen er basert på en militær risikohåndteringsmetode og prosess kjent under navnet Operations Security (OPSEC)[16].

1.2 Problemstilling

Hvordan kan en stole på at forutsetningene som er lagt til grunn for et sikkerhetsnivå i et informasjonssystem forsatt er gyldige når omgivelsene endres kontinuerlig? Dagens løsninger for risikohåndtering er ikke tilstrekkelig når tempoet og omfanget av endringene økes.

1.3 Begrunnelse, motivasjon og gevinstpotensial

Et informasjonssystem som består av mobile enheter, vil få endrede fysiske omgivelser hver gang en enhet forflyttes til et nytt geografisk område. Omfattende utskiftinger av materiellkomponenter, applikasjoner eller personell vil også medføre en betydelig endring som kan påvirke sikkerhetsnivået. Det er behov for et sikkerhetskonsept som gir en kontinuerlig vurdering av omgivelsene og indikerer et avvik på en korrekt og gyldig måte slik at nødvendige tiltak kan iverksettes så tidlig som mulig for å forhindre eller begrense sikkerhetstruende hendelser. Tradisjonelle revisjonsprosesser vil ikke kunne fange opp avvik hurtig nok når endringer skjer med høyt tempo eller på annen måte endrer forutsetningene som ligger til grunn for et sikkerhetsnivå.

Resultatet av denne MSc oppgaven vil være høyst relevant for flere beslutningstakningssituasjoner. For eksempel:

- Informasjonssystemeiere: ”Er sikkerhetstiltakene tilstrekkelig, eller må det gjennomføres en ny og omfattende risikoanalyse?”
- Kontrollmyndigheter: ”Er grunnlaget for den sikkerhetsmessige godkjenningen av informasjonssystemet forsatt gyldig?”
- Sikkerhetsledere: ”Hvordan kan jeg effektivt iverksette hensiktsmessige sikkerhetstiltak for å møte nye forutsetninger som er oppstått som følge av oppdukkende hendelser?”

Forsvaret er systemeier av flere virksomhetskritiske informasjonssystemer som opereres i dynamiske omgivelser. Konsept for nettverksbasert anvendelse av militærmakt bygger på en ide for hvordan militære operasjoner kan gjennomføres ved å knytte sammen militære kapasiteter i nettverk ved bruk av informasjonsteknologi [15]. Konseptet baserer seg i følge Forsvarssjefens militærfaglige utredning 2003 på ”informasjonsoverlegenhet og utnyttelse av slik overlegenhet for å oppnå økt felles situasjonsbevissthet, økt hastighet i utøvelse av kommando, økt tempo i operasjonene, ...” Det vil være en naturlig slutning å anta at konseptets avhengighet av informasjonssystemer og krav til tempo skaper en sårbarhet og derigjennom behov for et sikkerhetskonsept for informasjonssystemer som tar høyde for hurtige endringer i omgivelsene.

Utdannings og opplæringsvirksomheter innen informasjonssikkerhet trenger ny kunnskap innen dynamisk risikohåndtering for informasjonssystemer. Denne rapporten vil utgjøre et grunnlag og en akademisk forankring for et eget fag ved Hærens Ingeniørhøgskole som skal hete ”Operasjonssikkerhet for informasjonssystemer”. Dette faget skal tilbys sikkerhetspersonell, ledere og øvrige interessenter for virksomhetskritiske informasjonssystemer som anvendes i omgivelser som endres i høyt tempo.

Kontrollmyndigheter er tjent med at det tilbys relevant opplæring og undervisning for sikkerhetspersonell. En gjennomgående bedre forståelse for risikohåndtering blant ledere, drifts- og sikkerhetspersonell, vil bidra til å heve sikkerhetsnivået for virksomhetskritiske informasjonssystemer. Det gjelder særlig i tilfeller hvor store utskiftninger og andre endringer i omgivelsene har en høy frekvens. Dette kan illustreres med et eksempel: Det hjelper lite at det foreligger en grundig sikkerhetsdokumentasjon som er i henhold til krav og bestemmelser, dersom nøkkelpersonell er skiftet ut og nye medarbeidere ikke er kjent med innholdet i dokumentene, eller har nødvendige forutsetninger for å forstå tiltakene og prosedyrer som er beskrevet og lagt til grunn for sikkerhetsmessig godkjenning. Sikkerhetskonseptet vil gjøre det enklere å foreta en pålitelig og gyldig kontroll med at forutsetningene for den sikkerhetsmessige godkjenningen fortsatt er tilstede, og ikke er endret som følge av utskiftinger eller andre endringer i omgivelsene.

Sikkerhetskonseptet vil ta utgangspunkt i Forsvarets informasjonssystemer, men er også overførbart til andre systemer med dynamiske omgivelser hvor systemeieren er lovpålagt å gjennomføre og dokumentere risikohåndtering. Vi tror at formaliserte prosesser for risikohåndtering av informasjonssystemer er lite kjent hos systemeiere, og gjennomføres derfor i varierende utstrekning. I den grad risikohåndtering er utført og dokumentert, er det ønskelig å korte ned tiden mellom hver revisjonssyklus for å møte nye trusler og sårbarheter som introduseres gjennom endrede omgivelser så raskt som mulig. Dette taler for enkle prosedyrer som kan utføres av mange.

Operasjonssikkerhet for informasjonssystemer vil bli et eget fag som skal undervises ved Hærens Ingeniørskole i skoleåret 2004 - 2005. Fagområdet er relevant for både Forsvaret og andre organisasjoner med informasjonssystemer som er eksponert for store endringer. Det vil derfor tilbys som etterutdanning for sikkerhetspersonell i statlige og fylkeskommunale virksomheter, i tillegg til grunnutdanning på bachelorstudiet. MSc rapporten vil utgjøre et vesentlig bidrag for å utvikle faget Operasjonssikkerhet gjennom å beskrive hvordan den generelle metoden kan anvendes for virksomhetskritiske informasjonssystemer med et utvalg sikkerhetsmetrikker og sjekklister.

1.4 Forskningsspørsmål

Før en lager et sikkerhetskonsept som tar høyde for hurtige endringer i omgivelsene, er det nødvendig å undersøke hvordan risiko og sikkerhetsnivåer fastsettes for et informasjonssystem. Deretter må det undersøkes hvordan en hurtig og med rimelig grad av sikkerhet kan avdekke om forutsetningene som er lagt til grunn for risikofastsettelsen er endret eller ikke. Dette vil være avhengig av i hvilken grad det er mulig å måle endringer i faktorer som har innvirkning på informasjonssikkerheten på en hurtig og kosteffektiv måte.

Dersom det viser seg gjennomførbart å foreta kontinuerlige målinger og vurdering av risiko på en gyldig og pålitelig måte, vil det åpne muligheter for en fleksibel tilpasning av sikkerhetstiltak i takt med skiftende forutsetninger. Da kan en sikkerhetsmetrikk utgjøre en vesentlig del av et beslutningsgrunnlag for å avgjøre hvorvidt gjeldende sikkerhetstiltak er tilstrekkelig og relevant i forhold til de aktuelle truslene og sårbarhetene som de til enhver tid gjeldende omgivelsene innebærer.

Dette fører til at følgende forskningsspørsmål må besvares:

1. Hvordan fastsettes risiko og sikkerhetsnivå for et informasjonssystem?
2. Hvilke faktorer bør beskrives i et risikohåndteringskonsept for informasjonssystemer?
3. Hvordan kan opplæring i risikohåndtering gjennomføres?
4. Hvilke avvik er signifikante i forhold til forutsetningene for et sikkerhetsnivå?

Spørsmål 1 vil besvares under kapitlet ”relatert arbeid”, mens spørsmålene 2, 3 og 4 vil adresseres i egne kapitler.

1.5 Avgrensninger

Problemstillingen er gyldig for ethvert informasjonssystem som utsettes for endringer i omgivelsene over tid. Men for å gjøre oppgaven håndterbar og begrense omfanget av undersøkelsene, velger vi å konsentrere oss om en organisasjon.

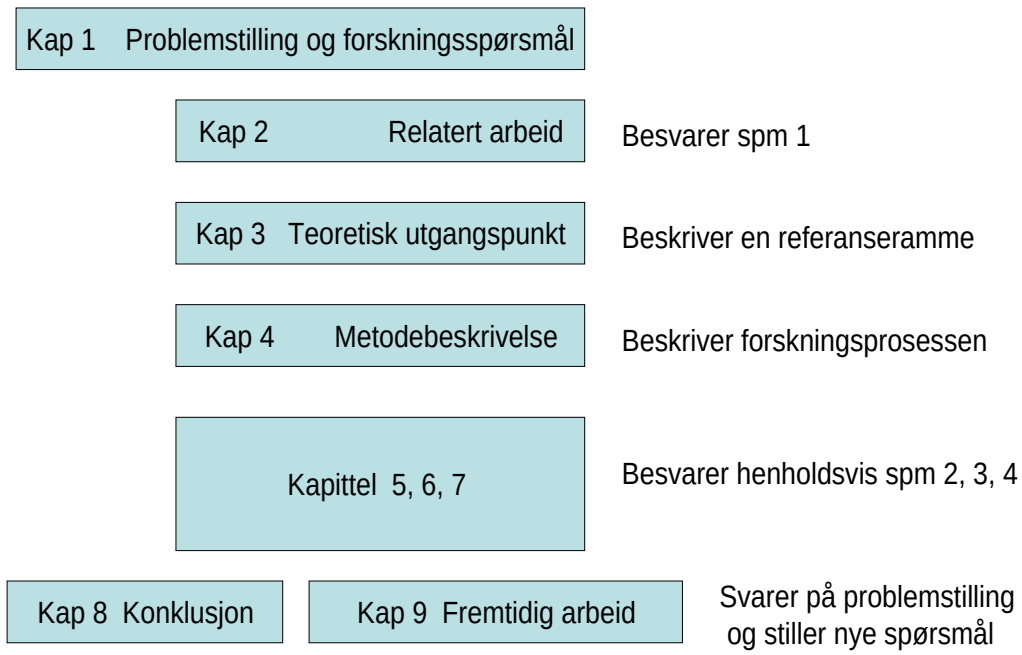
Forsvaret er en organisasjon som egner seg godt som undersøkelsesobjekt i denne sammenhengen. Den er relativt stor og har mange geografisk atskilte avdelinger som knyttes sammen med interne informasjonssystemer, både nasjonalt og internasjonalt. Omfanget av undersøkelsene for denne oppgaven vil derfor avgrenses til Forsvaret.

Forutsetningene for et valgt sikkerhetsnivå varierer selvsagt for ulike systemer, bruksområder og organisasjoner som eier dem. For å avgrense omfanget av forutsetninger,

velges det i denne oppgaven å fokusere på sikkerhetsgraderte informasjonssystemer som må sikkerhetsgodkjennes i henhold til Sikkerhetsloven før de kan tas i bruk.

1.6 Disposisjon

I kapittel to relatert arbeid, vil forskningsspørsmål en bli besvart. Deretter beskrives to teoretiske utgangspunkter, OPSEC prosessen og en helhetlig organisasjonsmodell kalt Leavitts diamant i kapittel tre. Teorien vil være et grunnlag for å forstå hvordan sikkerhetsgodkjenning og risikohåndtering utføres.



Figur 2: Disposisjon av oppgaven

Metoder som er brukt for innsamling av informasjon i denne oppgaven er beskrevet i kapittel fire. Funn fra intervjuer og dokumentanalyse vil sammen med teorikapitlet utgjøre grunnlaget for å beskrive et risikohåndteringskonsept i kapittel fem. Forskningsspørsmål fire vil dermed besvares i kapittel fem.

Kapittel seks vil beskrive utforming av et kurs i risikohåndtering og dokumentering av sikkerhetstiltak. Kurset ble gjennomført som et eksperiment for å vise hvordan opplæring kan gjøres. Effekten av kurset blir drøftet basert på tilbakemeldinger fremkommet av en

spørreundersøkelse blant kursdeltakerne. Kapittel seks vil følgelig besvare forskningsspørsmål tre.

Kapittel sju drøfter forskningsspørsmål fire som går ut på om det kan fastsettes hvilke endringer som er signifikant i forhold til forutsetningene i en sikkerhetsmessig godkjenning. Intervju av sikkerhetseksperter vil utgjøre en vesentlig del av drøftingsgrunnlaget.

Kapittel åtte er konklusjon og besvarer problemstillingen og oppsummerer funn fra tidligere kapitler. Kapittel ni foreslår spørsmål til fremtidig arbeid. Til slutt er det et appendikskapittel og et referansekapittel.

Kapittel

2 Relatert arbeid

Dette kapitlet omhandler hvordan risiko defineres, fastsettes og håndteres i forbindelse med sikkerhetsgodkjenninger av informasjonssystemer. Deretter refereres det til en vurdering av ulike metoder for risikofastsettelse som er tilgjengelig i Norge, før det beskrives i hvilken grad informasjonssikkerhet kan måles og hvordan en sikkerhetsmetrikk bør utformes.

2.1 Hvordan fastsettes risiko og sikkerhetsnivå?

Peter Bernstein [19] forklarer hvordan kontroll av risiko er en integrert del av hverdagen for de aller fleste av oss. Når for eksempel leger opererer pasienter, investorer kjøper aksjer, og ingeniører konstruerer byggverk, handler det i stor grad om risikohåndtering. Risikohåndtering er i følge Bernstein en form for kost/nytte vurdering som gjør oss effektive, og er derfor et symbol på fremskritt og bruk av moderne teknologi. For informasjonssystemer eksisterer det ulike metoder og prinsipper for å fastsette risiko og sikkerhetsnivå [9], [10], [22], [23].

Enkelte vektlegger systemets motstandskraft ved å måle robusthet/sårbarhet mot angrep gjennomført i et testmiljø [20]. Denne tilnærmingen går direkte på sikkerhetsnivået, uten å gå veien innom risiko. En annen innfallsvinkel er å definere hvilken risiko som aksepteres, og beregne risiko ut fra sannsynlighet for at en uønsket hendelse kan oppstå og hvilke konsekvenser hendelsen medfører [7], [11]. Sikkerhetsnivået utledes deretter av den aksepterte risikoen. En tredje måte å fastsette risiko på er gjennom en vurdering trusler, sårbarheter og verdiobjekter [5], [16], [21].

2.1.1 Motstanders innsatsfaktor

En måte å fastslå et sikkerhetsnivå for et informasjonssystem er å anslå hvor mye ressurser det vil koste en motstander å forberede og gjennomføre et angrep [20]. Dette bygger på en subjektiv vurdering da det antas at en motstander ikke kjenner til andre angrepsmetoder enn dem som modelleres og gjennomføres i en testsituasjon. Likevel er prinsippet anerkjent i forskningsmiljøer, og det bygger på det samme resonnementet som anvendes for å beregne styrken på safer. Dersom det tar 30 minutter for en motstander å bryte seg inn i den aktuelle safen, og motstanderen har tilgang til alle tenkelige ressurser, vil 30 minutter si noe om safens robusthet og derigjennom sikkerhetsnivå.

Fordelen med denne beregningsmetoden er at den fokuserer på egen robusthet/sårbarhet uten å komme inn på sannsynlighetsbetraktninger. En ulempe er at det er vanskelig å gjennomføre gyldige og pålitelige tester for komplekse systemer i dynamiske omgivelser.

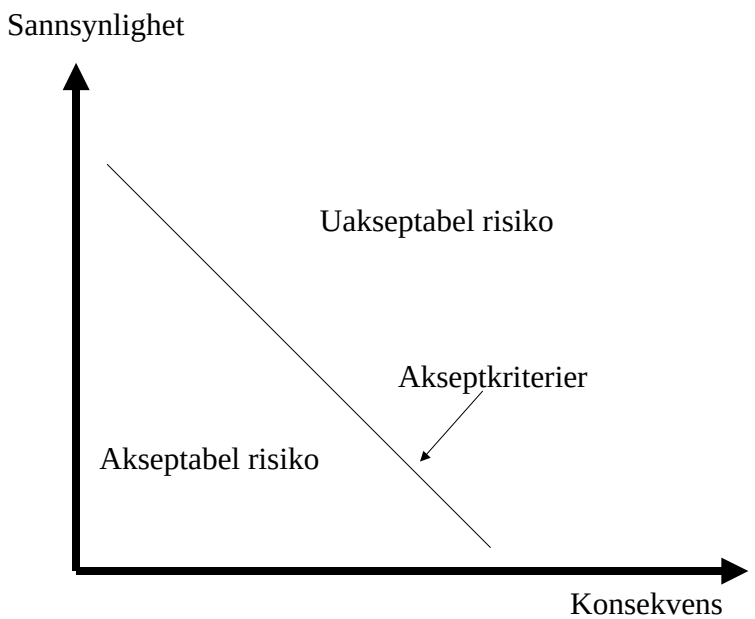
2.1.2 Risiko som produktet av sannsynlighet og konsekvens

I følge Sintef sine internettsider [14] er følgende tre spørsmål sentrale når en skal kartlegge risiko og sårbarhet:

1. Hva kan gå galt?
2. Hva er sannsynligheten for at det går galt?
3. Hva er konsekvensene hvis det går galt?

Det er utviklet en rekke metoder for å identifisere og evaluere risikoforhold. Noen metoder er baserte på ekspertvurderinger og gir kun en grov klassifisering av risiko, mens andre metoder er baserte på detaljert modellering og tallfesting av forventet tap. Sintef har bidratt til utvikling av en norsk og internasjonal standard som omhandler krav til risikoanalyser, NS 5814.

NS 5814 [7] definerer risiko som uttrykk for den fare som uønskede hendelser representerer for mennesker, miljø eller verdier. Risikoen uttrykkes ved sannsynligheten for og konsekvensene av de uønskede hendelsene. Akseptkriterier er definert som kriterier basert på forskrifter, standarder, erfaring og/eller teoretisk kunnskap som legges til grunn for beslutninger om akseptabel risiko. Akseptkriterier kan uttrykkes med ord eller være tallfestet.



Figur 3: Risiko og akseptkriterier

En risikoanalyse er en systematisk fremgangsmåte for å kartlegge uønskede hendelser og beskrive risiko [7], [10], [11]. Akseptkriterier indikerer sikkerhetsnivået, og det skal iverksettes sikkerhetstiltak for å møte uakseptabel risiko[4], [11]. Dersom kostnadene forbundet med nødvendige sikkerhetstiltak anses å være for høye, må enten akseptkriterier justeres til et høyere risikonivå eller en kan fjerne funksjonaliteten som utgjør risikoen. Dette er selve kjernen i en risikovurderingsprosess og resultatet vil medføre konsekvenser for det vedtatte sikkerhetsnivået [11]. Det hele kokes ned til en kost/nytte vurdering av sikkerhetstiltak opp mot akseptabel risiko [19].

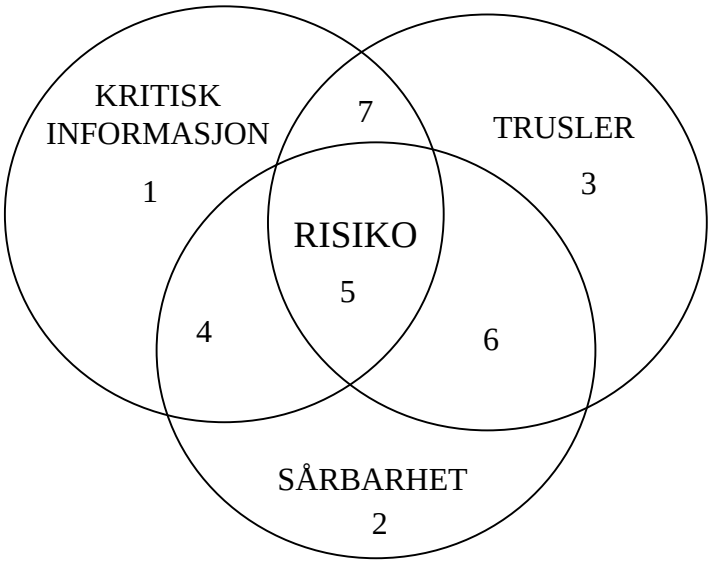
For sikkerhetsgraderte informasjonssystemer stilles det krav til hvilken risiko som er akseptabel av myndighetene gjennom lov og tilsynsmyndigheter [17]. Det samme gjelder informasjonssystemer som behandler informasjon underlagt annen lovgivning som eksempelvis personopplysninger [18]. Lovpålagte krav til informasjonssikkerhet er minimumskrav, og for mange systemeiere vil det være ønskelig med tilleggsikring for særlig kritisk informasjon. [17], [18].

Tilstedeværelse av tilfeldighet er et krav som må innfris før en kan gjøre sannsynlighetsberegninger og statistiske undersøkelser [24]. I safety scenarier kan det antas at hendelser inntreffer tilfeldig, og bruk av stokastiske metoder med estimater for sannsynlighet vil følgelig være gyldige. Men i et security perspektiv hvor det er snakk om tilsiktede handlinger som ikke er tilfeldige, vil sannsynlighetsberegninger medføre gyldighetsproblemer. For eksempel vil sannsynligheten være lik 1 og ikke en statistisk verdi fremkommet av erfaringsdata, når en motstander har bestemt seg for å gjennomføre et angrep. Dette illustrerer svakheten med den tradisjonelle risikodefinisjonen, og gjør det nødvendig å bruke flere perspektiver for å forstå risiko som et uttrykk for det totale trusselbildet og den faren som informasjonssystemer står ovenfor.

ROSS metoden [11] ble utviklet i et samarbeidsprosjekt mellom Sikkerhetsstaben i Forsvarets overkommando (FO/S), Norges teknisk-naturvitenskapelige universitet (NTNU) og Direktoratet for sivilt beredskap (DSB). Rapporten om ROSS [11] bruker risikodefinisjonen fra NS 5814 [7] som forutsetter tilfeldige hendelser. I følge forfatterne [11, side v], presenterer rapporten en metode for analyse av objekt og informasjonssikkerhet som er rettet mot fagfeltet security. Analysen konsentrerer seg om planlagte handlinger som blir utført med overlegg, såkalte tilsiktede handlinger. Tilfeldige handlinger omfattes ikke av analysen blir det videre slått fast av forfatterne. ROSS metoden behandler altså risiko i security perspektiv med definisjoner fra safety tradisjonen. Det medfører som nevnt gyldighetsproblemer å tilordne tilsiktede handlinger sannsynlighetsverdier, noe som krever tilstedeværelse av tilfeldighet. Flere kritikere har uttalt skepsis mot å bruke sannsynlighet i security, blant annet Jurki Kontio, Gerhard Getto og Dieter Landes i [22].

2.1.3 Overlappende trussel, sårbarhet og kritisk informasjon.

Shirley Payne hevder i [5] at verdier, trusler og sårbarhet er elementer i et overordnet risikobilde. Hvis en betrakter kritisk informasjon som en verdi, støttes denne tilnærmingen i doktrinen for OPSEC [16], som definerer risiko som det området hvor kritisk informasjon, trusler og sårbarheter overlapper hverandre. Tim Bass og Roger Robichaux utdyper forholdet mellom de tre faktorene trussel, sårbarhet og kritisk informasjon i [21] som vist på figuren under:



Figur 4: Faktorer som påvirker risiko

1. Kritiske objekter (informasjon, systemer, programmer, mennesker, utstyr eller fasiliteter) som ikke har noen kjente sårbarheter eller trusler.
2. Sårbarheter i systemer, programmer, mennesker, utstyr eller fasiliteter som ikke er assosiert med kritiske objekter og som ikke har kjente trusler.
3. Trussel omgivelser som har ingen kritiske objekter eller sårbarheter (eller sårbarhetsinformasjon).
4. Kritiske objekter som har kjente sårbarheter men ingen kjente trusler.
5. Kritiske objekter som har kjente sårbarheter og trusler. Dette er det mest sensitive området og utgjør risiko.
6. En trussel eller antall trusler har tilegnet seg kunnskap og/eller kapasitet til å utnytte en sårbarhet men ikke til et kritisk objekt.
7. Kritisk objekt som har ingen kjente sårbarheter, men det er eksponert for en spesifisert trussel.

Andrew Jones beskriver i [9] en kalkuleringsmetode for å beregne en trusselverdi for en ondsinnet trusselagent. Verdien framkommer gjennom en vurdering og fastsettelse av den enkelte trusselagentens motivasjon og kapasitet, samt forsterkende og hemmende faktorer i omgivelsene. Jones påpeker at aksess til informasjonssystemet er en forutsetning for at trusselagenten skal utgjøre en reell trussel, og poengterer at en trusselagent kan få motivasjon gjennom en oppstått situasjon, en katalysator. Trusselbildet endres følgelig dynamisk ved at trusselagenter som har kapasitet men ikke motivasjon kan bli en trussel, gitt en katalyserende hendelse.

Fordelen med en slik tilnærming til risiko, er at det virker konsistent og gyldig for security. En svakhet er at den lett blir for overordnet og generell til å kunne foreta en grundig analyse av informasjonssystemer, uten en spesifisering i form av sjekklister eller lignende. Opp mot denne oppgavens problemstilling, vil OPSEC tilnærmingen av risiko være best egnet for hurtig deteksjon av avvik fra forutsetninger på en pålitelig og gyldig måte. Dersom det forutsettes at en grundig risikoanalyse er gjennomført i det systemet tas i bruk, ved Tid = 0, vil det være mulig å foreta en risikovurdering lokalt ved de enkelte avdelingsenhetene i nettverket, uten å involvere sikkerhetseksperter eller andre kostbare knapphetsfaktorer. Forutsetningen er at personellet blir gitt opplæring i risikohåndtering.

Svakheten som er knyttet til at metoden ikke vil dekke alle forhold som kan påvirke årsakskjeder, oppveies slik vi ser det ved enkelheten det er mulig å oppnå. Dersom en sjekkliste var konstruert slik at den dekket de vesentlige faktorene, kunne det tenkes at en effektivt hadde avdekket forhold som anses som de viktigste forutsetningene for å opprettholde informasjonssikkerheten. Dette står i skarp motsetning til metoder som tilstreber å dekke alle mulige årsakskjeder. Det er uansett tvilsomt om idealet om kompletthet kan oppnås siden en ikke kjenner alle årsakskjeder med tilhørende virkninger i komplekse systemer [26].

Dette taler for et risikohåndteringskonsept som er enkelt å forstå, slik at personell med et kort kurs i risikohåndtering blir i stand til å avdekke vesentlige avvik ved hjelp av sjekklister. For systemer i dynamiske omgivelser, mener vi det vil være viktigere å avdekke signifikante avvik hurtig framfor grundige revisjonsprosesser som av kostnadsmessige årsaker må gjennomføres med et større tidsintervall. Følgelig vil MSc rapporten ha som målsetting å videreutvikle OPSEC metoden [16], slik at den ved hjelp av undervisning og bruk av sjekklister kan anvendes for å avdekke signifikante endringer i omgivelsene. Enkelhet forutsetter ekspertise i utvelgelsen av faktorer og kriterier som skal vektlegges [26], [28]. Kompleksiteten, vurdering av relevans og usikkerhet knyttet til årsak-virkning forhold gjør utvelgelsen av måleparametere helt avgjørende for om beslutningsgrunnlaget er gyldig og gir et riktig bilde av de faktiske forholdene [26], [28].

2.2 Vurdering av metoder for risikofastsettelse

En arbeidsgruppe nedsatt av ASIS Norway [10] har gjennomført en kartlegging av tilgjengelige metoder i Norge for risikoanalyse. Mandatet til gruppen var å undersøke hvilke metoder og verktøy som var tilgjengelig og avdekke eventuelle styrker og svakheter. Arbeidsgruppen skilte mellom sjekklister, kvalitative og kvantitative analyser. Sjekklister grenser til revisjon, tar kort tid, er billige og egner seg best når de er tilpasset den enkelte virksomhet. Ulempen er at de kan medføre unøyaktighet og en risikerer å sette inn beskyttelse på feil sted. Sjekklister er i større grad et verktøy for revisjon enn for risikoanalyser i følge arbeidsgruppen. Vurderte metoder var ISAP. For denne MSc rapporten vil ikke arbeidsgruppens skepsis til ISAP og bruk av sjekklister få andre konsekvenser enn å tjene som en påminnelse om tidligere nevnte behov for ekspertise i utvelgelsen av kriterier for å oppnå tilstrekkelig gyldighet [26], [28].

Kvalitative analyser er skjemastyrte hvor det tas utgangspunkt i de enkelte objekter eller uønskede hendelser. Resultatet presenteres ofte i risikomatriser, og hviler fullstendig på kvaliteten i gruppen som har gjennomført analysen. Hovedinnvendingen er subjektivitet i mangel på objektive målinger. Arbeidsgruppen konkluderer med at slike metoder gir et dårlig grunnlag for kost/nytte analyser av tiltak. Vurderte metoder var ROSS [11], Siple to

Apply Risk Analysis (SARA), Telerisk og en metode utviklet av Næringslivets Sikkerhetsorganisasjon (NSO) for sine medlemsbedrifter.

Kvantitative analyser forutsetter som oftest tilgang til et stort statistisk materiale. Fordelen er objektivitet i målinger og at resultatet kan uttrykkes i et ledelsesspesifikt språk med mulighet for kost/nytte betraktninger. Ulempen er at det sjelden eksisterer tilgang til stort statisk materiale og metodene benytter relativt komplekse beregninger. Vurderte metoder var Fundamental Information Risk Management (FIRM) og KvantRisk.

Det fins en alternativ kvantitativ metode, der man blander ny (subjektiv) informasjon med kjent (objektiv) informasjon. Subjektiv informasjon uttrykkes i en sannsynlighetsfordeling selv om man ikke har en kjent datamengde. Dette kalles for Bayesisk eller subjektivistisk statistikk og benyttes i dag blant annet for å analysere prosjektusikkerhet og nedetider.

2.3 I hvilken grad kan informasjonssikkerhet måles?

I [1] mener McHuge at ideen om å måle sikkerheten i et system er prisverdig, men at det vitenskapelige grunnlaget mangler. På grunn av manglende bevis for at sikkerhet kan måles, fastslås det at ideen ikke kan støttes. Blant annet pekes det på at dersom et system brukes på feil måte, eller at noen finner opp en ny måte å gjennomføre et angrep på som ingen har tenkt på tidligere, vil det være meningløst å bruke kvantitative verdier for å klassifisere sikkerheten til et system. Dette standpunktet kan eksemplifiseres ved at en bruker unnlater å følge sikkerhetsinstruksen som beskriver hvordan henvendelser skal håndteres. Videre vil det ikke være tilstrekkelig å konkludere med at en person som tidligere har avslørt og motstått et social engineering angrep, ikke vil la seg lure ved et nytt angrep som er utformet på en annen måte.

Videre gjør McHuge et poeng av at softwareutvikling foreløpig er et umodent fagfelt, hvor en ikke er kommet så langt at en med sikkerhet kan fastslå sammenhenger mellom egenskaper i programmer og gjennomsnittlig tid til systemer feiler. (Mean time between failures). Mennesker er ikke noe mindre kompliserte enn software, snarere tvert om. Ulike rasjonelle og irrasjonelle faktorer som ligger til grunn for en beslutning utgjør en enorm kompleksitet, som igjen gjør det vanskelig å fastslå måleenheter som sier noe om hvor god et menneske er til å fatte riktige beslutninger.

McCallam [2] sier han er motstander av nummeriske mål for å kvantifisere informasjonssikkerhet (Information Assurance). Hovedgrunnen ligger i at informasjonssikkerhet må betraktes fra et utvidet perspektiv, hvor prosess, teknologi og menneskelige faktorer er integrert. Det som i følge McCallam er viktig, er en tilnærming til informasjonssikkerhet som omfatter samhandling og utvikling av teknologi, mennesker og prosesser. Til tross for uttalt motstand mot nummeriske mål, foreslås en indeks med en skala fra 1 til 10 som kan klassifisere motstandskraften i et informasjonssystem. Resiliance Assurance Index (RAI) er en skala som beskriver kvalitative mål fra et ubeskyttet system til en fullverdig beskyttelse. Utgangspunktet for RAI er perspektivene fra en angriper og den som skal beskytte systemet. I nivå 0 har angriperen full kontroll, mens det i nivå 10 er beskytteren som har kontrollen. Angrep er kun mulig dersom beskytteren tillater det. Med dette som bakgrunn, vil det i følge McCallam være mulig å gjennomføre kvalitative bedømmelser av forutsetningene som ligger til grunn for et sikkerhetsnivå.

Absolutt sikkerhet er verken ønskelig eller oppnåelig i følge Odlyzko [3]. Fleksibiliteten som ligger i å kunne tøye regler er helt nødvendig for å kunne fungere effektivt. Et eksempel er en betrodd sekretær som forfalsker underskriften til sjefen og skriver under på dokumenter det er opplagt at sjefen ville godtatt, for å avlaste ham i en stressende hverdag. Dette frigir mer tid til sjefen, men er isolert sett et regelbrudd. Odlyzko hevder at mennesker liker å ha handlefrihet i livet generelt, og at de fleste av oss har problemer med å forholde seg til formelle regler og metoder. Dette er et trekk ved mennesker som kan representere en sårbarhet for social engineering.

Med bakgrunn i Odlyzko vil det være for snevert å forby alle forhold som kanskje kan komme til å skape sikkerhetsproblemer. En bedre løsning vil være å lage fartsdumper, som gjøre det vanskeligere å gjennomføre angrep. Dersom en for eksempel øker risikoen for å avsløre angripere i ettertid, vil organisasjonens robusthet i forhold til social engineering øke. Selv om en medarbeider har latt seg lure i et enkelt tilfelle, vil en høy deteksjonsgrad med påfølgende reaksjon være et signal til angripere om at slik aktivitet blir oppdaget og slått ned på.

Et slikt syn støttes også av Fran Nielsen [4, side 7], hvor det i forbindelse med risikofastsettelse framheves at det kan være billigere å rydde opp enn å ha et sterkt sikkerhetsopplegg som skal forhindre angrep. I følge Nielsen vil risikofastsettelse og akseptnivåer være er et viktig element i en sikkerhetsmetrikk, siden en ikke kan forutse hva som vil skje i framtiden basert på erfaringsdata. Da vil det være mer hensiktsmessig å øke robustheten ved å begrense skadeomfanget etter angrepet gjennom en rapport og påfølgende reaksjon.

2.4 Hvordan bør en sikkerhetsmetrikk utformes?

I [5] skiller Shirley Payne mellom målinger og metrikker. Måling uttrykker en enkeltstående observasjon av en spesifikk faktor, mens en metrikk er utledet over et tidsrom gjennom sammenligning av flere målinger. Målinger vil derfor si å telle forekomster av objektive hendelser, mens metrikker er en analyse av rådata som fremkommer av målingene.

Payne beskriver gode metrikker som SMART, det vil si spesifikk, målbar, gjennomførbar (attainable), repeterbar og tidsavhengig. Antall sikkerhetshendelser er ikke nødvendigvis noen god indikator på hvor god sikkerhet et system har, siden flaks spiller en betydelig rolle. Flaks kan vanskelig måles, og følgelig blir sikkerheten vanskelig å måle. Et program for sikkerhetsmetrikker bør i følge [5] ta utgangspunkt i et rammeverk som er kjent for organisasjonen fra før, og inneholde følgende trinn:

1. Definere en programmålsetting for sikkerhetsmetrikker.
2. Bestem hvilke metrikker som skal genereres.
3. Lag en strategi for å generere metrikkene.
4. Etabler et mål for metrikkene som skal oppnås, (benchmark).
5. Beslutt hvordan metrikkene skal rapporteres.
6. Utarbeid en gjennomføringsplan og iverksett den.
7. Etabler en formell revisjonssyklus for å forbedre metrikkene.

Metrikker som genereres skal kunne brukes som et element til å forbedre den overordnede sikkerheten, og derigjennom bidra til at å utvikle organisasjonen som en helhet.

Viktigheten av en klar definisjon av hva som skal måles er også framhevet i [6]. Når formålet er veldefinert og entydig, kan en velge enheter og skala. Det kan gjerne brytes ned i del komponenter som blir tillagt en vekting alt etter som hvor stor betydning de ulike faktorene antas å ha.

Kapittel

3 Teoretisk utgangspunkt

I dette kapitlet beskrives to teoretiske referanserammer som denne oppgaven bygger på, OPSEC og Leavitt's diamant. OPSEC er en velprøvd risikohåndteringsprosess som i denne oppgaven vil være et utgangspunkt for risikohåndtering av informasjonssystemer. Leavitt's diamant er en helhetlig organisasjonsmodell som viser sammenhenger mellom fenomener i en organisasjon som er i endring, og vil utgjøre en referanse for et risikohåndteringskonsept.

3.1 Operasjonssikkerhet

3.1.1 Hvorfor OPSEC?

OPSEC er en prosess og metode for å håndtere risiko som kan brukes i forhold til denne oppgavens problemstilling. OPSEC handler om å identifisere kritisk informasjon, vurdere sårbarheter og kjente trusler mot denne informasjonen. Dersom de tre faktorene er tilstede, fastsettes et risikonivå i en relativ skala som for eksempel lav, middels eller høy. Poenget er at beslutningen om hvilke sikkerhetstiltak som skal iverksettes er en konsekvens av risikofastsettelsen.

Problemstillingen om hvordan en kan stole på om forutsetningene for et sikkerhetsnivå er gyldige handler om tillit. En mulig framgangsmåte for å etablere tillit er at de som er ansvarlige for å utføre sikkerhetstiltakene som er forutsatt, forstår hensikten med dem. Dersom en slik forståelse ikke eksisterer eller er mangelfull, kan en risikere at sikkerhetstiltak som er nødvendige ikke gjennomføres. En annen fare er at risikobildet er endret som en følge av endringer i omgivelsene. Da vil ikke forutsetningene lengre være gyldige med de opprinnelige sikkerhetstiltakene som kan være utdaterte og mistet sin funksjon. Opprettholdelse av uhensiktsmessige sikkerhetstiltak vil være ressurskrevende og ikke tjene sikkerheten.

OPSEC metodikken er anerkjent og godt dokumentert. Den kan derfor være et egnet verktøy for å gjennomføre en kontinuerlig risikovurdering i dynamiske miljøer som er under kontinuerlig endring.

3.1.2 Bakgrunn

I følge Interagensy OPSEC Support Staff (IOSS) [30] mistet USA i en tidlig fase av Vietnamkrigen, et alarmerende antall piloter og fly. For å motvirke denne trenden ble et team satt til å analysere US militære operasjoner. Teamet, ”Purple Dragon” oppdaget at avgjørende planleggingsinformasjon ble avslørt gjennom rutinemønstre av atferd. Som en følge av denne oppdagelsen, ble mottiltak hurtig initiert.

Den analytiske prosessen som Purple Dragon benyttet ble kalt Operations Security eller OPSEC, og ble brukt av US militære de neste 20 årene. I 1988 formaliserte Reagan administrasjonen bruken til å gjelde hele regjeringsapparatet med forvaltning og opprettet Interagency OPSEC Support Staff for å tilby trening og veiledning til hele det nasjonale sikkerhetsmiljøet.

3.1.3 Definisjon

Operasjonssikkerhet (OPSEC) er prosessen med å identifisere egen kritisk informasjon og analysere egne handlinger relatert til operasjoner og andre aktiviteter som kan observeres av potensielle motstandere og finne indikatorer som kan avgi kritisk informasjon slik at de kan elimineres eller reduseres til et akseptabelt nivå i forhold til at en motstander kan utnytte dem [29], [16].

OPSEC er ikke en samling av spesifikke regler og instruksjoner, men en metode som kan benyttes i alle operasjonelle aktiviteter [29]. I denne konteksten anvendes metoden som en kontinuerlig revisjon av gjeldende sikkerhetstiltak opp mot det til enhver tid gjeldende trusselbildet i omgivelsene til et informasjonssystem.

3.1.4 OPSEC egenskaper

Målet med OPSEC er å identifisere informasjon og observerbare handlinger relatert til oppdrag, kapasiteter, begrensninger, og intensjoner i den hensikt å motvirke utnyttelse av potensielle motstandere. Operasjonell effektivitet forbedres når ledere og andre beslutningstagere bruker OPSEC i tidlige planleggingsfaser. OPSEC metoden byr på en trinnvis analyse av operasjoner og oppførsel sett fra en motstanders ståsted, gjennom å fastsette hvordan sårbarheter kan utnyttes. Informasjon som motstandere er avhengig av for å nå målene sine utgjør kritisk informasjon om våre operasjoner eller andre aktiviteter. Gjennom å identifisere og beskytte denne kritiske informasjonen, blir OPSEC prosessen et positivt og proaktivt middel for å nekte motstandere en viktig fordel.

OPSEC består av en serie analyser for å undersøke planlegging, forberedelser, utførelse og etterarbeid. OPESEC analyser gir beslutningstagere et grunnlag for å vurdere hvor stor risiko de er villige til å akseptere i gitte operasjonelle omgivelser.

OPSEC bør koordineres tett med øvrige sikkerhetsområder for å sikre at alle sider ved sensitive aktiviteter er beskyttet. Fokus for en OPSEC analyse bør være å hindre potensiell utnyttelse av åpne kilder og observerbare aktiviteter. Disse kildene er ugraderte og vil som en konsekvens være vanskeligere å kontrollere.

3.1.5 OPSEC planlegging

For å hindre at potensielle motstandere tilegner seg verdifull etterretning om egne operasjoner, må det planlegges og iverksettes OPSEC tiltak. For at de skal være effektive, må OPSEC tiltak vurderes så tidlig som mulig i løpet av planprosessen og deretter bli tilstrekkelig revidert for å tilpasses oppdukkende endringer i pågående operasjoner eller endringer i trusselbildet.

OPSEC planlegging og utførelse er en del av organisasjonens kommando og kontrollkrigføring. Sjefens målsetting for kommando og kontrollkrigføring er utgangspunkt for OPSEC planlegging. Følgende planleggingsfaktorer må vurderes i en OPSEC plan:

1. Sjefen spiller en avgjørende rolle. OPSEC planlegging må være en integrert del av sjefens overordende kommando og kontroll krigføringsplaner.
2. OPSEC er en operasjonell funksjon, ikke en sikkerhetsfunksjon. OPSEC planlegging må utføres av dem som planlegger operasjoner. De blir assistert av organisasjonens OPSEC program personell, sammen med deltakere fra andre stabselementer.
3. Planlegging må fokusere på å identifisere og beskytte kritisk informasjon. Å nekte all informasjon om egne operasjoner eller aktiviteter er sjeldent kosteffektivt eller realistisk.
4. Den overordnede målsettingen for OPSEC er økt operasjonell effektivitet. Gjennom å hindre en motstander i å fastslå egne intensjoner eller kapasiteter, bidrar OPSEC til å redusere egne tap og øker sannsynligheten for at operasjoner lykkes.
5. OPSEC bør være en av faktorene som vurderes i utarbeidelsen og utvelgelsen av egen handlemåte.
6. OPSEC planlegging er en kontinuerlig prosess. I løpet av utførelsesfasen av en operasjon vil det komme tilbakemeldinger på hvorvidt OPSEC tiltak er vellykket eller ikke og OPSEC planen bør justeres i henhold til disse. Tilbakemeldinger kan komme fra egne etterretnings eller kontra etterretningsorganisasjoner, monitoring eller en OPSEC survey.
7. Pressetalsmenn bør delta i OPSEC planlegging for å vurdere mulige effekter av mediedekning og for å koordinere OPSEC tiltak.
8. Opphør av OPSEC tiltak må fremgå av OPSEC planen for å unngå at fremtidige motstandere utvikler mottiltak for vellykkede OPSEC tiltak.

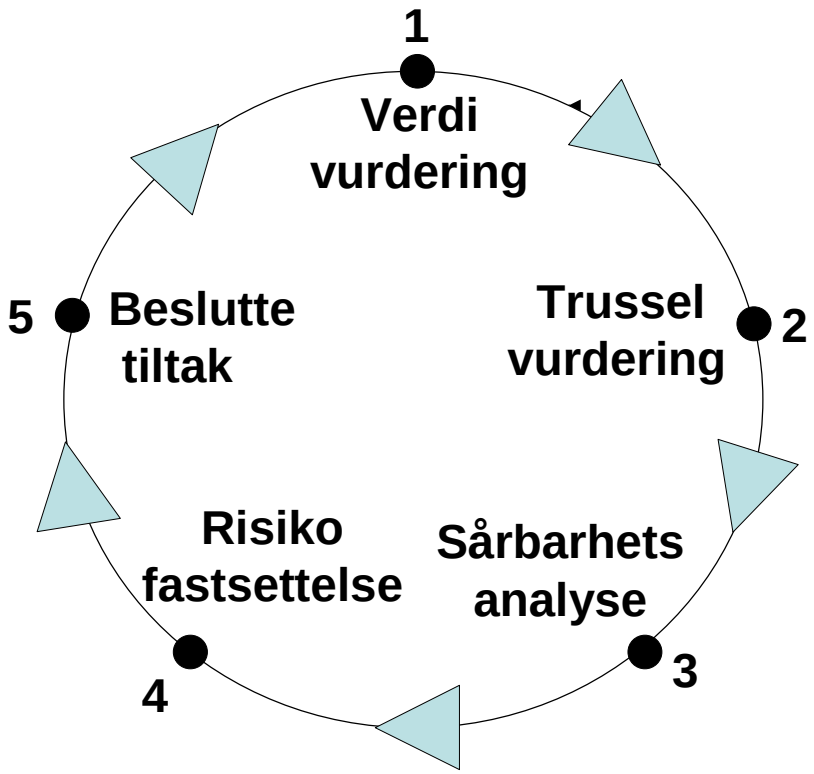
3.1.6 OPSEC prosessen

OPSEC planlegging oppnås gjennom bruk av OPSEC prosessen, som er illustrert i figur 5. Den består av fem trinn som utføres sekvensielt gjennom planleggingen. I dynamiske situasjoner kan imidlertid individuelle handlinger bli revidert til enhver tid. Ny informasjon om motstanders etterretningsinnsamling kapasiteter vil for eksempel kreve en ny trusselvurdering.

Følgende begreper er nødvendig å utdype før prosessen kan forklares.

1. **Kritisk informasjon**. Spesifikke opplysninger om egne intensjoner, kapasiteter og aktiviteter som er nødvendig for at en motstander kan planlegge og utføre tiltak som fører til uakseptable konsekvenser for oss eller at egne operasjoner mislykkes.

2. **OPSEC indikatorer**. Egne observerbare aktiviteter og åpen kilde informasjon som kan analyseres og settes sammen av en motstander for å utlede kritisk informasjon.
3. **OPSEC sårbarhet**. En tilstand hvor egne handlinger avgir OPSEC indikatorer som kan innhentes og nøyaktig evalueres av en motstander tidlig nok til å utgjøre et effektivt beslutningsgrunnlag.



Figur 5: Operasjonssikkerhetsprosessen

Som det framgår av figur 5 består de fem OPSEC handlingene av verdivurdering, trusselvurdering, sårbarhetsanalyse, risikofastsettelse og beslutte tiltak. La oss se nærmere på hva de enkelte handlingene innebærer:

a. OPSEC handling 1 – Identifisering av kritisk informasjon.
I planprosessen når en vurderer egne handlinger opp mot motstanders, søker sjefen og hans stab å identifisere hvilke spørsmål de tror motstanderen vil spørre om egne intensjoner, kapasiteter og aktiviteter. Disse spørsmålene er såkalte ”essensielle elementer av informasjon om egne styrker” (EEIE). I en operasjonsplan eller ordre er EEIE listet i et eget vedlegg.

Kritisk informasjon er et subset av EEIE. Det er bare informasjon som er strengt nødvendig for en motstander. Identifisering av kritisk informasjon er viktig fordi

det legger premissene for det resterende av prosessen som fokuserer på å beskytte vital informasjon framfor å forsøke å beskytte all gradert eller sensitiv informasjon.

b. OPSEC handling 2 – Trusselanalyse

Denne handlingen består av søk og analyse av etterretningsinformasjon, kontra etterretning, rapporter og åpen kilde informasjon for å identifisere hvem som er sannsynlige motstandere for den planlagte operasjonen.

Operasjonsplanleggere søker svar på følgende spørsmål:

- Hvem er motstanderne? Hvem har intensjon og kapasitet til å true den planlagte operasjonen?
- Hva er motstandernes mål? Hva søker motstanderne å oppnå?
- Hva er motstandernes strategi for å motarbeide den planlagte operasjonen? Hvilke handlinger vil bli utført?
- Hvilken kritisk informasjon har motstanderne allerede kjennskap til? Hvilken informasjon er det allerede for sent å beskytte?
- Hvilke etterretningskapasiteter har motstanderne til rådighet?

I tillegg til kjennskap til motstanders kapasiteter for etterretningsinnsamling, er det nødvendig å forstå hvordan etterretningsprosessen fungerer.

c. OPSEC handling 3 – Sårbarhetsanalyse

Hensikten med denne handlingen er å identifisere en operasjons eller aktivitets OPSEC sårbarheter. Det kreves en undersøkelse av planlagte operasjoner for å identifisere hvilke OPSEC indikatorer som kan avsløre kritisk informasjon og deretter sammenholde det med motstanders etterretningsinnsamlingskapasiteter i tidligere handling.

Operasjonsplanleggerne søker svar på følgende spørsmål:

- Hvilke indikatorer (egne aktiviteter og åpen kilde informasjon) av kritisk informasjon som ikke er kjent av motstanderen vil skapes av egne aktiviteter som følge av den planlagte operasjonen?
- Hvilke indikatorer kan motstanderen samle inn?
- Hvilke indikatorer kan motstanderen bruke for å skade egne styrker? Kan motstanderen analysere informasjonen, gjøre en beslutning og gjennomføre tilstrekkelige tiltak tidsnok til å forringe den planlagte operasjonen?

d. OPSEC handling 4 – Fastsette risiko

Denne handlingen har to komponenter. Først analyseres OPSEC sårbarheter som er fremkommet i tidligere handlinger og mulige OPSEC tiltak identifiseres for hver sårbarhet. Deretter velges det ut hvilke OPSEC tiltak som skal iverksettes basert på en risikofastsettelse utført av sjefen og hans stab.

OPSEC tiltak er ment å redusere sannsynlighet for at motstander enten samler inn eller er i stand til å analysere betydningen av informasjonen korrekt. OPSEC tiltak kan brukes for

- Forhindre at motstander oppdager en indikator
- Skape en alternativ analyse av en indikator, og/eller
- Angripe motstanders innsamlingssystem

Mer enn et mulig tiltak kan identifiseres for hver sårbarhet. Motsatt kan et tiltak dekke mer enn en sårbarhet. De mest ønskelige tiltakene er de som kombinerer høyest mulig beskyttelse med minst tap av operasjonell effektivitet. Risikofastsettelse forutsetter en sammenligning av beregnede kostnader forbundet med implementering av hvert mulig OPSEC tiltak i forhold til negative konsekvenser for manglende måloppnåelse dersom en motstander utnytter en spesifikk sårbarhet.

OPSEC tiltak medfører vanligvis noen kostnader i form av tid, ressurser, personell eller forstyrrelser av pågående aktiviteter. Hvis kostnader i forhold til operasjonseffektivitet overstiger skaden en motstander kan utrette, skal ikke tiltaket implementeres. Siden beslutningen om å ikke implementere spesifikke OPSEC tiltak innebærer en risiko, vil dette steget kreve sjefens involvering.

Typiske spørsmål som kan stilles når denne analysen gjennomføres er:

- Hva er risikoen og sannsynligheten for forringet operasjonseffektivitet dersom et OPSEC tiltak implementeres?
- Hva er risikoen og sannsynligheten for suksess dersom et OPSEC tiltak ikke implementeres?
- Hva er risikoen og sannsynligheten for suksess dersom et OPSEC tiltak ikke er effektivt?

Effekten av OPSEC tiltak må analyseres. I enkelte tilfeller kan tiltak skape indikatorer på kritisk informasjon. For eksempel vil kamuflering av en tidligere ukamuflert installasjon være en indikator på forberedelser for en militær aksjon. Utvelgelsen av tiltak må koordineres med andre faktorer i kommando og kontroll krigføring slik at de kan inngå som en integrert del av en overordnet plan og ikke motvirker denne.

e. **OPSEC handling 5 – Iverksette hensiktsmessige OPSEC tiltak**
I dette tinnet implementerer ledelsen OPSEC tiltakene, eller dersom det er snakk om planlagte operasjoner, inkluderer tiltakene i OPSEC planer. Under gjennomføring av OPSEC tiltakene, monitoreres reaksjonen til motstanderne for å vurdere effekten. Planleggerne bruker tilbakemeldinger for å tilpasse pågående aktiviteter og fremtidig OPSEC planlegging. Tilgang til tilbakemeldinger må koordineres med avdelingens etterretnings og kontra-etterretningspersonell for å sikre tiltrekkelig prioritet i innsamlingsarbeidet. I tillegg til etterretningskilder kan OPSEC undersøkelser fremskaffe anvendelig informasjon om hvorvidt OPSEC tiltakene er vellykkede eller ikke.

3.2 Helhetlig organisasjonsperspektiv

3.2.1 Hvorfor bruke en modell?

Denne oppgaven skal foreslå og drøfte et risikohåndteringskonsept for Forsvaret som er en stor og kompleks organisasjon. Før en foreslår endringer i en organisasjon, er det nødvendig å forstå hvordan den fungerer for å lykkes i omstillingsarbeidet. Derfor kan det være hensiktsmessig å bruke en modell som viser hvordan en organisasjon fungerer i konseptarbeid generelt. Risikohåndteringskonseptet vil være en skisse til løsning for hvordan en organisasjon kan gjennomføre risikohåndtering av informasjonssystemer og dokumentere prosessen underveis.

Organisasjoner er komplekse, uklare og ofte vanskelige å forstå. Vår persepsjon avgjør hva vi ser, hva vi gjør og hva vi oppnår. Derfor blir perspektiver som er for enkle eller for snevre, villedende for den som ønsker å forklare eller endre en praksis. De fleste lederes verden er full av kompleksitet, uklarhet, vanskelige verdivalg, politisk press og motstridende interessegrupper [31]. Ved hjelp av en organisasjonsmodell kan en anvende ulike fortolkningsrammer for å unngå en overforenkling og dermed ufullstendige eller feilaktige løsninger på problemer i organisasjoner.

Det finnes flere organisasjonsmodeller å velge mellom, og i følge Payne [5] vil det være hensiktsmessig å ta utgangspunkt i en modell som er kjent og allerede i bruk hos Forsvaret.

3.2.2 Hvorfor Leavitt?

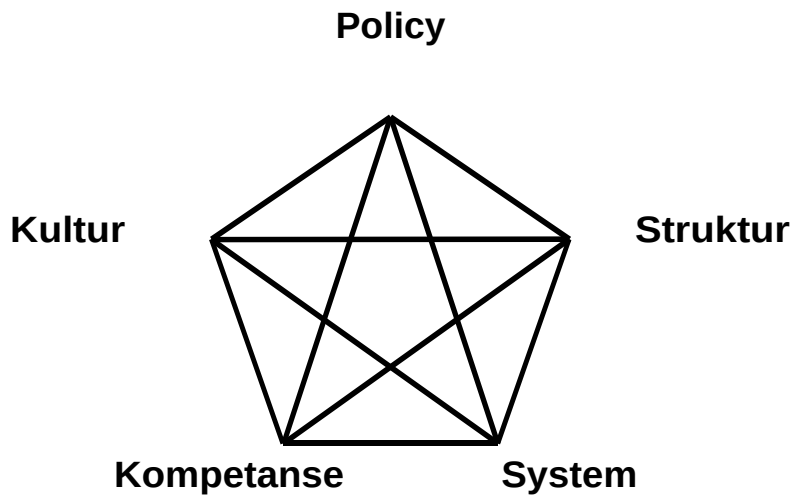
Tor Hernes og Elin Nilsen presenterer i [12] ”Leavitts diamant” som er en modell basert på Harold Leavitts bok ”Applied Organizational Change in Industry”. Den viser sammenhenger mellom ulike faktorer i en organisasjon og egner seg derfor til å sikre et helhetlig perspektiv.

Modellen er tidligere brukt i Kryptokonsept for taktiske informasjonssystemer i Forsvaret [13], som beskriver hvordan håndtering av kryptomateriell skal utføres i taktiske avdelinger, og tilfredsstiller dermed Paynes anbefaling.

Modellen deler inn en organisasjon i fem faktorer og viser hvordan de henger sammen og påvirker hverandre. Endringer i en av faktorene vil påvirke de andre og medfører et endringsbehov i disse for at omstillingen skal få ønsket effekt. Et risikohåndteringskonsept for informasjonssystemer i Forsvaret må beskrive alle faktorene i Leavitts diamant for at ønsket effekt skal oppnås når konseptet blir implementert.

3.2.3 Forklaring til modellen

Leavitt’s diamant er et rammeverk som viser sammenhenger i en organisasjon mellom fem definerte områder; policy, struktur, system, kompetanse og kultur. Figur 6 viser hvordan de ulike bestanddelene henger sammen og påvirkes av hverandre. Poenget er at en endring i en av faktorene medfører et endringsbehov i de andre som må oppfylles dersom omstillingen skal lykkes og konseptet bli implementert i henhold til intensjonen.



Figur 6: Leavitt's diamant

Policy er en fellesbenevnelse for alle styringsdokumenter, lover, forskrifter og regelverk som regulerer utførelsen av risikohåndtering. De angir hvilke krav som skal oppfylles av den enkelte avdeling og gir retningslinjer for utførelsen og omfang av risikohåndteringen. Ofte dreier det seg om minimumskrav som til enhver tid skal være oppfylt. Policy er den endringsvariabelen som er lettest å endre sett fra et ledelsesperspektiv, da en policyendring involverer relativt få mennesker. Hvor vellykket implementeringen av policy endringer vil være er derimot avhengig av hvor godt tilrettelagt de andre faktorene er.

Struktur er et uttrykk for oppgave og ansvarsdeling i organisasjonen. Roller og ansvar skal beskrives for å klargjøre hvem som skal gjøre hva i en risikohåndteringsprosess. Det innebærer både ansvarsdeling internt i en avdeling og ansvarsdeling i Forsvarets militære organisasjon. Strukturendringer alene vil ikke gi ønsket omstillingseffekt, og vil på samme måte som policy endringer være avhengig av at øvrige faktorer tilpasses de nye oppgavene og ansvarsområdene.

Med **Systemer** menes den nødvendige samhandlingen mellom aktørene i sikkerhetsorganisasjonen internt i en avdeling og mellom avdelinger i Forsvaret. Det dreier seg om prosesser, distribusjon og iverksetting av sikkerhetstiltak, kontroll og rapportering. Innføring av nye systemer påvirker øvrige deler av organisasjonen både sentralt og lokalt, og vil medføre endringsbehov hos disse.

Kompetanse betegner et utdanningsnivå og angir krav til hvilke kunnskaper og ferdigheter personellet må inneha for å kunne fylle roller i sikkerhetsorganisasjonen. Kompetansenivået hos medarbeidere i nøkkelroller anses å være avgjørende for at avdelingene og organisasjonen kan fungere i henhold til målsettingen.

Med **Kultur** menes normer for oppgaveløsning i avdelingen som utvikles over tid. Når alle elementene er tilrettelagt gjennom velfungerende systemer, en hensiktsmessig struktur, relevant kompetanse og personellet har forstått policy, er grunnlaget for en god kultur lagt.

Kapittel

4 Metodebeskrivelse

I dette kapitlet begrunnes valg av forsknings strategi og innsamlingsmetoder av informasjon for å belyse problemstillingen. Det er valgt en kvalitativ tilnærming fordi risikohåndtering er en prosess som kan resultere i forskjellige løsninger avhengig av situasjonsbestemte faktorer. Samtaler med involverte aktører, dokumentanalyse og ekspertintervju har avdekket viktige forutsetninger som ligger til grunn for en sikkerhetsmessig godkjenning av et informasjonssystem. Et kurs i risikohåndtering er utarbeidet og gjennomført som et eksperiment for en utvalgt gruppe. Hensikten har vært å demonstrere hvordan opplæring i risikohåndtering kan utføres. Kurset skal gjøre ansvarlig personell bedre i stand til å håndtere risiko som skiftende omgivelser innebærer for et informasjonssystem slik at en kan stole på at forutsetningene som ligger til grunn for et sikkerhetsnivå er gyldige.

4.1 Valg av forskningsstrategi

Det skilles mellom to ulike strategier for informasjonsinnsamling, kvalitative og kvantitative designs. Kvantitative undersøkelser kjennetegnes ved at de ofte er ferdigstrukturerte i løpet av teori og problemutviklingsfasen. Dette gjør at selve behandlingen av data er mye enklere enn ved kvalitative opplegg. I tillegg finnes det et stort antall statistiske teknikker til disposisjon for analyse av data. Den kvalitative tilnærmingens natur forutsetter fysisk nærhet, gjensidig tillit og forståelse mellom forsker og respondent. Her søkes en mest mulig sann gjengivelse av hendelsene, slik at rapporten beskriver hva forskeren ut fra god vilje mente faktisk skjedde. Videre bør rapporter med et kvalitativ design inneholde direkte sitat som viser undersøkelsesenhetens måte å uttrykke seg på.

Ved valg av forskningsstrategi er det naturlig å se på hvilken tilnærming som er best egnet til å belyse den problemstillingen som foreligger. For denne MSc oppgaven er det valgt en kvalitativ strategi, først og fremst på grunn av at det ikke fins bare ett fasitsvar på problemstillingen. Vi ønsker en bred forståelse og et tilnærmet helhetsperspektiv innenfor risikohåndtering av informasjonssystemer som er det sentrale i løsningen av problemstillingen om hvordan en kan stole på at forutsetningene for en sikkerhetsmessig godkjenning fremdeles er gyldige etter endringer i omgivelsene.

4.2 Valg av undersøkelsesobjekt

Problemstillingen gjelder ethvert informasjonssystem som gjennomgår en sikkerhetsgodkjenningsprosess av et eller annet slag. Forsvaret er valgt ut som undersøkelsesobjekt på grunn av flere egenskaper som gjør organisasjonen velegnet til formålet. Først og fremst er Forsvaret en relativt stor organisasjon med avdelinger i Norge og i utlandet. Videre stilles det strenge krav til informasjonssystemene som skal sikkerhetsgodkjennes. Noen kan hevde at kravene til Forsvarets informasjonssystemer er strengere og dermed ikke sammenlignbare med sivile bedrifters systemer. Andre vil hevde at nettopp de strenge kravene setter en *benchmark* eller *best practice* innen informasjonssikkerhet, og dermed noe å strekke seg etter for andre aktører. Uten å ta stilling til om nivået for sikkerhetsgodkjenning er for høyt, er Forsvarets informasjonssystemer interessante som undersøkelsesobjekt i denne oppgaven.

Valget av undersøkelsesobjekt er også motivert ut fra at undertegnede er og har vært ansatt i Forsvaret de siste 15 årene. Det er både fordeler og ulemper med å velge forskningsobjekter en selv står så nært. Problemer knyttet til nødvendig avstand for å fremstå uhildet i forhold til problemstillingen er opplagte forhold som taler mot å velge egen organisasjon som undersøkelsesobjekt. På den andre siden gir ansettelsesforholdet og arbeidserfaringen en innsikt i organisasjonens indre liv og utfordringer. Tillitsforholdet mellom forsker og intervjuobjekter er allerede etablert til sentrale aktører i Forsvaret. Fordelene med å velge Forsvaret som undersøkelsesobjekt ble derfor vurdert til å oppveie ulempene, slik at totalt sett var organisasjonen egnet til å belyse problemstillingen for denne oppgaven.

4.3 Valg av forskningsmetoder

Innledningsvis vil det være naturlig å redegjøre for hva vi legger i begrepet metode. Metode betyr ”systematisk fremgangsmåte” og stammer opprinnelig fra ”det å følge en viss vei mot et mål” av meta (etter) og hodos (vei) [43, s 140].

En metode er et redskap, en framgangsmåte for å løse problemer eller for å få en dypere forståelse av et fenomen. Metoden gir oss ikke svar på spørsmålene våre, men er et virkemiddel som skal gi en bedre og mer riktig forståelse av det problemet en søker kunnskap om. I vårt tilfelle ønsker vi å undersøke hvordan en kan stole på at forutsetningene som ligger til grunn for en sikkerhetsgodkjenning fremdeles er gyldige etter det er skjedd endringer i omgivelsene rundt et informasjonssystem. Et bevisst valg av metode er derfor en nødvendig forutsetning for å kunne gjøre et best mulig undersøkelses- og forskningsarbeid.

Arbeidet ble gjort ut fra to grunnleggende antagelser, hvor den ene var at sikkerhetsnivået øker ved tilstedeværelse av klart definerte, enkle og lettfattelige regler og prosedyrer som er kjent av alle involverte aktører. Den andre antagelsen for arbeidet med rapporten var at enkelhet er bedre enn fullstendighet når tempoet og omfanget av endringer øker.

4.3.1 Formulering av problemstilling

I arbeidet med denne undersøkelsen har samtaler med involverte aktører i sikkerhetsgodkjenning av informasjonssystemer skapt interesse og motivasjon for å

undersøke gyldigheten til forutsetningene som legges til grunn for en sikkerhetsmessig godkjenning. Gjennom egne erfaringer fra å dokumentere sikkerhetstiltak for graderte informasjonssystemer, hadde vi fra før av kjennskap til at forutsetningene som ble lagt til grunn og dokumentert som en del av godkjenningsgrunnlaget ikke nødvendigvis var kjent av personellet som skulle bruke og drifte informasjonssystemet.

Tilstedeværelse av sikkerhetsdokumentasjon har vært et krav fra godkjenningsmyndigheter, og det kunne av og til virke som om dokumentasjonen hadde en egenverdi. Med egenverdi menes at det var dokumentene i seg selv som var viktige, ikke at innholdet var lest og forstått av dem som skulle bruke og drifte systemet. Hvordan skal en kunne ivareta sikkerheten dersom en ikke har forstått hensikten med de ulike sikkerhetstiltakene som er dokumentert? Det kunne virke som om systemeiere var mer opptatt av å tilfredsstille godkjenningsmyndigheter framfor å sikre informasjonssystemet sitt. Denne observasjonen førte til en økende interesse for å undersøke gyldigheten av forutsetningene som ligger til grunn for en sikkerhetsgodkjenning.

Ved bruk av kvalitativ metode vil problemstillingen justeres underveis i forskningsprosessen. Under samtaler eller intervjuer har det blitt avdekket faktorer som ikke var kjent i problemformuleringsfasen. Slike faktorer har rimeligvis påvirket oppgavens retning og utdypet den opprinnelige problemstillingen.

4.3.2 Innhenting av skriftlig kildemateriale

Først var det nødvendig å sette seg inn i hvordan et sikkerhetsnivå for et informasjonssystem blir fastsatt. For å besvare det første forskningsspørsmålet ble det gjennomført en dokumentanalyse av tilgjengelig litteratur. Et viktig moment i denne fasen var å finne ut om lignende undersøkelser var gjort tidligere. Søk i litteratur avdekket beslektede temaer, som gav svar på de neste to forskningsspørsmålene og er beskrevet i kapittel 2, Relatert arbeid.

Så var det nødvendig å sette seg inn i gjeldende regelverk for informasjonssystemer i Forsvaret. Sikkerhetsloven [17] med forskrifter [39-42] og veiledning til gjennomføring av sikkerhetsgodkjenning utarbeidet av NSM [32] utgjør de skriftlige retningslinjene som systemeiere må forholde seg til, deriblant Forsvaret.

I tillegg ble det under samtaler med involverte aktører i godkjenningsprosessen vist til interne dokumenter som er utarbeidet i forbindelse med tidligere sikkerhetsgodkjenninger. Dette bidro til en økt forståelse hos undertegnede for hvilke konkrete forutsetninger som legges til grunn for sikkerhetsgodkjenning av spesifikke systemer. Det dreide seg blant annet om kravspesifikasjoner og testrapporter for operative informasjonssystemer som ikke kan gjengis i undersøkelsen på grunn av sikkerhetsgradering på dokumentene.

4.3.3 Utforming av kurs i risikohåndtering

Det skriftlige kildegrunnlaget beskriver blant annet at systemeiere skal gjennomføre risikohåndtering av informasjonssystemene [40]. I Forskrift for Sikkerhetsadministrasjon § 4-1står det at ”Virksomhet med skjermingsverdig informasjon skal utøve risikohåndtering, ved å fastsette og gjennomføre sikkerhetstiltak etter en risikovurdering.” Men det framgår ikke *hvordan* en slik risikohåndtering og vurdering kan gjøres.

Gjennom samtaler med sikkerhetspersonell i Forsvaret og NSM, ble det avdekket at svært få aktører hadde tilstrekkelig kunnskap om hvordan risikohåndtering av informasjonssystemer skulle utføres. Videre ble det også klart at det ikke fantes noen kurs som dekket opplæringsbehovet som tilsynelatende eksisterte. Det ble derfor på et tidlig tidspunkt i forskningsarbeidet satt fokus på behovet for opplæring i risikohåndtering og dokumentering av sikkerhetstiltakene som forutsettes utført av brukere og driftspersonell. I tillegg framsatte vi en grunnleggende antakelse om at enkelhet er bedre enn kompletthet når det gjelder sikkerhetsdokumentasjon som et redskap for å gjøre personell i stand til å ivareta sikkerheten for informasjonssystemer.

Med dette utgangspunktet ble vi motivert til å utarbeide et kurs som skulle gi en innføring i hvordan en kan gjennomføre risikohåndtering gjennom å fastsette sikkerhetstiltak og gjennomføre en risikovurdering. Kurset skulle være et virkemiddel for å gjøre deltakerne i stand til å forstå hensikten med sikkerhetstiltakene som utgjorde forutsetningene for den sikkerhetsmessige godkjenningen. Denne innsikten er nødvendig for å drive risikohåndtering som innebærer at en endrer på sikkerhetstiltak i takt med skiftende omgivelser og endret risiko.

4.3.4 Revidering av kursinnhold

Kursopplegget ble utarbeidet med bakgrunn i avdekket informasjon fra samtaler med involverte aktører i godkjenningsarbeid, dokumentanalyse av forutsetninger for sikkerhetsmessig godkjenning og egne erfaringer fra arbeid med utarbeidelse av sikkerhetsdokumentasjon for informasjonssystemer.

Dette kursopplegget ble så forevist sikkerhetseksperter i NSM og FSA. I tillegg ble det gjennomført et seminar over en dag ved SBUKS for å gjennomgå innholdet i kurset. Justeringer ble gjort på bakgrunn av innspill og kommentarer fra sikkerhetseksperter under seminaret.

Det reviderte kursopplegget ble deretter brukt som utgangspunkt for å lage leksjonsopplegg for de enkelte timene i kurset. Dette var en svært arbeidskrevende prosess.

4.3.5 Utvelgelse av elever

For å teste ut om kurset hadde ønsket effekt, var det viktig å velge ut elevene som skulle delta i eksperimentet slik at de hadde tilstrekkelige faglige forutsetninger for å bedømme kursinnholdet i forhold til målsettingen. Derfor ble sikkerhetseksperter fra alle informasjonssikkerhetsmiljøene spurt om å delta på kurset. Interessen for å delta var svært høy, og det stilte representanter fra Nasjonal sikkerhetsmyndighet, Forsvarets sikkerhetsavdeling, Forsvarets logistikkorganisasjon, Felles operativt hovedkvarter og Utdannings og kompetansesenter for Hærens samband som kursdeltakere. Hensikten var at deltakerne kunne evaluere kurset sett fra deres egen avdelings ståsted. På denne måten var alle aktørene i sikkerhetsgodkjenningsprosessen representert under eksperimentet.

Dersom det bare hadde vært sikkerhetseksperter til stede under eksperimentet, kunne en risikert en forskyvning av innholdet mot sikkerhetseksperter, noe som var intensjonen for kurset. Derfor ble det lyst ut kursplasser på Forsvarets interne nett i en kort periode. Dette medførte at sikkerhetspersonell fra ulike avdelinger meldte seg som kursdeltakere. Deres erfaringsnivå varierte fra svært lite til erfarne sikkerhetsmedarbeidere.

Elevgruppen besto nå av representanter fra alle aktører i godkjenningsprosessen og representanter fra tilfeldige avdelinger i Forsvaret. Til sammen 22 elever utgjorde

testgruppen som fikk undervisning i risikohåndtering. De av elevene som holdt leksjoner i forbindelse med undervisningen, deltok ikke i evalueringen av kurset.

4.3.6 Evaluering av opplæring

Det ble delt ut et evalueringsskjema til hver kursdeltaker og gitt informasjon om det eksperimentet de deltok i. Et standard evalueringsskjema ble benyttet, og det inneholdt blant annet en del administrative spørsmål som ikke er relevant for denne oppgaven. Besvarelsene skulle være anonyme. Anonymitet ble valgt for å oppnå en større gyldighet, basert på en antagelse om at respondenter vil svare ærligere dersom navn ikke kobles til besvarelsen. Det var ikke noe mål for denne undersøkelsen å koble besvarelsene til identiteter.

Deltakerne ble bedt om å oppgi eget erfaringsnivå. Hensikten var å vurdere tilbakemeldinger i lys av erfaringsnivået til respondenten. I tillegg ble det satt av en time siste dag, hvor kursdeltakerne fikk klasserommet for seg selv for å evaluere gjennomføringen uten instruktører tilstede. Den eldste eleven framførte deretter et hovedinntrykk fra alle kursdeltakerne som var basert på en felles evaluering. Resultatene fra spørreskjemaene er presentert i kapittel 6.9.

4.3.7 Forberedelser og gjennomføring av intervju

For å besvare de siste forskningsspørsmålene og utdype faktorer som påvirker risikohåndtering av informasjonssystemer, ble det gjennomført fire formelle ekspertintervjuer. Relatert til denne oppgavens problemstilling mener vi at den beste måten å få klarhet i intervjuobjektets tankegang og holdninger var å gjennomføre et kvalitativt intervju.

Innledningsvis i forskningsprosessen gjennomførte vi samtaler med involverte aktører i sikkerhetsgodkjenningsarbeidet. Erfaringene fra disse samtalene sammen med funn fra dokumentanalysen dannet grunnlag for utforming av en intervjuguide.

Intervjuguiden utformet vi som et semistrukturert spørreskjema. Dette valget var bevisst på grunn av et ønske om minst mulig styring fra intervjueren, og at intervjupersonens frie syn skulle komme til uttrykk. Intervjuguiden inneholdt en grov skisse over de hovedemnene vi ønsket belyst. Hensikten med å velge denne metoden var å fokusere på intervjuobjektenes egne meninger og tolkninger av hvilke forutsetninger som legges til grunn for en sikkerhetsmessig godkjenning og hvordan en kan stole på gyldigheten til disse etter endringer i omgivelsene.

Utvelgelse av intervjuobjekter er også et sentralt element i en undersøkelse. Grunnlaget for hele oppgaven kan lett spoleres hvis en velger feil personer [44, s 99]. Derfor ble det valgt ut eksperter fra informasjonssikkerhetsmiljøet hos de involverte aktørene i godkjenningsprosessen. De med antatt best forutsetning for å belyse problemstillingen hos hver av de identifiserte aktørene ble intervjuet. Det vil si eksperter fra NSM, FSA, SBUKS og FLO ble intervjuet. FOHK sin representant var ikke tilgjengelig for et formelt intervju i forskningsperioden. Dette har imidlertid blitt oppveid av utstrakte samtaler om temaet. Samtalene kan ikke betegnes som et formelt intervju, siden det ikke er skrevet noe referat som er kontrollert og gjennomlest av kilden.

En bevisst holdning til intervjusituasjonen er også et viktig. Intervjuguide ble sendt ut 1 uke i forveien for at intervjuobjektet kunne gjøre seg kjent med hensikt og spørsmål. Intervjuene ble gjennomført i enerom, hvor personalia med erfaringsbakgrunn for intervjuobjektet ble notert. Det ble også tidspunk og sted for gjennomføringen. Intervjuet ble gjennomført som en fri samtale med liten grad av styring fra intervjuer. Referat ble skrevet på PC av intervjuer under selve intervjuet. Dette skriftlige materialet utgjorde versjon 1.

Når den ferdige utskriften forelå, ble den etter intervjuet var gjennomført forsiktig korrigert slik at den fremsto mer språklig korrekt. I tillegg anonymiserte vi utskriften der det var nødvendig. Dette produktet utgjorde versjon 2 av intervjuet, som ble sendt tilbake til intervjuobjektet med spørsmål om innholdet var korrekt gjengitt. Intervjuobjektene sendte så tilbake intervjureferatet hvor det var rettet opp enkelte momenter. Den gjennomleste og justerte teksten ble kalt versjon 3, og kommentarer fra intervjuobjektene ble lagt inn til slutt i intervjureferatet. Versjon 3 ble brukt som kilde for sitater i oppgavebesvarelsen.

Hensikten med dette var å sikre at intervjuobjektene kunne godkjenne innholdet og ha mulighet til å korrigere for eventuelle feiltolkninger og faktiske feil. Faren ved å gjøre dette er at den intervjuede kan angre sine uttalelser og trekke disse tilbake, selv om det er deres oppriktige mening. Dette er noe som igjen kan svekke troverdigheten til besvarelsene. Vi mener imidlertid at dette oppveies av fordelen ved å få korrigert for faktiske feil og misforståelser. I ettertid viste det seg at det kun var ubetydelige korrigeringer som ble påpekt. Disse ble tatt hensyn til og innarbeidet i intervjuene.

4.4 Analyse av data

Analysefasen definerer vi fra innsamlet informasjon er dokumentert til det ferdige resultatet foreligger i rapportform. For intervjuer vil det si fra referatet er utskrevet, selv om analyseprosessen faktisk starter under selve intervjuet. For å etablere en første orden i materialet, valgte vi å sortere deler av besvarelsene fra alle aktørene i forhold til konsept, opplæring og signifikansnivå.

4.4.1 Konsept for risikohåndtering

Med utgangspunkt i OPSEC modellen og Leavitt's diamant ble det beskrevet et risikohåndteringskonsept tilpasset Forsvarets informasjonssystemer. Oppbyggingen av konseptet fulgte Leavitt's faktorer, mens metodikken som skulle anvendes i risikohåndteringsarbeidet var basert på OPSEC modellen.

Konseptet omfattet en beskrivelse av sikkerhetsgodkjenningsarbeid for informasjonssystemer som behandler sikkerhetsgradert informasjon. Konseptet går ut på en kontinuerlig revisjonsprosess som skal avklare hvorvidt en kan stole på at forutsetningene som ligger til grunn for sikkerhetsgodkjenningen ikke er endret.

Først var det nødvendig å gjøre seg kjent med Forsvarets organisasjon for å identifisere relevante aktører i konseptet. Deretter måtte det kartlegges hvilke policy dokumenter som gjelder for informasjonssystemene. Så skulle utførelsen av selve risikohåndteringen beskrives under system. Dette medførte et kompetansebehov hos de menneskene som skulle utføre risikohåndteringen og dokumentere prosessen. Til slutt ble det beskrevet kulturmålsettinger som skulle bidra til forankring av risikohåndtering som en naturlig del av kulturen i Forsvaret.

For å kartlegge erfaringer med OPSEC metoden, ble det gjennomført dokumentanalyse. Denne fasen med kartlegging ble ansett som meget viktig, da det kunne vise seg at noen hadde erfaringer som var direkte anvendbare i prosjektet. Litteratursøk avdekket imidlertid ikke slik erfaring opp mot informasjonssystemer, men kun erfaringer i generell risikohåndtering for militære operasjoner.

4.4.2 Opplæring i risikohåndtering

Opplæringen er en vesentlig av risikohåndteringskonseptet. Først ble det beskrevet hvordan kurset ble til og redegjort hvorfor innholdet ble valgt. Etter at kurset var ferdig utarbeidet, ble det gjennomført som et eksperiment over tre dager. Det som skulle testes var om undervisningen har hatt ønsket effekt i forhold til forståelse av sikkerhetsdokumentasjon som ligger til grunn for sikkerhetsgodkjenningen. Relevant litteratur og egenprodusert materiale ble undervist for sikkerhetspersonell. Innsamlet data skulle belyse hvorvidt opplæringen er et egnet virkemiddel som gjør det mulig å håndtere risiko på lokalt nivå slik det er ment i risikohåndteringskonseptet. Det ble også gjennomført samtaler med representanter fra kontrollmyndigheter for å avdekke om undervisningen og veiledningen har hatt ønsket effekt sett fra deres ståsted.

4.4.3 Fastsetting av signifikansnivå for endringer

Dokumentstudier avdekket hvilke krav som gjelder for sikkerhetsgraderte informasjonssystemer i Forsvaret. Hensikten var å kartlegge krav som stilles til sikkerhetsnivå og akseptabel risiko. Ekspertintervju ble gjennomført for å identifisere hvilke forutsetninger intervjuobjektene med sin erfaringsbakgrunn vurderte som særlig viktig. Det var spesielt hvilke endringer som regnes som vesentlige som var fokus i samtalene med ekspertene. Målsettingen var å finne ut om det i det hele tatt var mulig å skille ut enkelte forutsetninger som kunne brukes som en indikator på signifikante avvik. Beskrivelsen av avvikshåndtering som kommer ut av drøftingen, ville dermed bli en del av risikohåndteringskonseptet. På denne måten ble funn om avvikshåndtering knyttet inn i det foreslåtte konseptet for risikohåndtering av informasjonssystemer i dynamiske omgivelser.

Videre ble det gjennomført dokumentanalyse av tilgjengelige sjekklister og inspeksjonsskjemaer som brukes i godkjenningsprosesser og sikkerhetsrevisjoner. Samtaler med personer som har gjennomført sikkerhetsinspeksjoner og revisjonsarbeid i forbindelse med sikkerhetsgodkjenning ble gjort for å identifisere hvilke avvik de vektlegger under inspeksjoner eller revisjonsarbeidet.

4.5 Reliabilitet, validitet og generaliserbarhet

I alle forskningsopplegg vil det være naturlig å vurdere om sluttresultatet som foreligger er valid og reliabelt. Med reliabilitet mener vi hvor pålitelig undersøkelsen er. Hvordan er den gjennomført og hvor nøyaktig man behandler dataene [46, s 164]. I kvalitativ forskning blir gjerne reliabilitet sammenfallende med validitet og kan derfor vanskelig studeres separat.

Validiteten forteller oss om oppgavens gyldighet. Analyserer vi det som vår problemstilling skal avklare? [46, s 160]. Validiteten er viktigst fra problemstillingsfasen til det stadium hvor intervjuguiden foreligger.

Reliabiliteten, her forstått som objektivitet og nøyaktighet i behandling og analyse av data, er først og fremst sentral i det videre arbeidet fram til endelig sluttrapport. En kvalitativ undersøkelse innebærer at problemet med validitet er langt mindre enn i kvantitative tilnærminger, fordi de ikke skal reprodusere data på samme måte. Ved å la intervjuobjektene lese gjennom intervjuet i etterkant, mener vi det er med på å øke graden av både reliabilitet og validitet.

Det kan stilles spørsmål om en slik kvalitativ tilnærming gir grunnlag for å generalisere. Det hersker delte meninger om dette, da en lik forskning tar utgangspunkt i intervjuobjekter som ikke tilhører gjennomsnittet, men som representerer spisskompetanse. Det er to måter å legge opp til en generalisering:

- Forskergeneralisering, hvor forskeren analyserer funnene og argumenterer for at de er generaliserbare.
- Lesergeneralisering. Her legges det til rette for at hver leser selv kan bedømme om funnene kan generaliseres.

I begge tilfeller kreves det at informasjonsgrunnlaget er stort nok til at en generalisering kan foretas. Denne undersøkelsen gir etter vår mening tilstrekkelig grunnlag for å generalisere for Forsvaret og Forsvarets informasjonssystemer.

Kapittel

5 Uforming av et konsept

I dette kapitlet vil et risikohåndteringskonsept for informasjonssystemer skisseres og drøftes med utgangspunkt i Leavitts diamant og ekspertintervju av involverte aktører i sikkerhetsgodkjenningsprosesser i Forsvaret. Først beskrives det hvordan en sikkerhetsgodkjenning foregår, deretter hvordan sikkerheten skal opprettholdes og forutsetningene kontrolleres.

5.1 Innledning

Problemstillingen for denne rapporten er hvordan en kan stole på om forutsetningene for en sikkerhetsmessig godkjenning fremdeles er gyldig etter endringer i omgivelsene til et informasjonssystem. Forutsetningene som ligger til grunn for en sikkerhetsmessig godkjenning uttrykkes gjennom sikkerhetsdokumentasjonen for det aktuelle informasjonssystemet. I et av ekspertintervjuene ble det utrykt på følgende måte:

> *”Dokumentasjonen er forutsetningen for godkjenning. Dokumentasjonen må selvfølgelig stemme med virkeligheten.”*

For å kunne stole på at dokumentasjonen gjenspeiler faktiske forhold, gjennomføres det kontroll etter en viss tid ved hjelp av inspeksjonsteam.

> *”Det vil en eventuell inspeksjon vise. Det er det også når virksomhetens leder er godkjenningsansvarlig.”*

I følge Leavitt [12], vil endringer i en av faktorene policy, struktur, system, kompetanse og kultur påvirke de andre og medfører et endringsbehov i disse for at omstillingen skal få ønsket effekt. Et risikohåndteringskonsept for inforasjonssystemer i Forsvaret må derfor beskrive alle faktorene i Leavitts diamant for å sikre en vellykket implementering.

Dette kapitlet vil besvare forskningsspørsmålet ”Hvilke faktorer bør beskrives i et risikohåndteringskonsept for informasjonssystemer?”. Først vil det beskrives hvordan sikkerhetsgodkjenning gjennomføres. Deretter vil det beskrives hvordan sikkerheten opprettholdes og forutsetninger kontrolleres. Med dette som bakgrunn vil det foreslås et konsept med utgangspunkt i Leavitts fem faktorer. Til slutt i vil det bli referert til erfaringer fra sikkerhetsinspeksjoner for å vise at det er et reelt behov for et risikohåndteringskonsept for informasjonssystemer i Forsvaret.

5.2 Sikkerhetsgodkjenning

5.2.1 Styringsdokumenter

Følgende offentlige dokumenter er gjennom litteratursøk og ekspertintervjuer identifisert som relevante i forhold til sikkerhetsgodkjenning av informasjonssystemer i Forsvaret:

- Sikkerhetsloven [17]
- Forskrift om sikkerhetsadministrasjon [40]
    - Veiledning til Forskrift om sikkerhetsadministrasjon § 4-4 Gjennomføring av sikkerhetsrevisjon og ledelsens evaluering [37]
- Forskrift om informasjonssikkerhet [39]
    - Veiledning til Forskrift om informasjonssikkerhet § 5-10 Gjennomføring av konfigurasjonskontroll [32]
    - Veiledning til Forskrift om informasjonssikkerhet § 5-15 Gjennomføring av sikkerhetsgodkjenning av informasjonssystemer [33]
    - Veiledning til Forskrift om informasjonssikkerhet § 5-22 Utarbeidelse av kravspesifikasjon for sikkerhet (KSS) [34]
    - Veiledning til Forskrift om informasjonssikkerhet § 5-25 Utarbeidelse av driftsinstruks [35]
    - Veiledning til Forskrift om informasjonssikkerhet § 5-26 Utarbeidelse av brukerinstruks [36]
- Forskrift om sikkerhetsgraderte anskaffelser [41]

Sikkerhetsloven § 13 omhandler sikkerhetsmessig godkjenning av informasjonssystemer. I lovteksten heter det: ”Før skjermingsverdig informasjon behandles, lagres eller transporteres i et informasjonssystem, skal Nasjonal Sikkerhetsmyndighet, eller den Nasjonal sikkerhetsmyndighet bemyndiger, godkjenne systemet for angjeldende sikkerhetsgrad.”

5.2.2 Krav til sikkerhetsdokumentasjon

Sikkerhetsloven med forskrifter stiller konkrete krav til forutsetninger som må innfris før et informasjonssystem kan gis sikkerhetsmessig godkjenning. Nasjonal sikkerhetsmyndighet eller den som regnes som virksomhetens leder er godkjenningsansvarlig, avhengig av informasjonssystemets sikkerhetsgradering og valgt operasjonsmåte.

I følge Sikkerhetsloven § 11 skal en av følgende sikkerhetsgrader benyttes:

- STRENGT HEMMELIG
- HEMMELIG
- KONFIDENSIELT
- BEGRENSET

I følge Forskrift om informasjonssikkerhet [39] § 5-1 skal virksomheter som eier et informasjonssystem som skal sikkerhetsgodkjennes, utarbeide et sikkerhetskonsept. I sikkerhetskonseptet skal faktorer som er avgjørende for sikkerheten beskrives. Relevante

faktorer er bruksområde for systemet, informasjonens sikkerhetsgrad, klarering og autorisasjon for personell med tilgang, geografisk og fysisk plassering, inndeling i fysiske områder, forbindelser utenfor eget kontrollert område, sammenkobling med andre systemer og tempestrisiko. Sikkerhetskonseptet skal oppdateres ved endringer i relevante faktorer, og danner grunnlaget for og inngår som en del av kravspesifikasjon for sikkerhet (KSS).

I følge [39] §5-2 skal en av følgende operasjonsmåter benyttes:

- *Dedikert operasjonsmåte*; når alle brukere er autorisert for all informasjon på informasjonssystemet og alt tilknyttet utstyr er godkjent for høyeste sikkerhetsgrad i systemet.
- *Fellesnivå operasjonsmåte*; når alle brukere er sikkerhetsklarert for høyeste sikkerhetsgrad i systemet, men ikke alle er autorisert for all informasjon på systemet, og alt tilknyttet utstyr og forbindelser er godkjent for høyeste sikkerhetsgrad i systemet.
- *Flernivå operasjonsmåte*; når det er informasjon gradert KONFIDENSIELT eller høyere i systemet, og det er tilknyttet utstyr eller forbinderser som ikke er godkjent for høyeste sikkerhetsgrad i systemet eller det er brukere som ikke er klarert for høyeste sikkerhetsgrad i systemet.

	Dedikert	Fellesnivå	Flernivå
BEGRENSET / FORTROLIG / STRENGT FORTROLIG	- Skjema - Bruker-instruks (BI)	- Skjema - BI - Driftsinstr. (DI) - Kravspes. for sikkerhet (KSS)	- BI - DI - KSS
KONFIDENSIELT	- Skjema - BI - Tempest-risikovurd.	- Skjema - BI & DI - Tempest-risikovurd. - KSS	- BI - DI - Tempest-risikovurd. - KSS
HEMMELIG	- Skjema - BI - Tempest-risikovurd.	- BI - DI - Tempest-risikovurd. - KSS	- BI - DI - Tempest-risikovurd. - KSS
STRENGT HEMMELIG	- Skjema - BI - Tempest-risikovurd.	- BI - DI - Tempest-risikovurd. - KSS	- BI - DI - Tempest-risikovurd. - KSS

Figur 7: Krav til sikkerhetsdokumentasjon

I [39] §§ 5-22, 5-24, 5-25 og 5-26 stilles det krav til hvilken sikkerhetsdokumentasjon som skal utarbeides som en del av godkjenningsrunnlaget. Forsvarets sikkerhetsavdeling (FSA) har presisert hvilke dokumenter som skal foreligge ved godkjenning av

informasjonssystemer med ulike graderinger og operasjonsmåter, og fremgår i figur 7. Grønn farge illustrerer at virksomhetens leder er godkjenningsansvarlig, mens blå farge angir at Nasjonal sikkerhetsmyndighet skal gi godkjenning.

5.2.3 Godkjenning av referanseløsning

I Forskrift om sikkerhetsadministrasjon [40] og Forskrift om informasjonssikkerhet [39] samt i ekspertintervjuene ble godkjenningsprosessen utdypet nærmere. Sikkerhetsgodkjenningen deles inn i administrative og tekniske moduler som behandles hver for seg.

> *"Vi i NSM godkjenner en referanseløsning først. Det innebærer å undersøke om systemet kan godkjennes teknisk. For dette arbeidet trengs det en overordnet KSS, driftsinstruks og brukerinstruks på et mer generelt nivå."*

Først gjennomføres det en godkjenning av en såkalt referanseløsning. Referanseløsningen er en prototyp av informasjonssystemet som består av de nettverkskomponentene som skal benyttes. Komponentene blir utsatt for en grundig sikkerhetstest hver for seg og sammen som et system. Dersom komponentene består testen, utstedes en godkjenning av referanseløsning av informasjonssystemet. For å gjøre godkjenningsarbeidet enklere, er det utarbeidet veiledninger av NSM som skal benyttes av systemeiere for å standardisere godkjenningsprosessen.

5.2.4 Godkjenning for operativt bruk

Når godkjenning av referanseløsningen foreligger, gjennomføres det en godkjenning for operastivt bruk.

> *"Så skal systemet godkjennes lokalt. Da er fokuset på om sikkerheten rundt systemet er ivaretatt i avdelingen som skal ta det i bruk. Vi kontrollerer blant annet lokal sikkerhetsorganisasjon, Grunnlagsdokument for sikkerhet, personellsikkerhet og fysisk sikkerhet. Kort sagt alt som ligger i skjemaet*. Vi fokuserer på om sikkerhetsdokumentasjonen som legges til grunn for godkjenningen er tilpasset lokale forhold. Dette utgjør i grovt forutsetninger for godkjenning lokalt for operativ bruk." *(NSM inspeksjonsskjema[38])*

Denne fasen av godkjenningsarbeidet skal kontrollere at informasjonssystemet konfigureres og brukes i henhold til forutsetningene som er gjort i forbindelse med godkjenning av referanseløsning. Det legges spesiell vekt på å kontrollere administrative rutiner rundt informasjonssystemet, slik at ikke nye trusler og sårbarheter introduseres som følge av feil konfigurering og bruk.

NSM kan delegere godkjenningsfullmakt til andre. Forsvarets sikkerhetsavdeling (FSA) ønsker at godkjenning for operativt bruk for Forsvarets informasjonssystemer blir delegert ned til dem. Slik uttrykte en sikkerhetsekspert i FSA seg om godkjenningsprosessen:

> *"Vi ønsker at noe av godkjenningen i Forsvaret skal gå gjennom oss. Vi kan deretter eventuelt delegere fullmakt til FOHK og FLO. Vi ønsker å oppnå bedre kontroll og oversikt over sikkerhetsarbeidet i Forsvaret. Da har vi til enhver tid kontroll over hvilke systemer som er godkjent eller ikke."*

(FOHK er en forkortelse for Fellesoperativt hovedkvarter og FLO er en forkortelse for Forsvarets Logistikk Organisasjon) Dette virker som en rimelig løsning gitt at FSA har det overordnede sikkerhetsansvaret for informasjonssystemer i Forsvaret. Sikkerhetseksperten fortsetter:

> *Vi godkjenner ikke systemer nå. FLO og FOHK gir midlertidig brukstillatelse. I noen tilfeller er dette også bare muntlige avtaler. Det må utarbeides skriftlige avtaler mellom NSM og FSA slik at godkjenningsarbeidet blir formalisert og forankret hos oss, forutsatt at NSM vil delegere myndighet ned til oss.*

En løsning der NSM gir sikkerhetsgodkjenning, men delegerer fullmakt til FSA for å avgjøre om endringer i omgivelsene er tilstrekkelig signifikant til at sikkerhetsgodkjenningen ikke lenger er gyldig, støttes også av en sikkerhetsekspert i NSM som uttalte:

> *"Vi må se på måten vi gir sikkerhetsgodkjenninger på. Det vil antakelig være bedre om vi gir en sikkerhetsgodkjenning uten tidsbegrensning, men krever ny godkjenning ved endringer som påvirker sikkerheten i systemet. Hensikten er å ha fokus på om endringer påvirker sikkerheten."*

Dette viser at NSM er åpen for å endre sine godkjenningsrutiner, noe som åpner for at FSA kan få delegert fullmakt. Dette viser også at NSM er opptatt av å fokusere på endringer som kan påvirke sikkerheten.

5.3 Opprettholdelse og kontroll av forutsetninger

Litteratursøk og ekspertintervjuer ble brukt til å identifisere sentrale aktører som må være med i risikohåndteringskonseptet. Siden sikkerhetsgodkjenning av informasjonssystemer ikke er noe nytt fenomen, ble det valgt å ta utgangspunkt i gjeldende praksis med oppgaver og ansvarsdeling.

Forsvaret er imidlertid inne i store strukturendringer, noe som har medført usikkerhet rundt hvilken avdeling som skal ha ansvar for enkelte oppgaver. Omstillingsprosessen innebærer blant annet en kraftig nedbemanning av forvaltningsfunksjoner. Dette medfører en kamp for tilværelsen blant avdelinger som har hatt noenlunde like ansvarsområder om å få oppgaver tilført for å unngå nedleggelse. Denne observasjonen bør være en del av tolkningsgrunnlaget når personer som representerer de ulike avdelingene blir intervjuet og uttaler seg om ansvarsdeling mellom avdelinger. Representanter fra ulike avdelinger kan når de uttaler seg om ansvarsdeling oppfattes som konkurrenter om de samme oppgavene i Forsvaret.

5.4 Struktur

Med struktur menes fordeling av oppgaver og ansvar i organisasjonen. I denne sammenhengen vil det være interessant å se på Forsvaret som organisasjon og den enkelte avdeling som benytter informasjonssystemer.

5.4.1 Aktører i Forsvaret

Dokumentanalyse og ekspertintervjuer avdekket følgende aktører i Forsvarets militære organisasjon som relevante for risikohåndteringskonseptet.

- Forsvarets Logistikk Organisasjon (FLO)
- Felles Operativt Hovedkvarter (FOHK)
- Utdannings- og kompetansesenter for Hærens Samband (SBUKS)
- Forsvarets Sikkerhetsavdeling (FSA)
- Operative avdelinger i Hæren, Sjøforsvaret, Luftforsvaret og Heimevernet

5.4.2 Ansvarsdeling i Forsvaret

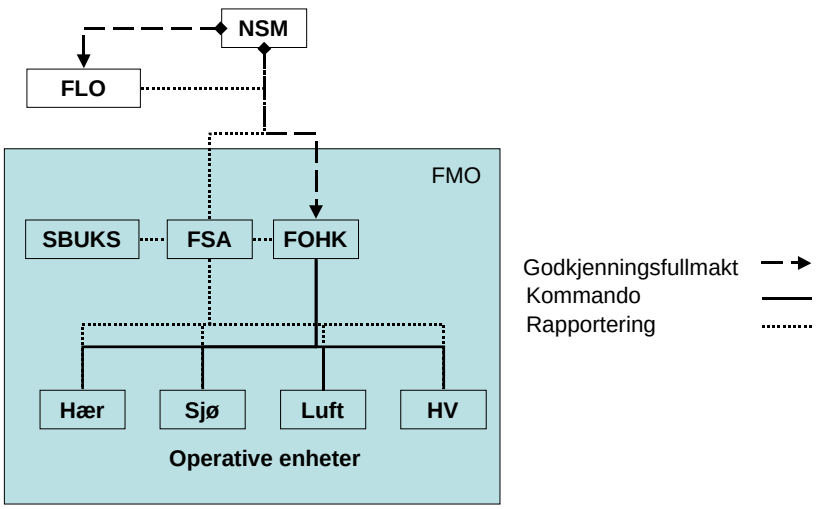
Forsvarets Logistikkorganisasjon (FLO) drifter infrastrukturen til sikkerhetsgraderte informasjonssystemer i Forsvaret. NSM er godkjenningsmyndighet for operativt bruk, men kan delegere fullmakt til FLO som gjennom ”Arbeidsgruppe sikkerhet” gjennomfører stedlig godkjenning for operativt bruk.

NSM kan også delegere fullmakt til godkjenning for operativt bruk til Fellesoperativt hovedkvarter (FOHK). FOHK fører kommando over Forsvarets operative enheter, og kan gi midlertidig brukstillatelse disse avdelingene.

Forsvarets sikkerhetsavdeling (FSA) utarbeider bestemmelser for sikkerhetstjenesten i Forsvaret. FSA kontrollerer sikkerheten ved avdelinger i Hær, Sjø, Luft og HV ved hjelp av kontroll og veiledningsteam.

Utdannings- og kompetansesenter for Hærens Samband (SBUKS) gjennomfører opplæring for brukere, driftspersonell, og sikkerhetspersonell i Forsvaret. Videre skal SBUKS støtte FSA med ressurser for kontroll og veiledning blant alle Forsvarets avdelinger.

Dagens praksis for gjennomføring av sikkerhetsgodkjenning og rapportering fremgår av figuren under:

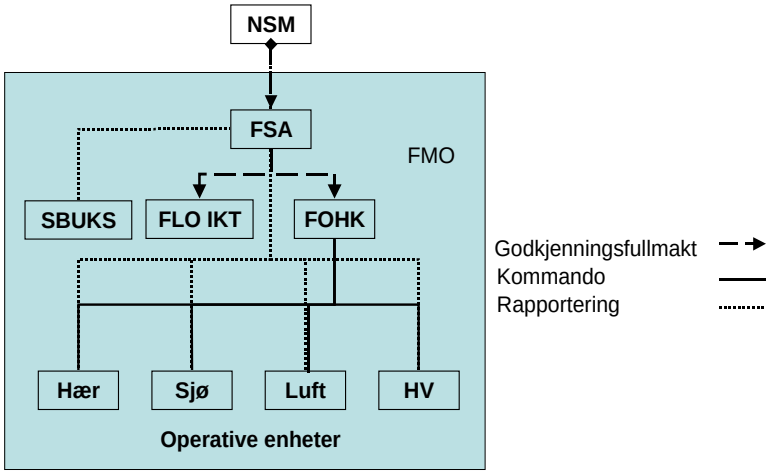


Figur 8: Godkjenningsfullmakt og rapportering etter dagens praksis

I følge et uttalt ønske fra FSA om at sikkerhetsgodkjenning for operativt bruk bør gå gjennom dem, bør imidlertid ansvarsdelingen i godkjenningsprosessen endres. Dagens praksis fører til at FSA ikke får nødvendig oversikt, noe som fremkom under intervju av sikkerhetseksperten i FSA.

> *"I dag har vi ikke god nok oversikt over systemer og sikkerhetsgodkjenning."*

Dersom NSM delegerer godkjenningsfullmakt for operativt bruk av Forsvarets informasjonssystemer til FSA, vil det gi FSA en mulighet for å bedre kontrollen og oversikten over sikkerhetsgodkjente systemer for hele Forsvaret.



Figur 9: Forslag til godkjenningsfullmakt og rapportering

En struktur som vist i figuren over vil også bidra til å klargjøre ansvarsforhold internt i Forsvaret. En sikkerhetsekspert i NSM uttrykte følgende bekymring:

> *"I forbindelse med omorganiseringen i Forsvaret er det avdekket problemer med å avklare ansvarsforhold. Når en skal koble seg til et system er det nødvendig å vite hvem som er systemeier, sikkerhetsansvarlig og ha tilgjengelig oppdatert dokumentasjon. Dette fordi noen må ha ansvar for å implementere sikkerheten i et system."*

Dersom NSM får et kontaktpunkt til Forsvaret, og FSA får den overordnede kontrollen med alle Forsvarets informasjonssystemer, vil det kunne bidra til å få klarhet i ansvarsforhold internt i Forsvaret.

5.4.3 Sikkerhetsorganisasjon i en avdeling

Virksomhetens leder har overordnet ansvar for den forebyggende sikkerhetstjenesten innen sitt ansvars og myndighetsområde jf [40] §2-1. For å utøve dette ansvaret skal den som er virksomhetens leder utnevne en sikkerhetsorganisasjon.

Det er imidlertid varierende i hvor stor grad sikkerhetsorganisasjonene fungerer etter intensjonen. Noen avdelinger har velfungerende sikkerhetsorganisasjoner, mens hos andre er de ikke hensiktsmessig etablert. Slik uttaler en sikkerhetsekspert seg om sine erfaringer fra inspeksjoner:

> *"Sikkerhetspersonell er enten unge og uerfarne, eller tannløse og tilårskomne. Dette kan skyldes at det tradisjonelt ikke har vært karriereassosiasjoner forbundet med sikkerhet."*

Dette synet bekreftes av en annen sikkerhetsekspert tilhørende et annet sikkerhetsmiljø, som uttaler:

> *"Fortsatt er det en trend at ASO er befal på lavere nivå med liten erfaring og forankring i ledelsen."*

ASO er en forkortelse for Avdelingens sikkerhetsoffiser. For å motvirke denne trenden ser vedkommende for seg å lage regionale sikkerhetsorganisasjoner ved å samle sikkerhetsressursene som er spredt ute i avdelingen.

Det er likevel mange ledere som tar sikkerheten på alvor. En tredje ekspert uttaler at vedkommende har god erfaring og at ledere er seriøse. Men også denne eksperten peker på et forbedringspotensial når det gjelder holdninger blant sjefer og prioritering av sikkerhetsorganisasjonen. Vedkommende sier på spørsmål om forbedringspotensial:

> *"Av og til sjefers holdninger. En bør kanskje fokusere mer på sjefsnivå. Å ha et gradert informasjonssystem er et sjefsansvar, ikke alle har tatt inn over seg hva de har signert for."*

Det er viktig at personer som utpekes til å fylle roller i en sikkerhetsorganisasjon er kvalifisert for oppgaven og har nødvendig myndighet internt for å få gjennomslag hos sjefen i sikkerhetsspørsmål. En ekspert uttalte:

> *"Det er stor forskjell på råd fra en erfaren G-3 og råd fra en junior sikkerhetsmedarbeider."*

Dersom ikke sikkerhetsleder, eller andre som bekler roller i sikkerhetsorganisasjonen har tilstrekkelig autoritet internt, vil det være god grunn til å stille spørsmål om sikkerhetsorganisasjonen fungerer etter intensjonen i [40] § 2-5.

Figur 10: Sikkerhetsorganisasjon i en avdeling

En sikkerhetsorganisasjon kan organiseres slik det er vist i figuren over. Poenget er at det identifiseres en ansvarlig for hvert sikkerhetsfagfelt. Det kan godt være samme person som har ansvar for flere sikkerhetsområder.

5.5 Forslag til policy for OPSEC konsept

Med bakgrunn i nevnte funn fra dokumentanalyse og ekspertintervju, foreslås følgende policy for et OPSEC konsept i Forsvaret:

OPSEC program

Det skal etableres et OPSEC program for Forsvaret

Sikkerhetsmessig godkjenning

Nasjonal sikkerhetsmyndighet (NSM) skal godkjenne informasjonssystemet før det tillates brukt til angjeldende sikkerhetsgrad, jf Sikkerhetsloven §§ 13, 14.

Forsvarets sikkerhetsavdeling (FSA) skal godkjenne Forsvarets informasjonssystemer for operativt bruk. Denne fullmakten kan delegeres til Felles operativt hovedkvarter (FOHK) eller Forsvarets Logistikkorganisasjon.

Sikkerhetsorganisasjon

Selvstendige avdelinger i forband som har sikkerhetsgraderte informasjonssystemer skal etablere en sikkerhetsorganisasjon med minimum en sikkerhetsleder og informasjonssystemsikkerhetsleder med stedfortredere, jf Informasjonssystemsikkerhetsforskriften § 7-6, jf Sikkerhetsadministrasjonsforskriften kapittel 2.

Sikkerhetspersonellet skal være faglig kvalifisert og ha nødvendig myndighet i avdelingen, jf Informasjonssikkerhetsforskriften § 7-6 andre ledd. Det anses som avgjørende at alder og grad gjenspeiler krav til myndighet og kvalifisering. Relativt ungt og uerfarent befal skal som hovedregel ikke benyttes i rollene.

Virksomhetens leder

Avdelingssjef for selvstendig avdeling i forband regnes som virksomhetens leder. Avdelingssjefen er ansvarlig for den forebyggende sikkerhetstjenesten i sin avdeling og plikter å avsette nødvendige ressurser for å ivareta sikkerhetstjenesten, jf Informasjonssikkerhetsforskriften § 7-7.

Avdelingssjefen er ansvarlig for OPSEC bevissthet i sin avdeling og for å integrere OPSEC prosessen i planlegging og utførelse avdelingens oppdrag.

Avdelingssjef gir autorisasjon for tilgang til gradert informasjon. Autorisasjonsprosessen skal formaliseres og dokumenteres. Avdelingssjefen skal utnevne sikkerhetspersonell skriftlig.

Sikkerhetsleder

Det skal utnevnes en sikkerhetsleder i avdelinger som har sikkerhetsgraderte informasjonssystemer.

Sikkerhetsleder skal ha oversikten over alt sikkerhetsarbeidet i avdelingen.

Informasjonssystemsikkerhetsleder

Det skal utpekes en informasjonssystemsikkerhetsleder i avdelinger som har sikkerhetsgraderte informasjonssystemer. Informasjonssystemsikkerhetsleder er ansvarlig for tilgangskontroll av brukere og driftspersonell. Tilgang gis etter gjennomført opplæring er gjennomført, underskrift av taushetserklæring og autorisasjonssamtale er gjennomført.

Driftsansvarlig

Driftsansvarlig og informasjonssystemsikkerhetsleder bør ikke være samme person. Det bør tilstrebes å skille rollene så langt det er praktisk gjennomførbart.

Dokumentering av sikkerhetstiltak

Det skal forligge en dokumentert oversikt over alle relevante sikkerhetstiltak i avdelingen hos sikkerhetsleder.

Opplæring

Personell som utpekes for å bekle roller i sikkerhetsorganisasjonen skal gis nødvendig relevant opplæring.

5.6 Systembeskrivelse

I følge Leavitt, er ”system” et uttrykk for samhandling mellom aktørene som er identifisert under struktur. I denne konteksten vil det si å beskrive gjennomføring av risikohåndtering, rapporteringsrutiner og kontrolltiltak for å forsikre seg om at forutsetningene som ligger til grunn for den sikkerhetsmessige godkjenningen er gyldig etter en viss tid med forandringer i omgivelsene.

Identifiserte aktører i og i tilknytning til Forsvaret som en organisasjon er NSM, FSA, FOHK, FLO, SBUKS samt operative avdelinger i Forsvaret fra alle forsvarsgrener.

Identifiserte aktører internt i en avdeling i Forsvaret er roller som skal fylles i en sikkerhetsorganisasjon. Det omfatter virksomhetens leder, sikkerhetsleder, datasikkerhetsleder, driftsansvarlig, fysisk sikringsansvarlig, personellsikkerhetsansvarlig, kryptosikkerhetsleder og kryptoforvalter.

”Det er alltid et sett av risikoer knyttet til oppdragene våre. Det gjelder å identifisere riktig beslutningsnivå for å akseptere risikoen.”

Generalmajor Harald Sunde
Kommandør for landstridskreftene

Figur 11: Beslutningsnivå for å akseptere risiko

I forbindelse med militære operasjoner er det et sammensatt risikobilde av flere forhold som kan gå galt. Generalmajoren ble kontaktet i forbindelse med MSc prosjektet. Han fokuserte på viktigheten av å identifisere riktig beslutningsnivå for å akseptere risikoen. I følge Landkommandøren innebærer det å akseptere risiko også en erkjennelse om å ta ansvar for sikkerheten. Dersom det går galt, skal en ikke lete etter syndebukker for å legge all skyld på, men undersøke om gjeldende sikkerhetstiltak og prosedyrer ble fulgt.

Med riktig beslutningsnivå menes at beslutninger som går ut på å endre sikkerhetstiltak i forhold til eksisterende krav krever eierskap til systemet. Derfor kan det ikke være opp til hvem som helst å vedta endringer i vedtatte sikkerhetstiltak, da det vil medføre endret risiko.

5.6.1 Sikkerhetsdokumentasjon som godkjenningsgrunnlag

En av sikkerhetsekspertene uttalte i et intervju:

> *”Det er ikke enkelt å si hvem som eier systemene. Det er uklart og bør konkretiseres for hvert enkelt system.”*

Ansvarsforhold må være klarlagt før en beskriver samhandling mellom aktørene. Når eierskap til systemet er fastlagt, kan en også identifisere hvem som har eierskap til *risikoen* som er forbundet med informasjonen i systemet. I kapittel 2, Relatert arbeid ble det beskrevet hvordan akseptkriterier fastsettes og endres av systemeiere og godkjenningsansvarlig etter en kost/nytte vurdering av ulike sikkerhetstiltak. Sikkerhetstiltakene dokumenteres i deretter i dokumenter som utgjør en vesentlig del av godkjenningsgrunnlaget. Under et av intervjuene sa en sikkerhetsekspert fra NSM følgende:

> *”Dokumentasjonen er ikke noe mål i seg selv, kun et middel for å gjøre ting i riktig rekkefølge.”*

Dette faktumet er det tydeligvis ikke alle som har fått med seg. Eksperten forstetter:

> *”Jeg møter ofte ’å går det an å foreta en risikovurdering av kravene?’ Mange tror at de utarbeider dokumentasjonen for å tilfredsstille NSM. Da blir jeg litt provosert. Hensikten med dokumentasjonen er å sørge for at systemet er sikkert, ikke å tilfredsstille NSM.”*

Det kan virke som om enkelte tror de utarbeider sikkerhetsdokumenter for å tilfredsstille godkjenningsmyndigheter. Dette er i så fall feil, og kommenteres av intervjuobjektet slik:

> *"Jeg har opplevd at en tykk perm blir vist fram under inspeksjoner og det blir fortalt at alle brukere må kvittere for å ha lest innholdet. Når denne permen inneholder så mye som både er foreldet og har liten relevans for brukere, spør jeg: Hva er vitsen? Kun det som gjelder for brukeren bør være det som skal leses og være forstått. Jo enklere jo bedre, for da oppfatter en det."*

Andre sikkerhetseksperter bekrefter inntrykket av at sikkerhetsdokumentasjonen får preg av symbolverdi framfor det å være et redskap for å dokumentere sikkerhetstiltakene for informasjonssystemet. Dette er noen sitater fra forskjellige intervjuobjekter som uttaler seg om deres erfaringer med sikkerhetsdokumentasjon for informasjonssystemer.

> *"Dokumentene har definitivt veldig stor symbolverdi. Det er viktig å få dokumentene utarbeidet for å få systemene i drift. Så snart de er i drift, virker det som om en ikke forholder seg til dem."*

> *"Dokumentasjonen står i hylla og tas fram under inspeksjoner."*

> *"Dokumentasjonen er generell og lite tilpasset den avdelingen som benytter den."*

Dette tyder på at sikkerhetsdokumentasjonen ikke anvendes slik den er ment og at det er et betydelig forbedringspotensial i å forenkle dokumentene slik at de blir brukt aktivt av alle involverte aktører. Dette faktumet er erkjent av aktørene og arbeidet med å forbedre sikkerhetsdokumentasjonen er allerede påbegynt. Representanten fra NSM uttaler:

> *"Generelt arbeider vi med å forbedre forskrift og veiledninger for å forenkle godkjenningsarbeidet for systemeiere og brukere."*

En annen ekspert kommenterer arbeidet med å forbedre sikkerhetsdokumentasjonen for informasjonssystemer slik:

> *"Tradisjonelt veldig omfattende dokumenter. Lite lesbare, til dels med motstridende innhold. Der har vi gjort vesentlige forbedringer de siste årene. Spesielt når det gjelder konsistens, enkelhet og det å være tydelig."*

Når det gjelder det konkrete innholdet i sikkerhetsdokumentasjonen, vil det kommenteres nærmere i kapittel 6 Opplæring i risikohåndtering. Et annet moment som ble trukket fram i intervjuene var omfanget av sikkerhetsinstruksene. En ekspert uttalte seg slik:

> *"Prøver å få ned omfanget på brukerinstruksen fordi at dersom instruksen blir for omfattende, er det ingen som leser den. Derfor er det viktig å få med det vesentlige og kutte ut perifere forhold."*

Men å vite hva som er vesentlig og hva som er perifere forhold krever ekspertise. Likevel bør det ikke overlates til eksperter alene å utforme sikkerhetsdokumentasjonen. Det blir av intervjuobjektet også pekt på den bevisstgjøringsprosessen det innebærer å skrive sikkerhetsdokumenter selv.

> *"Da tvinger en også dem som skriver brukerinstruksen til å tenke gjennom hva som er vesentlig eller ikke. Viktig bevisstgjøringsprosess."*

Dette støttes av OPSEC teorien hvor sikkerheten ikke er et sett med regler, men en kontinuerlig prosess som det må tas stilling til for involverte aktører. Risikoanalyse er en prosess, hvor selve deltakelsen i prosessen kanskje er like viktig som selve produktet av analysen.

5.6.2 Kontroll av forutsetninger

Når sikkerhetstiltakene er dokumentert på en kortfattet og hensiktsmessig måte, må det jevnlig kontrolleres at forutsetningene for sikkerhetsnivået ikke endres. Her skilles det mellom signifikante avvik som må håndteres, og avvik som aksepteres og som ikke innebærer en endring av sikkerhetsnivået.

Hva som regnes som et signifikant avvik vil drøftes i kapittel 8. Dette konseptet baseres på to metoder som er hensiktsmessige for å kontrollere om forutsetningene fremdeles er gyldige

- Egenkontroll ved lokal sikkerhetsorganisasjon
- Kontroll og veiledning team

Lokale ledere og sikkerhetspersonell gjennomfører kontinuerlig risikohåndtering gjennom OPSEC planlegging og ved egenkontroller. Målsettingen er å håndtere flest mulig avvik på lokalt nivå. Forutsetningen for dette er at lokalt personell har kunnskap om hvilke forutsetninger som ligger til grunn for sikkerhetsnivået i informasjonssystemet. En annen forutsetning er at de har et bevisst forhold til hvilke avvik som regnes som signifikante og som krever reaksjon og oppfølging fra overordnet nivå, og hvilke avvik som ikke skal rapporteres.

Kilder opplyser at det til tider har blitt sendt for mange rapporter om sikkerhetstruende hendelser som egentlig ikke burde vært rapportert. For mange rapporter bidrar til å fjerne fokus fra det som betyr noe for sikkerheten. Siden det ikke er alle forunt å vite hva som betyr noe for sikkerheten, er det avgjørende viktig å presisere hvilke forhold som ønskes rapportert.

Et kontroll og veiledningsteam er en ressurs som blir styrt av overordnet nivå der hvor behovet antas å være størst.

5.6.3 Rapportering

Rapporteringslinjer fremgår av figur 10. Det er viktig at aktørene internt ved en avdeling og mellom avdelinger i Forsvaret vet

- hva som skal rapporteres
- hvor det skal rapporters

Signifikante avvik fra forutsetningene som kan få betydning for andre aktører må rapporteres umiddelbart slik at mottiltak kan iverksettes så snart som mulig for å begrense et potensielt skadeomfang. Men det må også være slik at forhold som ikke får betydning for andre aktører ikke rapporteres på samme måte. Da vil en ikke skille mellom det som anses å påvirke sikkerhetsnivået for andre aktører og det som kan ordnes opp i lokalt. Slike hendelser som ikke er signifikante kan rapporteres i samleoversikter ved utgangen av en rapporteringsperiode.

5.6.4 Reaksjonsoppfølging

Ved alvorlige sikkerhetstruende hendelser kan det være hensiktsmessig å sette inn store ressurser på kort varsel. Et Computer Incident Reaction Team (CIRT) ville vært en slik ressurs å spille på. FSA kunne i så fall hatt en beredskap og på bakgrunn av alvorlighetsgrad i innkomne rapporter ha gitt CIRT konkrete oppdrag. Det bør vurderes i senere arbeid hvordan en CIRT for Forsvaret bør utrustes.

5.6.5 Opplæring i risikohåndtering

Det må utarbeides et kurs i risikohåndtering som skal tilbys ledere, sikkerhets og driftspersonell ute ved de enkelte avdelingene som skal tilknyttes det sikkerhetsgraderte informasjonssystemet. Dette beskrives i kapittel 6.

> *"Det stilles krav til tekniske, organisatoriske og utdanningsmessige forutsetninger. Det er kun innen fagområdet krypto hvor det stilles krav til formalisert utdanning."*
>
> Representant fra Forsvarets Utdannings og kompetansesenter

Figur 12: Krav til formalisert utdanning

5.7 Kompetanse

Med kompetanse forstås i denne sammenhengen hvilke kompetansekrav som må stilles til aktørene for at de skal være i stand til å løse oppgavene som må utføres for å oppfylle ansvaret beskrevet i struktur og samhandling beskrevet i system. På spørsmål om hvilke krav som stilles til opplæring og utdanning for å håndtere sikkerhetsgraderte informasjonssystemer ble det gitt følgende svar:

> *"Det er kun innen fagområdet krypto det stilles krav til formalisert utdanning."*

Dette bekreftes av en annen kilde som utdyper hvilke krav som gjelder i dag:

> *"Når det gjelder innhold, stilles det lite krav unntatt kryptosikkerhet. Det samme gjelder kunnskapstester. Kunnskapstester blir kun gjennomført på fagutdanning på ingeniørnivå og for kryptopersonell. Det har vært historisk strenge krav til kryptotjenesten i form av Natodirektiver."*

Krypto er et fagfelt som står sterkt i Forsvaret, noe som kan forklares ut fra historisk vektlegging og betydning for sikker kommunikasjon med andre NATO land. Dersom ikke kryptotjenesten hadde blitt utført på en sikker og tillitskapende måte, ville andre NATO land ikke delt skjermingsverdig informasjon.

Denne logikken virker enkel å forholde seg til. En kan tenke seg en lignende tilnærming til øvrige deler av informasjonssystemet, og stille tilsvarende krav til andre aktører som brukere, driftspersonell og sikkerhetsledere. Et gjennomgående trekk hos alle intervjuobjektene er at det er ønskelig med mer opplæring.

> *"Det burde vært mer opplæring. "*

På spørsmål om hvordan brukeropplæringen foregår ble det svart:

> *"For brukere blir det gjerne organisert kurs i forkant av øvelser hvor informasjonssystemet skal brukes. Gjennomføring av opplæring for brukere er preget av ad hoc tiltak. Dette begynner å bli bedre."*

Dette kan bety at det mangler en helhetlig oversikt over hvem som skal bruke informasjonssystemene og som medfører at behov for opplæring ikke blir identifisert før personellet skal benytte systemet i et konkret oppdrag. Ideelt burde en gjennomført brukeropplæring før en skal ta i bruk systemene. Men siden en i praksis ikke har mulighet til å forutse alle forhold som kan oppstå, vil det være vanskelig å gjennomføre for absolutt alle.

> *"Brukere får opplæring. Om den er bra nok kan diskuteres. Litt avhenging av systemer…(her ble ulike systemer og praksis nevnt)… Det er et forbedringspotensial i å samkjøre krav til brukerkurs."*

Om en derimot så på innholdet i brukeropplæringen som gis for de ulike informasjonssystemene, kunne en identifisert faktorer som påvirker sikkerheten og stilt som krav at det skal gjennomføres som en del av brukeropplæringen. Dette bør også sees i sammenheng med brukerinstrukser. Sikkerhetsdelen av brukeropplæringen bør være en gjennomgang av brukerinstruksen, som bør være så kortfattet og konkret som mulig. Da oppnår en å fokusere på det som er vesentlig for at en bruker kan utføre for å ivareta sikkerheten.

Driftspersonellet har i følge kildene for denne undersøkelsen en bedre forutsetning for å ivareta sikkerheten gjennom utdanningen sin.

> *"Driftspersonell har god opplæring gjennom fagutdanningen."*

> *"Driftspersonellet er stort sett greie. De som er på de taktiske systemene får utdanning hos SBUKS og derigjennom en bra bakgrunn."*

Dette virker logisk forutsatt at utdanningen driftspersonellet har gjennomgått inneholder sikkerhetsfag. Ved SBUKS skolesenter vektlegges sikkerhet i utdanningen, noe som gjenspeiles ute ved avdelingene som mottar ferdigutdannede ingeniører som skal drifte informasjonssystemene.

Når det gjelder sikkerhetspersonell står det ikke så bra til ved Forsvarets avdelinger i følge flere av kildene. En ekspert uttalte følgende:

> *"Sikkerhetspersonell har tradisjonelt sett hatt lite og dårlig utdanning av generell karakter. Vi har iverksatt tiltak for dette."*

En annen ekspert nyanserte bildet litt mer og pekte på store variasjoner mellom ulike avdelinger i Forsvaret. Vedkommende peker på en sammenheng mellom tid til rådighet og kompetansenivå.

”Sikkerhetspersonellet er både og. De som er bevisste og går inn for oppgaven er veldig bra. De som har fått oppgaven trådd nedover seg er ikke tilfredsstillende. Typisk ASO i 20 % stilling. Mangler kurs og forutsetning for å løse pålagte oppgaver.” (ASO: Avdelingens sikkerhetsoffiser)

Nettopp tid til å utføre sikkerhetsoppgavene blir pekt på som et viktig poeng i følge en av kildene som svarer på spørsmål om hva som kan forbedres:

”Opplæring. At det gis tilstrekkelig med tid til å gjennomføre DSL tjenesten. Han er som regel nedlesset i andre oppgaver.”

Sist men ikke minst er det nødvendig å se på kompetansekrav som stilles til ledere som skal være ansvarlig for å opprettholde sikkerheten i sin avdeling. Tradisjonelt har det ikke vært vanskelig for en leder å forstå hva et sikkerhetsansvar innebærer for å beskytte et geografisk område. Men det virker som om det er vanskeligere å forstå ansvaret for informasjonssikkerhet i et nettverk hvor et angrep kan gjennomføres mot en node som er dårlig sikret og få konsekvenser for hele organisasjonen, også de avdelingene som har gode sikkerhetstiltak.

I et informasjonssystem som knytter geografisk atskilte avdelinger sammen, vil sikkerheten ikke være sterkere enn hos den avdelingen som har de svakeste sikkerhetstiltakene implementert. Dette medfører ikke bare et ansvar for sikkerheten i eget geografisk område, men for en del av et integrert system. Derfor hadde det vært naturlig å stille krav til kompetanse for ledere som har autorisasjonsansvar og som fyller rollen som virksomhetens leder. Dette forholdet blir pekt på av flere kilder. En sier:

”Ledere får stort sett ingen utdanning.”

En annen utdyper hvordan en ville forbedret sikkerheten for et omfattende informasjonssystem.

”En bør kanskje fokusere mer på sjefsnivå. Å ha et gradert informasjonssystem er et sjefsansvar, ikke alle har tatt inn over seg hva de har signert for.”

På spørsmål om å identifisere forbedringspotensial i forhold til dagens situasjon svarte en kilde:

”Av og til sjefers holdninger.”

Holdninger vokser fram gjennom kompetansen som opparbeides over tid gjennom erfaringer. Holdninger er også en viktig faktor som er med på å forme kulturen i en organisasjon.

5.8 Kultur

Kompetanse og kultur henger nøye sammen i følge Leavitt. Kompetanse er et uttrykk for kunnskaper og ferdigheter som må til for å løse organisasjonens oppgaver. Edgar Schein definerer kultur i [47] som ”et mønster av felles grunnleggende antakelser som en gruppe har kommet fram til etter hvert som den har løst sine problemer når det gjelder ytre tilpasning og integrering, som har fungert godt nok til å ble betraktet som holdbare, og som derfor læres bort til nye medlemmer som den riktige måten å oppfatte, tenke og føle på i forhold til disse problemene”. Kortfattet kan det uttrykkes som ”måten vi gjør ting på her hos oss” i følge Bolman og Deal [31, s 244].

Når alle elementene er tilrettelagt gjennom velfungerende systemer, en hensiktsmessig struktur, relevant kompetanse og personellet har forstått policy, er grunnlaget for en god kultur til stede. Ønsket tilstand bør formuleres som målsettinger, da en kultur ikke kan iverksettes eller beordres gjennomført, men må vokse fram over tid. Ved å formulere delmål som er mer konkrete enn overordnede kulturmål, kan en måle om ønsket tilstand er nådd.

"Vi prøver å være mer åpne nå enn før. Tidligere hvis en hadde kontakt med FO/S hadde en sannsynligvis gjort noe galt."

Representant fra Forsvarets Sikkerhetsavdeling, tidligere FO/S

Figur 13: Kulturendring

En sikkerhetsekspert la vekt på at sikkerheten må ha forankring hos ledelsen.

> *"Det er veldig viktig at sikkerheten er forankret hos ledelsen. Det har inspeksjoner avdekket."*

Andre ekspertintervjuer avdekket flere forhold som kan tolkes negativt i forhold til eksisterende kultur. En kilde uttalte følgende:

> *Generelt er sikkerheten dårlig forankret. Enkelte ledere tar ikke ansvar for sikkerheten i informasjonssystemene deres.*

På spørsmål om hva som kan gjøres for å bedre forholdet, ble det svart:

> *"Knytt sikkerhetsvurderingen til de operative vurderingene som gjøres kontinuerlig i en militær avdeling. Da blir ikke sikkerheten et utstillingsvindu for inspektører, men en integrert del av operasjonene."*

Et annet virkemiddel som kan benyttes er kompetanseheving.

> *"Utdann stabsoffiser i operasjonssikkerhet og risikohåndtering. Risikovurderinger og tilhørende sikkerhetstiltak for informasjonssikkerhet må være en integrert del av styrkebeskyttelsen for å få en optimal effekt."*

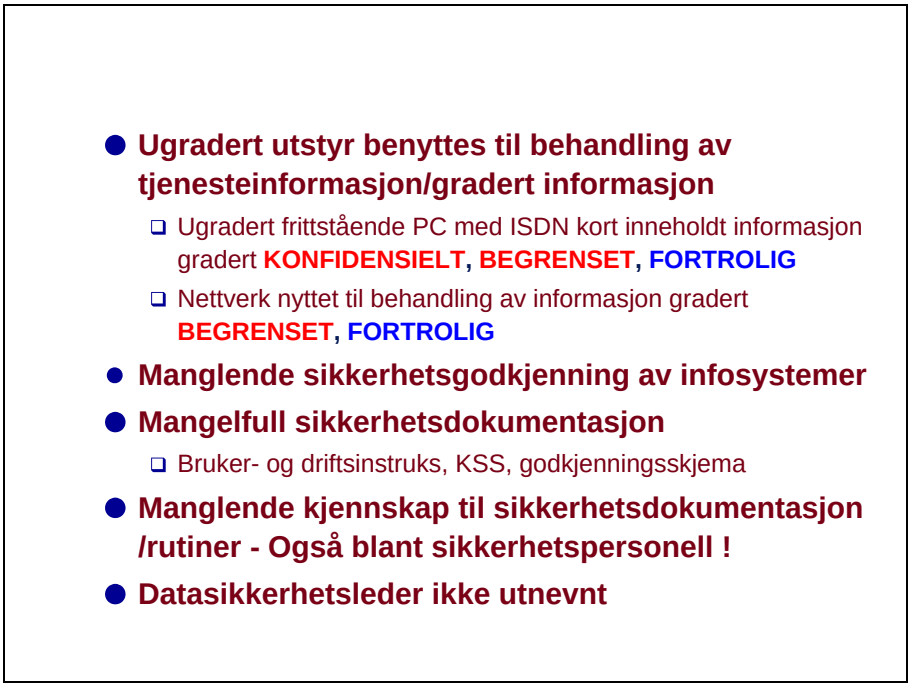
Styrkebeskyttelse vil si alle tiltak som går ut på fysisk sikring av mannskaper. Dette er noe Forsvarets avdelinger har erfaring med og er en del av kulturen. Ledere forstår behovet for styrkebeskyttelse og iverksetter derfor nødvendige tiltak.

> *"Sikkerhetspersonell og ledere må forstå policy som ligger bak. Med policy mener jeg regler og retningslinjer som må følges for å ivareta sikkerheten etter forutsetningene for sikkerhetsgodkjenningen. Det er min erfaring at de kjenner dette for dårlig."*

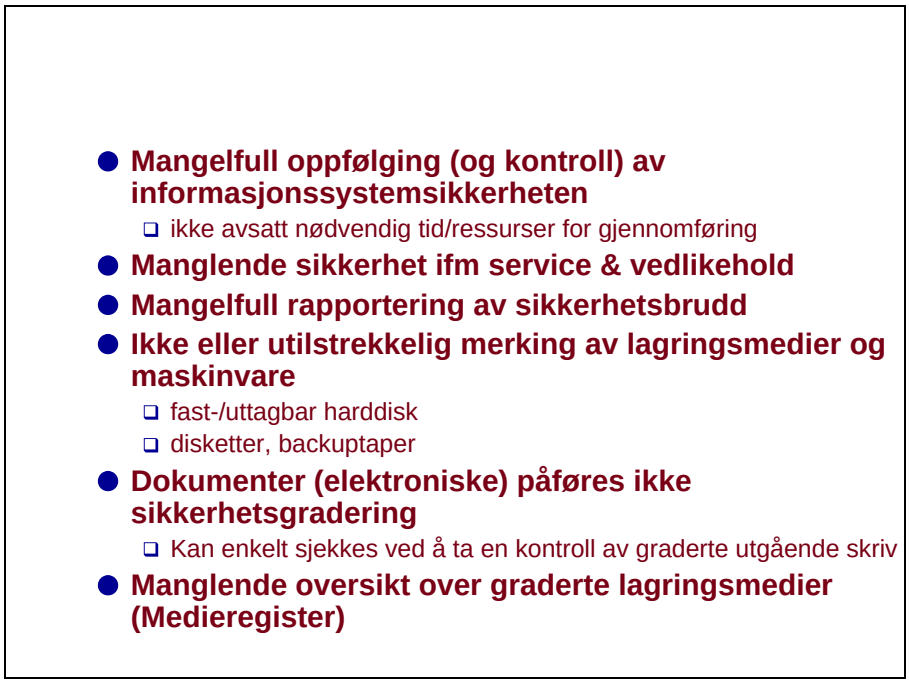
Igjen vises det til at opplæring og utdanning er veien å gå. Et kurs i risikohåndtering og en gjennomgang av hvilke forutsetninger som ligger til grunn for sikkerhetsnivået i informasjonssystemene, vil i følge kilden bidra til å påvirke kompetansenivået og deretter kulturen i Forsvaret.

5.9 Erfaring fra inspeksjoner

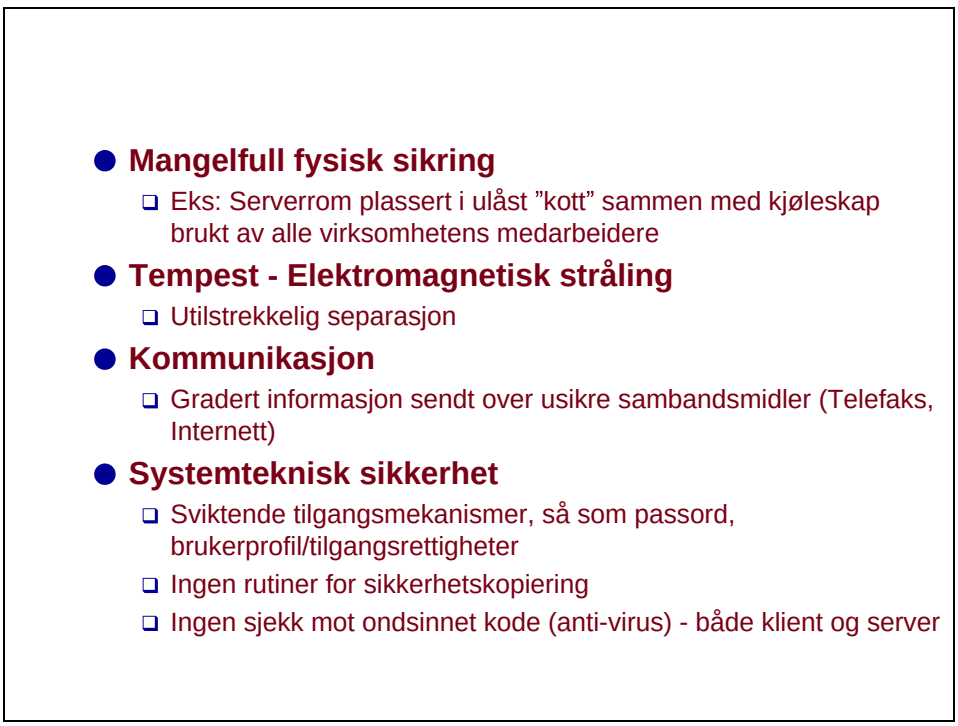
Konkrete mangler og spesielle forhold hos navngitte avdelinger er sikkerhetsgradert informasjon. Men generelle erfaringer fra inspeksjoner av mange avdelinger har blitt frigitt til denne undersøkelsen som ugradert informasjon. Disse erfaringene viser at det er et reelt behov for et risikohåndteringskonsept for informasjonssystemer i Forsvaret.



Figur 14: Erfaringer fra sikkerhetsinspeksjoner



Figur 15: Erfaringer fra sikkerhetsinspeksjoner 2



Figur 16: Erfaringer fra sikkerhetsinspeksjoner 3

Kapittel

6 Opplæring i risikohåndtering

Først beskrives hvordan et grunnkurs i risikohåndtering ble utformet for å dekke beskrevet kompetansemangel. Dette kurset ble deretter gjennomført som et eksperiment for en liten gruppe sikkerhetspersonell. Etter gjennomført kurs ble oppfattelsen av effekten målt ved hjelp av tilbakemeldinger gitt ved kursavslutning og utfylte spørreskjemaer. Hensikten med dette kapitlet er å gi en beskrivelse av hvordan opplæring i risikohåndtering kan tilpasses en organisasjons behov for kompetanse og gjennomføres i løpet av to og en halv dag.

6.1 Bakgrunn

Som nevnt i kapittel 4, ble det på et tidlig tidspunk i forskningsprosessen klart at det ikke fantes noe kurs i risikohåndtering av informasjonssystemer tilgjengelig for Forsvaret. Så godt som alle involverte aktører i sikkerhetsgodkjenningsprosesser av informasjonssystemer har pekt på at det er et stort behov for opplæring i risikohåndtering.

På spørsmål om hvor det er forbedringspotensial i forhold til om en kan stole på at ikke forutsetningene for den sikkerhetsmessige godkjenningen er endret, svarte en sikkerhetsekspert:

> *"Opplæring av lokale datasikkerhetsledere og driftspersonell slik at de forstår hensikten med sikkerhetstiltak og kan bidra til å opprettholde sikkerheten i et system."*

Det å forstå hensikten med sikkerhetstiltakene er en forutsetning for å kunne endre dem i takt med skiftende omgivelser. Dersom en fjerner et sikkerhetstiltak en ikke skjønner hensikten med, kan det medføre alvorlige konsekvenser. Men om en forstår hensikten, og ser at sikkerhetstiltaket ikke er egnet til formålet blir det noe helt annet. Da kan en effektivisere tiltakene uten at det går ut over sikkerhetsnivået. Her ligger den store forskjellen mellom det at en forstår hensikten med hvorfor sikkerhetstiltakene er implementert og det på den annen side bare å forholde seg til dem uten å forstå hvilken funksjon de skal ivareta. Dette med å forstå hensikten med sikkerhetstiltak ble derfor en av målsettingene for kurset i risikohåndtering.

En annen sikkerhetsekspert gav følgende svar på spørsmål om forbedringspotensial:

> *"Utdanning på alle nivå og særlig for stabsoffiserer. Når jeg nevner stabsoffiserer spesielt, skyldes det at det er der beslutninger tas."*

Som det ble poengtert i forrige kapittel er utdanning et virkemiddel for å heve kompetansen for involverte aktører. Gjennom kompetanse skapes holdninger som igjen legger premisser for hvilken kultur som organisasjonen har. Det hjelper lite å utdanne en liten gruppe sikkerhetspersoner dersom det ikke er forståelse for informasjonssikkerhet blant øvrige medarbeidere. Spesielt viktig er det å gi reelle beslutningstakere kompetanse i risikohåndtering. Intervjuobjektet fortsetter:

> *"Sikkerhet må være knyttet til operasjonsvurderingen."*

Det nytter ikke å behandle sikkerhet isolert, men som en integrert del av virksomhetens daglige gjøremål. Dette poengteres også i OPSEC doktrinen som beskriver operasjonssikkerhet som en kontinuerlig prosess som skal gjøres av operasjonspersonell og ikke bare sikkerhetspersonell. Dette innebærer at målgruppen for risikohåndteringskurset ikke bare skal være sikkerhetspersonell, men også stabsmedarbeidere og ledere som har reell beslutningsmyndighet.

En tredje ekspert svarte følgende på spørsmål om forbedringspotensial i forhold til å kunne stole på at ikke forutsetningene for sikkerhetsgodkjenningen er endret:

> *"Kompetanse hos sikkerhetspersonell og forankring i ledelsen."*

Kompetansen som det siktes til må inkludere en helhetlig forståelse av sikkerhetsdokumentasjonen som ligger til grunn for sikkerhetsgodkjenningen. Derfor ble en helhetlig forståelse av sikkerhetsdokumentasjonen en målsetting med kurset. En fjerde ekspert bekreftet inntrykket og svarte dette på det samme spørsmålet:

> *"Opplæring og forankring av det som står i dokumentasjonen i alle ledd i organisasjonen.*

Fellesnevneren for alle svarene er at opplæring er kanskje det største forbedringspotensialet i forhold til problemstillingen om hvorvidt en kan stole på om forutsetningene for en sikkerhetsmessig godkjenning fremdeles er gyldig etter at det er gjort endringer i omgivelsene for et informasjonssystem. Målsettingen for kurset ble derfor utformet slik den er beskrevet under.

6.2 Målsetting

Kurset skal kvalifisere deltakere til å fylle roller i virksomhetens sikkerhetsorganisasjon, jf Forskrift om sikkerhetsadministrasjon [40] § 2-5.

Etter gjennomført kurs skal deltagerne være i stand til å håndtere risiko for et sikkerhetsgradert informasjonssystem jf Forskrift om sikkerhetsadministrasjon [40] § 4-1. Dette innebærer:

- En helhetlig forståelse av sikkerhetsdokumentasjonen som ligger til grunn for den sikkerhetsmessige godkjenningen av systemet.
- Å forstå hensikten med risikovurdering og sikkerhetstiltak som iverksettes for å møte relevante trusler mot informasjonssystemet.
- Å kjenne til sammenhengen mellom trusler, sårbarhet, risiko og tiltak
- Å forstå hvordan sikkerhetstiltak og sikkerhetsdokumentasjon skal revideres og betydningen av at tiltakene som er beskrevet etterleves.

6.3 Utforming av Operasjonssikkerhet Grunnkurs

Prosessen med å utforme kurset er beskrevet i kapittel fire. Det var en rekke forhold som måtte avveies underveis. Hvor detaljert skulle et slikt kurs være? Ideelt sett ville det vært ønskelig å gjennomføre en grundig opplæring over lang tid. Men i virkeligheten er det ikke tid til å gjennomføre lange undervisningsopplegg. I forhold til den grunnleggende hypotesen om at enkelhet er viktigere enn kompletthet må en gjøre valg som medfører at en prioriterer det som er viktigst å få med seg innenfor en tidsramme som er realistisk å gjennomføre.

Risikohåndtering av informasjonssystemer er et fagfelt som det kan utdannes på i løpet av flere år ved en høyskole. Men det må altså være mulig å komprimere det viktigste ned til noen få dagers kurs om en skal ha forhåpninger om å få gjennomført opplæring for ledere og stabsmedarbeidere.

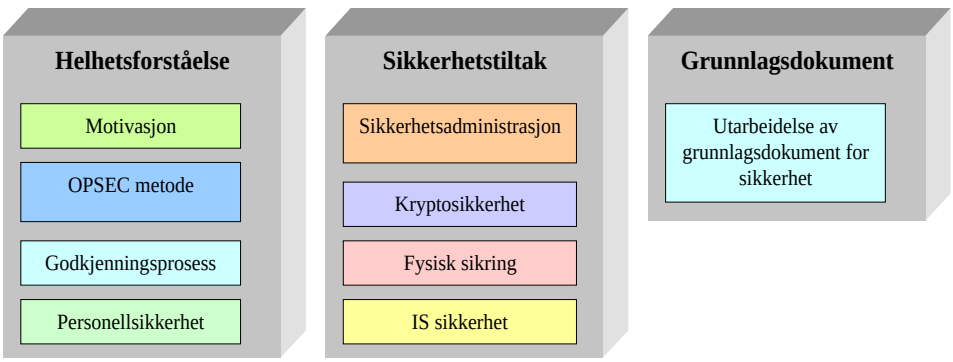
6.3.1 Omfang

Det er tidligere slått fast et behov for opplæring i risikohåndtering for informasjonssystemer. Men det er ikke dermed noen automatikk i at det prioriteres i en travel hverdag. En sikkerhetsekspert fra FSA uttalte følgende:

> ”*Det har vært innkalt til lederseminar innen sikkerhet. Det skjærer seg fordi enkelte ikke har anledning til å stille. De prioriterer det ikke høyt nok… Det gjelder å finne en gylden middelvei.”*

Det er behov for et kurs som ikke tar for lang tid å gjennomføre. For å få til det til ble det fastsatt og gjennomføre kurset over to og en halv dag.

6.3.2 Struktur



Figur 17: Kursoppbygning over tre dager

Den første dagen skal gi motivasjon og forståelse for sikkerhetsarbeidet, ved at elevene får en innføring i operasjonssikkerhet og risikohåndtering. Hensikten er å gi elevene en helhetlig forståelse av sammenhengen mellom trusler, sårbarhet, risiko og tiltak.

Dag to er en gjennomgang av alle relevante sikkerhetstiltak. Dagen er inndelt i fagområder, og følger en logisk oppbygning som er identisk med inndelingen i sikkerhetspermen som

kan inneholde en avdelings sikkerhetsdokumentasjon. Dag tre er avsatt for å gi veiledning til å skrive et grunnlagsdokument for sikkerhet.

Grunnlagsdokument for sikkerhet er nevnt spesielt i Forskrift for sikkerhetsadministrasjon § 3-3 og skal ”identifisere grunnleggende forutsetninger for virksomhetens håndtering av skjermingsverdig informasjon.” Grunnlagsdokumentet er med andre ord det dokumentet hvor forutsetningene for sikkerheten lokalt skal fremgå.

En representant fra godkjenningsmyndighetene nevner grunnlagsdokumentet som en av faktorene som kontrolleres ved sikkerhetsinspeksjoner.

> *”Vi kontrollerer blant annet lokal sikkerhetsorganisasjon, Grunnlagsdokument for sikkerhet, personellsikkerhet og fysisk sikkerhet.”*

Med blant annet dette som bakgrunn, ble grunnlagsdokumentet viet så stor oppmerksomhet under kurset.

6.3.3 Målgruppe

Med bakgrunn i tidligere nevnt informasjon om hvem som bør være målgruppen for dette kurset ble følgende utpekt som den primære målgruppen for kurset:

- Ledere og mellomledere for avdelinger med sikkerhetsgraderte informasjonssystemer.
- Sikkerhetspersonell i avdelinger med sikkerhetsgraderte informasjonssystemer.
- Brukere og driftspersonell av sikkerhetsgraderte informasjonssystemer.

6.3.4 Krav til forkunnskaper

Det ble vurdert om hvorvidt det skulle stilles noen krav til forkunnskaper hos kursdeltakerne. Dette kurset alene ville ikke gi nødvendig formell kompetanse til å fylle roller i en sikkerhetsorganisasjon. For eksempel stilles det krav til gjennomført kryptokvalifisering for kryptopersonell slik det ble nevnt i et tidligere kapittel om kompetansekrav. Dersom en stilte for høye krav til forkunnskaper, kunne en risikere at det ikke ville være noen deltakere å kjøre kurset for. Det ville i så fall ikke være hensiktsmessig. Derfor ble det ikke satt absolutte krav. Det ble opplyst følgende krav til forkunnskaper:

Nødvendig kvalifiserende utdanning innen et av sikkerhetsområdene. Det kan eksempelvis være Kryptokvalifiseringsgrad I kurs for kryptosikkerhetspersonell. Grunnkurs datasikkerhet for datasikkerhetsledere. Lignende utdanning for andre sikkerhetsfunksjoner.

6.4 Timeplan

Timeplanen for kurset ble først endelig fastsatt etter flere runder med innspill fra involverte aktører i sikkerhetsgodkjenningsprosessen. Første utkast til kursinnhold ble forevist sikkerhetseksperter i NSM, FSA, og FLO slik at de kunne kommentere innholdet i kurset.

Deretter ble det satt av en hel dag ved SBUKS hvor sikkerhetspersonell gjennomførte et arbeidsmøte for å forbedre innholdet. Dette arbeidsmøtet ble også brukt til å fordele undervisningsoppgaver til instruktørene som skulle holde kurset. Den endelige timeplanen som ble gjennomført under eksperimentet 3 til 5 februar er vist i figuren under.

		Dag 1	Dag 2	Dag 3
1	07^{45} - 08^{30}	**Kursåpning kl. 08:00** Målsetting for kurset og adm forhold	**Godkjenning og revisjon**	**Grunnlagsdokument I** Praktisk øvelse i å skrive et grunnlagsdokument for sikkerhet.
2	08^{40} - 09^{25}	**Motivasjon**	**Beredskapsplan**	
3	09^{35} – 10^{20}	**OPSEC metode**	**Fysisk sikkerhet** Instruks for adgangskontroll, Autorisasjonsliste.	
4	10^{30} - 11^{15}	**Verdivurdering**	**Kryptosikkerhet** Lokal kryptosikkerhetsinstruks med vedlegg	**Avslutning og evaluering**
	11^{15} - 12^{00}	- L u n c h -	- L u n c h -	- L u n c h -
5	12^{00} - 12^{45}	**Risikofastsettelse**	**Informasjonssystemsikkerhet** Brukerinstruks, Driftsinstruks	
6	12^{55} - 13^{40}	**Tiltak**	**Informasjonssystemsikkerhet** Konfigurasjonsskontroll, Autorisasjon, Mediejournal	
7	13^{50} - 14^{35}	**Godkjenningsprosessen** Bestemmelser, KSS Aktører og funksjoner	**Tempestrisikovurdering** Bestemmelser for installasjoner MKM krav til etablering	
8	14^{45} - 15^{30}	**Personellsikkerhet** Klarering og autorisasjon Opplæring	**Faktorer og signifikans** Forutsetninger som en sikkerhetsgodkjenning bygger på	
9	15^{35} –			

Figur 18: Timeplan for Operasjonssikkerhet grunnkurs

6.5 Fagbeskrivelser

Kurset skulle gjennomføres i løpet av tre dager, hvor den første dagen skulle skape en helhetsforståelse og vektlegge sammenhenger mellom risiko og sikkerhetstiltak. Den andre dagen skulle være en gjennomgang av dokumenterte sikkerhetstiltak, mens den tredje dagen skulle brukes til å utforme et grunnlagsdokument for sikkerhet. Dette medførte at kurset fikk tre hovedtemaer som ble kalt:

- Helhetsforståelse
- Dokumentering av sikkerhetstiltak
- Utforming av et grunnlagsdokument for sikkerhet

6.6 Helhetsforståelse

Etter kursåpning med målsetting for kurset og administrative forhold var gjennomgått, var det klart for å presentere OPSEC metoden som et verktøy for å vurdere sikkerhetstiltak opp mot gjeldene trussel, sårbarhet og verdier.

> *"Sikkerhet koster som sagt ressurser, og man kan ikke sikre systemene 100 % fordi det vil være for resurskrevende"*

Sikkerhetsdokumentasjonen er ikke noe mål i seg selv, kun et middel for å beskrive et sikkerhetsnivå som systemet er sikkerhetsgodkjent for. I tillegg er sikkerhetsdokumentasjon en forutsetning for at medarbeidere kan bidra til å opprettholde sikkerheten ved avdelingen. Budskapet er at sikkerhet skal være en nødvendig egeninteresse, ikke bare noe en gjør for å tilfredsstille sikkerhetsmyndigheter.

6.6.1 Operasjonssikkerhet metode

Operasjonssikkerhetssløyfen:

- Identifisere kritisk informasjon
- Trusselanalyse
- Sårbarhetsanalyse
- Fastslå risiko
- Iverksette hensiktsmessige mottiltak.

Konsekvenser ved dårlig operasjonssikkerhet kan være katastrofale. Operasjonssikkerhet gir egne operasjoner større effektivitet ved at sikkerhetstiltak iverksettes i et kost/nytte perspektiv. Å beholde initiativet og fordelen som ligger i å være pro aktiv, er verdt en investering i sikkerhet. God operasjonssikkerhet vil hindre at en motstander forutser hvilke disposisjoner egen avdeling vil gjøre, og dermed iverksetter tiltak for å tilrive seg initiativet og fordelen.

6.6.2 Godkjenningsprosessen

Lover og bestemmelser

- Sikkerhetsloven med forskrifter og veiledninger

Aktører og funksjoner

- NSM, FSA, SBUKS, FOHK, FLO/IKT, brukende avdelinger.

Kravspesifikasjon for sikkerhet (KSS)

- Sikkerhetskonsept, sikkerhetskrav, sikkerhetstiltak, sikkerhetstest, risikohåndtering.

6.6.3 Personellsikkerhet

- Personkontroll, klarering og autorisasjon gjennomføres for å sikre at ikke personell som kan utgjøre en sikkerhetsrisiko, får tilgang til informasjon eller informasjonssystemer.
- Opplæring er en viktig forutsetning for at personell skal kunne bidra til å opprettholde sikkerhetsnivået i avdelingen.
- Personellsikkerhet er en dynamisk prosess. Grunnlag for sikkerhetsmessig skikkethet kan endres.
- Må sees i en helhetlig sammenheng. Autorisasjon griper inn i andre fagområder:
    - Adgang til kommandoplassen. (Fysisk sikring)
    - Adgang til kryptorom. (Kryptosikkerhet)
    - Tilgang til informasjonssystemer. (Informasjonssystemsikkerhet)

6.7 Dokumentering av sikkerhetstiltak

En av sikkerhetsekspertene formulerte seg slik på spørsmål om hvordan en kan stole på om forutsetningene for en sikkerhetsgodkjenning er gyldige etter en tid hvor omgivelsene er endret:

> *"Man må ha en oppdatert oversikt over hva en har og hvor en har det. Hvis ikke en har kontroll, kan forutsetningene være brutt."*

En annen sikkerhetsekspert uttalte seg slik på det samme spørsmålet.

> *"Man må vite hva forutsetningene er. Eneste måten en kan vite det er at alle endringer dokumenteres og en har kontroll over systemet."*

Det ble foreslått en inndeling av sikkerhetsdokumentasjonen i fagområder. Fagområdene var:

- Sikkerhetsadministrasjon
- Fysisk sikring
- Kryptosikkerhet
- Informasjonssystemsikkerhet

Dette ble ansett å være hensiktsmessig blant annet fordi eierskap til de enkelte sikkerhetsdokumentene lett kunne identifiseres. Med utgangspunkt i sikkerhetsorganisasjonen som er vist på figur 10 er fagområdene sammenfallende med ansvarsområder for de enkelte rollene som skal bekles i sikkerhetsorganisasjonen. Sikkerhetsleder er den som har eierskap og oppdateringsansvar for dokumentene under sikkerhetsadministrasjon. Fysisk sikringsansvarlig skal oppdatere instruks for adgangskontroll, kryptosikkerhetsleder skal oppdatere lokal kryptosikkerhetsinstruks. Datasikkerhetsleder har ansvar for å oppdatere alle dokumentene under informasjonssystemsikkerhet.

Ideen med en slik tilnærming til sikkerhetsdokumentasjonen var å gjøre den tilgjengelig i en perm som ble oppbevart hos sikkerhetsleder. Dette vil gjøre sikkerhetslederen i stand til

å ha full oversikt over dokumenterte sikkerhetstiltak. Samtidig er ansvaret for oppdatering delegert ned til øvrige aktører i sikkerhetsorganisasjonen.

Sikkerhets-administrasjon	1 Godkjenning
	2 Grunnlagsdokument
	3 Beredskapsplan
	4 Sikkerhetsrevisjon
Fysisk sikring	5 Instruks for adgangskontroll
	6 Autorisasjonsliste
Krypto sikkerhet	7 Krypto sikkerhetsinstruks
	8 Vedl A: Utnenvnelser
	9 Vedl B, C: Autorisasjon
	10 Vedl D: Brukerinstruks MRR
	11 Vedl E: Nødmakuleringsplan
Informasjonssystem sikkerhet	12 Brukerinstruks
	13 Driftsinstruks
	14 Konfigurasjonskontroll
	15 Konfigurasjonsoversikt
	16 Kommunikasjon og kabling
	17 Autorisasjonsliste
	18 Tempest risikovurdering
	19 KSS-L
	20

Figur 19: Innholdsfortegnelse for sikkerhetsdokumentasjon

Som det framgår i figur 19, er de dokumenterte sikkerhetstiltakene inndelt i fagområdene sikkerhetsadministrasjon, fysisk sikring, kryptosikkerhet og informasjonssystemsikkerhet. La oss se på de enkelte delene innenfor hvert fagområde

6.7.1 Sikkerhetsadministrasjon

Gir en helhetsoversikt over sikkerhetstiltakene i avdelingen. Normalt sikkerhetsleder sitt ansvar å oppdatere dokumentasjonen i denne mappen.

Godkjenning

Godkjenningsskrivet og kopi av framsendt søknad. Skal kontrolleres ved sikkerhetsinspeksjoner. Hensikten er å fjerne tvil om gyldighet av sikkerhetsgodkjenning. Godkjenningsstrategien hører også hjemme her dersom den foreligger hos avdelingen.

Grunnlagsdokument for sikkerhet

Kortfattet helhetsoversikt for avdelingens sikkerhetsgraderte informasjonssystemer og sikkerhetstiltak. Har henvisninger til mer detaljerte dokumenter innen de ulike fagområdene. Eierskap til dokumentasjon gjennom sikkerhetsorganisasjonen.

Beredskapsplan

Oversikt over kritiske ressurser og en tiltaksplan for hvordan ressursene skal opprettholdes eller gjenopprettes ved en beredskapssituasjon.

Instruks for sikkerhetsrevisjon

Bestemmelser for hvordan sikkerhetstiltak og sikkerhetsdokumentasjon skal oppdateres for å sikre at beskrevne rutiner er korrekte og etterleves.

6.7.2 Fysisk sikring

Instruks for adgangskontroll

Instruks for vaktansvarlig som kontrollerer atkomst til kontrollert, beskyttet og sperret område.

Autorisasjonsliste

Oversikt over alt autorisert personell som har adgang til området. Autorisasjon gis av avdelingssjefen, kontrolleres av vaktansvarlig.

6.7.3 Kryptosikkerhet

Kryptosikkerhetsinstruks

Lokal kryptosikkerhetsinstruks for kryptoforvalter. Bestemmelser for utøvelse av kryptotjenesten ved avdelingen. Utarbeides av kryptosikkerhetsleder.

Utnevnelser av kryptoforvalter og kryptosikkerhetsleder

Skriftlig utnevnelser med signatur.

Adgang til kryptorom

Skjema for kryptoautorisasjon. Oversikt over kryptoautorisert personell.

Nødmakuleringsplan

Beskrivelse av hva som skal makuleres, hvordan og i hvilken rekkefølge.

Brukerinstruks krypterte sambandsmidler (MRR)

Sikkerhetsbestemmelser som regulerer hvordan brukere av krypterte sambandsmidler skal håndtere utstyret.

6.7.4 Informasjonssystemsikkerhet

Brukerinstruks

Kortfattet sammendrag av sikkerhetsbestemmelser som angår brukere av informasjonssystemet.

Driftsinstruks

Kortfattet sammendrag av sikkerhetsbestemmelser som angår driftspersonell av informasjonssystemet.

Instruks for konfigurasjonskontroll

Konfigurasjonskontroll er nødvendig for å unngå at endringer i godkjent konfigurasjon medfører redusert sikkerhet eller tap av materiell. Skal også vise kommunikasjon og kabling, samt en konfigurasjonsoversikt.

Autorisasjon

Autorisasjonsskjema for brukere. Oversikt over autorisert personell.

Mediejournal

Oversikt som viser beholdning av lagringsmedier med sikkerhetsgradert informasjon

Tempestrisikovurdering

Et estimat på risiko for at sikkerhetsgradert informasjon kompromitteres ved elektromagnetisk stråling fra komponenter i informasjonssystemet.

Kravspesifikasjon for sikkerhet (KSS-L)

Kravspesifikasjon skal danne grunnlag for en felles forståelse mellom eier av informasjonssystemet og godkjenningsansvarlig. Skal vise hvordan eventuelle avvik mellom krav og tiltak håndteres lokalt.

6.8 Hvordan skrive Grunnlagsdokument for sikkerhet

Elevene skal anvende kunnskapen fra de to første dagene gjennom å utarbeide et utkast til grunnlagsdokument.

Hensikt og funksjon

Hensikten med grunnlagsdokumentet er å skille ut det vesentlige av sikkerhetsrelevant informasjon, for at leseren skal få et helhetlig overblikk. Dokumentet er en kortfattet oversikt som viser hva slags sikkerhetsgradert informasjon og informasjonssystemer som avdelingen disponerer. I tillegg fremkommer ansvar og inndeling i fysiske områder, samt en henvisning til fyldigere informasjon.

Praktisk oppgave

Utarbeidelse av grunnlagsdokument.

Gjennomgang og oppsummering

Presentasjon av ulike løsninger. Kommentarer til de enkelte forslagene.

6.9 Evaluering av opplæring

I forbindelse med gjennomføringen av Operasjonssikkerhet grunnkurs, ble det utdelt et evalueringsskjema (se vedlegg) til alle kurselevene. I tillegg ble respondentene bedt om å kategorisere sitt eget erfaringsnivå på følgende skala:

Nybegynner	0-1 års erfaring	N
Middels	1-3 års erfaring	M
Erfaren	3-5 års erfaring	Er
Ekspert	Over 5 års erfaring	Ex

Svaralternativene var 1 (lite god) til 5 (meget god) for hvert av spørsmålene. * indikerer utfyllende skriftlig kommentar (se vedlegg).

Figur 20: Kursevaluering resultater

	Sv 1	Sv 2	Sv 3	Sv 4	Sv 5	Sv 6	Sv 7	Sv 8	Sv 9	Sv 10	Sv 11	Sv 12	Sv 13	Sv 14	Sv 15	Sv 16
Kursdeltagers erfaringsnivå	N	Er	Ex	Er	Er	Ex	Ex	Ex			M	N	N	M	M	Ex
Helhetsvurdering av kurset	4	4	4	4	4	4	4	4	4	5	5	4	4	4	5	4
Vurdering av delmål 1	4	4	4	5	4	4	4	5	2	4	5	2	4		5	4
Vurdering av delmål 2	5	5	3	5	3	5	5	4	4	5	5	3	4	4	4	4
Vurdering av delmål 3	4	5	4	5	4	5	5	4	4	4	5	5	4	5	5	4
Vurdering av delmål 4	4	4	5	4	4	4	3	5	4	5	5	3	3*	5	5	4
Forpleining under kurset	5	4	5			4	3	5		5	5	4	3*	5		
Forlegning under kurset	5	3	5	5	5	4	4	4	5	5	5	4	5	3	5*	
Kursåpning	4	4	5		4	4	4	5	3	5	5	4	5	3	5	4
Kvalitet på klasserommet	4	4	5	5	4	4	4	5	4	5	3*	2	3*	4	5	3
Oppfølging generelt	4	4	5		4	4	5	5	5	5	5	3	4	4	5	
Oppfølging av kursleder		5	5	5	5	3*	5	5	5		5	3	5*	5	5	
Administrativt opplegg	4	4	5	5	5	5	4	5	5	5		4	4	4*	5	3
Vurdering av leksjon 1	4	4	3	5	2	4	4	4	3	5	5	3	4	4	3	4
Vurdering av leksjon 2	4	4	3	5	3	4	4	4	4	5	4	3	4	4	3	3
Vurdering av leksjon 3	4	4	3	5	4	4	5	4	3	5	5*	4	4	4	*	4
Vurdering av leksjon 4	4	4	4	4	3	3	3	4	4	5	4*	4	3	4	4	4
Vurdering av leksjon 5	4	3	4	4	4	4	3	4	4	5	5	3	3	3*	4	4
Vurdering av leksjon 6	4	3	3	4	3	4	3	4	3	5	4*	3	4	4	4	4
Vurdering av leksjon 7	4	4	4	4	3	4	3	3	3	4	5	4	3*	4	4	4
Vurdering av leksjon 8	5	3	4	4	3	4	5	4	4	5	5	2	3*	4	2*	4
Vurdering av leksjon 9	4	3	3	5	4	4	4	4	4	5	5*	3	4	4	4	4
Vurdering av leksjon 10	4	3	3	4	4	2	2	4	2	4	4*	3	3*	4	3	
Vurdering av leksjon 11	4	3	3	4	4	2	4	4	2	5	5	3	3*	4	4	4
Vurdering av leksjon 12	4	3	3	4	2	2	3	5	2	5	4*	3	3*	3	4	4
Vurdering av leksjon 13	4	3	4	4	3		4	3	4	5	5*	4	3*	3	3	4
Vurdering av leksjon 14		4	4	5	4	4	4	5	3	5	5			4*	5	4
Diskusjon ift forelesning	4		5	4	4	2*	5	5	5	5	5	4	3*	4*	3	4
Vektlegging av emner	4		4	4	4	5	4	4	4	5	5	4	4	4	3*	4
Praktisk nytte av kurset	4		5	5	4	5	4	5	5	5	5	5	2*	5*	3	4
Kommentarer til kurset	*		*		*	*		*		*	*	*		*	*	

Det ble benyttet et standard kursevalueringsskjema som brukes ved Utdannings- og kompetansesenter for Hærens samband, noe som kan forklare hvorfor enkelte spørsmålsformuleringer ikke er direkte relevant for denne rapporten.

Kurset fikk gjennomgående positiv respons fra kursdeltakerne. Hovedinntrykket var at kurset egnet seg godt til formålet som var å gi en innføring i risikohåndteringsprosesser rundt et informasjonssystem. Et utvalg tilbakemeldinger uttrykte følgende:

> *"Veldig bra kurs for å få inn prosesser og hva som er viktig i forhold til dokumentasjon."* (Ekspert)
>
> *Nyttig kurs som en bør forsøke å markedsføre ovenfor ansvarlige ledere."* (Middels)
>
> *"Meget bra innhold og gjennomføring!"* (Middels)
>
> *"Hovedinntrykket virker svært bra!"* (Nybegynner)

> *"Sitter igjen med et godt inntrykk og klart økt forståelse av fageltet."* (Nybegynner)

Erfaringsnivået til kildene er satt i parentes. I spørreundersøkelsen som ble gjennomført er eksakte svarverdier gjengitt i kapittel 5, hvor det også framgår kriterier for fastsetting av erfaringsnivå. Svaralternativene var 1 (lite god) til 5 (meget god). På spørsmål om helhetsvurdering vurderte samtlige kursdeltakere det til 4 eller 5. Med andre ord har kurset truffet med hovedinnholdet i forhold til målsettingen som var formulert slik:

> "Kurset skal kvalifisere kursdeltakere til å fylle roller i virksomhetens sikkerhetsorganisasjon. Etter gjennomført kurs skal deltakerne være i stand til å håndtere risiko for et sikkerhetsgradert informasjonssystem."

Deretter ble deltakerne spurt om å vurdere måloppnåelse i forhold til de fire delmålene for kurset. Siste spørsmål var om hvilken praktisk nytte kursdeltakerne forventet å få ut av kurset i sin nåværende jobb. Svarene framgår i tabellen under.

Figur 21: Vurdering av måloppnåelse og nytteverdi

Spørsmålstekst	**1**	**2**	**3**	**4**	**5**
Helhetsvurdering av kurset.	0	0	0	13	3
Vurdering av delmål 1. En helhetlig forståelse av dokumentasjonen som ligger til grunn for den sikkerhetsmessige godkjenningen.	0	2	0	9	4
Vurdering av delmål 2. Å forstå hensikten med risikovurdering og sikkerhetstiltak som iverksettes for å møte relevante trusler, sårbarhet, risiko og tiltak.	0	0	3	6	7
Vurdering av delmål 3. Å kjenne sammenhengen mellom trusler, sårbarhet, risiko og tiltak.	0	0	0	8	8
Vurdering av delmål 4. Å forstå hvordan sikkerhetstiltak og sikkerhetsdokumentasjon skal revideres og betydningen av at tiltakene etterleves	0	0	3	7	6
Forventer du å få praktisk nytte av kurset i den jobben du har nå?	0	1	1	4	9

Som en forklaring til hvorfor vedkommende hadde krysset av 2 for nytteverdi ble det skrevet følgende forbehold:

> *"Har hatt lite å gjøre med infosystemer, slik at nytteverdien får jeg verifisert når jeg kommer hjem."* (Nybegynner)

Det tolkes av oss som et godt tegn at kursdeltakere har et kritisk utgangspunkt til nytteverdien av kurset. Litt av hensikten med evalueringen var å avdekke forhold som kunne løftet kurset. I forbindelse med kursavslutningen ble det gitt en felles tilbakemelding som ble fremført av eldste elev. Elevene pekte på følgende forhold:

> "*Undervisning var meget bra generelt, og det oppfattes positivt at undervisningstekniske virkemidler ble variert. Det ville hevet kurset om det var gjort tilgjengelig et dokumenthierarki som viste hvor en kan finne maler og informasjon for å lage lokal dokumentasjon. Videre bør det klargjøres hem*

som har ansvar for å utarbeide de ulike dokumentene. Andre momenter som kom fram i plenumsdiskusjonen var:

- *Ikke forutsett ekspertnivå blant elevene.*
- *Noen savner maler for sikkerhetsdokumenter.*
- *Kurset var til tider litt vel akademisk opplagt.*
- *Noe mer tid til oppgaver.*
- *Det bør henvises til konkrete paragrafer*

Kurset bør gjøres kjent for hele Forsvaret ved en felles adressegruppe. Det er mange som bør gjennomgå et slikt kurs. "

Det ble gjennom tilbakemeldingene klart at ulike forutsetninger blant kurselevene påvirket oppfattelsen av innholdet. Prosessfokus under kurset ble av de fleste oppfattet positivt. Men for noen ble innholdet til tider for teoretisk og akademisk i forhold til egen erfaringsbakgrunn.

"Generelt høyt nivå på kursforelesere, deltakere og faglig innhold. Formuleringer og diskusjoner bør forventes å være på et lavere nivå når kursdeltakere ikke har så solid bakgrunn i faget som dette kurset." (Nybegynner)

"Noe teoretisk, akademisk, men veldig fin prosess." (Ekspert)

I følge OPSEC doktrinen [16] er OPSEC en prosess, ikke et sett med regler som er gyldige til en hver tid. Det er nettopp derfor OPSEC metoden egner seg til å forstå hensikten med sikkerhetstiltak. Dette står imidlertid i motstrid til et ønske om å få ferdige utarbeidede løsningsforslag til hvordan sikkerhetstiltakene skal dokumenteres. Slike ønsker kom også til uttrykk i tilbakemeldingene:

"For mye overflatisk synsing. Kurset bør i større grad fokusere på konkrete verktøy (Ringperm med sikkerhetsdokumentasjon). Dagens gjennomgang blir overflatisk teoretisk. Savner konkrete eksempler som er gjennomarbeidet (Skolens løsning)" (Middels)

"Teoretisk bra, men ønsker mer praktiske eksempler … veldig høytsvevende og teoretisk … lite engasjerende, men budskap ok… Litt på siden av mitt nåværende fagfelt, men en del temaer er klart aktuelle… " (Nybegynner)

Dette illustrer paradokset i denne oppgavens problemstilling: Dersom forutsetningene for å stole på sikkerheten til et informasjonssystem fremgår av sikkerhetsdokumentasjonen, kan en stole på at innholdet er kjent og forstått av de ansvarlige om sikkerhetsdokumentene er ideelle fasitsvar? Spesielt gjelder dette i tilfeller hvor en vet at de ansvarlige har erfaringsnivå som nybegynnere eller middels. En av deltakerne foreslo følgende forslag til løsning som kan adopteres som et ideal for framtidige kurs:

"Ta utgangspunkt i mal – utdype detaljer – vise mangfold i løsninger slik at malen likevel ikke blir fasit." (Nybegynner)

Et annet poeng som kom fram var behovet for å klargjøre ansvarsdeling i sikkerhetsarbeid generelt og dokumentering av de ulike sikkerhetstiltakene.

"Et ønske om en time hvor ansvar diskuteres." (Erfaren)

> *"En dobbelttime om ansvarsplassering er ønskelig. Kurset må gi eleven noe 'handfast' å ta med seg hjem."* (Ekspert)
>
> *"Det børe opplyses om hva sikkerhetsledere kan få gratis av instrukser."* (Erfaren)
>
> *"Kan være noe mer konkret når det gjelder henvisninger og eksempler. Særlig på fremtidige kurs med middels til nybegynner som nivå."* (Ekspert)
>
> *"Kunne godt ha innehold mer om dokumentasjonen rundt S-arbeid, siden enkelte deltakere ikke er helt på topp når det kommer til akkurat dette."* (Nybegynner)

Dette er alle gyldige momenter som må tas hensyn til dersom en ønsker å forbedre undervisningen som et virkemiddel for å kunne stole på at forutsetningene for et sikkerhetsnivå ikke endres som følge av endringer i omgivelsene. Når en, som i dette tilfellet, velger å inngå et kompromiss mellom innhold og tid til rådighet, sier det seg selv at ikke alle faktorer kan bli belyst tilstrekkelig i løpet av to og en halv dag.

En mulighet er følgelig å differensiere målgruppen ytterligere og skreddersy opplæring i risikohåndtering ut fra tid til rådighet og hvilken funksjon den enkelte skal ha. Dette kurset har vist en måte å dokumentere risikohåndtering av informasjonssystemer.

Kapittel

7 Fastsetting av signifikansnivå

I dette kapitlet drøftes det i hvilken grad det går an å skille mellom signifikante avvik og naturlig varians når en skal vurdere ulike endringer i forutsetningene for et informasjonssystem. Med utgangspunkt i om sikkerhetsmessige godkjenninger har betydning for den reelle sikkerheten, vil det bli satt fokus på hvem som skal avgjøre i hvilken grad et avvik er signifikant.

7.1 Innledning

Opp mot problemstillingen som er hvordan en kan stole på om forutsetningene som ligger til grunn for et sikkerhetsnivå er gyldig etter endringer i omgivelsene, er det nødvendig å undersøke signifikansnivå for endringer. En kan tenke seg at noen endringer ikke får konsekvenser for sikkerhetsnivået. Slike endringer kan karakteriseres som en naturlig varians som ikke bare er akseptabel, men en nødvendig forutsetning for at informasjonssystemet skal kunne fungere over tid. Komponenter går i stykker og må skiftes ut, medarbeidere skifter arbeidsplass og programmer oppdateres for bedre ytelser. Endringer er med andre ord ikke bare noe uønsket og forstyrrende i et velfungerende og levende system, men noe som bidrar til å opprettholde tilgjengeligheten av tjenester. Tilgjengelighet er en av de grunnleggende informasjonssikkerhetsegenskapene.

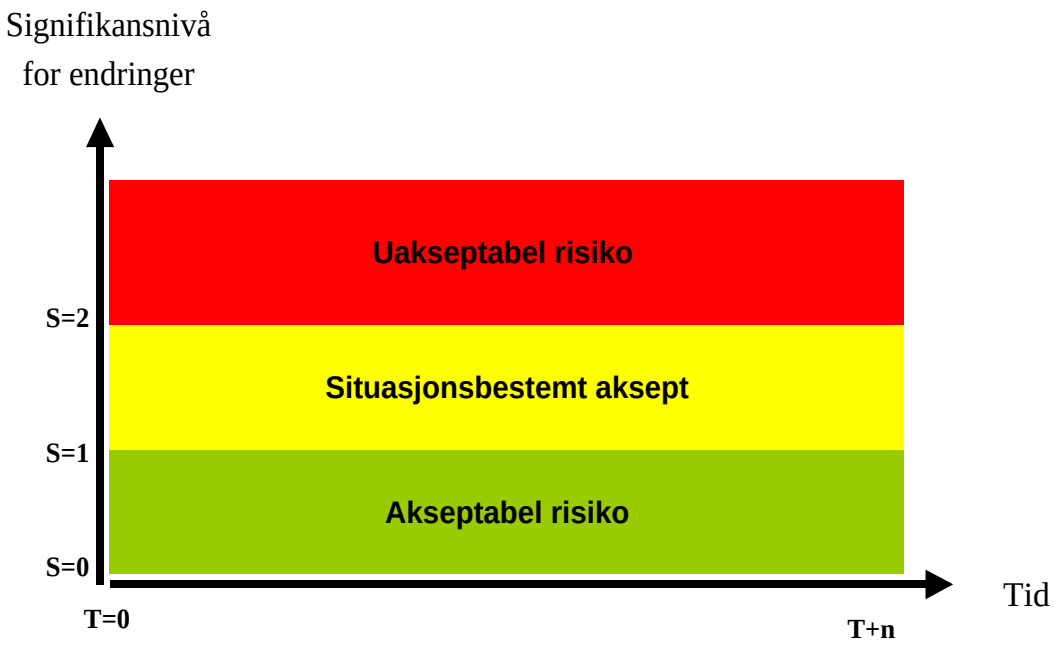
- Hva er et signifikant avvik fra forutsetningene?
- Kan det i noen tilfeller være situasjonsavhengig hvorvidt avviket er signifikant eller ikke?
- Hvem skal i så fall avgjøre om et avvik er signifikant eller ikke?

Dette er spørsmål som søkes besvart i dette kapitlet.

Som et utgangspunkt for drøftingen, har vi laget en figur som viser avvik og tid på to akser. Vi tror at det er viktig å avdekke signifikante avvik så hurtig som mulig, slik at reaksjonstiltak kan iverksettes på et tidlig stadium for å begrense et mulig skadeomfang. Vi

tror også at det er viktig at mindre avvik ikke rapporteres på samme måte som signifikante, fordi det vil skape støy og fjerne fokus fra det som har størst betydning for sikkerheten.

Figuren under viser en inndeling i tre nivåer. Dersom avviket kan betegnes som en naturlig varians, vil det på skalaen i figuren være mellom S0 og S1. Et signifikant avvik vil være større eller lik S2.



Figur 22: Signifikansnivå av endringer over tid

En tradisjonell tilnærming til å kontrollere om forutsetningene for sikkerhetsnivået fremdeles er gyldig etter en tid er gått, er å gjennomføre sikkerhetsrevisjoner ved fastsatte perioder. Det kan være ved T= 1 år, T= 3 år eller andre tidsperioder. Ved å gi et stort antall aktører kompetanse i risikohåndtering, mener vi signifikante avvik kan oppdages langt raskere enn ved årlige revisjoner. Dersom det gjennomføres kontinuerlige risikovurderinger av personer som har blitt gitt nødvendig opplæring mener vi det vil øke tilliten til at sikkerheten blir ivaretatt også etter endringer har funnet sted.

Men før vi tar stilling til hvilke avvik som er signifikante, vil det være naturlig å drøfte hvorvidt en formell sikkerhetsmessig godkjenning har en reell innvirkning på sikkerhetsnivået i et informasjonssystem.

7.2 Betydning av sikkerhetsmessig godkjenning

Er sikkerheten bedre ivaretatt for systemer som har gjennomført en sikkerhetsgodkjenning? Har det noen reell betydning for sikkerheten at en godkjenning foreligger? Eller kan det tenkes at sikkerhetsnivået er uavhengig av formelle godkjenninger? En representant fra NSM uttalte på generelt grunnlag, og ikke nødvendigvis bare om Forsvarets systemer følgende:

> *"Det er et gjennomgående trekk at det mangler godkjenning på systemene. Som regel er det slik at når det formelle mangler er også sikkerheten dårligere fordi en ikke har et bevisst forhold til sikkerhet. Det er to sider av samme sak."*

Sikkerhetsgodkjenningsprosessen gir med andre ord større oppmerksomhet rundt sikkerhetsspørsmål og bidrar til økt sikkerhetsbevissthet. Sett i dette lyset vil en sikkerhetsgodkjenning en betydning for sikkerhetsnivået. Sikkerhetseksperten utdyper nærmere:

> *"Ved sikkerhetsinspeksjoner avdekker vi at det ikke foreligger sikkerhetsgodkjenning. Det er som oftest dokumentasjon og godkjenning som mangler. Vår erfaring tilsier at det er en sammenheng mellom en formell sikkerhetsgodkjenning og det faktiske sikkerhetsnivået ved en virksomhet."*

På spørsmål om hvorfor det ikke foreligger en sikkerhetsgodkjenning av systemer som det i Sikkerhetsloven stilles krav til skal godkjennes, ble det svart:

> *"Hovedårsaken er manglende opplæring. De visste ikke hva som lå i en godkjenning og hva som må være på plass før en godkjenning kan utstedes. Videre skyldes det dårlig forankring av sikkerhet i organisasjonen. De ansvarlige har ikke spurt om råd, noe som gjelder på alle nivåer."*

Manglende opplæring blir igjen trukket fram som en årsak, og behov for kurs av typen som er beskrevet i et tidligere kapittel er åpenbart. Dette gjelder ikke bare i Forsvaret og Forsvarets systemer, men også for aktører utenfor Forsvaret som må forholde seg til Sikkerhetsloven.

Knappe ressurser og prioritering av det som oppfattes å være mest nødvendig for å uføre oppgavene som påhviler organisasjon kan være en mulig forklaring på hvorfor det ikke er startet en sikkerhetsgodkjenningsprosess.

> *"Ressursmangel er en annen mulig årsak til manglende prioritering av sikkerhet."*

En annen forklaring kan i følge eksperten være at det er et stort antall regelverk og aktører å forholde seg til.

> *"Det er mange regelverk og aktører på sivil side, og det er vanskelig å orientere seg om hva som er viktig når det er mange krav og aktører å forholde seg til."*

Denne uttalelsen viser at godkjenningsmyndighetene har forståelse for at det oppleves som vanskelig for systemeiere å vite hva som kreves av tiltak for å få systemet sikkerhetsgodkjent. Dette er forhold som NSM jobber med for å forbedre gjennom å forbedre eksisterende veiledninger som er gjort tilgjengelig på Internett.

> *"Det største problemet i sivil sektor er manglende verdivurdering av informasjonen. Da vet de ikke at de er omfattet av sikkerhetsloven heller."*

Verdivurdering er i OPSEC modellen ansett som forutsetningen for det videre risikohåndteringsarbeidet. Når en ikke har verdivurdert informasjonen rett, er det heller ikke mulig å fastslå et korrekt risikobilde. Verdivurdering av informasjon er noe som bør vektlegges ved senere anledninger, og vil bli tatt opp som et moment til videre arbeid.

Som en midlertidig ordning, kan det utstedes en midlertidig brukstillatelse under forutsetning av at forhold som ikke er på plass enda blir utbedret i løpet av perioden.

> *"Vi må i større grad ta i bruk sanksjoner (eks kutte forbindelser) for å understreke alvoret ved mangelfulle sikkerhetstiltak. Vi gir midlertidig brukstillatelse med en frist for å utbedre forhold som ikke er tilfredsstillende."*

Dette har ikke alltid fungert etter intensjonen. Intervjuobjektet utdyper hvorfor det er nødvendig å vurdere sanksjonsmidler.

> *"Av og til har et system hatt en midlertidig brukstillatelse som har gått ut på dato. Da har alle trodd at sikkerhetsgodkjenningen har vært i orden og det har kanskje blitt en sovepute for de sikkerhetsansvarlige."*

Representanten fra NSM sier det fra godkjenningsmyndighetenes side er ønskelig å få ned antall midlertidige brukstillatelser for å kunne gjøre seg ferdig med godkjenningsprosessen.

> *"Veldig mange systemer har midlertidig brukstillatelse. Vi sjekker om krav er oppfylt og om det er gjort en risikohåndtering av avvik. Så lenge systemeier godtar avvik, skal det mye til for at vi overprøver det."*

Her er det viktig å skille mellom godkjenning av referanseløsninger og godkjenning for operastivt bruk. Det er NSM som setter akseptkriterier for godkjenning av referanseløsninger. Systemeiere kan sette akseptkriterier for godkjenning til operativt bruk. Sikkerhetseksperten fra FLO uttaler:

> *"Hvem avgjør om restrisikoen er akseptabel? Det kommer an på om det dreier seg om typegodkjenning eller operativ bruk. Jeg har erfart flere ganger at vi ikke får aksept for det nivået vi legger oss på hos NSM."*

Intervjuobjektet uttalte seg om godkjenning av referanseløsninger. Setter NSM for strenge krav til sikkerhetsgodkjenning og er det NSM som bør sette akseptkriteriene?

> *"Det er kanskje FSA som i større grad burde hatt myndighet til å legge lista i Forsvaret. Jeg synes NSM bør være strenge når det gjelder krav for ellers har det ikke noen verdi. Forsvarets systemer har et sterkere fokus på need to know systemteknisk sikring enn sivile.*

Eksperten i NSM utdyper hvordan godkjenningsmyndigheten ønsker at signifikansnivå skal beskrives:

> *"Det vi ønsker er at representanter for systemeier beskriver hvilke endringer som kan gjøres innefor rammen av godkjenningen, og hvilke endringer som eventuelt ikke kan gjøres. Har en konkret sak nå hvor det er beskrevet hva som kan gjøres innenfor godkjenningen."*

Dette avsnittet har vist at sikkerhetsgodkjenning av informasjonssystemer i følge informasjonskildene til denne oppgaven har en betydning for sikkerhetsnivået, og at formell godkjenning og sikkerhetsnivå kan sies å være to sider av samme sak. Dermed kan det være grunnlag for å hevde at manglende formell godkjenning av informasjonssystemet innebærer et dårligere sikkerhetsnivå og et signifikant avvik fra forutsetningene som legges til grunn. Manglende verdivurdering av informasjonen gjør at mange aktører utenfor Forsvaret ikke forstår at de kommer inn under Sikkerhetslovens bestemmelser og krav til at systemet skal ha en sikkerhetsmessig godkjenning. Sikkerhetsgodkjenning er først og fremst en bevisstgjøringsprosess som skal øke tilliten til at sikkerheten for informasjonssystemet er ivaretatt.

Men det er også et annet inntrykk som har festet seg ved sikkerhetsgodkjenninger som bør nevnes. Når det gjennomføres en evaluering av godkjenningsmyndigheter, kan det virke

som om at sikkerhetsdokumentasjon får en egenverdi i kraft av at den utgjør vurderingsgrunnlaget, framfor det å være et middel for å dokumentere sikkerhetstiltak. Vi får dermed en fordreining hvor middelet blir til målet. Brukere tror sikkerhetstiltak skal beskrives for å tilfredsstille godkjenningsmyndigheter, og mister dermed fokus på hva som er det vesentlige i sikkerhetsarbeidet – å ivareta sikkerheten av egeninteresse, ikke det å tilfredsstille en ekstern aktør.

7.3 Hvem avgjør om et avvik er signifikant?

Opp mot problemstillingen for denne oppgaven som handler om fastslå hvorvidt forutsetningene for sikkerhetsnivået er gyldige etter endringer, er det nødvendig å identifisere aktører som kan gjøre endringer. Det er også nødvendig å identifisere aktører som må ta stilling om til oppståtte og uforutsette endringer er signifikante i forhold til akseptkriteriene som er fastsatt. En sikkerhetsekspert forklarte ansvarsforholdet i Forsvarets militære organisasjon slik:

> *"I FMO er det Forsvarsstaben som kan endre akseptkriterier. FSA legger fram risikovurdering for forsvarsstaben som tar beslutning om akseptkriterier. Forsvarsstaben på vegne av forsvarssjefen kan regnes som systemeier. De har også et eget konfigurasjonsråd i FST."*

Systemeiere er ansvarlig for sikkerheten og kan endre akseptkriterier innenfor rammen av referanseløsningen som er godkjent av Nasjonal sikkerhetsmyndighet. Men i praksis er det ofte lokalt personell som må ta stilling til avvik som oppstår. En av sikkerhetsekspertene uttalte følgene:

> *"Det er lokal datasikkerhetsleder som skal gjøre disse vurderingene. Dersom han er i tvil, går han til prosjekt sikkerhetsleder."*

Prosjektsikkerhetsleder er den som er ansvarlig for at sikkerhetskrav og tiltak blir implementert i informasjonssystemet i prosjektfasen. En annen sikkerhetsekspert uttalte følgende om kravspesifikasjon for sikkerhet:

> *"KSS utarbeides av prosjektsikkerhetsansvarlig. I teorien er det prosjektsikkerhetsleder som har ansvar for å forankre sikkerhet i systemet. Dette svikter ofte når det gjelder litt større systemer fordi det er for dårlig dialog mellom systemutviklere og sikkerhetsansvarlig når det gjelder den tekniske sikkerheten."*

Vedkommende hadde førstehånds erfaring fra prosjekter for materiellanskaffelser av informasjonssystemer.

> *"Vi har også eksempler på at industrien som skal levere informasjonssystemer som skal sikkerhetsgodkjennes mangler kompetanse for å implementere sikkerhetskrav som har vært godt beskrevet i en kravspesifikasjon for sikkerhet. Det er meningen at systemeier beskriver sikkerhetskrav, mens leverandør beskriver sikkerhetstiltak og testing."*

Dette viser at det også hos industrien som utvikler systemene har manglende kompetanse inne sikkerhet.

> *"I et bestemt prosjekt måtte industrien leie inn konsulenter for å ta seg av KSS momenter. Det er to godkjente konsulentfirmaer som gjør dette, Systemsikkerhet og Norconsult."*

Tilbake til datasikkerhetsleder som etter systemet er tatt i bruk må ta stilling til avvik for å fastsette signifikansnivå.

> *"En DSL har i dag i mange tilfeller ikke forutsetning for å foreta risikovurdering fordi vedkommende mangler opplæring."*

Behovet for opplæring er et stadig tilbakevendende tema, og det henvises til kurset i risikohåndtering som ble testet i forrige kapittel. Det er behov for å søke støtte i mange tilfeller:

> *"Hvis ikke prosjektsikkerhetsleder eksisterer, må en søke råd hos NSM. FSA bør vurdere det for Forsvarets avdelinger. Regionale områder kanskje?"*

Dette synet deles også av representanten fra FSA, som også hadde tenkt seg en større sentralisering for å skape sterkere fagmiljøer i forhold til enkeltpersoner ute ved avdelinger.

> *"Vi er ikke fornøyd med tilstanden til nå. Sikkerhetsorganisasjonen har vært fragmentert og lite kommunikasjon har flytt mellom enheter. Dette prøver vi aktivt å forbedre nå bl a gjennom å formalisere horisontal samarbeid og organisasjonsendring. På personellsikkerhet er alle stillinger blitt dratt inn til oss. Tidligere ble det utført av mange aktører rundt om i Forsvaret. Egentlig en sentralisering av sikkerhetsoppgaver. Mer enhetlige løsninger og mer kosteffektivt."*

Dette viser at en sentralisering av sikkerhetsfunksjoner blir vurdert som et virkemiddel for å styrke fagmiljøene. Det er datasikkerhetsleder som skal ta stilling til om et avvik er signifikant i forhold til forutsetningene som gjelder for informasjonssystemet. Vi har sett at prosjektsikkerhetsansvarlig skal sørge for at sikkerhetskrav og tiltak blir implementert i informasjonssystemet under prosjektfasen. Videre har det vært eksempler på at det også hos industrien som skal produsere informasjonssystemet vært mangelfull kompetanse for å tilfredsstille krav i henhold til Sikkerhetsloven. Opplæring av alle aktørene som må ta stilling til om avvik er signifikante eller ikke blir pekt på som et viktig virkemiddel av kildene for denne oppgaven.

7.4 Hva er signifikante endringer av forutsetningene?

Et viktig spørsmål i forhold til denne oppgavens problemstilling er å klargjøre hvilke endringer som er signifikante avvik i forhold til forutsetningene. Når er forutsetningene ikke lengre gyldige? Det er tidligere avdekket at det ofte omtales at "vesentlige endringer som kan påvirke sikkerhetsnivået" krever ny sikkerhetsgodkjenning.

Sikkerhetseksperter ble spurt og ordla seg på følgende måte:

> *"Ofte er det en subjektiv vurdering som må foretas og en må spørre hva som regnes som en vesentlig endring."*
>
> *"Det tas individuelt i hvert tilfelle."*
>
> *"Systemeiere må vurdere i hvert tilfelle. Sikkerhetsloven beskriver minimumskrav."*

Fellesnevneren er at det må vurderes i hvert enkelt tilfelle. Vi tror at det hadde vært enklere å gjøre disse vurderingene om det hadde vært spesifisert mer nøyaktig fra systemeier hvilke typer endringer som faller inn i henholdsvis grønt, gult og rødt område i figur 20.

Da ville grunnlaget for en risikovurdering blitt mer konkretisert og økt sannsynligheten for en ensartet vurdering av tilsvarende endringsvariabler. Dette ville igjen ledet til at grunnlaget for å stole på at forutsetningene for sikkerhetsnivået er gyldig etter endringer har skjedd i omgivelsene.

Det er med andre ord svært vanskelig og lite hensiktsmessig å definere eksakte avvik som kan plasseres inn i figur 20. Men det er likevel noen egenskaper ved endringer som lar seg beskrive og kategoriseres i forhold til om det regnes som vesentlig eller ikke. Sikkerhetseksperter ble bedt om å gi eksempler på signifikante endringer og svarte:

> *"Organisasjonen kan være det for eksempel dersom sikkerhetsledd fjernes. Litt interessant nå fordi FLO er i endring. Har på papiret mange sikkerhetspersonell, men mange stillinger er vakante."*

Dette er et interessant fenomen som har gyldighet for alle organisasjoner som driver omstilling i effektiviseringens navn. Sikkerhetsfunksjoner som inngår som en integrert del av forutsetningene, kan ikke fjernes uten videre. Det vil helt klart påvirke gyldigheten om sikkerhetspersonell forsvinner. Et annet fenomen er rekruttering av nye medarbeidere, når noen slutter.

> *"Vi tillater utskiftinger av personell relativt ukritisk relatert til sikkerhet. Det er et veldig fokus på å fylle stillinger. Det stilles ikke krav til sikkerhet, men andre krav som gjennomført stabsskole og relevant tjenesteerfaring."*

Når det gjelder teknologi, blir operativsystemet pekt på som en vesentlig endring. En ekspert uttalte seg slik:

> *"Bytting av operativsystem krever ny godkjenning. Det er opp til systemeier om applikasjoner over operativsystemet skal endres eller installeres. Det må i så fall foretas en risikovurdering før en endring av applikasjoner implementeres."*

Programmer som legges inn oppå operastivsystemet, skal vurderes i hvert enkelt tilfelle.

> *"Alle applikasjoner som skal legges inn på en godkjent plattform, skal gjennomgå en sikkerhetsvurdering og godkjenning."*
>
> *"Større systemer har en godkjenningsstrategi. Der beskrives hva som er tillatt. Større endringer krever en ny godkjenning som for eksempel*
>
> - *Utskifting av servere*
> - *Bytte av operativsystemer. Men ikke patcher.*
> - *Når en tar i bruk nye lokaler skal det også godkjennes.*
> - *Bygningstekniske endringer krever ny godkjenninger.*
> - *Når en ugradert telefon blir installert nært en hemmelig PC – Avstandskrav på 1 meter.*
> - *Men økning i antall PC-er i godkjente områder kan installeres.*
> - *Flytting av PC går greit innenfor samme området."*

Som det fremkommer av svarene, er det ikke enkelt å vurdere signifikansnivå for endringer som gjelder teknologi. Det vises til at det må gjøres selvstendige vurderinger i hvert tilfelle. Slike vurderinger krever innsikt og kompetanse som er mangelvare hos mange av aktørene som skal gjennomføre risikovurderinger. Igjen er det behov for opplæring og kurset som er beskrevet i tidligere kapittel kan være et virkemiddel for å høyne kompetansenivået.

7.5 Betydning av konfigurasjonskontroll

Opp mot problemstillingen som er hvorvidt en kan stole på om forutsetningene er gyldige etter endringer er det nødvendig å undersøke betydningen av å opprettholde en form for konfigurasjonskontroll. I forhold til figur 22, kan det tenkes at små endringer ikke har betydning for sikkerheten siden det regnes som en naturlig varians. Slike endringer vil være innenfor det grønne området i figur 22. Kan en tillate at små endringer gjøres uten at det går ut over forutsetningene?

> ”*Man må ha en oppdatert oversikt over hva en har og hvor en har det. Hvis en ikke har kontroll, kan forutsetningene være brutt”*
>
> Sikkerhetsekspert ved
> Forsvarets Logistikkorganisasjon

Figur 23: Konfigurasjonskontroll som en forutsetning

En av sikkerhetsekspertene peker på konfigurasjonskontrollen som en viktig forutsetning for i det hele tatt å kunne stole på at forutsetningene som ligger til grunn for sikkerhetsnivået ikke er brutt.

> *”Forutsetningen er god konfigurasjonskontroll som kommer til uttrykk gjennom Instruks for Konfigurasjonskontroll. Konfigurasjonskontroll innebærer alt, både mennesker, maskiner og organisasjon. Dette innebærer at den som er datasikkerhetsleder må vite hva som kan godkjennes av endringer, noe som igjen forutsetter et vist kompetansenivå.”*

Sett i lys av dette utsagnet, skulle en tro at konfigurasjonskontroll kan være en indikator på om forutsetningene er gyldige. Kanskje mangelfull konfigurasjonskontroll er et signifikant avvik?

> *”Jeg vet at det slurves med konfigurasjonskontroll. Det er vesentlig at en gjør det fordi god konfigurasjonskontroll er en forutsetning for å opprettholde sikkerhet. Spesielt mediehåndtering, merking og journalføring. Jeg tror det er mye å hente på dette området ute blant avdelingene. Kan skyldes manglende opplæring, tid og holdning.”*

Dette er konkrete forhold som kan operasjonaliseres inn i en metrikk, hvor manglede merking eller journalføring kan gis en vekting i forhold hvor alvorlig manglene anses å være. Når NSM gjennomfører inspeksjoner, brukes et inspeksjonsskjema [38] hvor slike

forhold blant annet inngår. Det hadde vært interessant å undersøke om skjemaet kan brukes som en del av en metrikk hvor de ulike forholdene vektes og summen av alle forholdene gir en verdi som kan indikere hvorvidt forutsetningen er brutt eller ikke. I dag gjøres en kvalitativ analyse, som ikke er poengbasert. Dette bør imidlertid undersøkes i senere arbeider.

Et annet poeng som kom fram under intervjuene var forskjellen mellom hardware og software endringer. En av ekspertene uttalte:

> *"Hardware er synlig og dermed lett og kontrollere for om det er gjort endringer. Dette medfører et større fokus på HW enn andre forhold."*
>
> *"Software er mindre synlig og det opereres ofte med flere SW versjoner, tilleggsprogramvare og ulik konfigurering. Dersom en for eksempel mangler tegneprogrammet VISIO legger en inn det, uten å sikkerhetsmessig vurdere effekten."*

Hensynet til ytelse og funksjonalitet er ofte motivasjonen bak konfigurasjonsendringer i forhold til opprinnelig utgangspunkt.

> *"Det samme gjelder konfigurering, hvor det ofte omkonfigureres for å oppnå ytelse og funksjonalitet. Det er min erfaring at vi tolerer større endringer for SW enn HW fordi det er mindre synlig."*

Når det gjelder sikkerhetsgodkjenning i forhold til endringer kommenterte en sikkerhetsekspert fra NSM følgende:

> *"Vi må se på måten vi gir sikkerhetsgodkjenninger på. Det vil antakelig være bedre om vi gir en sikkerhetsgodkjenning uten tidsbegrensning, men krever ny godkjenning ved endringer som påvirker sikkerheten i systemet. Hensikten er å ha fokus på om endringer påvirker sikkerheten."*

Vi har sett at god konfigurasjonskontroll er nødvendig for å kunne stole på at forutsetningene er gyldig over tid. Det er ofte lettere å godta softwareendringer siden konsekvensene er mindre synlige i forhold til hardware endringer. Mangelfull oversikt og kontroll er ikke tillitsvekkende. Kontroll over egen kritisk informasjon er en nødvendig forutsetning for å fastsette risiko. Det er særlig viktig i et dynamisk miljø, hvor endringer i trusselbildet og introduksjon av nye sårbarheter gjennom utskiftinger påvirker risikobildet på en måte som vanskelig kan forutsees hundre prosent. En kan tenke seg at de tre sirklene i figur 4 som representerer kritisk informasjon, trusler og sårbarheter beveger seg i forhold til hverandre. Dette kan illustrere hvorfor det må gjøres en kontinuerlig vurdering av faktorene for å fastslå risiko og hvorfor det er så vanskelig å peke ut konkrete avvik som vil være signifikante.

Kapittel

8 Konklusjon

Denne rapporten har vist hvordan en kan ta stilling til om forutsetningene som ligger til grunn for en sikkerhetsmessig godkjenning fortsatt er gyldig etter omgivelsene til et informasjonssystem har endret seg. Sikkerhetstiltak skal være dokumentert og en kontroll av dokumentasjonen og om denne stemmer overens med faktiske forhold utføres for å fastslå om en kan stole på om forutsetningene er gyldige eller ikke.

Gjennom en opplæring av beslutningstakere, stabsmedarbeidere og sikkerhetspersonell i risikohåndtering av informasjonssystemer basert på operasjonssikkerhetsmodellen, vil de bli bedre rustet til å forstå hensikten med de forskjellige sikkerhetstiltakene som utgjør forutsetningen for sikkerhetsgodkjenningen. Sikkerhetstiltakene må være dokumentert for at systemeiere, godkjennings og kontrollmyndigheter skal kunne stole på gyldigheten av forutsetningene. Dokumentasjonen må gjenspeile faktiske forhold, og oppdateres jevnlig av de personene som fyller de ulike rollene i en avdelings sikkerhetsorganisasjon. Denne rapporten har avdekket tilfeller hvor sikkerhetsdokumentasjonen ikke har gjenspeilet faktiske forhold, har vært for omfattende og i det hele tatt lite egnet til det formålet den egentlig skal fylle. Sikkerhetsdokumentasjon får lett en symbolverdi framfor å være et verktøy for aktører som anvender informasjonssystemene. Opplæring av nøkkelpersoner er et virkemiddel som kan motvirke dette.

For å kunne fylle en sikkerhetsrolle tilfredsstillende, må det stilles kompetansekrav til dem som blir utpekt. Denne oppgaven har avdekket at det i praksis ikke stilles formelle krav til sikkerhetsopplæring ut over fagfeltet kryptosikkerhet. Det bør tilbys kurs i risikohåndtering av informasjonssystemer slik at de som skal fungere i roller i en sikkerhetsorganisasjon får nødvendig opplæring.

For å ha en helhetsoversikt over sikkerhetstiltakene ved en lokal avdeling, stilles det i Forskrift om sikkerhetsadministrasjon krav til at det utarbeides et Grunnlagsdokument for sikkerhet. Dette dokumentet skal gi nødvendig oversikt, og henviser til andre sikkerhetsdokumenter hvor en mer detaljert beskrivelse av sikkerhetstiltakene innen de ulike fagområdene. Erfaringer fra arbeidet med denne oppgaven har vist at det kan være hensiktsmessig å gruppere sikkerhetsdokumentasjon inn i fagområdene sikkerhetsadministrasjon, fysisk sikkerhet, kryptosikkerhet, og informasjonssystemsikkerhet. Da kan ansvar for oppdatering av de ulike dokumentene tilfalle de ulike rollene i sikkerhetsorganisasjonen, hvor sikkerhetslederen har det overordnede ansvar og samler all dokumentasjon i en perm. Personellsikkerhet er en integrert del av de øvrige fagområdene gjennom autorisasjon av personer som skal ha tilgang til ulike systemer eller fysiske områder.

Ideen bak risikohåndteringskonseptet beskrevet i denne oppgaven er at opplæring av lokale beslutningstakere og sikkerhetspersonell, skal gjøre det mulig å håndtere risiko lokalt ved en avdeling som er knyttet til en virksomhets informasjonssystem. På denne måten antas det at avvik vil avdekkes hurtigere og kan håndteres umiddelbart av lokalt personell i stedet for å vente til en årlig revisjonssyklus fanger opp forholdene. Dette kan bidra til å gjøre sikkerhetsarbeidet mer kosteffektivt ved at det stilles kritiske spørsmål til hensikten med sikkerhetstiltak. Dersom omgivelsene er endret slik at risikobildet ikke lenger stemmer med det som lå i forutsetningene for en sikkerhetsgodkjenning, må sikkerhetstiltakene endres tilsvarende. Dette gjelder både for heving og senking av det forutsatte sikkerhetsnivået.

Endring av sikkerhetstiltak krever eierskap til informasjonssystemet. Denne rapporten har avdekket at det ikke alltid er klart definert hvem som er eier av et informasjonssystem og hvem som har beslutningsmyndighet til å akseptere restrisiko som følge av endring i sikkerhetsrutiner og tiltak.

Denne rapporten har også vist hvordan et kurs i risikohåndtering kan gjennomføres over to og en halv dag. Det ble gjennomført et eksperiment hvor det ble holdt et kurs for en sammensatt testgruppe bestående av nybegynnere og sikkerhetseksperter for å teste om undervisningen er et egnet virkemiddel for å høyne kompetansen i risikohåndtering og dokumentering av sikkerhetstiltak. Evaluering viste at det egnet seg meget bra i forhold til målsettingen med kurset, som var å kvalifisere deltakere til å fylle roller i en sikkerhetsorganisasjon.

Erfaringer fra sikkerhetsinspeksjoner har vist at en stor del av sikkerhetsdokumentasjonen ved lokale avdelinger er kopier av eksempler som er gitt ut av prosjektansvarlige. Dersom sikkerhetsdokumentasjonen ikke gjenspeiler faktiske forhold, men er gjenskrift av ideelle forhold, mister de troverdighet. Da får sikkerhetsdokumentasjon en symboleffekt og en egenverdi, og fungerer ikke som et verktøy for å dokumentere reelle sikkerhetstiltak.

Under evalueringen av kurset, ønsket flere av kursdeltakerne å få utdelt et sett med ferdig beskrevne sikkerhetstiltak, en slags skolens løsning. Det vil utvilsomt forenkle jobben med å dokumentere sikkerhetstiltak når en har en fasit å se etter. På den annen side er selve hensikten med å gjennomføre en operasjonssikkerhetsvurdering at det ikke skal være et sett med regler og instruksjoner som en fasit innebærer, men en metode for å vurdere sikkerhet i et kost/nytte perspektiv. Det er et motsetningsforhold mellom å gi ut skolens løsning og det å kunne stole på gyldigheten av sikkerhetsdokumentasjonen, når det ved sikkerhetsinspeksjoner viser seg at innholdet i stor grad er en kopi av en idealbesvarelse.

Det vises til at vesentlige endringer som kan få betydning for sikkerheten til informasjonssystemet krever en ny sikkerhetsgodkjenning. I lys av denne oppgaven vil en vesentlig endring være det samme som et signifikant avvik. Det skilles i liten grad mellom hvilke avvik som er signifikante, og hvilke avvik som kan godtas. Enkelte nyere prosjekter har likevel presisert egenskaper for avvik som aksepteres innenfor den gjeldende godkjenningen.

Det er lokal datasikkerhetsleder som skal foreta en risikovurdering ved endringer for å fastslå om avviket er signifikant eller ikke. Dette krever innsikt og kompetanse som mange lokale datasikkerhetsledere mangler. Opplæring i risikohåndtering av lokale datasikkerhetsledere, og avsetting av tilstrekkelig tid for å fylle rollen vil gjøre forutsetningene for å foreta en gyldig risikovurdering bedre. Videre vil en større differensiering i hvilke endringer som er signifikante og typiske endringer som er naturlig varians i dokumentet Kravspesifikasjon for sikkerhet (KSS) være med på å lette den lokale risikovurderingen. En regional datasikkerhetslederfunksjon som kan bistå og støtte lokale

datasikkerhetsledere kan også være et virkemiddel for at lokal risikovurdering skal bli styrket.

Konsekvenser av hardware endringer er mer synlige enn software endringer. Som et resultat av dette, blir ofte softwareendringer akseptert uten å kjenne konsekvensene fullt ut. Ved omorganiseringer, kan redusering eller fjerning av sikkerhetsfunksjoner og driftsfunksjoner være signifikant i forhold til forutsetningene.

Det er vanskelig å gjøre rede for konkrete forhold som vil være signifikante avvik fra forutsetningene. En mulig forklaring kan være at forholdet mellom kritisk informasjon, trusler og sårbarheter er i stadig endring. Sirklene som representerer kritisk informasjon, trusler og sårbarheter i OPSEC modellen beveger seg i forhold til hverandre etter påvirkninger fra omgivelsene. Omgivelsene styres ikke av systemeier, og det er vanskelig å forutse alle konstellasjoner som vil utgjøre en uakseptabel risiko. Likevel bør det arbeides videre med å forstå risikobildet, slik at det kan være mulig å skille ut vesentlige faktorer som det bør fokuseres på, framfor å forsøke å beskytte seg mot alle tenkelige forhold. Denne tilnærmingen til risiko vil gjøre sikkerhetsarbeidet lettere for den enkelte medarbeider og på den måten bidra til at de kan bidra til å opprettholde informasjonssikkerheten i organisasjonen.

Denne rapporten har gjennom en kvalitativ studie av Forsvarets informasjonssystemer vist hvordan en kan etablere et risikohåndteringskonsept som kan bidra til å etablere tillit til at sikkerheten blir ivaretatt for informasjonssystemer som utsettes for store endringer i omgivelsene. Det er gjennomført et eksperiment for å demonstrere hvordan en opplæring i risikohåndtering og dokumentering av sikkerhetstiltak kan gjennomføres, og det er drøftet hvilke avvik som er signifikante i forhold til et vedtatt sikkerhetsnivå.

Kapittel

9 Framtidig arbeid

I dette kapitlet neves områder som ble avdekket under forskningsprosessensom denne rapporten ikke gir svar på og som det derfor bør arbeides videre med ved en senere anledning.

I en kvalitativ studie som denne, vil det dukke opp momenter underveis som det ikke var tenkt på i prosjektplanleggingsfasen. Noen slike momenter ble fanget opp og tatt med i arbeidet med denne oppgaven. Men det ble også avdekket nye spørsmål som det bør arbeides videre med.

Gjennom samtaler og intervjuer av sikkerhetseksperter ble det avdekket et behov for å verdivurdere informasjonen. Verdivurdering er en forutsetning for det etterfølgende OPSEC arbeidet. Motivet for å gjennomføre en verdivurdering er først og fremst å bli bevisst på hvilke verdier informasjonen en forvalter innebærer. Men det er etter vår mening også en annen motivasjon for å lære mer om verdivurdering. Dersom en skal konsentrere seg om å beskytte kritisk informasjon, er det nødvendig å skille ut all informasjon som ikke krever beskyttelse. Etter undersøkelsene som ble gjort i denne studien, sitter vi med et inntrykk av at det hersker stor usikkerhet rundt *hva* som er kritisk informasjon. Et resultat blir ofte at hensyn til et legitimt informasjonsbehov hos medarbeidere og eksterne aktører blir skadelidende i den tro at det tjener sikkerheten. Dersom informasjon som ikke er kritisk holdes tilbake, tror vi det vil bidra til å svekke den totale sikkerheten på grunn av misforståelser og unødvendige sikkerhetstiltak. Kanskje er need-to-protect et mer hensiktsmessig utgangspunkt enn det tradisjonelle need-to-know i dagens informasjonssystemer? Dette er interessant å få belyst, og verdivurderinger av informasjonen vil være en nødvendig forutsetning for å ta stilling til et slikt spørsmål.

Det ble også avdekket at det var uklarheter rundt hvem som har eierskap til informasjonssystemer foruten den øverste lederen. For store organisasjoner som Forsvaret, er det nødvendig å ha klare ansvarsforhold for eiere av delsystemer. Hvor går grensene mellom disse systemene? Fastsetting av eierskap til informasjonssystemene er en nødvendig forutsetning for å klargjøre hvem som eier risikoen. Det ble av generalmajor Sunde påpekt viktigheten av å identifisere riktig beslutningsnivå for å akseptere risiko. Andre aktører som har uttalt seg om risikohåndtering, peker også på behovet for en slik ansvarsdeling for å klargjøre grensene for eierskap til deler av et informasjonssystem. Skal en slik inndeling følge geografiske regioner? Er det andre faktorer som bør vurderes? En differensiering er nødvendig for å synliggjøre ansvar og eierskap, og det vil være interessant å finne hvilke kriterier som bør legges til grunn for en slik inndeling i komplekse nettverk.

I arbeidet med å foreslå et operasjonssikkerhetskonsept, ble det etter hvert klart at det bør etableres et program for operasjonssikkerhet i Forsvaret. Et slikt program er beskrevet for amerikanske militære styrker, og går ut på at en sentral aktør gir opplæring og bestemmelser innen operasjonssikkerhet som skal være en integrert del av virksomheten ved alle operative avdelinger. Hver avdeling utnevner en program manager, som gis opplæring sentralt. Deretter får vedkommende et ansvar for at operasjonssikkerhet implementeres ved den lokale virksomheten. Dette gjøres ved skriftlige utnevnelser og planer. Det hadde vært interessant å beskrive et operasjonssikkerhetsprogram for det norske Forsvaret, med utgangspunkt i risikohåndteringskonseptet som er beskrevet i denne oppgaven.

Når sikkerhetstruende hendelser har inntruffet, er det ønskelig at disse i størst mulig grad blir håndtert lokalt. Men det oppstår også et spørsmål om reaksjonsoppfølging ved alvorlige sikkerhetstruende hendelser, hvor den lokale sikkerhetsorganisasjonen trenger støtte for å gjenopprette sikkerheten. Hvordan bør et CIRT (Computer Incident Response Team) for en stor organisasjon som Forsvaret utrustes og organiseres? Hvilke oppdrag ville vært relevante for en slik enhet? Kan det tenkes flere anvendelsesområder for en slik kapasitet? Bør Forsvaret ha en slik kapasitet, eller bør andre aktører i Norge stelle med slikt? Dette er interessant i forhold til en nasjonal beredskap for informasjonssikkerhet som bør studeres nærmere.

Et annet moment som ble avdekket i løpet av arbeidet var forholdet mellom karriere og sikkerhet. Vil en få dyktigere sikkerhetsfolk dersom karriereplaner utarbeides og sikkerhetsfunksjoner blir karrierebringende? Fins det erfaringer i andre organisasjoner hvor sikkerhetsfunksjoner er karrierefremmende? Det hadde vært interessant å se nærmere på en slik tilnærming i forhold til sikkerhetsnivået generelt og informasjonssystemer spesielt.

NSM har et inspeksjonsskjema som brukes for stedlige kontroller ved sikkerhetsgodkjenning, revisjoner og inspeksjoner. Det hadde vært interessant å vurdere en sikkerhetsmetrikk basert på dette inspeksjonsskjemaet. Kan momentene på skjemaet operasjonaliseres inn i en metrikk? Hvordan bør en i så fall gjøre poengberegning og vekting av de ulike faktorene på en pålitelig og gyldig måte? Ved alle målinger er det en fare for at en tilpasser seg det en blir målt på. Men på den annen side kan en påvirke atferden i ønsket retning ved å videreutvikle inspeksjonsskjemaet til metrikker som kan gi svar på sikkerhetsstatusen mer fleksibelt og på andre måter enn i dag. En mulighet kan være å kombinere metrikker og et operasjonssikkerhetsprogram for organisasjoner som vil fastsette egen sikkerhetsstatus og treffe tiltak etter hvert som omgivelsene endrer seg.

Kapittel

10 Referanser

[1] John McHugh: Quantitative Measures of Assurance: Prophecy, Process, or Pipedream? CERT/CC, Software Engineering Institute, Carnegie Mellon University, 2001.

[2] Dennis McCallam: The Case Against Numerical Measures for Information Assurance: Logicon Northrop Grumman Company.

[3] Andrew Odlyzko: Economics, Psychology, and Sociology of Security: Economics of Security, Financial Cryptography 2003 Conference, 2003.

[4] Fran Nielsen: Approaches to security metrics: National Institute of Standards and Technology (NIST), 2000.

[5] Shirley C. Payne: A Guide to Security Metrics: SANS Security Essentials GSEC Practical Assignment, 2001.

[6] Chenxi Wang: A framework for security measurement: NISSC 97.

[7] Norsk Standard: Risikoanalyse NS 5814: Norges standardiseringsforbund (NSF), 1991.

[8] Norsk Standard NS-ISO/IEC 17799: Administrasjon av informasjonssikkerhet: ISO/IEC, 2001. (Code of practice for information security management)

[9] Andrew Jones: Identification of a Method for the Calculation of Threat in an Information Environment: QinetiQ, 2002.

[10] Ole-Arnt Johnsen, Roar Gulbrandsen, Jan O. Svartvadet, Roy Stranden, Jan Kraft og Siri Mollat: Metoder og verktøy for gjennomføring av risikoanalyser: American Society of Industrial Security (ASIS) Norway, 2002.

[11] Einar Idsø og Øyvind Jakobsen: Objekt- og informasjonssikkerhet – metode for risiko- og sårbarhetsanalyse: Norges teknisk-naturvitenskapelig universitet (NTNU), ROSS Risiko- og sårbarhetsstudier, 2000.

[12] Tor Hernes og Elin Nilsen: Personalledelse – begrepsmessige og teoretiske forståelsesmodeller: Foredragsnotater fra Personalledelse under omstilling: Universitetet i Tromsø, 1997.

[13] Forsvarssjefen: Kryptokonsept for taktiske informasjonssystemer: Utdannings- og kompetansesenter for Hærens Samband, 2003.

[14] Stiftelsen for industriell og teknisk forskning ved Norges tekniske høgskole: Risiko og sårbarhetsanalyse, 2003. http://www.sintef.no

[15] Forsvarssjefens militærfaglige utredning 2003: Konsept for nettverksbasert anvendelse av militærmakt – grunnlag: Arbeidsgruppe NBF, 2003. http://www.mil.no

[16] Chairman of the Joint Chief of Staff: Joint Doctrine for Operations Security: Joint Pub 3-54, 1997. http://www.citeseer.nj.nec.com/update/347198

[17] Lov av 20 mars 1998 nr 10 om forebyggende sikkerhetstjeneste (Sikkerhetsloven): http://www.lovdata.no
[18] Lov av 14 april 2000 nr 31 om behandling av personopplysninger (Personopplysningsloven): http://www.lovdata.no
[19] Peter L. Bernstein: Against the Gods – The Remarkable Story of Risk: John Whiley & Sons, 1998: ISBN 0-471-12104-5.
[20] Gregg Schundel og Bradley Wood: Adversary workfactor as a Metric for Information Assurance: New Paradigms in Security Workshop, side 23-30. Association of Computer Machinery, 2000.
[21] Tim Bass og Roger Robichaux, "Defense-In-Depth: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations". IEEE MILCOM 2001.
[22] Jurki Kontio, Gerhard Getto and Dieter Landes, "Experiences in improving risk management processes using the concepts of the Riskit method". SIGSOFT'98 Sixth International Symposium on the Foundations of Software Engineering, 1998.
[23] Jurki Kontio and Victor R. Basili, "Empirical Evaluation of a Risk Management Method". SEI Conference on Risk Management, 1997, Atlantic City, NJ. Edgar H.
[24] Douglas R. Stinson: Cryptography theory and practice:
CRC press, 1995. ISBN 0-8493-8521-0.
[25] rwegian Information Security Laboratory (NISLab), 2003.
[26] Jo Sivertsen: Vitenskap og Rasjonalitet: Gyldendal Akademisk Forlag, 1996. ISBN: 82-417-0750-9.
[27] Rayford B. Vaughn, Ronda Henning, Ambareen Siraj: Information Assurance Measures and Metrics- State of Practice and Proposed Taxonomy: Workshop in Williamsburg, VA 2001.
[28] Hubert Dreyfus, Stuart Dreyfus: Mind Over Machine – The Power of Human Intuition and Expertise in the Era of the Computer: The Free Press, 1986.
[29] HQ USAF/XO: Air Force Instruction 10-1101 Operations Security, 1997. http://afpubs.hq.mil
[30] Interagency OPSEC Support Staff (IOSS): History of OPSEC, 2004. http://ioss.gov/history.html
[31] L. G. Bolman og T. E. Deal: Nytt perspektiv på organisasjon og ledelse. Strukturer, sosiale relasjoner, politikk og symboler. Ad Notam Gyldendal forlag, 1997.
[32] Nasjonal Sikkerhetsmyndighet: Veiledning til Forskrift om informasjonssikkerhet § 5-10 Gjennomføring av konfigurasjonskontroll, 2002 http://www.nsm.stat.no/dokumenter/Veiledning_i_Konfigurasjonskontroll_v2_0.doc
[33] Nasjonal Sikkerhetsmyndighet: Veiledning til Forskrift om informasjonssikkerhet § 5-15 Gjennomføring av sikkerhetsgodkjenning av informasjonssystemer, 2002.
http://www.nsm.stat.no/dokumenter/Veiledning_i_Gjennomforing_av_sikkerhetsgodkjenning_v2_0.doc
[34] Nasjonal Sikkerhetsmyndighet: Veiledning til Forskrift om informasjonssikkerhet § 5-22 Utarbeidelse av kravspesifikasjon for sikkerhet (KSS), 2002.
http://www.nsm.stat.no/dokumenter/Veiledning_i_Utarbeidelse_av_KSS_v2_0.doc

[35] Nasjonal Sikkerhetsmyndighet: Veiledning til Forskrift om informasjonssikkerhet § 5-25 Utarbeidelse av driftsinstruks, 2002. http://www.nsm.stat.no/dokumenter/Veiledning_i_Utarbeidelse_av_Driftsinstruks_v2_0.doc

[36] Nasjonal Sikkerhetsmyndighet: Veiledning til Forskrift om informasjonssikkerhet § 5-26 Utarbeidelse av brukerinstruks, 2002. http://www.nsm.stat.no/dokumenter/Veiledning i Utarbeidelse_av Brukerinstruks versjon 2-0.doc

[37] Nasjonal sikkerhetsmyndighet: Veiledning til Forskrift om sikkerhetsadministrasjon § 4-4 Gjennomføring av sikkerhetsrevisjon og ledelsens evaluering, 2002. http://www.nsm.stat.no/dokumenter/Veiledning_i_Sikkerhetsrevisjon_v2_0.doc

[38] Nasjonal sikkerhetsmyndighet: Skjema for godkjenning, inspeksjon og revisjon av informasjonssystem, 2000. http://www.nsm.stat.no/dokumenter/02-02-04_UGRADERT_Wo_9892a.zip

[39] Forskrift om informasjonssikkerhet. Forskrift til Sikkerhetsloven ved kongelig resolusjon av 29 juni 2001 nr 721. http://www.lovdata.no

[40] Forskrift om sikkerhetsadministrasjon. Forskrift til Sikkerhetsloven ved kongelig resolusjon av 29 juni 2001 nr 723. http://www.lovdata.no

[41] Forskrift om sikkerhetsgraderte anskaffelser. Forskrift til Sikkerhetsloven ved kongelig resolusjon av 29 juni 2001 nr 753. http://www.lovdata.no

[42] Forskrift om personellsikkerhet. Forskrift til Sikkerhetsloven ved kongelig resolusjon av 29 juni 2001 nr 722. http://www.lovdata.no

[43] Morten Stene: Vitenskapelig forfatterskap – Hvordan lykkes med skriftlige studentoppgaver. Kolle Forlag, 2 utgave, 2003. ISBN: 82-463-0025-3.

[44] Idar M Holme og Bernt K Solvang: Metodevalg og Metodebruk, TANO forlag, 3 utgave 1996. ISBN 82-518-3427-9.

[45] Knut Halvorsen: Å Forske på Samfunnet – En Innføring i Samfunnsvitenskapelig metode, 3. utgave, Bedriftsøkonomens Forlag, 1997. ISBN 82-7037-794-5.

[46] Steinar Kvale: Det kvalitative forskningsintervju, Ad Notam Gyldendal forlag, 1997.

Kapittel

11 Appendiks

11.1 Intervju guide

Ekspertintervju

Personalia

Navn	
Tittel	
Arbeidsgiver	
Arbeidsoppgaver	
Bakgrunn	

Tid og sted for gjennomføring

1. Hvilke forutsetninger ligger til grunn for en sikkerhetsmessig godkjenning?
    a. Hvor fremgår det hvilke forutsetninger som er lagt til grunn?
    b. Hvem er det som typisk setter seg inn i detaljer rundt forutsetningene?
    c. Foreligger det en godkjenning for et system du kjenner til?
        i. Når ble den gitt?
        ii. Hvor lenge gjelder den?
        iii. Hva er omfanget av godkjenningen?
        iv. Er det uttrykt noen forutsetninger i godkjenningsskrivet?

2. Hvor godt er disse forutsetningene kjent blant medarbeidere som kommer i kontakt med informasjonssystemet?
    a. Brukere?
    b. Driftspersonell?
    c. Sikkerhetspersonell?
    d. Ledere?

3. Hvilke endringer eller utskiftinger tillates informasjonssystemet utsatt for?
    a. Personell?
        i. Brukere
        ii. Driftspersonell
        iii. Sikkerhetspersonell?
        iv. Ledere?
        v. Vedlikeholdspersonell?
    b. Hardware?
        i. Klienter med PC, skjerm og tastatur?
        ii. Filservere?
        iii. Skrivere?
        iv. Deler av klienter eller servere?

   c. Software?
      i. Nye programmer / applikasjoner?
      ii. Oppdatering av programmer?
   d. Fasiliteter, for eksempel bygningsendringer, eller fysisk forflytning av utstyr?
      i. Oppussing av lokaler?
      ii. Forflytning til nye omgivelser?
   e. Organisasjonmessige endringer?
      i. Omorganisering?
      ii. Prosjektorganisasjon?

4. Hvilke endringer vil du hevde er signifikante avvik fra forutsetningene?
   a. Personell
   b. Hardware
   c. Software
   d. Fasiliteter
   e. Organisasjon

5. I hvilken grad skilles det mellom signifikante endringer og naturlig varians i dokumentasjonen hvor forutsetningene fremgår?
   a. Klart og tydelig?
   b. Brukes uttrykk som
      i. ”alle endringer skal …”?
      ii. ”ingen endringer er tillatt…”?
   c. I hvilken grad fremkommer akseptkriterier fram i dokumentasjonen?
      i. Hvor står akseptkriteriene?
      ii. Hvem kan utforme og endre akseptkriteriene?
      iii. Hvem eier informasjonssystemet?

6. I hvilken grad blir det gitt opplæring til involverte aktører som har interesser i informasjonssystemet?
   a. Kategorier
      i. Brukere?
      ii. Driftspersonell?
      iii. Sikkerhetspersonell?
      iv. Ledere?
   b. Stilles det krav til at opplæring skal gjennomføres?
   c. Stilles det krav til innhold i opplæringen?
      i. Gjennomgang av brukerinstruks eller driftsinstruks?
      ii. Gjennomføres det en kunnskapstest?

7. Hvilke erfaringer har du med sikkerhetsdokumentasjon for informasjonssystemer?
   a. Dokumenter
      i. Godkjenningsstrategi?
      ii. KSS?
      iii. Brukerinstruks?
      iv. Driftsinstruks?
      v. Instruks for sikkerhetsrevisjon?
      vi. Instruks for konfigurasjon?
      vii. Andre?

   b. I hvor stor grad gjenspeiler sikkerhetsinstruksene faktiske forhold?
      i. Gyldig på godkjenningstidspunktet men ikke oppdatert etter utskiftinger og endringer?
      ii. Urealistisk og symbolsk kun for å tilfredsstille krav til formaliteter?

8. Hvor mener du det er forbedringspotensial i forhold om en kan stole på at ikke forutsetningene for den sikkerhetsmessige godkjenningen er endret?

9. Er det andre forhold som du mener er relevant for problemstillingen ”Hvordan kan en stole på at ikke forutsetningene for sikkerhetsmessig godkjenning av et informasjonssystem er endret etter forandringer i omgivelsene”?

Kommentarer

Fra intervjuer:

Fra intervjuobjekt:

11.2 Evalueringsskjema for kurs

Kursopplegget og gjennomføring av kurset blir vurdert fortløpende. Dine synspunkter er derfor verdifulle for oss.

Skriv gjerne utfyllende!

Kursets mål

"Kurset skal kvalifisere deltakere til lå fylle roller i virksomhetens sikkerhetsorganisasjon. Etter gjennomført kurs skal deltakerne være i stand til å håndtere risiko for et sikkerhetsgradert informasjonssystem. Dette innebærer:

1. *En helhetlig forståelse av dokumentasjonen som ligger til grunn for den sikkerhetsmessige godkjenningen.*
2. *Å forstå hensikten med risikovurdering og sikkerhetstiltak som iverksettes for å møte relevante trusler, sårbarhet, risiko og tiltak.*
3. *Å kjenne sammenhengen mellom trusler, sårbarhet, risiko og tiltak*
4. *Å forstå hvordan sikkerhetstiltak og sikkerhetsdokumentasjon skal revideres og betydningen av at tiltakene som er beskrevet etterleves."*

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Helhetsvurdering av kurset						

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Vurdering av delmål 1						

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Vurdering av delmål 2						

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Vurdering av delmål 3						

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Vurdering av delmål 4						

Administrativt

Innkalling og mottak ved UKS Hærens samband

Hvordan var omfanget av - og innholdet i innkallingen?

Kom innkallingen tidsnok?

Kost og losji

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Hvordan var forpleiningen (befalsmessa på Jørstadmoen)?						
Hvordan var forlegningen (Comfort Home hotell Hammer) ?						

Mottak ved kurset

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Hvordan var kursåpning (presentasjon, innhold) ?						
Hvordan var klasserommet ?						

Oppfølging under kurset

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Hvordan var den generelle servicen ?						
Hvordan ble kurset fulgt opp av kursleder ?						

Administrative forhold - helhetsvurdering

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Helhetsvurdering av administrative forhold						

Faglig innhold

Overlappet noen av forelesningene hverandre i sjenerende grad? (Hvis Ja, utdyp)

De enkelte leksjoner:

1 – lite god 5 - meget god	Vurdering av leksjonene						
Leksjon	**1**	**2**	**3**	**4**	**5**		**Kommentarer**
1 Kursåpning Målsetting							
2 Motivasjon Ola Holm							
3 OPSEC metode Ola Holm							
4 Verdivurdering Roger Johnsen							
5 Risikofastsettelse og tiltak Ola Holm							
6 Sikkerhetsgodkjenning Roger Johnsen							
7 Personellsikkerhet Ola Holm							
8 Godkjenning og revisjon Ola Holm							
9 Beredskapsplan Roger Johnsen							
10 Fysisk sikring Norunn Dahl							
11 Informasjonssystem sikkerhet Dagfinn Kristoffersen							
12 Tempestrisikovurdering Roger Johnsen							
13 Faktorer og signifikans Ola Holm							
14 Praktisk øvelse Ola Holm Roger Johnsen							

Pedagogikk

Undervisningen

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Var det rimelig balanse mellom forelesninger, diskusjoner og oppgaver?						
Hvordan var vektleggingen av emnene?						

Generelt

1 – lite god 5 - meget god	1	2	3	4	5	Kommentarer
Forventer DU å få praktisk nytte av kurset i den jobben du har nå?						

Kommentarer til kurset:

Takk for at du tok deg tid til å fylle ut skjemaet – og dermed hjelpe oss til å forbedre og utvikle kurset.

11.3 Om forfatter

Ola Holm er offiser ved Forsvarets Utdannings og kompetansesenter for Hærens Samband (SBUKS) hvor han arbeider som seniorinstruktør i informasjonssikkerhet. Han har en Cand. Mag grad fra Høgskolen i Gjøvik som bygger på Krigsskolen, bedriftsøkonomi og statsvitenskap. Holm underviser ved Hærens Ingeniørhøgskole, og er sikkerhetsrådgiver i materiellinvesteringsprosjekter for Hæren. Han har tidligere deltatt i og ledet utvikling av sikkerhetskonsepter innen informasjonssikkerhet i Forsvaret, og han driver veiledning av sikkerhetspersonell ved militære avdelinger som anvender sikkerhetsgraderte informasjonssystemer.