SINTEF

A25874 - Åpen

Rapport

Behov knyttet til informasjonssikkerhet i forvaltningen

Prioritering av forventninger og behov knyttet til Difis nyopprettede kompetansemiljø for informasjonssikkerhet

Forfatter(e)
Inger Anne Tøndel
Nils Brede Moe
Daniela Soares Cruzes

SINTEF IKT
Systemutvikling og sikkerhet
2014-01-30

SINTEF

SINTEF IKT

Postadresse:
Postboks 4760 Sluppen
7465 Trondheim

Sentralbord: 73593000
Telefaks: 73594302

postmottak.IKT@sintef.no
www.sintef.no
Foretaksregister:
NO 948 007 029 MVA

Rapport

Behov knyttet til informasjonssikkerhet i forvaltningen

Prioritering av forventninger og behov knyttet til Difis nyopprettede kompetansemiljø for informasjonssikkerhet

EMNEORD:
Informasjonssikkerhet; risikovurdering; ledelsesforankring; styringssystem for informasjonssikkerhet; åpenhet om hendelser; sikkerhet i utvikling av IKT-systemer

VERSJON
1.0

DATO
2014-01-30

FORFATTER(E)
Inger Anne Tøndel
Nils Brede Moe
Daniela Soares Cruzes

OPPDRAGSGIVER(E)
Direktoratet for forvaltning og IKT (Difi)

OPPDRAGSGIVERS REF.
13/01141

PROSJEKTNR
102005877

ANTALL SIDER OG VEDLEGG:
48, inkl. 4 vedlegg

SAMMENDRAG

Denne rapporten kommer med anbefalinger til prioriterte aktiviteter for Difis nyopprettede kompetansesenter for informasjonssikkerhet. Anbefalingene er gjort på bakgrunn av resultatene fra fire fokusgrupper, samt en spørreundersøkelse knyttet til bruk av styringssystemer for informasjonssikkerhet. Både departementer og etater var representert i begge aktivitetene.

På bakgrunn av funnene anbefales Difi å fokusere sine aktiviteter og tiltak innen to hovedområder: Kompetansebygging og koordinering. Den viktigste årsak til dagens og fremtidige utfordringer i statsforvaltningen er manglende kompetanse innen faget informasjonssikkerhet. Her kan Difi bidra med kurs, foredrag og lavterskel rådgivning, samt være en pådriver for bedre utdanning. Innen koordinering anbefaler rapporten at Difi samarbeider med og søker å påvirke andre relevante sikkerhetsmiljøer, tilsynsmyndigheter og kravstillere. I tillegg bør Difi legge til rette for god koordinering i statsforvaltningen gjennom etablering av praksisfellesskap.

UTARBEIDET AV
Inger Anne Tøndel

SIGNATUR
Inger Anne Tøndel

KONTROLLERT AV
Martin Gilje Jaatun

SIGNATUR

GODKJENT AV
Eldfrid Øvstedal

SIGNATUR
Eldfrid Øvstedal

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
A25874	978-82-14-05343-2	Åpen	Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2014-01-30	Første versjon

SINTEF

Innholdsfortegnelse

Utvidet sammendrag

Denne rapporten kommer med anbefalinger til prioriterte aktiviteter for Difis nyopprettede kompetansesenter for informasjonssikkerhet. Anbefalingene er gjort på bakgrunn av resultatene fra fire fokusgrupper, samt en spørreundersøkelse knyttet til bruk av styringssystemer for informasjonssikkerhet. Til sammen 18 virksomheter i statsforvaltningen deltok i fokusgruppene, og spørreundersøkelsen ble distribuert til 59 deltagere på en workshop der 43 virksomheter deltok. Både departementer og etater var representert i begge aktivitetene.

I rapporten er resultatene fra fokusgruppene organisert innen seks temaområder: Integrasjon mot virksomhetens mål, styringssystemet og virksomheten, åpenhet, forståelse av risiko, sikkerhet under utvikling av IT-systemer, og kompetanse. De viktigste funnene er oppsummert i Tabell 1.

På bakgrunn av funnene anbefales Difi å fokusere sine aktiviteter og tiltak innen to hovedområder: Kompetansebygging og koordinering. Den viktigste årsak til dagens og fremtidige utfordringer i statsforvaltningen er manglende kompetanse innen faget informasjonssikkerhet. Her kan Difi bidra med kurs, foredrag og lavterskel rådgivning, samt være en pådriver for bedre utdanning. Innen koordinering anbefaler rapporten at Difi samarbeider med og søker å påvirke andre relevante sikkerhetsmiljøer, tilsynsmyndigheter og kravstillere. I tillegg bør Difi legge til rette for god koordinering i statsforvaltningen gjennom etablering av praksisfellesskap.

Tiltakene og aktivitetene som er foreslått i denne rapporten vil være kjente både for Difi og statsforvaltningen. For at Difi skal kunne utnytte ressursene på en slik måte at de har stor effekt, må hvert tiltak skreddersys i forhold til den målgruppa de forskjellige tiltakene er rettet mot. En forutsetning for å kunne skreddersy tiltak og aktiviteter på området informasjonssikkerhet er å ha en god forståelse av de utfordringer statsforvaltningen har, hva som fungerer bra i dag, og hvordan eksterne mekanismer og aktører påvirker dagens arbeid med informasjonssikkerhet. En annen forutsetning for skreddersøm er å forstå diversiteten når det gjelder behov, kunnskapsnivået og modenhet blant de ulike virksomheter, samt at det relativt unge fagområdet informasjonssikkerhet er i sterk og kontinuerlig endring. Det viktigste i denne rapporten er derfor ikke tiltakene som anbefales, men derimot beskrivelsene av virksomhetenes erfaringer og refleksjoner rundt arbeidet med informasjonssikkerhet.

Tabell 1. Oversikt over funn

Tema	Funn
Integrasjon mot virksomhetens mål	Ledelsesforankring kommer i dag primært som følge av eksternt press
	Språkbruk i tildelingsbrev, lovverk og regelverk må være enkelt for at ledere skal prioritere informasjonssikkerhet
	God gjennomføringsevne og indre motivasjon er sentralt.
Styringssystemet og virksomheten	Gradvis etablering av styringssystem er viktig, og det bør startes enkelt.
	Informasjonssikkerhet bør integreres i virksomhetens eksisterende styringssystem
	Forankring, kompetanse og ressurser trengs for å tilpasse styringssystemet til virksomheten.
	Styringssystemene stemmer ikke med virkeligheten.
	Måten tilsyn gjøres på i dag fører til styringssystemer som er for lite tilpasset behovene.
	For å lykkes med innføring må styringssystemet være brukervennlig og ha et enkelt språk.
	Det er vanskelig å bygge god sikkerhetskultur. Tekniske tiltak oppleves enklere og blir dermed prioritert.
	Knapphet på ressurser vanskeliggjør vedlikehold og forbedring av styringssystemet.
Åpenhet	Hendelser underrapporteres, og det er lite fokus på å lære av mindre avvik.
	En god kultur for avviksrapportering er viktigere enn et perfekt avviksrapporteringssystem.
	Manglende åpenhet vanskeliggjør deling av hendelsesinformasjons på tvers av virksomheter for felles læring.
	Feil blir dekket over for å se bedre ut ved tilsyn.
Forståelse av risiko	Virksomheter mangler felles forståelse av hva risiko er og hvilken risiko som er akseptabel.
	Informasjonssikkerhet forbindes med konfidensialitet, mens det er lite fokus på integritet og tilgjengelighet.
	Ved deltakelse i sikkerhetsarbeid øker forståelse av risiko.
	Regelverk bør understøtte en risikobasert tilnærming, men samtidig ta høyde for at ikke alle har kompetanse til å jobbe risikobasert
Sikkerhet under utvikling av IT-systemer	Det er økende fokus på sikkerhet under utvikling av nye systemer.
	Informasjonssikkerhet involveres ofte for sent i utviklingsprosessen.
	Funksjonalitet vinner over sikkerhetskrav i utviklingsprosjekter.
	Både bestiller og leverandør mangler kompetanse om hvordan ivareta sikkerhetskrav i utviklingsprosjekter.
Kompetanse	Teknisk kompetanse er tilfredsstillende.
	Kompetanseutfordringer finnes på alle nivåer og områder i og utenfor virksomheten.
	Det trengs bedre oversikt over regelverk og lovverk som påvirker sikkerhetsarbeid.
	Det kreves god kompetanse på organisasjonsutvikling for å lykkes med sikkerhetsarbeid.
	Kompetanseutfordringene er størst hos mindre virksomheter.

1 Innledning

Samfunnet er i dag avhengig av informasjons- og kommunikasjonsteknologi (IKT). IKT er en grunnleggende infrastruktur for samhandling. Dette gjør at sikkerheten knyttet til IKT-systemene er viktig i et samfunnsperspektiv.

Informasjonssikkerhet handler om å ivareta konfidensialitet, integritet og tilgjengelighet til informasjon[1] i tilstrekkelig grad. Siden informasjon i dag i stor grad eksisterer og utveksles i IKT-systemer, er informasjonssikkerheten avhengig av sikkerheten knyttet til den teknologien som benyttes. Samtidig eksisterer informasjonen og IKT i en større sammenheng der menneskene og organisasjonene som er involvert også har en betydelig rolle i det å ivareta informasjonssikkerheten. Kravene til informasjonssikkerhet knyttet til ulik informasjon vil være forskjellige. Noe informasjon skal være åpen og har derfor lave krav knyttet til konfidensialitet, mens krav knyttet til integritet og tilgjengelighet kan være høye. Annen informasjon kan igjen ha strenge konfidensialitetskrav, men lave tilgjengelighetskrav.

I Norge er det etablert en Nasjonal strategi for informasjonssikkerhet [1] som definerer fire overordnede mål for det felles informasjonssikkerhetsarbeidet:

1. Styrket samordning og felles situasjonsforståelse
2. Robust og sikker IKT-infrastruktur i hele samfunnet
3. Sterk evne til å håndtere uønskede IKT-hendelser
4. Høy kompetanse og sikkerhetsbevissthet

Som del av handlingsplanen tilknyttet strategien [2] ble det besluttet å etablere et kompetansemiljø for informasjonssikkerhet i statsforvaltningen i Difi (tiltak 0.5). Dette kompetansemiljøet skal være en pådriver når det gjelder bedre styring av informasjonssikkerhet i statsforvaltningen, og er tiltenkt en sentral rolle når det gjelder informasjons- og opplysningsvirksomhet knyttet til informasjonssikkerhet i statlige etater.

For å kunne løse denne oppgaven på en god måte, må det nyopprettede senteret har en god forståelse av hvordan informasjonssikkerhetsarbeidet gjøres i dag i statsforvaltningen: Hva fungerer bra, hva oppleves som utfordringer, hvilken rolle har informasjonssikkerhet når det gjelder måloppnåelse i forvaltningen, og hvordan kan statsforvaltningen settes i bedre stand til å gjøre effektivt sikkerhetsarbeid?

Det finnes allerede en del tilgjengelig informasjon som kan gi svar på noe av disse spørsmålene. Riksrevisjonen har i Dokument 1 (2010-2011) [2] identifisert store svakheter i informasjonssikkerheten i statsforvaltningen. Difi har innhentet erfaringer med standardene ISO/IEC 27001 og ISO/IEC 27002 i offentlige virksomheter [4]. Difi har også selv gjennomført en workshop med 59 deltakere fra 43 statlige virksomheter, med formål å identifisere forventinger og behov knyttet til den nyopprettede seksjonen for informasjonssikkerhet [5]. I tillegg gir NSMs rapport om sikkerhetstilstanden i Norge [6] samt Datatilsynets årsmelding [7] nyttige perspektiver i denne sammenhengen.

I denne rapporten presenteres resultater fra fire fokusgrupper med deltakere fra til sammen 18 virksomheter i statsforvaltningen, både departementer og etater. Formålet med disse fokusgruppene var å identifisere behov og forventninger knyttet til den nyopprettede seksjonen hos Difi, og få et grunnlag for å gjøre en prioritering blant disse behovene. Resultatene fra fokusgruppene utdyper resultatet fra workshopen som Difi selv har arrangert. Fokusgruppene ble lagt opp som en diskusjon rundt det arbeidet med informasjonssikkerhet som gjøres i virksomhetene, både når det gjelder hva som fungerer bra, hva som oppleves som utfordrende, og hvorfor. Diskusjonene dekket både sikkerhetsarbeid i selve virksomheten og sikkerhet under utvikling av nye IKT-systemer. I tillegg presenteres resultater fra en spørreundersøkelse knyttet til bruk av styringssystemer for informasjonssikkerhet.

[1] Konfidensialitet handler om at kun autoriserte personer skal ha tilgang til informasjonen, integritet handler om at informasjonen skal være gyldig, tilgjengelighet handler om at informasjonen skal være tilgjengelig for de som har rett til og behov for tilgang.

Rapporten er strukturert på følgende måte: Kapittel 2 gir en beskrivelse av metoden som er benyttet. Kapittel 3 presenterer resultater fra fokusgruppene, samt hovedresultater fra spørreundersøkelsen. Kapittel 4 gir anbefalinger til Difi basert på resultatene fra studien, og knytter viktige funn opp mot andre tilgjengelige rapporter, samt forskningslitteratur. Detaljerte resultater fra spørreundersøkelsen finnes i vedlegg.

2 Metode for datainnsamling og rangering av resultater

I dette arbeidet har vi benyttet teknikken fokusgruppe [8]. En fokusgruppe kan forstås som er et strukturert gruppeintervju som har en uformell form. Den som leder intervjuet følger gjerne en intervjuguide, og i tillegg gis det mulighet for at deltakerne kan komme med egne tema og innspill.

Fokusgruppeteknikken ble valgt for dette arbeidet fordi den er velegnet for å identifisere forbedringsområder ut fra hva deltakerne opplever eller savner, ideer til hva som bør gjøres annerledes, og forslag til tiltak. Poenget med å samle deltakerne i en gruppe – i stedet for å intervjue deltakerne enkeltvis - er at deltakerne forholder seg til hverandres meninger. Når deltakerne samtaler om sine erfaringer får man også frem mer informasjon enn ved å intervjue ett og ett gruppemedlem.

2.1 Deltakerne

Det ble invitert til fire fokusgrupper. To forskere fra SINTEF ledet disse fire fokusgruppeintervjuene a tre timer med fire til åtte deltakere. Til sammen deltok 21 personer i fokusgruppene fra 18 statlige virksomheter (inkludert fire departementer). En av deltakerne var forsker innen relevant område. Deltakerne ble rekruttert ved at Difi sendte invitasjon til utvalgte virksomheter om å delta i fokusgruppene. Virksomhetene var valgt ut slik at det totalt sett skulle være en blanding av store og små virksomheter, noen modne og noen mindre modne i forhold til arbeid med informasjonssikkerhet, samt noen som hadde fått merknader fra Riksrevisjonen i Dokument 1 (2010-2011) [2]. Det var primært et ønske at deltakerne hadde ansvar tilknyttet informasjonssikkerhet i sin virksomhet. En gruppe bestod av virksomheter som har kommet langt i moderniseringsarbeidet, mens en gruppe var bestod primært av departementer. De to resterende gruppene var mer blandede grupper.

Fokusgruppene ble arrangert i lokalene til Difi. De som ble invitert mottok først en e-post, og ble så purret opp med telefon og e-post. I tillegg ble det sendt en påminnelse uka før selve fokusgruppeintervjuet.

To av gruppene startet klokken 09.00 og avsluttet med felles lunsj klokken 12.00. De to andre gruppene startet med felles lunsj klokken 11.30 og avsluttet klokken 15. Få av deltakerne kjente hverandre fra før, derfor ble det benyttet idemyldringsteknikker i starten av hver fokusgruppe for å bygge opp tillitt mellom deltakerne og stimulere til åpenhet. En vellykket fokusgruppe er avhengig av at deltakerne tør å dele sine erfaringer.

2.2 Intervjuguide og kjøreplan

Alle gruppene fulgte den samme prosessen og den samme intervjuguiden, noe som har gjort det mulig å analysere resultatene på tvers av gruppene. Innledningsvis ble bakgrunnen til deltakerne kartlagt, etterfulgt av et kort innlegg av Difi om den nye seksjonen som er opprettet, og motivasjon for fokusgruppa. Representanten fra Difi forlot gruppa etter sitt innlegg og kom tilbake helt på slutten av dagen for å svare på eventuelle spørsmål fra deltakerne.

Etter innledningen ble det gjennomført en kort idemyldring hvor hver deltaker svarte på følgende spørsmål: *Hva fungerer bra og hva er utfordrende i arbeidet med informasjonssikkerhet hos dere?* Gjennom denne idemyldringen fikk alle mulighet til å snakke tidlig, og vi fikk effektivt kartlagt hva som fungerer bra og hva som er utfordrende hos de ulike virksomhetene. Viktige momenter fra idemyldringen ble diskutert i første tema i selve gruppeintervjuet. Gruppeintervjuet dekket følgende tema:

1. Sikkerhetskultur og forankring
2. Styringssystemer og risikovurderinger
3. Krav, utvikling, forvaltning av nye informasjonssystemer.

4. Oppsummering

Selve intervjuguiden finnes i Vedlegg D.

De forskjellige virksomhetene hadde ulike erfaringer og utfordringer, noe som medførte at deltakerne og gruppene hadde ulik tilnærming til de ulike temaene. I tillegg til spørsmålene fra intervjuguiden fikk gruppe 2, 3 og 4 presentert viktige funn fra tidligere grupper og ble bedt om å kommentere på disse funnene. På denne måten bygget vi en forbindelse mellom de ulike gruppene. Gruppe 1 fikk presentert resultater fra spørreundersøkelsen, og ble bedt om å kommentere på disse resultatene.

En forsker fra SINTEF var ansvarlig for å ta detaljerte notater fra diskusjonene. For å sikre at vi fikk med alle viktige detaljer i gruppesamtalen ble samtalene tatt opp. Deltakerne ble spurt om å samtykke til at forskerne gjorde et slikt opptak. Opptaket ble kun brukt av forskerne og det vill bli slettet etter at resultatene fra fokusgruppene er publisert.

Etter hver fokusgruppe reflekterte forskerne over hvordan gruppene fungerte; i hvor stor grad alle deltok, grad av enighet/diversitet, og deltakernes evne til å bygge på hverandres argumentasjon. I noen av gruppene gikk diskusjonen livlig, mens andre grupper hadde utfordringer med å få til gode diskusjoner rundt de tema som skulle belyses. For å forstå resultatene, er det nødvendig å forstå konteksten resultatene har kommet frem i. Ved utarbeidelse av denne rapporten har vi derfor tatt hensyn til observasjoner knyttet til gruppedynamikk, informasjon om bakgrunn og erfaring fra de enkelte deltakere, samt modenhet i virksomheten de kom fra.

Gjennom å basere arbeidet på den samme intervjuguiden og i tillegg be gruppene reflektere over resultater fra tidligere grupper, kom det frem klare forskjeller mellom gruppene. Et eksempel på dette var at noen ønsket at Difi skulle tilby konsulenttjenester ovenfor små virksomheter, mens andre (og større virksomheter) mente at Difi aldri må tilby konsulenttjenester og dermed konkurrere med konsulentselskap som jobber med informasjonssikkerhet.

Fokusgruppene gav et rikt datamateriale. I tillegg vurderte deltakerne gruppene som veldig nyttige, fordi gruppene var gode arenaer for utveksling av erfaringer. Deltakerne opplevde at de lærte mye av hverandre i løpet av de tre timene som var satt av.

2.3 Spørreundersøkelse

Offentlig sektor har økende fokus på styringssystemer for informasjonssikkerhet (SSIS), blant annet på grunn av de mål som er beskrevet Nasjonal strategi for informasjonssikkerhet [1]. Det er derfor viktig at det nyopprettede kompetansesenteret for informasjonssikkerhet hos Difi har en aktiv rolle i å støtte statsforvaltningens arbeid med SSIS. For bedre å forstå dagens bruksnivå av SSIS og hvilke behov forvaltningen har knyttet til SSIS, har vi utført en empirisk undersøkelse av faktorer som påvirker akseptanse og bruk av SSIS. Den empiriske undersøkelsen er basert på Technology Acceptance Model (TAM), samt erfaringer med bruk av TAM i tidligere studier [9]. To avhengige variabler ble undersøkt:

- *Dagens bruk av SSIS*, noe som er et mål på vellykket etablering og innføring av SSIS
- *Intensjon om fremtidig bruk*, noe som gjenspeiler sannsynligheten for at SSIS vil bli innført i fremtiden.

Selve spørreundersøkelsen (spørreskjemaet er gjengitt i Vedlegg C) ble gjennomført den 5. november 2013 under en workshop arrangert av Difi [5], hvor formålet var å kartlegge behov forvaltningen har til Difi og den nye seksjonen. Invitasjon til workshopen gikk ut til alle statlige virksomheter, og workshopen hadde totalt 59 deltagere som representerte 43 virksomheter. I alt ble 59 spørreskjemaer distribuert og vi fikk

tilbake 51 brukbare svar, noe som resulterer i en god samlet svarprosent på 86 %.

Spørreskjemaet bestod av to deler. I den første delen ble respondentene bedt om å gi generell bakgrunnsinformasjon knyttet til stilling, profesjonell ansiennitet, utdanningsnivå, primær jobbfunksjon og erfaring med SSIS. Den andre delen av spørreskjemaet ble brukt til å måle dybden og bredden av SSIS-bruk, intensjon om fremtidig bruk, og det som oppfattes som viktig for å bruke SSIS. Helt til slutt ble respondentene oppfordret til å beskrive sitt SSIS.

Vedlegg B gir en grundig innføring i metoden som ble benyttet samt resultatene av undersøkelsen. Oppsummeringen av resultatene fra fokusgruppene i kapittel 3, inneholder også de viktigste resultatene fra spørreundersøkelsen.

2.4 Dataanalyse

For å få tilbakemelding fra fokusgruppedeltakerne på resultatene mens deltakerne enda hadde diskusjonene friskt i minne, fikk deltakerne raskt tilbake en rapport med en midlertidig analyse av resultatene fra den gruppen de var med i. Denne rapporten oppsummerte de viktigste temaene, konklusjonen og de viktigste anbefalingene til Difi fra den enkelte gruppen. I tillegg fikk deltakerne et stikkordsmessig notat fra selve diskusjonene i sin gruppe. Til sammen seks deltakere kom med tilbakemeldinger på analysen. Tilbakemeldingene var positive i forhold til at rapporten dekket det som kom frem i diskusjonene. De få endringsforslagene som kom var knyttet til enkeltformuleringer, og en feil referanse til en standard. En deltaker hadde forslag til tema som burde dekkes grundigere i senere grupper, og dette innspillet ble tatt med videre.

Gjennom en sammenlignende analyse av resultatene fra hver enkelt fokusgruppe identifiserte vi et sett av temaer, funn og anbefalinger. Disse temaene, funnene og anbefalingene er beskrevet i detalj i neste kapittel.

3 Identifiserte forventninger og behov

I dette kapitlet beskriver vi de temaområder som har kommet frem gjennom en sammenlignende analyse av de fire fokusgruppene. Resultatene fra spørreundersøkelsen er gruppert inn under disse temaene. Temaene er:

- Integrasjon mot virksomhetens mål
- Styringssystemet og virksomheten
- Åpenhet
- Forståelse av risiko
- Sikkerhet under utvikling av IT-systemer
- Kompetanse

For hvert temaområde beskriver vi bakgrunn og motivasjon for hvorfor dette er et viktig område, hvordan virksomhetene arbeider med dette i dag, de utfordringene virksomhetene opplever, og forutsetninger for å lykkes videre. Vi beskriver også konkrete tips fra deltakerne, basert på hva enkeltvirksomheter lykkes med i dag.

3.1 Integrasjon mot virksomhetens mål

Informasjonssikkerhet konkurrerer med mange andre viktige områder i statlige virksomheter. For å få den nødvendige prioriteten og komme på ledelsens agenda, må informasjonssikkerhet integreres mot virksomhetens øvrige mål. Informasjonssikkerhet kommer på ledelsens agenda når sikkerhet blir sett på som viktig for å kunne levere virksomhetens tjenester og/eller ledelsen opplever et sterkt eksternt press i forhold til informasjonssikkerhet.

Funn 1: Ledelsesforankring kommer i dag primært som følge av eksternt press

En stor andel av de virksomhetene som var representert i fokusgruppene opplever at arbeidet med informasjonssikkerhet er forankret hos ledelsen. Graden av forankringen varier imidlertid mye mellom de forskjellige virksomhetene. Noen av de modne miljøene (miljøer som har kommet langt i arbeidet med informasjonssikkerhet) beskrev en hverdag der ledelsen ser informasjonssikkerhet som en forutsetning for å nå virksomhetsmålene. Andre (og mindre modne miljøer) opplever at ledelsen har blitt opptatt av informasjonssikkerhet først etter press fra departement og tilsynsmyndigheter, eller gjennom negative oppslag i media. I diskusjonene knyttet til ledelsesforankring var det enighet om at det viktigste er å få forankring hos toppledelsen. Flere virksomheter opplever imidlertid at det er mellomledere som i praksis får ansvaret for gjennomføring av informasjonssikkerhetsarbeidet, og at det er store utfordringer knyttet til å få disse mellomlederne til å forstå viktigheten av god informasjonssikkerhet, og deres rolle i dette.

Når det gjelder press fra eksterne, ble spesielt forholdet til departementene og Riksrevisjonen kommentert:

- De mer modne miljøene opplever at departementene er lite opptatt av informasjonssikkerhet og savner oppfølging.
- Det er behov for bedre kompetanse på informasjonssikkerhet hos de som deltar på etatsmøtene fra departementene sin side.
- Flere deltakere fra modne miljøer beskrev at kritikk fra Riksrevisjonen har gitt det ledelsesfokus som var nødvendig for å kunne gjennomføre viktige tiltak for informasjonssikkerheten, slik som etablering av styringssystemer og innføring av øvelser for å trene på å håndtere hendelser.
- Gjennom samarbeid og dialog med Riksrevisjonen – med ledelsens velsignelse – oppnådde en moden virksomhet at de og Riksrevisjonen hadde felles retning i informasjonssikkerhetsarbeidet. Sikkerhetsansvarlig fikk støtte fra Riksrevisjonen angående nødvendige tiltak, som gjorde det lettere å forankre disse tiltakene hos ledelsen.

Tildelingsbrevet fra departementet er sentralt for å få informasjonssikkerhet til å bli en del av virksomhetsmålet. Det er imidlertid avgjørende *hvordan* informasjonssikkerhet omtales i denne type dokumenter. Inneholder tildelingsbrevet mye vanskelig terminologi og mange forkortelser, forsterker det opplevelsen av informasjonssikkerhet som noe for de spesielt interesserte og uten praktisk betydning for organisasjonen. Den samme problemstillingen er aktuell når det gjelder formuleringer brukt i lovverk og regelverk, og brev fra viktige tilsynsmyndigheter. *Hvordan* informasjonssikkerhet blir kommunisert, kan påvirke om temaet reelt sett blir sett på som noe ledelsen er ansvarlig for, eller om det blir et tema kun for teknologene.

Funn 2: Språkbruk i tildelingsbrev, lovverk og regelverk må være enkelt for at ledere skal prioritere informasjonssikkerhet

Funn 3: God gjennomføringsevne og indre motivasjon er sentralt.

Som tidligere beskrevet er eksternt press viktig for at informasjonssikkerhet skal bli en del av virksomhetsmålet. De virksomheter som lykkes har imidlertid også indre motivasjon og god gjennomføringsevne, blant annet i form av dedikerte sikkerhetsfolk som er flinke til å kommunisere informasjonssikkerhet både mot ledelsen og resten av organisasjonen. Men selv de som jobber i en moden organisasjon opplever det som utfordrende å kommunisere viktigheten og nytten av arbeidet med informasjonssikkerhet, fordi det er vanskelig å kvantifisere (måle) hvor god sikkerhet en virksomhet har. Spørsmålet som ofte stilles men som er vanskelig å svare på er: Hva har virksomheten igjen for det sikkerhetsarbeidet som gjøres?

Tips og gode erfaringer fra fokusgruppedeltakerne:

- **Problemforståelse først:** Når man er i dialog med ledere om informasjonssikkerhet er det viktig å bruke tid på å presentere og skape forståelse for problemene og utfordringene før eventuelle tiltak legges frem. Fokuseres det for mye på tiltakene vil ikke ledelsen opparbeide forståelse av problemene, noe som igjen medfører mangel på eierskap til tiltakene. Problemer som presenteres bør knyttes opp mot virksomhetsmålene.
- **Øvelser gir økt forståelse:** Planlegging og gjennomføring av øvelser viser på en effektiv måte hva som mangler når det gjelder informasjonssikkerhet. Det kan være en utfordring å få ledelsen til å prioritere deltakelse på lengre øvelser, og da kan korte øvelser (1-2 timer) være en løsning. Om ikke leder kan stille er det viktig at stedfortreder stiller.
- **Ledelsen må holdes informert:** Om ledelsen skal prioritere informasjonssikkerhetsarbeid må den holdes informert. En årlig "ledelsens gjennomgang" er viktig, men ikke nok. Det å opplyse om og diskutere hendelser man opplever i fora der ledelsen er, er en god måte å holde ledelsen informert på gjennom hele året.

3.2 Styringssystemet og virksomheten

Det er et krav om at virksomhetene i statsforvaltningen skal ha en internkontroll på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Dette fremgår av Digitaliseringsrundskrivet. ISO 27001 er den standarden som imøtekommer kravet "anerkjent" og er således tatt inn i Difis referansekatalog over anbefalte forvaltningsstandarder.

Det er stor variasjon i hvor langt statsforvaltningen har kommet med etablering og innføring av et styringssystem for informasjonssikkerhet, hvilken strategi som er brukt på innføring og hvordan styringssystemet for informasjonssikkerhet er integrert med virksomhetens øvrige styringssystem. I våre beskrivelser skiller vi på det å få etablert et styringssystem (få på plass nødvendig dokumentasjon i form av

ansvarsbeskrivelser, policy og rutiner), og det å få innføre styringssystemet i virksomheten (slik at systemet etterleves i praksis). I tillegg er det et behov for å vedlikeholde og kontinuerlig forbedre et styringssystem. Vi gir først en oversikt over hva som er status for etablering, og beskriver erfaringer deltakerne har gjort seg rundt både etablering og innføring av styringssystemer. Videre beskriver vi hva deltakerne opplever som viktig i et styringssystem for at styringssystemet skal ha nytte for dem.

Virksomhetene som deltok i fokusgruppene er på ulike stadier og har ulikt syn når det gjelder både etablering og innføringen av et styringssystem for informasjonssikkerhet. Noen har hatt et styringssystem i flere år, mens andre er i en oppstartsfase. Resultatene fra spørreundersøkelsen (se Vedlegg B) viser tilsvarende variasjoner. Noen deltakere opplever at et styringssystem er nødvendig og nyttig, mens andre ser dette kun som et pålegg utenifra. Noen av de minste virksomhetene ser det som en umulig oppgave å få etablert et styringssystem for informasjonssikkerhet.

Funn 4: Gradvis etablering av styringssystem er viktig, og det bør startes enkelt.

De som opplever å ha lykkes i å få etablert et styringssystem, identifiserte gradvis innføring som et suksesskriterium. Det er viktig å starte enkelt og ta utgangspunkt i det absolutt nødvendige, og så kan styringssystemet utvides etterhvert som behovet oppstår. Oppfyllelse av hele ISO-standarden i seg selv er ikke noe mål, selv om mange virksomheter oppfatter at Riksrevisjonen kommuniserer dette. Når man skal i gang med etablering av et styringssystem vil trolig mange av dokumentene og prosessene allerede finnes som resultat av annet arbeid. Det må derfor brukes tid på å knytte styringssystemet opp mot eksisterende prosedyrer og dokumentasjon. Eksisterer det et styringssystem innenfor andre områder vil dette systemet ofte kunne utvides for også å dekke informasjonssikkerhet, noe som gjør etablering og innføring enklere. Erfaringene fra de organisasjonene som har et integrert system (som også dekker informasjonssikkerhet) er at lite av dokumentasjonen er spesifikk for informasjonssikkerhet. I dag er imidlertid styringssystemet for informasjonssikkerhet ofte ikke integrert med styringssystemet for virksomheten ellers. Da er det lett at informasjonssikkerhet oppfattes som enda en ekstra rutine med påfølgende krav om dokumentasjon, samt ekstra regler ansatte må forholde seg til. Informasjonssikkerhetsarbeidet kan også oppleves som lite koordinert med annet arbeid i virksomheten: En uke kommer noen fra HMS og krever risikoanalyse, og neste uke kommer informasjonssikkerhet.

Funn 5: Informasjons-sikkerhet bør integreres i virksomhetens eksisterende styringssystem

Viktige faktorer som ser ut til å skille de som lykkes fra de som strever med å etablere styringssystemer, er kompetanse og ledelsesforankring. Uten riktig kompetanse går man seg fort vill i kravene som blir stilt i ISO-standarden, og man mister motet på grunn av alt som skal dokumenteres og alle tiltak man må forholde seg til i vedlegget. Uten en motivert virksomhet og forankring i ledelsen, får man ikke det engasjementet og de ressurser som er nødvendige for å gjøre arbeidet som kreves. Virksomheter som mangler kompetanse og interne ressurser kan fristes til å "bestille" et ferdig styringssystem gjennom å leie inn konsulenter – med resultat at styringssystemet i liten grad er forankret i virksomheten og dermed umulig å innføre. Resultater fra spørreundersøkelsen viser at bruken av styringssystemet er større når brukere opplever stor grad av samsvar mellom styringssystemet og de verdier, behov og tidligere erfaringer de selv har. Selv om konsulenter og andre eksterne kan gi verdifulle bidrag i å fasilitere prosessen med å etablere og innføre et styringssystem, er det essensielt at virksomheten selv lager og tilpasser sitt eget styringssystem til virksomheten.

Funn 6: Forankring, kompetanse og ressurser trengs for å tilpasse styringssystemet til virksomheten.

Spørreundersøkelsen peker på opplevd nytte som den viktigste faktoren som påvirker ønske om framtidig bruk av et styringssystem for informasjonssikkerhet. Da begrepet "nytte" ble diskutert var mange opptatt av at styringssystemet bør fungere som et slags organisasjonskart for informasjonssikkerhet. Med dette menes at

styringssystemet må beskrive roller og ansvar knyttet til informasjonssikkerhet, i tillegg til å være det stedet hvor viktige dokumenter, sikkerhetsstrategier, og rutiner er samlet. Styringssystemet må også beskrive tydelige mål for sikkerhetsarbeidet. Dette inkluderer blant annet hvordan avvik i forhold til målsetningen i strategien skal måles. Som nevnt i avsnitt 3.1, er det vanskelig å kvantifisere hvor god sikkerhet en virksomhet har. Resultatene fra spørreundersøkelsen viser også at de fleste ikke har noen mening om hvorvidt styringssystemet for informasjonssikkerhet fører til forbedringer i sikkerheten eller sikkerhetsarbeidet. Noen deltakere har fått spørsmål fra tilsyn rundt effekten av tiltakene som er gjennomført. Få virksomheter har gode svar på dette.

Funn 7: Styringssystemene stemmer ikke med virkeligheten.

En utfordring som går igjen hos alle som har etablert et styringssystem, er å få styringssystemet innført i virksomheten. Styringssystemet stemmer ofte ikke med det virkelige liv. Det er flere grunner til at dette skjer, og vi vil i det følgende peke på de viktigste årsaker som kom frem i fokusgruppene.

Funn 8: Måten tilsyn gjøres på i dag fører til styringssystemer som er for lite tilpasset behovene.

Som beskrevet i avsnitt 3.1 kommer ofte informasjonssikkerhetskravene utenfra. Dette gjelder også krav om å etablere et styringssystem. Flere virksomheter ender da opp med å lage et styringssystem som tilfredsstiller disse eksterne kravene, men glemmer hva styringssystemet skal brukes til internt. Da blir det heller ikke brukt. En utfordring i denne sammenheng er hvordan tilsyn på styringssystemet oppleves i dag. ISO/IEC 27001 inneholder en omfattende liste av tiltak, hvor ikke alle er relevante for virksomheten. Siden det blir oppfattet at tilsyn ofte reviderer etter denne tiltakslista, prioriterer mange virksomheter å dokumentere hva de gjør knyttet til denne lista av tiltak, fremfor å lage et sikkerhetsregime som er tilpasset de lokale behovene. Dette resulterer igjen i styringssystemer som er for omfattende og store, og dermed lite brukervennlige.

Funn 9: For å lykkes med innføring må styringssystemet være brukervennlig og ha et enkelt språk.

Styringssystemene brukes primært av de som har fått ansvaret med å følge opp informasjonssikkerheten. Det er en oppfatning av at få andre forholder seg til styringssystemet. Dette skyldes delvis dårlig brukervennlighet og et komplisert språk, samt at styringssystemet ofte er stort. Et mulig virkemiddel for å gjøre et styringssystem mer tilgjengelig er å splitte opp styringssystemet etter områdene som er definert i standarden, slik at ikke alle må forstå og forholde seg til alt. Samtidig er det essensielt å lett kunne forstå hvordan delene i systemet henger sammen. Etterlevelse av styringssystemet bør ikke være avheng av at alle ansatte må ha lest styringssystemet. Arbeid med å bygge sikkerhetskultur har her en viktig rolle. Det må bygges en forståelse hos både ledere og ansatte om at sikkerhet er viktig, og dette må omsettes i praktiske tiltak og endring av adferd. Å bygge en god sikkerhetskultur oppleves som veldig utfordrende. Mange har gode enkelttiltak, for eksempel knyttet til deltakelse i den nasjonale sikkerhetsmåneden, noe som gir effekt på kort sikt. For å lykkes med å bygge sikkerhetskultur må man være god til å kommunisere med andre og påvirke ut i organisasjonen. Ettersom dette oppfattes som vanskelig, oppleves det lettere å kjøpe teknologi.

Funn 10: Det er vanskelig å bygge god sikkerhetskultur. Tekniske tiltak oppleves enklere og blir dermed prioritert.

Funn 11: Knapphet på ressurser vanskeliggjør vedlikehold og forbedring av styringssystemet.

Det er utfordrende å følge opp tiltak over tid. Det kommer stadig nye viktige oppgaver som gjør at fokus skiftes. Innføring, vedlikehold og forbedring av styringssystemet henger gjerne bare på én ildsjel, noe som gjør at arbeidet med informasjonssikkerhet blir sårbart. Det blir krevende å holde dokumentasjonen oppdatert, samt å følge opp om etablerte rutiner blir fulgt.

Tips og gode erfaringer fra fokusgruppedeltakerne:

- **Gjør det enkelt:** Start med et enkelt styringssystem for informasjonssikkerhet. Innfør gradvis. Ta bare med det absolutt nødvendige.
- **Forankring i toppledelsen:** Få toppledelsen til å signere på sikkerhetsstrategien.
- **Integrer med andre styringssystemer:** Det er lite som er spesifikt for informasjonssikkerhet. Arbeidet med å etablere et styringssystem blir mye enklere om man knytter seg opp virksomhetens eksisterende styringssystem.
- **Referer til styringssystemet:** I kommunikasjon rundt sikkerhet bør det refereres til innholdet i styringssystemet. Det gir legitimitet, samt at det øker bevissthet rundt og kjennskap til styringssystemet i virksomheten.
- **Bruk allerede innarbeidede prosesser:** Innarbeid risikovurderinger som en del av årlig rapporteringsprosess, knyttet til prioriteringer av aktiviteter for neste år.

3.3 Åpenhet

Hendelser og avvik er en viktig og god kilde til læring og forbedring. For å ta ut læringseffekten er imidlertid åpenhet en forutsetning. I det følgende beskriver vi hvordan fokusgruppene reflekterte rundt temaet åpenhet, samt hvordan de så på dagens praksis rundt rapportering og læring fra hendelser. Vi går så inn på årsaker til manglende åpenhet internt, og manglende åpenhet i møte med eksterne virksomheter og tilsyn.

Flere deltakere opplever at avviksrapporter gir god kunnskap om hva som bør prioriteres i arbeidet med informasjonssikkerhet. Noen leser gjennom alle rapporterte avvik på sikkerhet, og oppfatter at dette gir en god oversikt over utfordringene. Flere er opptatt av å få en god oppfølging av *alvorlige* hendelser, i form av både å kartlegge hva som har skjedd og foreslå tiltak. For alvorlige hendelser er som regel ledelsen godt informert. Det er imidlertid enighet om at det er en klar underrapportering av hendelser. I tillegg har mange virksomhetet liten oversikt over informasjonssikkerhetshendelser som oppdages knyttet til drift. Manglende rapportering og åpenhet om hendelser fører til at man ikke vet om sikkerhetsbrudd som har skjedd. Dermed gjøres det heller ikke tiltak for å forhindre lignende hendelser i fremtiden. Det er generelt lite fokus på *mindre* avvik, både når det gjelder rapportering og læring fra disse. Noen få miljøer forteller imidlertid om stor åpenhet om avvik, og at spesielt folk i IT-avdelingen er flinke til å rapportere.

Funn 12: Hendelser underrapporteres, og det er lite fokus på å lære av *mindre* avvik.

Selve rapporteringen av avvik oppleves som utfordrende. Noen virksomheter har svært mange ulike avviksrapporteringssystem, noen har mangelfulle systemer, mens andre mangler avviksrapporteringssystem ut mot brukerne. Selv om det er store problemer med systemene, ligger den største utfordringen i å skape en kultur for rapportering. Underrapporteringen man opplever handler i liten grad om uvilje mot å rapportere, men er i følge deltakerne et resultat av den "den norske kulturen": Man foretrekker å løse problemet selv der og da, og ønsker ikke å bruke tid på rapportering når ikke noe alvorlig har skjedd. Ansatte i virksomhetene må kontinuerlig motiveres for hvorfor de skal rapportere avvik, og bli påminnet når de skal gjøre det. Ledere har en viktig rolle i å bygge en god kultur for rapportering, samt sørge for at avviksmeldinger blir håndtert på en god måte i etterkant. Om ledere ikke ser poenget med rapportering, eller de bruker rapportene til å peke ut en ansvarlig for det som har skjedd, demper det motivasjonen til å rapportere i organisasjonen. Dersom hendelser er forårsaket av ledere er det bred enighet om at rapportering er spesielt utfordrende.

Funn 13: En god kultur for avviksrapportering er viktigere enn et perfekt avviksrapporteringssystem.

Sikkerhetshendelser og avvik er som nevnt en viktig kilde til læring og forbedring. Denne læringen kan økes ytterligere om man deler informasjon om hendelser på tvers av virksomheter. Å få til slik deling i praksis blir imidlertid sett på som utfordrende, fordi de fleste virksomheter ikke er interessert i å dele informasjon om egen sårbarhet. Selv om deling er vanskelig og det er liten åpenhet mellom virksomheter, foregår noe deling i dag i lukkede fora. For å få slike fora til å bli gode, er det viktig å være klar over at ulike virksomheter opplever ulik risiko. Læring på tvers er nyttig, men det blir oppfattet som mindre nyttig å sette i gang aktiviteter knyttet til å samle inn hendelsesinformasjon, og analysere denne informasjonen på tvers av virksomheter. Målet med å belyse enkelthendelser må være å lære, og ikke å henge ut en etat.

Funn 14: Manglende åpenhet vanskeliggjør deling av hendelsesinformasjons på tvers av virksomheter for felles læring.

Funn 15: Feil blir dekket over for å se bedre ut ved tilsyn.

Problemer knyttet til åpenhet finner man også i møte med tilsyn. Virksomheter ønsker ikke at tilsynet finner feil fordi dette medfører masse ekstraarbeid. Resultatet er at virksomhetene dekker over feil for å se bedre ut enn det de er, og dermed er det ikke mulig å lære av egne feil.

Tips og gode erfaringer fra fokusgruppedeltakerne:

- **Fortell om hendelsene:** Bruk virkelige hendelser som eksempler når sikkerhet diskuteres internt i virksomheten. Dette øker rapporteringen, og gir bedre forståelse for hvorfor sikkerhet er viktig.
- **Pek aldri på ansvarlig:** Så langt det er mulig bør man unngå å utpeke en ansvarlig for hendelsen.
- **Evaluer hendelser:** Ved hendelser er det viktig å kartlegge hva som har skjedd, og foreslå tiltak. Dette bør gjøres med mandat fra toppledelsen, og de må få resultatet av evalueringen.

3.4 Forståelse av risiko

For at en virksomhet skal kunne ta effektive beslutninger knyttet til informasjonssikkerhet er det viktig å ha en god forståelse av hvilken risiko virksomheten blir utsatt for. Deltakerne i fokusgruppene beskrev store utfordringer knyttet til å oppnå en felles forståelse av risiko i organisasjonen, samt utfordringer med oppnå en felles forståelse av hva informasjonssikkerhet er og hvorfor det er viktig. Flere deltakere hadde erfaring med at ansatte og ledere fikk økt forståelse for risiko knyttet til informasjonssikkerhet ved å delta aktivt i sikkerhetsarbeid. Risikovurderinger er en viktig teknikk i så måte. I det følgende gir vi en beskrivelse av erfaringer knyttet til å oppnå en felles forståelse av risiko i virksomhetene. Vi tar spesielt for oss erfaringer deltakerne har gjort seg knyttet til risikovurderinger.

Funn 16: Virksomheter mangler felles forståelse av hva risiko er og hvilken risiko som er akseptabel.

Forståelse av risiko innebærer forståelse av *hva* som medfører risiko, og *hvor stor* risikoen er. Virksomheter må også ha en formening om hvilken risiko som er akseptabel. Det er umulig, og heller ikke kostnadseffektivt, å fjerne all risiko. Forståelsen av risiko varierer mye mellom ulike grupper i virksomheten, for eksempel mellom teknikere og ledere. Som eksempel vil teknikere gjerne overdrive risikoen, mens ledere raskere aksepterer risiko. Vurdering av risiko avhenger ofte av den intuitive forståelsen de involverte har av hvilken risiko som er akseptabel. Denne forståelsen er imidlertid ofte ikke dokumentert og heller ikke diskutert i ledelsen. Siden ledere er ansvarlige for informasjonssikkerheten og er de som tar viktige beslutninger, er det aller viktigst at ledere har en god forståelse av hva risiko er og hva som er akseptabelt nivå.

Det å skape en felles forståelse av risiko i virksomheten er utfordrende, og tar tid. Dette skyldes blant annet de faktorer som er nevnt tidligere: Manglende måling av informasjonssikkerhet, manglende sikkerhetskultur,

samt manglende integrasjon mot virksomhetsmål. I tillegg er forståelsen av risikoen knyttet til IT-systemene lav så lenge systemene virker. Et annet moment er at informasjonssikkerhet for mange hovedsakelig er knyttet til konfidensialitet, og så lenge systemene i stor grad skal være åpne, sees ikke informasjonssikkerhet som særlig relevant.

Funn 17: Informasjons-sikkerhet forbindes med konfidensialitet, mens det er lite fokus på integritet og tilgjengelighet.

Funn 18: Ved deltakelse i sikkerhetsarbeid øker forståelse av risiko.

Deltakelse i risikovurderinger og øvelser er viktig for å øke forståelse for risiko, og det er avgjørende at de som eier risikoen deltar i slike aktiviteter. Informasjonssikkerhetsfolk kan gjerne fasilitere. Det er imidlertid en rekke utfordringer knyttet til å gjøre risikovurderinger:

- **Verdiklassifisering:** For å kunne vurdere risiko knyttet til ulike hendelser trengs det en oversikt over egne verdier, og en riktig og omforent klassifisering av disse verdiene. Utfordringen er at for mange verdier rangeres høyt, noe som gjør det vanskelig å prioritere i det videre arbeidet.
- **Metodeusikkerhet:** Det finnes en lang rekke veiledninger som beskriver hvordan risikovurderinger skal gjøres. De mange forskjellige faglige tilnærmingene skaper imidlertid forvirring og medfører at det går mye tid til å velge metode. Dessuten benyttes noen ganger ulike metoder i samme virksomhet, noe som gjør at det blir vanskelig å se resultater fra ulike analyser i sammenheng.
- **Kompetanse:** Det å jobbe risikobasert krever forståelse av teknologien, organisasjonen, trusler og gjensidige avhengigheter, samt kunnskap om hvordan gjennomføre risikovurderinger. Manglende kompetanse medfører at de risikovurderinger som blir gjort er av svært ulik kvalitet. Når beslutninger tas på bakgrunn av risikovurderinger av lav kvalitet gir det lite effektive tiltak og falsk følelse av kontroll.
- **Tid og ressurser:** I store virksomheter er det mye som skal risikovurderes, noe som krever mye ressurser. Noen ledere skjønner viktigheten av risikovurderinger og prioriterer dette arbeidet. Andre ser risikovurderingen kun som en pest og en plage – og de ender opp med å gjøre minst mulig.
- **Etablering av rutiner:** Det er et krav at overordnede risikovurderinger skal dokumenters, men risikovurderinger som skjer mer uorganisert, f.eks. i ledermøter eller i det daglige arbeidet, er ofte ikke dokumentert. Det er også vanskelig å følge opp om risikovurderinger faktisk blir gjort, f.eks. ved endringer eller innføringer av nye IT-systemer.

Funn 19: Regelverk bør understøtte en risikobasert tilnærming, men samtidig ta høyde for at ikke alle har kompetanse til å jobbe risikobasert

Det er ulike oppfatninger om hva som er best av en risikobasert og en regelbasert tilnærming til informasjonssikkerhet. Gjennom en risikobasert tilnærming, vil den risiko som oppleves være utgangspunktet for hvilke sikkerhetskrav som stilles, og resultatet er at de viktigste problemene blir løst først. En risikobasert tilnærming har imidlertid større krav til kompetanse enn det en regelbasert tilnærming har. De mange kravene knyttet til informasjonssikkerhet, f.eks. fra tildelingsbrev og lovverk, forstås som en del av et regelbasert perspektiv, og er ofte i konflikt med den risikobaserte tilnærmingen. En av grunnene til denne konflikten er at regelverket ofte har mest fokus på konfidensialitet, mens tilgjengelighet kan være viktigere når man ser på risikobildet til virksomheten. En regelbasert tilnærming er imidlertid fornuftig der det trengs minimumsstandarder på tvers av virksomheter. Spesielt gjelder dette når sikkerheten i en etat kan påvirke sikkerheten hos andre. Selv om det oppfattes at regelbasert og risikobasert tilnærming kan være i konflikt, kan de også kombineres. En regelbasert tilnærming kan for eksempel fremsette krav om risikovurdering. Hos noen deltakere var det klart at risikovurderinger primært ble gjort når det var spesifikt krav om dette.

Selv om risikovurderinger er komplisert og utfordrende arbeid, er slike vurderinger nyttige for å øke forståelse for risikoen i en virksomhet. Det er også viktig å være klar over at det å *gjennomføre* en risikovurdering som regel er viktigere enn *hvordan* den gjøres. Diskusjonene er viktigere enn selve resultatet.

Tips og gode erfaringer fra fokusgruppedeltakerne:

- **Involver nøkkelpersoner i sikkerhetsarbeidet:** Det å delta i sikkerhetsarbeid er en effektiv måte å øke forståelsen for informasjonssikkerhet og risiko på. Risikoeiere bør delta i risikovurderinger.
- **Vær tydelig på mål og kontekst:** Deltakerne må få vite at målet med analysen er å vurdere informasjonssikkerheten, og at de skal ta utgangspunkt i verdiene til virksomheten. Det må klargjøres hvilke typer konsekvenser risiko skal vurderes opp i mot (for eksempel økonomiske konsekvenser eller omdømmekonsekvenser). Ofte er det fornuftig å gjøre fokuserte analyser som kun tar for seg utvalgte deler av systemet.
- **Dyrk diskusjonene:** Risikovurderingene blir bedre gjennom gode diskusjoner, hvor man evner å få frem ulike perspektiver. Dette bør det tas hensyn til i sammensetning av en gruppe og i forhold til hvordan prosessen fasiliteres.
- **Vurder ekstern fasilitator:** Eksterne fasilitatorer har bidratt til å få opp ledelses- og styringsperspektiver i risikovurderinger.

3.5 Sikkerhet under utvikling av IT-systemer

Blant virksomhetene som deltok i fokusgruppene er det stor variasjon i hvor stor grad informasjonssikkerhet er et tema ved utvikling av IT-systemer. Noen deltakere forteller at nylig utviklede systemer har hatt lite fokus på informasjonssikkerhet, mens andre har definerte prosedyrer som omhandler informasjonssikkerhet i utviklingsprosjekter. Det virker imidlertid som en trend at utviklingsprosjekter har økende fokus på informasjonssikkerhet. Flere virksomheter har fått enorme utfordringer fordi sikkerhetsproblemer har blitt oppdaget sent i utviklingsprosessen. I det følgende beskriver vi ulike måter informasjonssikkerhet har blitt håndtert på under utvikling, og erfaringer som er gjort.

Funn 20: Det er økende fokus på sikkerhet under utvikling av nye systemer.

Generelt har gjennomføringen av utviklingsprosjektene blitt bedre selv om systemene har blir mer komplekse og mer omfattende. Forretningssiden forstår at de må stille klare krav og gjennomføre risikovurderinger, og at systemene må være pålitelige og støtte virksomhetens mål. Representanter for informasjonssikkerhet involveres i større grad i selve utviklingsprosjektene, men ofte er involveringen tilfeldig og for liten, og skjer for sent i prosessen. Informasjonssikkerhet blir fortsatt sett på som et teknologianliggende, noe som gjør at sikkerhet forventes dekt av IT-avdelingen. Sikkerhet er derfor ikke et tema når det jobbes med løsningsbeskrivelsen. Men situasjonen er ikke bare dyster. Hos noen virksomheter er for eksempel representanter for informasjonssikkerhet involvert i både krav- og løsningsbeskrivelsesprosessene. En viktig grunn til at det er lite bevissthet rundt informasjonssikkerhetskrav, er at utviklingsorganisasjonen mangler risikoforståelse. Et typisk eksempel som har blitt henvist til av mange virksomheter, er at det mangler en avklaring av hvilke behov virksomheten har knyttet til tilgjengeligheten av et nytt system. I tillegg er det liten bevissthet og kompetanse knyttet til de krav lovverk stiller til sikkerhet. Her er en nøkkel å få til en god kommunikasjon mellom jurister og IT.

Funn 21: Informasjons-sikkerhet involveres ofte for sent i utviklingsprosessen.

Som tidligere beskrevet er informasjonssikkerhetsressurser sjelden involvert i selve utviklingsprosessen. Noen virksomheter har imidlertid god involvering gjennom jevnlige risikovurderinger og andre møter. Det finnes gode eksempler på sikkerhetsfolk som har tipset utviklere om OWASP og gått gjennom sjekklister sammen med utviklingsorganisasjonen. Tidspresset i prosjektene gjør imidlertid gjerne at informasjonssikkerhetskrav blir utsatt og nedprioritert: Funksjonalitet vinner over sikkerhet. Dette blir sett på som en enda større utfordring i smidig utvikling. Ved bruk av en fossefallsmetode var alle krav definert før prosjektet startet og leverandørene måtte levere alt i kravlista. I dag sitter tjenesteansvarlig i sprintmøter og tar store beslutninger som blant annet også angår informasjonssikkerhet. Ofte er det en konflikt mellom funksjonalitet og ressurser i en sprint og da blir gjerne sikkerhetskrav skjøvet til neste sprint. Noen sikkerhetskrav blir utsatt helt til forvaltningsfasen. Noen opplever arkitekter som allierte i arbeidet med informasjonssikkerhet, mens andre opplever at arkitekter bryr seg lite om sikkerhet. Det fremheves imidlertid at det er en forutsetning at sikkerhet er en del av arkitektur- og designarbeidet, og at det er en god dialog mellom arkitektene og de som jobber med informasjonssikkerhet. Informasjonssikkerhet må være en del av mandatet til arkitekten.

Funn 22: Funksjonalitet vinner over sikkerhetskrav i utviklingsprosjekter.

Noen steder er sikkerhet et aspekt i den kontinuerlige testprosessen, men dette er ikke vanlig. En av grunnene er at det er vanskelig å teste ikke-funksjonelle krav (inkludert informasjonssikkerhet) i en tidlig fase. For å bøte på dette leier noen inn eksterne sikkerhetstestere ved slutten av prosjektet, men i denne fasen er det ofte dyrt å rette opp feil.

En utfordring som går igjen i utviklingsprosjekt er manglede kompetanse på informasjonssikkerhet. Utviklere har generelt lite kompetanse om hvordan ivareta informasjonssikkerhet, noe som blant annet skyldes at informasjonssikkerhet ikke er en obligatorisk del av utdanningen. Forretningssiden som stiller krav og leverandørene som skal levere en løsning, mangler også kompetanse på informasjonssikkerhet, og har manglende risikoforståelse. IT-avdelingen er ofte kun inne og gir støtte på tekniske tiltak som tilgangskontroll og logging, mens andre aspekter ved informasjonssikkerhet får lite oppmerksomhet.

Funn 23: Både bestiller og leverandør mangler kompetanse om hvordan ivareta sikkerhetskrav i utviklingsprosjekter.

Tips og gode erfaringer fra fokusgruppedeltakerne:

- **Identifiser sikkerhetskrav tidlig:** Hvis de som jobber informasjonssikkerhet ikke blir involvert fra starten av prosjekt, blir det vanskelig komme med og få prioritert sikkerhetskrav.
- **Spill på lag med jus:** Krav til sikkerhet kommer ofte fra lovverket. Derfor er det viktig å samarbeide med juristene. Et slikt samarbeid kan øke bevissthet rundt informasjonssikkerhet i hele utviklingsorganisasjonen.

3.6 Kompetanse

Kompetanse er en gjennomgående utfordring knyttet til alle temaområdene vi har beskrevet over. Det er nødvendig med kompetente og engasjerte personer som jobber med informasjonssikkerhet for å få:

- Informasjonssikkerhet integrert med virksomhetsmålene
- Etablert og innført et fungerende styringssystem for informasjonssikkerhet
- Åpenhet og en god forståelse av risiko
- Sikkerhet som en del av IT-systemene som utvikles.

I det følgende gir vi en oversikt over områder hvor det oppleves at forvaltningen har god kompetanse, samt områder hvor det er særskilt behov for å øke kompetansen. Vi beskriver også utfordringer med å opprettholde og utvikle kompetanse.

Nivå på sikkerhetskompetanse blant statlige virksomheter varierer stort. Noen virksomheter har små miljøer med lav formell og uformell kompetanse, mens andre virksomheter har store og dyktige miljø med god formell kompetanse. Det som skrives om kompetanse i dette kapitlet må ses i lys av denne diversiteten.

Funn 24: Teknisk kompetanse er tilfredsstillende.

Selv om tilgang på teknisk kompetanse knyttet til sikkerhet oppleves som en utfordring, er det vårt inntrykk at denne generelt er god blant de virksomheter som deltok i undersøkelsen. Områder som drift, nettverkssikkerhet og redundans virker å bli håndtert på en god måte. De fleste virksomheter har også god forståelse av krav knyttet til konfidensialitet og personvern og hvordan slike data kan sikres teknisk.

Funn 25: Kompetanse-utfordringer finnes på alle nivåer og områder i og utenfor virksomheten.

Det er kompetanseutfordringer på alle nivåer i virksomhetene: Hos vanlige brukere, ledere, og blant de som jobber med informasjonssikkerhet. Dette er en utfordring i det daglige arbeidet, og skaper usikkerhet rundt om virksomhetene er i stand til å kunne håndtere en større sikkerhetshendelse. Det oppleves også at departementene har lav kompetanse. Når de som stiller krav til informasjonssikkerhet mangler kompetanse, fører dette til uklare eller for tekniske krav, og at informasjonssikkerhet ikke blir ivaretatt når nye lover lages eller gamle endres. Følgende områder peker seg ut når det gjelder utfordring med kompetanse knyttet til informasjonssikkerhet:

- **Styringssystemer:** De som har kommet kort i å etablere og innføre styringssystem for informasjonssikkerhet har et stort behov for å forstå hvordan de skal drive dette arbeidet: Identifisere behov, involvere virksomheten i tilpasning, integrasjon mot eksisterende styringssystem, og innføring i virksomheten.
- **Risikovurderinger:** Gjennom en risikobasert tilnærming er det enklere å få en kostnadseffektiv sikkerhet fordi virksomheten vil ta det viktigste først. En risikobasert tilnærming krever imidlertid høy kompetanse. Siden kompetansen varierer, varierer også kvaliteten på risikovurderingene stort.
- **Regler:** Krav knyttet til informasjonssikkerhet er spredt ut over mange lover og regelverk, og kommer fra mange ulike myndigheter og organisasjoner. Det er en stor utfordring å holde oversikten over alle krav.
- **Sikkerhet i utvikling:** Forretningssiden, utviklere og eksterne leverandører mangler kunnskap om hvordan ivareta sikkerhet i utviklingsprosjekter. Dette medfører en nedprioritering av sikkerhetskrav i både små og store utviklingsprosjekter.

Funn 26: Det trengs bedre oversikt over regelverk og lovverk som påvirker sikkerhetsarbeid.

I tillegg til behov for økt kompetanse innen disse områdene, trenger de som jobber med informasjonssikkerhet også god kompetanse innen faget **organisasjonsutvikling:** Hvordan endre kulturen i en organisasjon, hvordan kommunisere og gjennomføre tiltak, hvordan øke kunnskapen og sikre læring, samt hvordan påvirke holdninger, meninger og adferd. Det er viktig med formell og uformell sikkerhetskompetanse, men det hjelper lite hvis fagpersonene ikke evner å endre organisasjonen.

Funn 27: Det kreves god kompetanse på organisasjonsutvikling for å lykkes med sikkerhetsarbeid.

Arbeidet med å bygge sikkerhetskompetanse i en virksomhet vanskeliggjøres av kompleks terminologi knyttet til informasjonssikkerhet. Informasjonssikkerhet oppleves som og er et utfordrende fag, og mye av terminologien som brukes kommuniserer dårlig mot andre i virksomheten. Informasjonssikkerhet er også et område i stor endring der det er behov for kontinuerlig oppdatering blant annet når det gjelder nye trusler. I

tillegg blir IT-systemene stadig mer komplekse. For virksomheter som har satt ut sin IT-drift til eksterne er det utfordrende å holde kontroll med sikkerheten og stille riktige krav til de som drifter systemene.

Manglende kompetanse er spesielt en utfordring hos små virksomheter. Dette handler mye om mulighet til å sette av tid og dedikerte ressurser til sikkerhetsarbeid, og sårbarhet knyttet til fravær hos nøkkelpersoner. Spesielt mindre virksomheter kjenner lite til kompetansehevende aktiviteter som Difi tilbyr, for eksempel Nettverk for Informasjonssikkerhet (NIFS).

Funn 28: Kompetanse-utfordringene er størst hos mindre virksomheter.

Tips og gode erfaringer fra fokusgruppedeltakerne:

- **"Learning by doing":** For å bygge opp kompetanse om sikkerhet i organisasjonen må de ansatte delta i sikkerhetsarbeid.
- **Opprettelse av fagfora i egen virksomhet:** Slike fora er viktig for å øke kompetansen, i tillegg til at sikkerhetsutfordringer hverken bli glemt eller faller mellom to stoler.
- **Fagnettverk utenfor egen virksomhet:** Det er viktig å delta i fagnettverk utenfor egen virksomhet. NIFS trekkes fram som en møteplass der man kan diskutere hva et styringssystem er, hva som fungerer og hva som ikke fungerer.

4 Diskusjon av forventninger og behov, og anbefalinger knyttet til aktiviteter for Difi

Forrige kapittel gav en oversikt over et sett av temaområder som ble identifisert gjennom en sammenlignende analyse av fokusgruppene. Ut fra disse temaene, vil vi nå gi noen anbefalinger når det gjelder hvilke aktiviteter og tiltak Difi bør prioritere for å møte de etterspurte forventningene og behovene fra offentlige virksomheter. Etter at tiltakene og aktivitetene er beskrevet vil vi knytte resultatene fra fokusgruppene opp mot tidligere undersøkelser og relevant forskning innen området.

4.1 Anbefalinger til aktiviteter for Difi

Beskrivelsene av temaområdene i forrige kapittel pekte på en rekke utfordringer og behov. Selv om Difi vil ha en nøkkelrolle og være en katalysator for å heve nivået på arbeidet med informasjonssikkerhet i offentlig sektor, er det klart at virksomhetene må gjøre selve arbeidet selv. Statlige virksomheter må:

- Knytte sikkerhet opp mot sine egne virksomhetsmål,
- Etablere et styringssystem som passer for dem,
- Gjøre sine egne risikovurderinger,
- Jobbe med kulturen i egen virksomhet
- Sette fokus på sikkerhet i sine egne utviklingsprosjekter.

Ut fra sin rolle i statsforvaltningen har imidlertid Difi en nøkkelrolle når det gjelder å sette virksomhetene i bedre stand til å gjøre dette arbeidet på en god og effektiv måte. Basert på resultatene presentert i denne rapporten, bør Difi prioritere kompetansebyggende aktiviteter. Som beskrevet i avsnitt 3.6 så er riktig kompetanse en forutsetning for å lykkes med informasjonssikkerhet, og manglende kompetanse knyttet til informasjonssikkerhet er hovedårsaken til dagens problemer og utfordringer. I tillegg anbefaler vi Difi å ta en sterkere koordinerende rolle, og således hjelpe virksomheter til å navigere blant og forholde seg til det mylder av lovkrav, veiledninger og aktører de møter på informasjonssikkerhetsområdet. En koordinerende rolle omfatter også å initiere og fasilitere ulike former for praksisfellesskap mellom statlige virksomheter.

En forutsetning for å lykkes med tiltakene Difi skal i gang med er at tilbudet må gjøres kjent hos virksomhetene og at de bærer preg av å være lavterskeltilbud. Gjennom analysen presentert i denne rapporten er det klart at de miljøer som har kommet kort i arbeidet med informasjonssikkerhet i mindre grad benyttet seg av eksisterende møteplasser. En annen observasjon er at det er tilfeldig hvem i organisasjonen som får informasjon om de tilbud som finnes.

4.1.1 Aktiviteter for å heve kompetanse

Virksomhetene har klare ønsker om støtte fra Difi for å heve egen kompetanse. Det gjelder ønsker om hjelp til samordning slik at ikke alle virksomheter må finne på alt selv, og ønsker om møteplasser, kurs, workshoper og foredrag. Mer umodne miljøer uttrykker også et behov for mer direkte støtte og rådgivning slik at de bedre mestrer å drive arbeidet selv. Det er også et sterkt behov for at Difi initierer og koordinerer arenaer for kompetansebygging i form av praksisfellesskap. Praksisfellesskap vil være omtalt mer i detalj i delkapittel 4.1.2.

Tabell 2 gir en oversikt over aktiviteter og tiltak som vil sette Difi i stand til å stimulere til økt kompetanse om informasjonssikkerhet i forvaltningen. Aktivitetene bør ta utgangspunkt i områder der det er et spesielt behov for bedre kompetanse. Disse områdene er detaljert beskrevet i avsnitt 3.6. Når det gjelder hvilken type kurs som bør benyttes så bør noen være samlingsbasert med høy interaktivitet (for eksempel innen området kultur og forankring, styringssystemet og sikkerhet i utvikling), mens andre kan være korte kurs (for eksempel risikovurdering, regler, og mer tekniske orienterte kurs). De korte kursene kan også være nettbaserte. Mange av virksomhetene er spredt rundt i hele landet, og for å nå de med lang reisevei kan det derfor være hensiktsmessig å tilby nettbaserte og videobaserte alternativer.

Tabell 2. Anbefalte aktiviteter knyttet til kompetanse

Aktivitet	Målgruppe	Beskrivelse
Kurs og workshoper	Sikkerhetsfolk i forvaltningen	Faglig oppdatering innen viktige tema som risikoanalyse, styringssystemer, sikkerhetskultur, ledelsesforankring og sikkerhet ved bestilling og utvikling av nye IKT-løsninger.
Foredrag	Ledere, utviklere, leverandører, studenter, sikkerhetsfolk	Difi bør være synlige på viktige møteplasser. Spesielt bør Difi være til stede der ledere i offentlig forvaltning møtes, for å bidra til økt fokus på og forståelse for informasjonssikkerhet blant ledere.
Utdanning	Studenter og de som tar videreutdanning	Difi bør ha en rolle med å holde foredrag i informasjonssikkerhetsfag og videreutdanningsprogram ved høgskoler og universiteter. Det er spesielt viktig å få informasjonssikkerhet inn i systemutviklingsutdannelsen. Difi bør være en pådriver her.
Lavterskel rådgivning	Sikkerhetsfolk i små/umodne miljøer	Difi bør være tilgjengelige for forvaltningen som en samtalepartner, og for å gi råd tilknyttet behov hos enkeltorganisasjoner. En viktig bit av dette er å hjelpe virksomheter med hvem de kan kontakte om ulike sikkerhetsrelaterte problemstillinger, inkludert spørsmål knyttet til bestilling og utvikling av nye IT-systemer.

Selv om flere deltakere etterlyste støtte i form av tilgjengelige maler og eksempler, har vi ikke lagt inn aktiviteter knyttet til dette i våre anbefalinger til prioriterte aktiviteter for Difi. I fokusgruppene var ønsket om maler og eksempler sterkest knyttet til styringssystemer og risikovurderinger. For eksempel var det ønske om at Difi tilbyr ulike grunnmodeller for styringssystemer tilpasset ulike typer virksomheter. Vi ser imidlertid en fare for at slike maler og eksempler kan bli brukt som en enkel løsning på å få etablert den formelle delen av styringssystemet. Da får man hverken nødvendig eierskap til styringssystemet i virksomheten, eller et styringssystemet som stemmer med organisasjonen. I stedet foreslår vi at de som har behov for støtte, for eksempel knyttet til å innføre et styringssystem for informasjonssikkerhet, kan få veiledning og utveksle erfaringer i en mindre gruppe sammen med andre med lignende utfordringer. De virksomhetene som har erfaring med temaet kan dras inn som ressurspersoner i slike grupper ved behov. Difi kan legge til rette for opprettelse av slike temagrupper og praksisfellesskap, og trekke seg ut når gruppen er blitt selvgående. Dette er nærmere beskrevet i delkapittel 4.1.2.

Difi bør også være tilgjengelige for råd og samtale for virksomheter som jobber med ulike typer sikkerhetsproblematikk, enten dette er innføring av styringssystemer eller bestilling eller utvikling av nye IT-systemer. Merk at selv om Difi bør være tilgjengelige for råd, bør de ikke ta rollen som konsulenter.

4.1.2 Aktiviteter knyttet til koordinerende rolle

I dag er det mange aktører som har en rolle knyttet til informasjonssikkerhet, og regelverket knyttet til informasjonssikkerhet er svært spredt. Området oppleves dermed som uoversiktlig. Derfor anbefaler vi at Difi prioriterer koordinerende aktiviteter som kan gjøre sikkerhetslandskapet mer oversiktlig for statlige virksomheter, samt hjelpe dem til å navigere i dette landskapet. En koordinerende roller innebærer også å legge til rette for opprettelsen og utvikling av ulike typer nettverk og praksisfellesskap. Tabell 3 gir en oversikt over tiltak vi anbefaler.

Tabell 3. Anbefalte aktiviteter knyttet til koordinerende rolle

Aktør	Aktiviteter
Sikkerhetsmiljøer	Koordinering og samarbeid med andre sikkerhetsmiljøer, for å sikre faglig tyngde, samordne veiledning samt avklare ansvarsområder slik at virksomheter vet hvem man skal kontakte om hva.
Tilsyn	Bygge bro mot tilsyn, ved å ta opp utfordringer virksomheter opplever med hvordan tilsyn gjøres. Difi har muligheten til å ha en nøytral rolle, og kan bidra til å samordne behovene både på tilsynssiden og i virksomhetene for å unngå de uheldige virkningene noen virksomheter opplever med tilsyn i dag, samt styrke de positive virkningene tilsyn har.
Kravstillere i departement og hos tilsynsmyndigheter	Styrke kompetanse hos kravstillere, samt ta rollen med å uttale seg om nye lover og forskrifter. Målet bør være både å passe på at det stilles krav til informasjonssikkerhet, og at kravene som stilles er fornuftige og presenteres i et språk som fremmer ledelsesforankring av informasjonssikkerhet i virksomhetene. Mot virksomhetene kan Difi bidra til å gi oversikt over relevant regelverk.
Andre virksomheter i statsforvaltningen - *Større konferanser* - *Temagrupper* - *Regionale fora*	Difi bør støtte opp om eksisterende møteplasser som er relevante for Difis målgruppe, samt etablere nye der det behov for det: - Difi bør bidra til møteplasser som samler alle de viktige aktørene, og som derfor er attraktive å delta på. - Difi bør bidra til at virksomheter med felles utfordringer og felles fokus kan opprette et praksisfellesskap der de utveksler erfaringer og støtter hverandre i arbeidet. Som eksempel kan en ha grupper av virksomheter som skal starte arbeidet med å innføre et styringssystem for sikkerhet, og grupper for virksomheter som er i gang med større bevissthetsarbeide. Slike grupper kan startes av Difi, for så å bli selvgående. - Flere deltakere ser nytte av å ha mindre fora der man kan etablere tillit over tid, og utveksle erfaringer. For å lette utfordringer med å sette av tid og ressurser til å møtes i slike fora kan Difi legge til rette for at det etableres regionale møteplasser der erfaringer knyttet til informasjonssikkerhet kan utveksles.

I Norge er det mange sikkerhetsmiljøer. Eksempler er NSM og NorSIS. I tillegg er det sterke miljøer i flere departementer og etater. Flere ulike tilsynsmyndigheter har også en viktig rolle ovenfor virksomhetene. Dette gjør at virksomheter kan oppleve det som utfordrende å finne ut hvilke miljøer man skal forholde seg til i ulike situasjoner. Utfordringene blir ekstra store de ganger de ulike sikkerhetsmiljøene har motstridende synspunkter. I tillegg opplever flere virksomheter en mangel på samordning i forhold til rapportering til ulike instanser: De må rapportere nesten den samme informasjonen til departementer, Riksrevisjonen og Statistisk sentralbyrå, og det å bruke tid på å lage ulike rapporter med mye av den samme informasjonen oppfattes som bortkastet. Som en konsekvens av de mange aktørene på området finnes det i dag mange veiledninger og anbefalinger knyttet til ulike deler av informasjonssikkehetsområdet. Et eksempel er beskrivelse og maler for hvordan man skal gjøre risikovurderinger. Dette oppleves forvirrende, og kompliserer arbeidet i de ulike virksomhetene.

Det er viktig at Difi ikke blir nok et fagmiljø en virksomhet må forholde seg til og som ikke er koordinert med de andre fagmiljøene. Difi bør derfor se det som en del av sin rolle å kommunisere og samordne statlige virksomheters behov ovenfor de tidligere beskrevne sikkerhetsmiljøer. Gjennom å søke samarbeid, vil Difi sette virksomhetene i stand til å utnytte den samlede kompetansen i sikkerhetsmiljøene. Rollen til Difis nye seksjon, samt hvilke relasjoner dette seksjonen har til andre miljøer, bør kommuniseres til seksjonens

brukergruppe. Difi bør være en aktiv pådriver for bedre samordning og harmonisering av veiledninger, i samarbeid med de andre sikkerhetsmiljøene. I tillegg må Difi være i stand til å gi klare anbefalinger når det gjelder hvilke veiledninger og maler statlige virksomheter bør benytte.

Difi må ha en tett dialog med tilsynsmyndigheter. I fokusgruppene har det blitt avdekket utfordringer knyttet til manglende åpenhet, som er et resultat av hvordan tilsyn gjøres. Det har også blitt avdekket utfordringer knyttet til hvordan Riksrevisjonen reviderer styringssystemet for informasjonssikkerhet i en virksomhet. Dagens praksis medfører at det lages mye sikkerhetsdokumentasjon for å tilfredsstille tilsyn, og ikke ut fra reelle behov i virksomheten. Slik dokumentasjon har ingen verdi når det gjelder å bedre informasjonssikkerheten i virksomheten. Tilsynsmyndighetene må derfor få en noe endret rolle ovenfor virksomhetene og Difi må lede dette arbeidet. Difi kan bidra til dialog og bedre forståelse av hvordan tilsyn kan gjennomføres, slik at målet om bedre informasjonssikkerhet i større grad blir nådd.

Når det gjelder kravstillere i departementer og hos tilsynsmyndigheter, er det et behov for at Difi både bidrar til bedre kompetanse om informasjonssikkerhet i disse miljøene, samt påvirker tekster og innhold i lover og forskrifter. Fokusgruppene avdekket at formuleringen av krav knyttet til sikkerhet er viktig for å sikre ledelsesforankring og unngå at informasjonssikkerhet blir sett på kun som en teknisk utfordring. I tillegg er kompetansen hos de som deltar i etatsmøtene (fra departementet sin side) viktig for å få ledelsen til å innse sitt ansvar for informasjonssikkerhet. For virksomhetene kan Difi bidra til å gi en bedre oversikt over relevant regelverk, slik at virksomheter blir i stand til å forholde seg til de riktige lovene og reglene.

I arbeid med å gi innspill til regelverk bør Difi gjøre vurderinger av om dagens krav i tilstrekkelig grad dekker tilgjengelighets- og integritetsaspektene ved informasjonssikkerhet. Det er også viktig at Difi har en formening om hvordan balansere behovet for regelstyring med behovet for en risikobasert tilnærming. Selv om statlige virksomheter har mye til felles, er det store variasjoner knyttet til trusler man opplever og verdien av informasjonen man håndterer. Dette må gjenspeiles i gjeldende regelverk.. Samtidig er det viktig å være bevisst at en risikobasert tilnærming krever mer av virksomhetene når det gjelder kompetanse, i forhold til en regelbasert tilnærming.

For å bidra til god koordinering av sikkerhetsarbeidet i forvaltningen, anbefaler vi at Difi prioriterer å legge til rette for opprettingen av nyttige møteplasser. Kompetanse utvikles godt når det oppstår en dialog der man reflekterer, diskuterer og deler erfaring med hverandre. Viktighetene av en slik tilnærming ble bekreftet da deltakerne evaluerte fokusgruppene, og trakk frem viktighetene av å ha mindre grupper hvor man kan dele erfaringer og lære av hverandre. Når Difi fasiliteter møter og workshoper med ulike virksomheter er det viktig å ikke bare identifisere områder der det er behov for hjelp og støtte, men også plukke opp praksiser som fungerer godt og som andre kan lære av. Dette kan så spres videre i ulike fora, for eksempel gjennom kurs og foredrag og i samtaler og dialog med ulike virksomheter.

4.2 Våre anbefalinger opp mot behov og ønsker identifisert i workshop arrangert av Difi

Som nevnt i innledningen har Difi selv gjennomført en workshop som har identifisert forventninger og behov til den nyopprettede seksjonen [5]. På denne workshopen ble spesielt følgende utfordringer trukket frem:

- Kunnskapsnivå, opplæring av ansatte og sikkerhetskultur
- Risikovurderinger, verdivurderinger og klassifiseringer
- Styringssystem for informasjonssikkerhet

I tillegg ble det diskutert utfordringer knyttet til elektronisk samhandling/kommunikasjon, fragmentert regelverk innen informasjonssikkerhet, ressursmangel, manglende erfaringsutveksling, utfordringer med å få

operasjonalisert/implementert sikkerhet i virksomheten og i tekniske løsninger, samt utfordringer knyttet til ny teknologi (skytjenester, økt behov for mobilitet). Følgende tiltak ble trukket frem:

1. Informasjonsdeling mellom offentlige virksomheter: Nettverk/forum/samarbeidsarenaer
2. Opplæring: Kurs, konferanser, foredrag i virksomhetene
3. Rådgivning mot enkeltvirksomheter: Sparringspartner, sikkerhetsgjennomgang
4. Verktøy: Maler, veiledninger, erfaringsdatabase, tips og råd, sjekklister.
5. Regelverk: Oppdatert oversikt, samt arbeid med nytt regelverk
6. Standardisering: Felles metodikk og felles verktøy for risikovurdering, m.m.
7. Felleskomponenter og felles tekniske løsninger: Teknologi for å sikre samhandling, f.eks. krypteringsløsninger, autentiseringsløsninger og nettsky.

Våre anbefalinger til Difi om å fokusere på kompetanseheving og koordinering innebærer en prioritering av tiltak 1, 2, 3 og 5 i lista over. De kompetansesøkende aktivitetene bør rettes mot områder der statsforvaltningen opplever spesielle utfordringer. De utfordringene som blir trukket frem fra workshopen stemmer i stor grad overens med de områdene fokusgruppene avdekker som særlig utfordrende: Styringssystemer, risikovurderinger, regler, sikkerhet i utvikling, samt organisasjonsutvikling (se avsnitt 3.6).

En prioritering av kompetansehevende og koordinerende aktiviteter, innebærer en nedprioritering av arbeid med verktøy og standardisering, samt arbeid med felleskomponenter (tiltak 4, 6 og 7 i lista over). Som nevnt tidligere er det et klart uttrykt ønske fra de som jobber med informasjonssikkerhet at Difi tilbyr og formidler maler og eksempler som de kan bruke direkte i sitt arbeid, for eksempel med etablering av styringssystemer eller gjennomføring av risikovurderinger. Fokusgruppene har imidlertid også avdekket en del farer ved å tilby for detaljert og omfattende veiledning.

Prosessen med å gjøre risikovurderinger og etablere et styringssystem er svært viktig for å øke forståelsen for informasjonssikkerhet. Det er også avgjørende å få etablert prosesser som stemmer med hvordan man jobber lokalt. Vi anbefaler derfor at Difi i størst mulig grad prioriterer kompetansehevende tiltak. Behov knyttet til felleskomponenter har i svært liten grad vært et tema i fokusgruppene.

4.3 Relevante resultater/anbefalinger i annen litteratur

Fokusgruppene og spørreundersøkelsen som er gjennomført har resultert i en god del funn som er viktige å ta hensyn til i arbeidet videre – spesielt i arbeidet med kompetansehevende tiltak. I det følgende beskriver vi en del rapporter og forskningsresultater som kan bidra til bedre forståelse av disse funnene, og slik være nyttig bakgrunn i det videre arbeidet. Beskrivelsen av disse relevante arbeidene er organisert i de samme temaområdene som ble brukt til å beskrive resultatene fra fokusgruppene i kapittel 3. Temaområdet kompetanse er imidlertid utelatt, da dette området på mange måter er en oppsummering av utfordringer på de andre temaområdene.

4.3.1 Integrasjon mot virksomhetens mål

Fokusgruppene har avdekket at i dag kommer ledelsesforankring primært som følge av eksternt press. Relevant forskning har vist at ledere ofte er for optimistiske når det gjelder å vurdere den risikoen virksomheten opplever knyttet til informasjonssikkerhet. I en forskningsstudie [10] ble ledere spurt om å rangere egen risiko opp mot risiko hos samarbeidspartnere og virksomheter i samme bransje. Lederne rangerte sin egen risiko som signifikant lavere enn gjennomsnittet. Forskerne konkluderer dermed at lederne

til en viss grad forstår risiko knyttet til informasjonssikkerhet, men de assosierer ikke denne risikoen med sin egen virkelighet.

Difis egen rapport knyttet til styringssystemer for informasjonssikkerhet [4] tar også for seg manglende ledelsesforankring. Rapporten uttaler at det krever gode sikkerhetsfolk med virksomhetsperspektiv for å skape engasjement hos ledelsen. Den peker også på at manglende engasjement hos ledelsen kan ha sammenheng med at få ledere blir målt på informasjonssikkerhet.

Mellomledere nevnes som en utfordrende gruppe i fokusgruppene. Denne gruppen trekkes også frem i en britisk forskningsstudie knyttet til rollen informasjonssikkerhetsledere har når det gjelder å bygge sikkerhetskultur [11] [2]. I de store virksomhetene som deltok i studien var ikke mellomlederne noen spesiell målgruppe i arbeidet med sikkerhetskultur, på tross av at de ofte ble opplevd som bremser i dette arbeidet. Mellomlederne har mange agendaer og mål, og informasjonssikkerhet faller lett gjennom om ikke toppledelsen legger spesielt til rette. Å nå gjennom hos mellomledere krever at toppledelsen gjør mer enn bare å snakke om sikkerhet.

I den samme studien [11] reflekterer forskerne rundt effekten av å ha en egen informasjonssikkerhetsfunksjon i organisasjonen. Det å ha en informasjonssikkerhetsleder gjør at toppledelsen på en grei måte oppfyller krav på dette området, og kan delegere ansvar til spesialister på informasjonssikkerhet. Samtidig gjør det at toppledelsen kan distansere seg fra informasjonssikkerhetsarbeidet. Dette innebærer også at de kan komme med unnskyldninger for å omgå sikkerhetspraksis, ved å vektlegge viktigheten av andre virksomhetsoppgaver over sikkerhet.

4.3.2 Styringssystemet og virksomheten

En spørreundersøkelse fra 2007 [12] blant en rekke virksomheter fra ulike deler av verden[3] viser at tiltak knyttet til ledelse og styring ofte er lavt prioritert i informasjonssikkerhetsarbeidet. Eksempler på slike tiltak er etablering av policy og prosedyrer. Resultatene fra undersøkelsen viser imidlertid at de som har slike tiltak implementert, ofte også rapporterer om bedre kvalitet på andre mer tekniske tiltak. Forskerne tolker dermed resultatene dithen at arbeid med policy og lignende tiltak har en viktig rolle i å øke kvaliteten på sikkerhetsarbeidet i organisasjoner, samt oppmerksomheten rundt informasjonssikkerhet.

Statsforvaltningen har nå krav på seg om å ha styringssystem for informasjonssikkerhet, og at styringssystemet skal være basert på anerkjente standarder [1]. Som allerede nevnt har Difi i 2012 innhentet erfaringer med standardene ISO/IEC 27001 og ISO/IEC 27002 i offentlige virksomheter [4]. Flere av funnene i den erfaringsrapporten stemmer overens med det som har blitt avdekket i fokusgruppene og spørreundersøkelsen. Rapporten fra 2012 beskriver at det kun er noen få som har et fullverdig fungerende styringssystem for informasjonssikkerhet. De få som har dette er store virksomheter. Viktige utfordringer som er identifisert er mangel på kompetanse, mangel på ledelsesengasjement, mangel på gode maler for dokumentasjon, og sikkerhetskultur. Ledelsesforankring er identifisert som en svært viktig suksessfaktor. Resultatet fra arbeidet med et styringssystem blir ofte ikke like bra om innføringen starter på grunn av initiativ lokalt i organisasjonen, f.eks. i IKT-miljøet, uten noe særlig grad av styring fra ledelsen. Dette støttes også av Datatilsynet [7] og NSM [6] som begge peker på utfordringer knyttet til ledelsesforankring og etablering av rutiner for internkontroll.

Spørreundersøkelsen avdekket usikkerheter knyttet til effekten av å etablere et styringssystem for informasjonssikkerhet: De fleste hadde ingen mening om hvordan styringssystemet påvirket prestasjonene i

[2] Se også blogginnlegg "Sikkerhetskultur? Vi har folk til slikt", Inger Anne Tøndel: http://infosec.sintef.no/informasjonssikkerhet/2013/11/sikkerhetskultur-vi-har-folk-til-slikt/

[3] Hovedvekt på nord-amerikanske virksomheter

sikkerhetsarbeidet. I sin rapport fant imidlertid Difi at flere av de som har etablert et styringssystem basert på ISO/IEC 27001 sa at dette har hatt en positiv effekt på kontroll med informasjonssikkerhet og ledelsens engasjement om temaet, og at nytten har forsvart kostnaden. Størst effekt fant man der det var etablert felles helhetlige styringssystemer for flere områder i virksomheten. Dette forenkler arbeidet og øker ledelsens oversikt, kontroll og engasjement. Der det er etablert et *eget* styringssystem for informasjonssikkerhet (som ikke henger sammen med virksomhetens styringssystem) karakteriseres ledelsesinvolveringen som *"noe mer aksepterende enn styrende*" og det blir mer fokus på IKT-sikkerhet (tekniske systemer) enn informasjonssikkerhet (beskyttelse av informasjonsverdiene).

De av fokusgruppedeltakerne som hadde et styringssystem for informasjonssikkerhet, opplevde utfordringer knyttet til å få innført styringssystemet i virksomheten: Styringssystemet stemmer ikke med det virkelige liv. Dette handler mye om å endre kultur i virksomheten, noe mange deltakere opplevde som utfordrende. Tekniske tiltak opplevdes enklere å implementere. Utfordringene deltakerne opplever rundt det å endre kultur i virksomheter er noe som også er kjent fra annen forskning. I den britiske studien nevnt over [11], fant man følgende i intervjuer med informasjonssikkerhetsledere i store virksomheter:

- Informasjonssikkerhetslederne er for frakoblet fra resten av organisasjonen. De bedriver i stor grad envegs-kommunikasjon. Derfor vet de heller ikke om budskapet fører til endrede handlinger og økt bevissthet hos dem som mottar budskapet.
- Informasjonssikkerhetslederne hadde generelt liten tro på seg selv og egne egenskaper når det gjaldt å bidra til kulturendring i virksomheten. Dette gjaldt spesielt egen evne til å kommunisere med brukere på en effektiv måte. De følte at de i deres rolle som informasjonssikkerhetsledere ofte måtte håndtere oppgaver som var utenfor deres ekspertise.
- Informasjonssikkerhetslederne hadde en sterk oppfatning om at informasjonssikkerhet var vanskelig å selge i organisasjonen – budskapet var upopulært. De forventet altså ikke å bli hørt, og ble da heller antagelig ikke det. Informasjonssikkerhetslederne var også klar over at de kanskje ikke var helt på bølgelengde med mottakerne av budskapet – de var for evangeliserende, for entusiastiske.

Informasjonssikkerhetslederne hadde to ulike roller mot brukerne:

- *Den autorative:* Informasjonssikkerhetslederne var spesialister, og ønsket å være en autoritet i organisasjonen. De ønsket at brukerne skulle følge reglene og prinsippene de la fram.
- *Hjelperen:* Informasjonssikkerhetslederne hadde tro på at brukerne var kompetente og ansvarsfulle, og ville ta gode valg om de bare ble minnet om det og fikk god opplæring. De hadde en rolle i å hjelpe og støtte brukerne slik at de ble satt i stand til å ta gode valg.

Disse to rollene var imidlertid i konflikt med hverandre, og forskerne hevdet at dette kunne være forvirrende for brukerne. Når informasjonssikkerhetslederne går inn i den autorative rollen, og samtidig presenterer informasjonssikkerhetsbudskapet ved hjelp av pizza og konkurranser, kommuniserer ikke det at brukerne selv er kompetente og ansvarsfulle. De må jo underholdes og nesten lures til å tenke på sikkerhet. Forskerne i denne studien stiller spørsmålet: Er brukerne barn som trenger at informasjonssikkerhetslederne beskytter dem (dermed kan de ikke holdes ansvarlige for feil de måtte gjøre) eller er de likeverdige i relasjonen (og dermed deler ansvaret for å beskytte organisasjonens informasjonsverdier)?

4.3.3 Åpenhet

Åpenhet om hendelser ble identifisert som en utfordring i fokusgruppene – både for å få oversikt internt over de hendelsene som skjer, og for å kunne lære av hendelser i etterkant og dele erfaringer med andre. Underrapportering av hendelser blir også sett på som en utfordring av NSM, i deres vurdering av sikkerhetstilstanden i Norge [6].

Om man klarer å øke åpenheten rundt hendelser, samt få en bedre rapportering internt, kan dette gi store gevinster. I den forbindelse vil vi trekke fram følgende forskningsresultater:

- Det finnes mange gode tekniske verktøy for å kunne oppdage informasjonssikkerhetshendelser. Likevel rapporterer flere studier at manuell rapportering fortsatt er svært viktig for å oppdage hendelser [13][14][15]. Dette gjelder rapportering internt, men også varsler utenfra. I en studie av et utvalg hendelser rapportert til CERT-FI (et finsk responsmiljø) [16] ble det observert at i ingen av disse hendelsene var offeret for hendelsen i stand til å oppdage og forstå omfanget av hendelsen selv. Eksterne hadde en nøkkelrolle i å gjøre organisasjonen klar over hva som skjedde.
- Kunnskap og kultur spiller en viktig rolle. I en studie av hvordan informasjonssikkerhetshendelser ble håndtert i tre norske virksomheter [14], ble det avdekket at få ansatte visste hvem slike hendelser skulle rapporteres til. De var også usikre på hvilke hendelser som skulle rapporteres.
- Det er mye å hente på å bruke hendelser til læring internt i organisasjonen. En australsk finansinstitusjon som har innført en prosess for å lære fra større hendelser, hevder at det i løpet av en 10-årsperiode har resultert i en reduksjon av større hendelser fra 200 til 16 per måned [17]. Det som er dokumentert av forskning på hvordan læring fra hendelser i praksis gjøres i dag peker på følgende hovedutfordringer:
    - Læringsprosesser involverer i hovedsak teknisk personell, og tar et teknisk perspektiv. Underliggende årsaker knyttet til f.eks. prosesser, dekkes ikke i stor nok grad. Erfaringer man gjør seg spres også i for liten grad ut over den gruppen som er involvert i å håndtere selve hendelsen [17][18].
    - Læring skjer primært knyttet til større hendelser. Det er lite fokus på å lære av mindre hendelser, eller nesten-hendelser, selv om dette kan være effektivt for å unngå at mindre hendelser fører til noe større [14][17].

4.3.4 Forståelse av risiko

Difi har tidligere avdekket [4] at risikovurderinger ofte oppleves som krevende, og det er mangel på intern kompetanse for å gjøre slike vurderinger. Spesielt er det krevende å finne gode kriterier for risikovilje og akseptabel risiko. Dette stemmer med funnene fra fokusgruppene, samt mye av den eksisterende forskningen på området.

Det finnes i dag mange forslag til hvordan man kan gå frem for å gjøre risikovurderinger knyttet til informasjonssikkerhet. I norsk sammenheng finnes det veiledninger fra flere ulike aktører som alle beskriver ulike metoder man kan bruke. I tillegg finnes det et vell av standarder, retningslinjer og forskningsartikler på et internasjonalt nivå, som gir anbefalinger om metode. Forskningen gir imidlertid få svar på hvilken metode man skal velge og hvilken effekt man kan forvente av å gjøre risikovurderinger [19]. De få studiene som finnes avdekker en del utfordringer. I en studie ble det avdekket at så mange som 25% av de 32 informasjonssikkerhetslederne som ble spurt, ikke gjennomførte risikovurderinger. En australsk studie [21] viser at virksomheter ofte gjør forenklinger i forhold til metodene som blir anbefalt. I noen tilfeller kan dette føre til at risikovurderinger i praksis blir en avviksanalyse: Man ser på hvordan virksomheten oppfyller et sett med krav i en standard. Dermed vurderer man egentlig ikke risikoen virksomheten er utsatt for.

Flere har hevdet at det er spesielt utfordrende å vurdere risiko knyttet til informasjonssikkerhet, sammenlignet med en del andre områder. Årsaker til dette er at det finnes lite historiske data å bygge vurderinger på, samt at risikofaktorer endrer seg raskt. Mange hendelser oppdages heller ikke. Informasjon er også en immateriell verdi som det er vanskelig å gi en nøyaktig verdi. Dette peker mot at kompetanse hos de som gjør risikovurderinger er svært viktig for å kunne stole på resultatene.

En studie utført av General Accounting Office i USA for nærmere 15 år siden [22] trekker fram følgende suksessfaktorer for å gjøre gode og effektive risikovurderinger knyttet til informasjonssikkerhet. Disse stemmer i stor grad overens med erfaringene i fokusgruppene:

- Ledelsesforankring
- Nøkkelressurser i organisasjonen som kan gi støtte til risikovurderinger
- Definerte prosedyrer
- Involvering av eksperter som til sammen dekker både teknisk side og virksomhetsperspektivet
- Ansvar plasseres i enhetene
- Begrenset omfang/fokus for hver analyse
- Dokumentasjon og tilgjengeliggjøring av resultatene

4.3.5 Sikkerhet under utvikling av IT-systemer

Det er en kjent utfordring at sikkerhetskompetanse blant utviklere, og også blant bestillere av IT-systemer, ofte er lav. Slik sett bekrefter resultatene fra fokusgruppene at dette også er tilfelle i utviklingsprosjektene tilknyttet statsforvaltningen. Det finnes en rekke aktiviteter som kan benyttes i ulike faser av utviklingsprosjekter for å håndtere informasjonssikkerhet på en grundigere måte, for eksempel dokumentert i BSIMM – The Building Security in Maturity Model [23].

Noen fokusgruppedeltakere beskrev at de opplevde utfordringene knyttet til informasjonssikkerhet større ved smidig utviklingsmetodikk, enn ved en tradisjonell fossefallstilnærming. Det finnes i dag få vitenskapelige studier som dekker informasjonssikkerhet ved smidig utvikling. Et unntak er en studie der ti smidig-utviklere ble intervjuet om hvordan de jobber med informasjonssikkerhet i sine prosjekter [24]. Også i denne studien ble det avdekket at det ofte er lite bevissthet hos kunden knyttet til informasjonssikkerhet. Det må gjerne hendelser eller medieoppslag til før dette temaet kommer ordentlig på banen. Men på tross av uklare krav og lav bevissthet opplevde over halvparten av utviklerne at det nære samarbeidet med kunden førte til bedre sikkerhetskrav.

De fleste deltakerne i studien [24] opplevde at utviklerteamene hadde kompetanse på sikkerhet. Kunnskap om sikkerhet ble spredt blant utviklere gjennom diskusjoner. Kompetansen var ofte også selvlært, f.eks. gjennom nyheter og blogger. Utviklerne følte i stor grad ansvar for prosjektet, og dermed også ansvar for sikkerheten. Imidlertid var det ofte press i sprintene om å gjøre synlig framgang, noe som spesielt kunne gå på bekostning av testing.

Gode tips til hvordan informasjonssikkerhet kan håndteres i smidig utvikling finnes blant annet hos Mircrosoft [25].

5 Oppsummering og videre arbeid

Gjennom en sammenlignende analyse av resultatene fra fire fokusgruppeintervjuer med 21 deltakere fra 18 statlige virksomheter har vi identifisert vi et sett av temaer, funn og anbefalinger. I tillegg har vi brukt resultatene fra en spørreundersøkelse med svar fra 51 deltakere for bedre å forstå resultatene fra fokusgruppene. Ut fra resultatene har vi foreslått tiltak knyttet til kompetanseheving og koordinering som Difi kompetansesenter for informasjonssikkerhet bør prioritere for å møte behovene i forvaltningen.

Informasjonssikkerhet i offentlig forvaltning er i konstant endring og har spesielt endret seg mye de siste årene. De tiltakene denne rapporten anbefaler Difi å prioritere, er basert på det vi opplever som dagens situasjon, og det virksomhetene forventer vil være gjeldende situasjon for de nærmeste årene.

Tiltakene som er beskrevet i rapporten vil være kjente for Difi og for resten av statsforvaltningen. Innen statsforvaltningen er det stor diversitet når det gjelder behov, utfordringer, kunnskapsnivå, og erfaringer, i tillegg til at rollen til informasjonssikkerhet i statsforvaltningen er i kontinuerlig endring. Det sentrale i denne rapporten er derfor innsikten den gir i bakgrunn og motivasjon for tiltakene. Dette er igjen en forutsetning for å kunne skreddersy de tiltak og aktiviteter som Difi vil lede. Et gitt tiltak eller aktivitet vil ikke passe for alle.

De tiltakene vi anbefaler i kapittel 5 er en blanding av langsiktige og kortsiktige tiltak, der noen er mer rettet mot små, noen mer mot store, noen mot modne og noen mot mindre modne virksomheter. Difi må nå ta disse prioriterte tiltakene og lage en tiltaksplan. En tiltaksplan er en enkel måte å beskrive de tiltakene som skal gjennomføres. De ved Difi som skal være involvert og lede tiltakene må sammen lage denne planen. Det vil være fornuftig å forankre arbeidet i hele den nye enheten. Vi anbefaler følgende prosess med utgangspunkt i de tiltak som er foreslått:

Trinn 1. *Relaterte tiltak grupperes sammen i "prosjekter".* Noen tiltak vil med fordel bli gruppert sammen, mens andre er så store at de bør stå alene.

Trinn 2. *Ranger listen med prioriterte tiltak og identifiser oppstartstidspunkt.* Alle tiltak kan ikke realiseres på en gang; derfor må man finne ut hvilke man skal starte med og når.

Trinn 3. *Beskriv tiltakene.* For hvert tiltak: kort beskrivelse, mål, forutsetninger, ressurser og varighet, og eventuelle milepæler. Mål bør omfatte målgruppe(r) og hva som skal gjøre for å skreddersy tiltakene mot målgruppen(e).

Trinn 4. *Finn ansvarlige for tiltakene.* Dette er den personen som skal følge opp at tiltakene blir gjennomført, og behøver ikke være den som skal utføre arbeidet.

Trinn 5. *Innføringsplan.* Lag en plan for hvordan tiltakene skal nå ut til virksomhetene.

Det er viktig å ha en klar formening om hvilke målgrupper som skal prioriteres og hvorfor. Det vil også være viktig å kunne kombinere både langsiktige og kortsiktige tiltak. De langsiktige tiltakene er viktig for å jobbe strategisk over lengre tid mot virksomhetene, mens de kortsiktige tiltakene er viktig for å få resultater raskt. Å se effekt av tiltakene er en viktig drivkraft og for motivasjonen hos Difi og hos virksomhetene.

En tiltaksplan må være realistisk. Urealistiske forestillinger om hva som kan og skal oppnås, vil bare virke demotiverende. Planen må reflekteres i budsjetter.

A Referanser

[1] Nasjonal strategi for informasjonssikkerhet. 17.12.2012. http://www.regjeringen.no/nb/dep/fad/dok/rapporter_planer/planer/2012/nasjonal-strategi-for-informasjonssikker.html?id=710469

[2] Handlingsplan - Nasjonal strategi for informasjonssikkerhet. Oslo, 17. desember 2012. http://www.regjeringen.no/nb/dep/jd/dok/rapporter_planer/planer/2012/handlingsplan---nasjonal-strategi-for-in.html?id=710471

[3] Riksrevisjonens Dokument 1 (2010-2011): Svakheter i oppgaveløsningen, mangelfull samhandling og alvorlige svakheter på informasjonssikkerhetsområdet. 19.10.2010. http://www.riksrevisjonen.no/Presserom/Pressemeldinger/Sider/Dokument1.aspx

[4] Direktoratet for forvaltning og IKT (Difi). Styringssystem for informasjonssikkerhet – Erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27001. Rapport 2012:15. ISSN 1890-6583. http://www.Difi.no/filearchive/Difi-rapport-2012-15-styringssystem-for-informasjonssikkerhet.-erfaringer-og-anbefalinger.pdf

[5] Seksjon for informasjonssikkerhet, Direktoratet for forvaltning og IKT. Oppsummering fra workshop: Hvor trykker informasjonssikkerhetsskoen – hva trenger dere fra oss? November 2013.

[6] Nasjonal Sikkerhetsmyndighet. Rapport om sikkerhetstilstanden 2012. https://www.nsm.stat.no/Documents/Risikovurdering/Ugradert%20rapport%20om%20sikkerhetstilstanden%202012.pdf

[7] Datatilsynet. Årsmeldingen for 2012. http://datatilsynet.no/Global/04_planer_rapporter/aarsmelding/%C3%85rsmeldingen2012.pdf

[8] Stewart, D.W., Shamdasani, P.N., Rook, D., "Focus Groups: Theory and Practice." Sage Publications (2007)

[9] Dybå, T, Moe, N.B., Mikkelsen, E.M., "An Empirical Investigation on Factors Affecting Software Developer Acceptance and Utilization of Electronic Process Guides," Proc. Int'l Software Metrics Symp., 2004.

[10] Hyeun-Suk, R., Ryu, Y.U., Kim, C.-T., "Unrealistic optimism on information security management." Computers & Security 31.2 (2012): 221-232.

[11] Ashenden, D, Sasse, A., "CISOs and organisational culture: Their own worst enemy?" Computers & Security 39 (2013): 396-405.

[12] Baker, W.H., Wallace, L., "Is information security under control?: Investigating quality in information security management." IEEE Security & Privacy, 5.1 (2007): 36-44.

[13] Metzger, S., Hommel, W., Reiser, H., "Integrated Security Incident Management – Concepts and Real-World Experiences." Sixth International Conference on IT Security Incident Management and IT Forensics (IMF). 2011. p. 107-121.

[14] Hove, C., Tårnes, M., "Information Security Incident Management: An Empirical Study of Current Practice." Norwegian University of Science and Technology. 2013.

[15] Line, M.B., "A Case Study: Preparing for the Smart Grids – Identifying Current Practice for Information Security Incident Management in the Power Industry." Seventh International Conference on IT Security Incident Management and IT Forensics (IMF). 2013. p. 26-32

[16] Koivunen, E., "Why Wasn't I Notifed: Information Security Incident Reporting Demystifed." 15th Nordic Conference in Secure IT Systems (Nordsec 2010). 2010.

[17] Ahmad, A, Hadgkiss, J., Ruighaver, A.B., "Incident response teams–Challenges in supporting the organisational security function." Computers & Security 31.5 (2012): 643-652.

[18] Jaatun, M.G., Albrechtsen, E., Line, M.B., Tøndel, I.A., Longva, O.H., "A framework for incident response management in the petroleum industry." International Journal of Critical Infrastructure Protection, 2.1 (2009): 26-37.

[19] Sulaman, S.M., Weyns, K., Höst, M., "A review of research on risk analysis methods for IT systems." Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering. April 2013. p. 86-96

[20] Jourdan, Z., Rainer Jr, R.K., Marshall, T.E., Ford, F.N., "An Investigation of Organizational Information Security Risk Analysis." Journal of Service Science (JSS), 3.2 (2010).
[21] Shedden P, Ruighaver A.B., Ahmad A., "Risk management standards– the perception of ease of use." Journal of Information System Security, 6.3 (2010): 23-41
[22] United States General Accounting Office (GAO). "Information Security Risk Assessment – Practices of Leading Organizations." GAO/AIMD-00-33. November 1999.
[23] BSIMM – V: The Building Security In Maturity Model, http://bsimm.com/
[24] Bartsch, S., "Practitioners' Perspectives on Security in Agile Development." Sixth International Conference on Availability, Reliability and Security (ARES), 2011.
[25] Microsoft Security Development Lifecycle, SDL for Agile, http://www.microsoft.com/security/sdl/discover/sdlagile.aspx

B Analyse av spørreundersøkelsen

For bedre å forstå hvilke behov forvaltningen har til Difis nyopprettede kompetansemiljø, har vi utført en empirisk undersøkelse av faktorer som påvirker akseptanse og bruk av styringssystem for informasjonssikkerhet (SSIS). Den empiriske undersøkelsen er basert på Technology Acceptance Model (TAM)[4]. Når vi presenterer resultatene fra undersøkelsen vil vi skille mellom *dagens bruk* og *intensjon om fremtidig bruk*. I de neste avsnittene presenterer vi modellen for teknologiakseptanse, som består av fire uavhengige og to avhengige variabler, og de tilsvarende hypoteser og resultater.

B.1 Konseptuell modell og hypoteser

Den konseptuelle modellen som ble testet i denne undersøkelsen er vist i Figur 1. To avhengige variabler ble undersøkt:

- Dagens bruk av SSIS, noe som er et mål på vellykket etablering og innføring av SSIS
- Intensjon om fremtidig bruk, noe som gjenspeiler sannsynligheten for at SSIS vil bli innført i fremtiden.

Dagens bruk av systemet ble definert som i hvilken grad SSIS brukes til å støtte viktige oppgaver i forbindelse med informasjonssikkerhet: Arbeid med tekniske sikkerhetstiltak, arbeid med organisatoriske sikkerhetstiltak, rapportering av sikkerhetsarbeidet til toppledelse, bevisstgjøringsaktiviteter i organisasjonen, prioritering av sikkerhetsarbeidet, planlegging og organisering av sikkerhetsarbeidet, og håndtering av sikkerhetsproblemer. Disse områdene ble valgt fordi de omhandler viktige deler av sikkerhetsarbeidet, og er områder som dekkes av standarden ISO/IEC 27001.

Vi målte to dimensjoner av bruk: (1) *dybde*, hvor ofte SSIS ble brukt på en informasjonssikkerhetsrelatert oppgave og (2) *bredde*, andelen av informasjonssikkerhetsoppgaver hvor SSIS blir brukt. For å kartlegge dette ble følgende fem punkts skala benyttet:

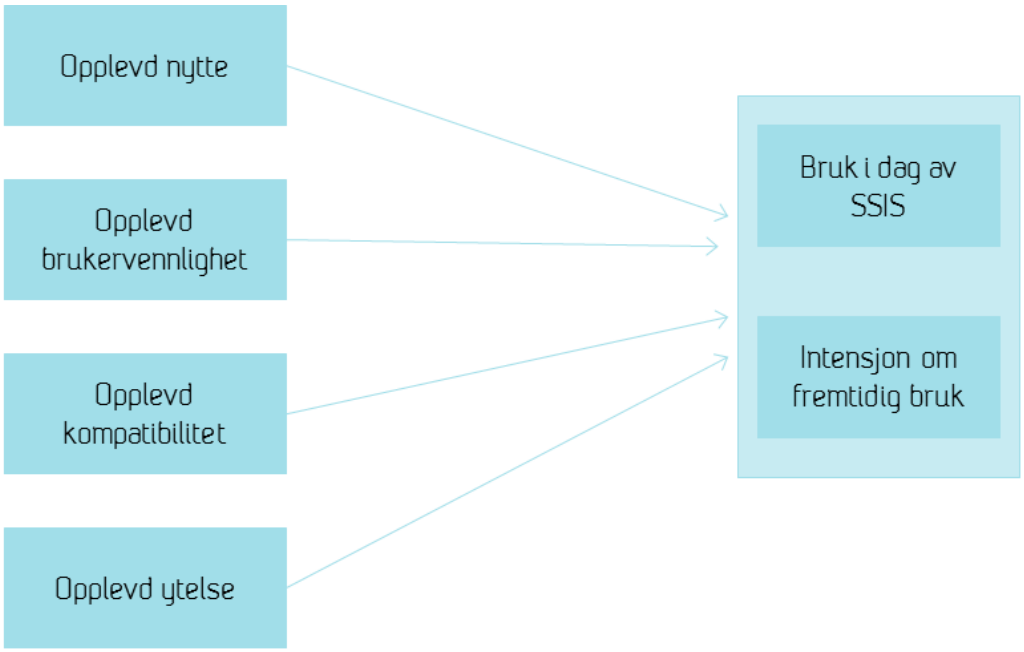
- 0: Ikke brukt
- 1: Brukt noen ganger
- 2: Jevnlig bruk i noen få aktiviteter
- 3: Jevnlig bruk i de fleste aktiviteter
- 4: Jevnlig bruk i alle aktiviteter

Bruksnivå for SSIS ble beregnet som forholdet mellom den totale bruken av SSIS på informasjonssikkerhetsoppgaver og den maksimale bruken på disse oppgavene.

Intensjon om fremtidig bruk ble definert i form av intensjon om å bruke og øke bruken av SSIS i sitt arbeid. Her ble det benyttet en 5 punkts skala: "Svært uenig", "Uenig", "Nøytral", "Enig", og "Svært enig".

Opplevd nytte er definert som i hvilken grad en person mener at det å bruke SSIS vil styrke hans eller hennes jobbytelse. Forskning på informasjonssystemer (IS) viser at opplevd nytte påvirker intensjon om fremtidig bruk, så vel som dagens faktiske bruk. Dermed kan man konkludere at en viktig grunn til å benytte et SSIS er at de som jobber med informasjonssikkerhet oppfatter at SSIS forbedrer deres prestasjoner. Ut fra dette foreslår vi følgende hypotese:

[4] Basert på artikkelen: T. Dybå, N.B. Moe, and E.M. Mikkelsen, "An Empirical Investigation on Factors Affecting Software Developer Acceptance and Utilization of Electronic Process Guides," Proc. Int'l Software Metrics Symp., 2004.



Figur 1. Konseptuelt rammeverk

H1: Opplevd nytte av SSIS er positivt assosiert med bruk av SSIS og intensjon om fremtidig bruk.

Opplevd brukervennlighet refererer til i hvilken grad en person mener at det å bruke et bestemt system vil kreve liten innsats. Opplevd brukervennlighet går igjen i flere studier som en viktig faktor for adopsjon av systemer. Dette tyder på at systemer som oppfattes å være lette å bruke og lite komplekse har en høyere sannsynlighet for å bli akseptert og brukt av potensielle brukere. Derfor tester vi følgende hypotese :

H2: Opplevd brukervennlighet av SSIS er positivt assosiert med bruk av SSIS og intensjon om fremtidig bruk.

Opplevd kompatibilitet refererer til i hvilken grad et system oppfattes å være i samsvar med de eksisterende verdiene, behov og tidligere erfaringer potensielle brukere har. Kompatibilitet har dermed blitt foreslått å være positivt relatert til spredning av et system innen en organisasjon. Vi foreslår derfor følgende hypotese:

H3: Opplevd kompatibilitet til SSIS er positivt assosiert med bruk av SSIS og intensjon om fremtidig bruk.

Opplevd ytelse refererer til i hvilken grad en person mener at bruk av systemet vil hjelpe ham eller henne til å oppnå gevinster i jobbutførelse. Vi foreslår følgende hypotese:

H4: Den opplevde ytelsen ved hjelp av SSIS er positivt assosiert med bruk av SSIS og intensjon om fremtidig bruk.

Vi anser opplevd nytte, brukervennlighet, kompatibilitet og ytelse som viktig for å påvirke bruksnivået av SSIS blant de som jobber med informasjonssikkerhet i offentlige virksomheter.

B.2 Forskningsmetode

Selve spørreundersøkelsen (spørreskjemaet er gjengitt i Vedlegg C) ble gjennomført den 5. november 2013 under en workshop arrangert av Difi [5] hvor formålet var å kartlegge behov forvaltningen har til Difi og det nye kompetansesenteret som er opprettet. Tema for workshopen var «hvor trykker informasjonssikkerhetsskoen – hva trenger dere fra oss»? Invitasjonen gikk ut til alle statlige virksomheter, og det var totalt 59 deltagere på workshopen som representerte 43 virksomheter.

I alt ble 59 spørreskjemaer distribuert og 51 brukbare svar ble mottatt, noe som resulterer i en god samlet svarprosent på 86 %. Gitt denne høye svarprosenten, ble ingen videre analyse gjort på forskjellene mellom respondenter og ikke-respondenter.

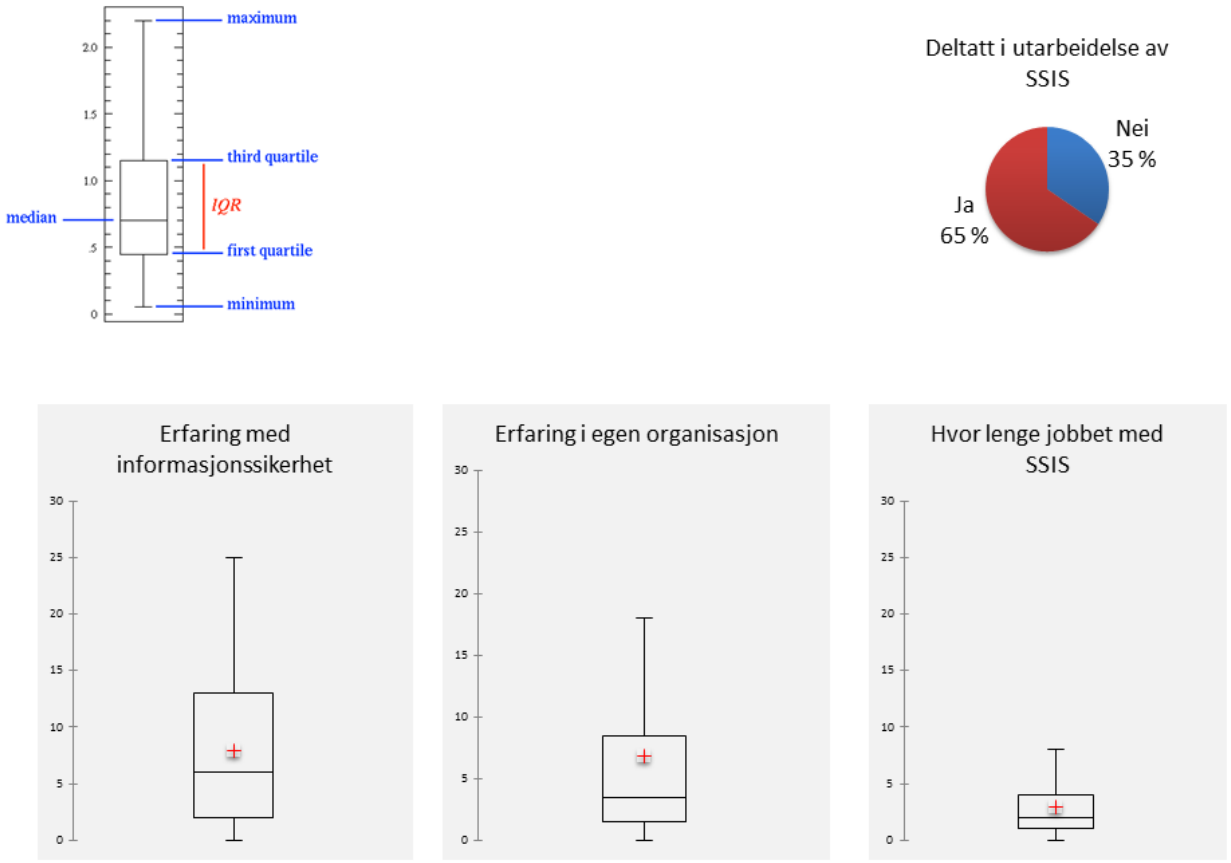
Spørreskjemaet bestod av to deler. I den første delen ble respondentene bedt om å gi generell bakgrunnsinformasjon knyttet til stilling, profesjonell ansiennitet, utdanningsnivå, primære jobbfunksjon og erfaring med SSIS. Den andre delen av spørreskjemaet ble brukt til å måle dybden og bredden av SSIS bruk, intensjon om fremtidig bruk, og det som oppfattes som viktig for å bruke SSIS. Helt til slutt ble respondentene oppfordret til å beskrive sitt SSIS.

B.3 Resultater

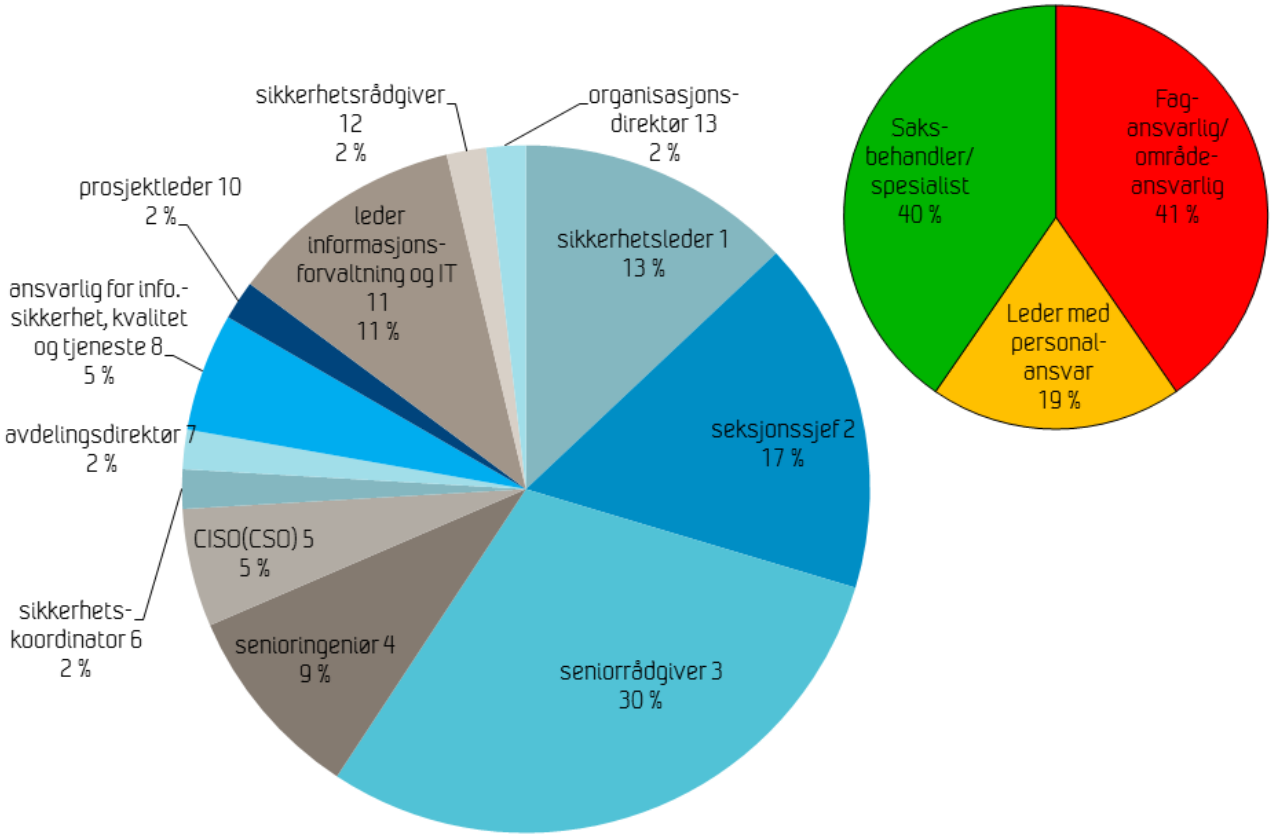
Alle de kvantitative analysene ble utført ved hjelp av verktøyene SPSS og XLSstat.

Figur 2 viser workshopdeltakerens erfaring (minimum, maksimum og median) når det gjelder hvor lenge de har jobbet i virksomheten, hvor lenge de har jobbet med SSIS og hvor lenge de har jobbet med informasjonssikkerhet. I tillegg har 65% av deltakerne vært med på utarbeidelsen av SSIS. Deltakerne hadde 2-9 års erfaring i organisasjonen hvor de jobber nå, og de fleste av deltakerne hadde mindre enn fem års erfaring med SSIS. Den lave erfaringen med SSIS var som forventet siden SSIS er noe som har fått økt fokus de siste årene. Det var stor spredning i antall års erfaring hver deltaker hadde når det gjelder informasjonssikkerhet (2 til 13 års erfaring). Hvis vi antar at workshopen hadde et representativt utvalg fra statlige virksomheter, er en mulig konsekvens at Difi må ha et veldig variert tilbud av aktiviteter og tjenester som retter seg både mot de erfarne og uerfarne. Hvilken type stilling deltakerne hadde var fordelt som vist i Figur 3.

Til sammen 41 av spørreskjemaene inneholdt kommentarer eller beskrivelser knyttet til virksomhetens SSIS. Seks av disse beskrivelsene forteller at den som svarte på skjemaet har lite eller ingen kjennskap til SSIS, eller at det ikke finnes noe SSIS. Fem forteller at et SSIS er under utarbeidelse. Tolv forteller at de har noe på plass, men at viktige dokumenter fortsatt mangler eller ikke er oppdatert. 13 forteller at de har de viktigste dokumentene på plass, mens sju gir indikasjoner også på praktisk bruk, for eksempel gjennom å beskrive ledelsesforankring eller gjennomføring av risikovurderinger. Ti skjemaer refererer til ISO/IEC 27001/2 i beskrivelsen. De ulike beskrivelsene som blir gitt tyder på at det er store forskjeller i hvor langt de ulike virksomhetene har kommet i sitt arbeid med å innføre et SSIS.



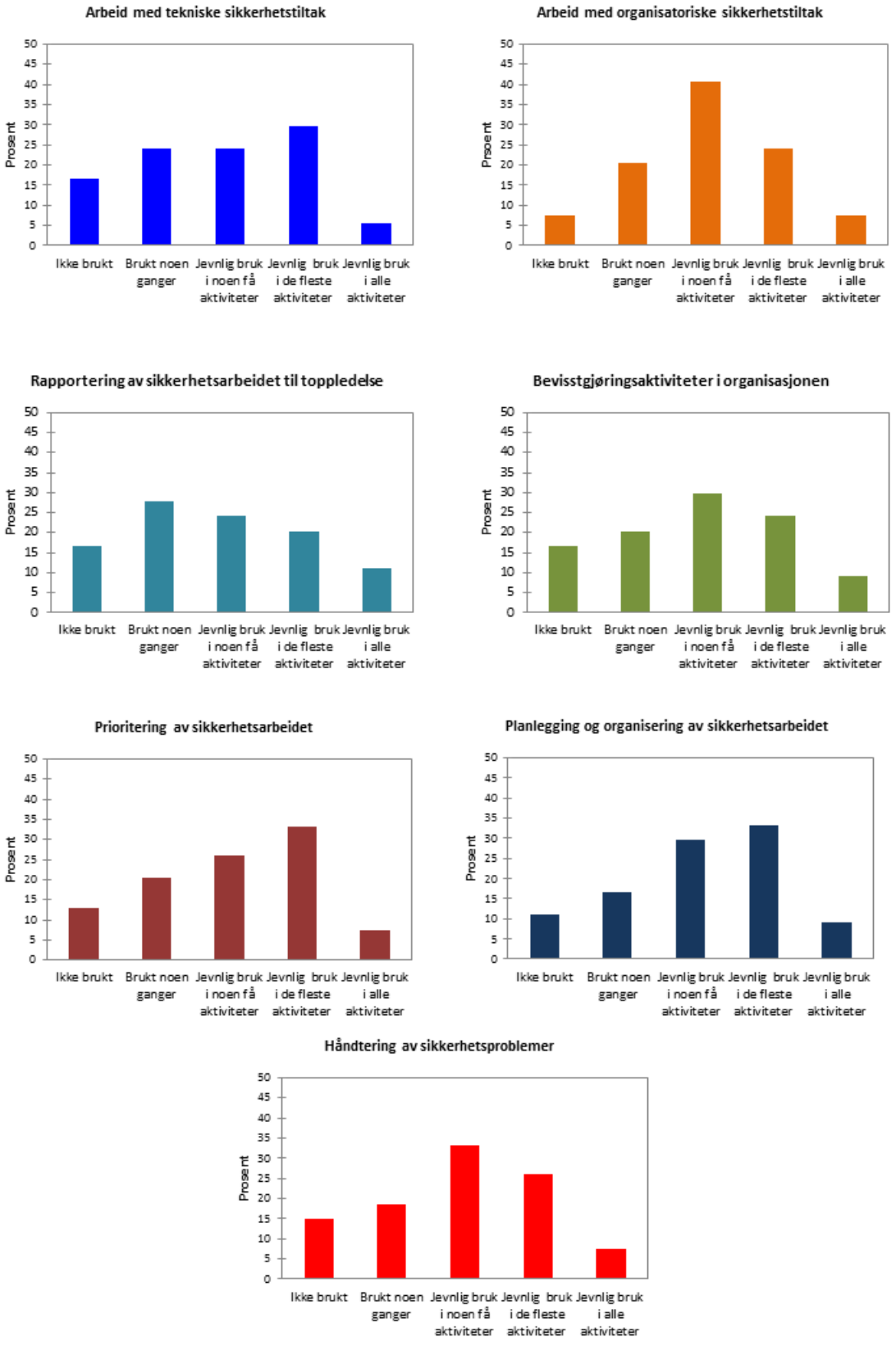
Figur 2. Workshopdeltakernes erfaringer



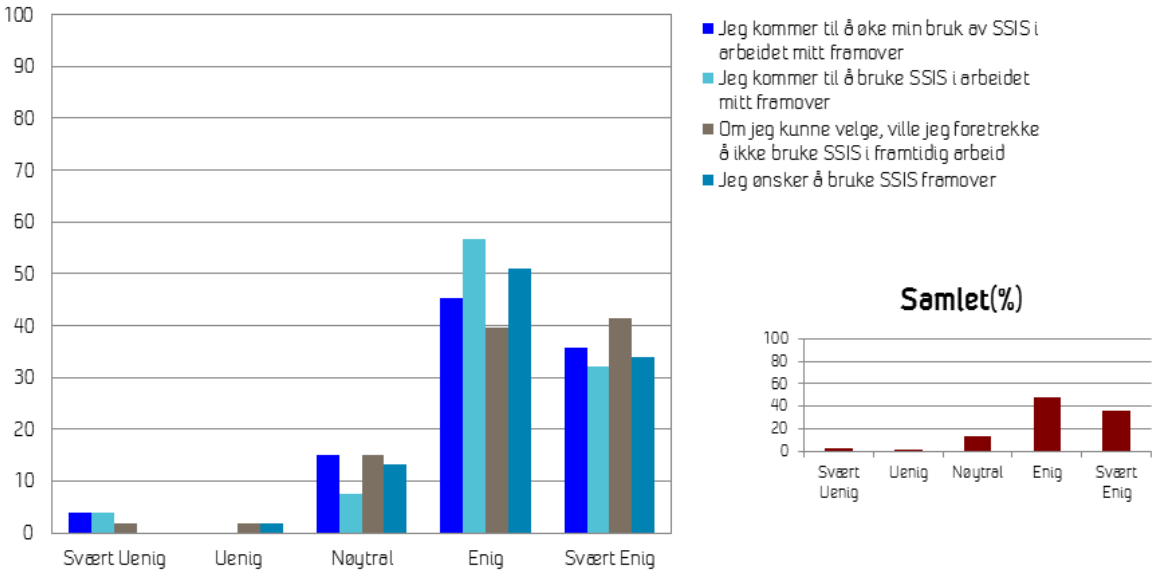
Figur 3. Stilling

Figur 4 viser nåværende bruk av SSIS. Som man kan se fra figuren varierer bruken fra område til område. To områder peker seg ut når det gjelder lav bruk: Arbeid med tekniske sikkerhetstiltak og rapportering av sikkerhetsarbeid til toppledelse. Disse resultatene fra spørreundersøkelsen ble presentert og diskutert i en av fokusgruppene. De fleste deltakerne i den fokusgruppa var fra mer modne miljøer. De var undrende til at det var lav bruk av styringssystemet mot ledelse, fordi de selv opplevde styringssystemet som nyttig i den sammenhengen. En mulig årsak til at svarene tyder på lav bruk på dette området, kan være at en del sliter med ledelsesforankring knyttet til informasjonssikkerhet, og dermed gjør lite rapportering. Når det gjelder bruk knyttet til tekniske tiltak, var oppfatningen i fokusgruppa at teknikere bruker andre kilder enn styringssystemet. Styringssystemet adresserer gjerne viktigheten av sikring uavhengig av om tiltaket er teknisk eller ikke. Dermed oppfattes ikke styringssystemet som særlig relevant for arbeid med tekniske tiltak.

På området intensjon om fremtidig bruk, virker deltakerne positive til å bruke SSIS mer i fremtiden, som vist i Figur 5. Dette vitner om at SSIS blir sett på som viktig i fremtidig arbeid med informasjonssikkerhet. Det må imidlertid presiseres at det å ha et SSIS er et krav, og dermed ikke noe de som har svart på undersøkelsen er frie til å velge bort. I Figur 5 er det er viktig å legge merke til at svaret på spørsmålet "om jeg kunne velge, ville jeg foretrekke å ikke bruke SSIS i fremtidig arbeid" er invertert slik at alle spørsmålene kan sammenlignes. Over 40 % var altså "Svært uenig" i denne påstanden, men i grafen er dette oversatt til "Svært enig".

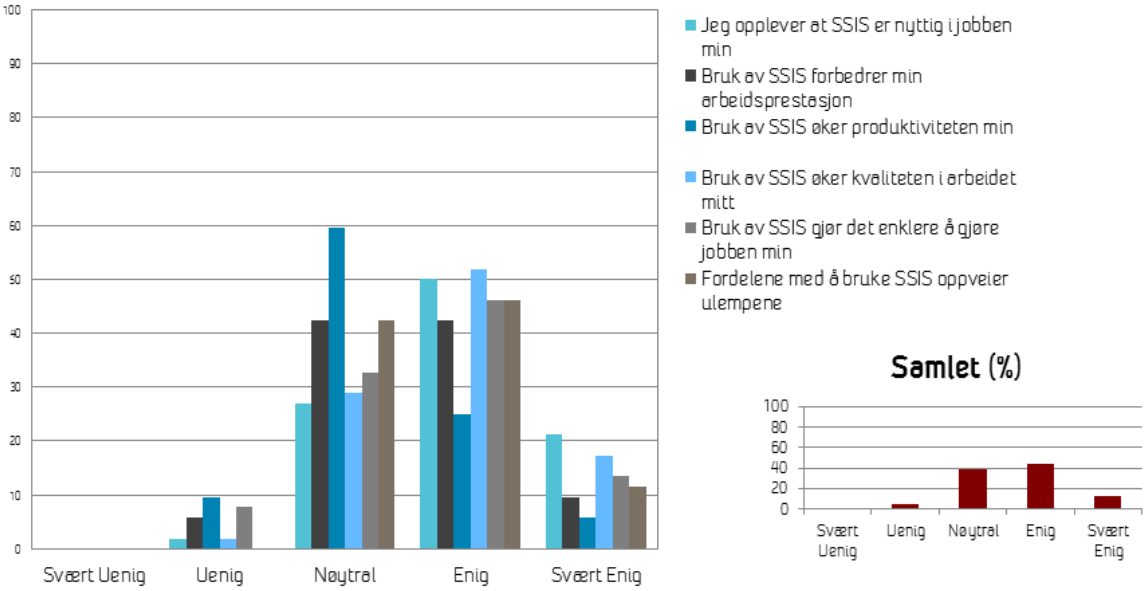


Figur 4. Nåværende bruk av SSIS



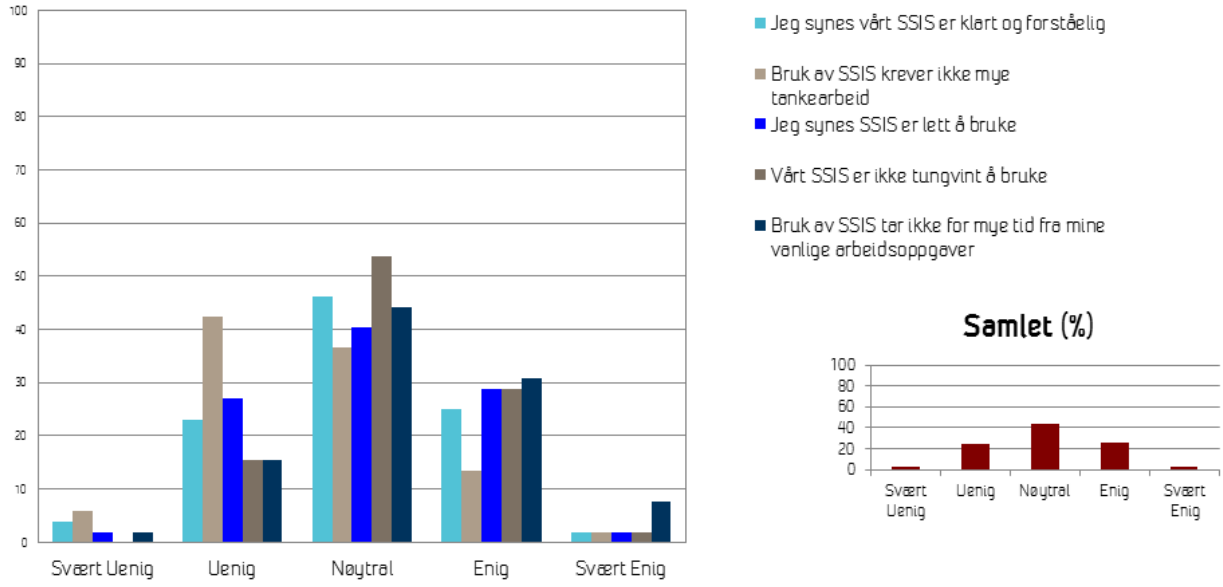
Figur 5. Intensjon om fremtidig bruk

Når det gjelder oppfattet nytte, virker det som om deltakere er enige i at SSIS er nyttig for jobben (se Figur 6). Imidlertid er det en del som er nøytrale i forhold til opplevd nytte og noen som mener SSIS ikke er nyttig. Det er hele 60 % som mener at SSIS verken øker eller reduserer produktiviteten.



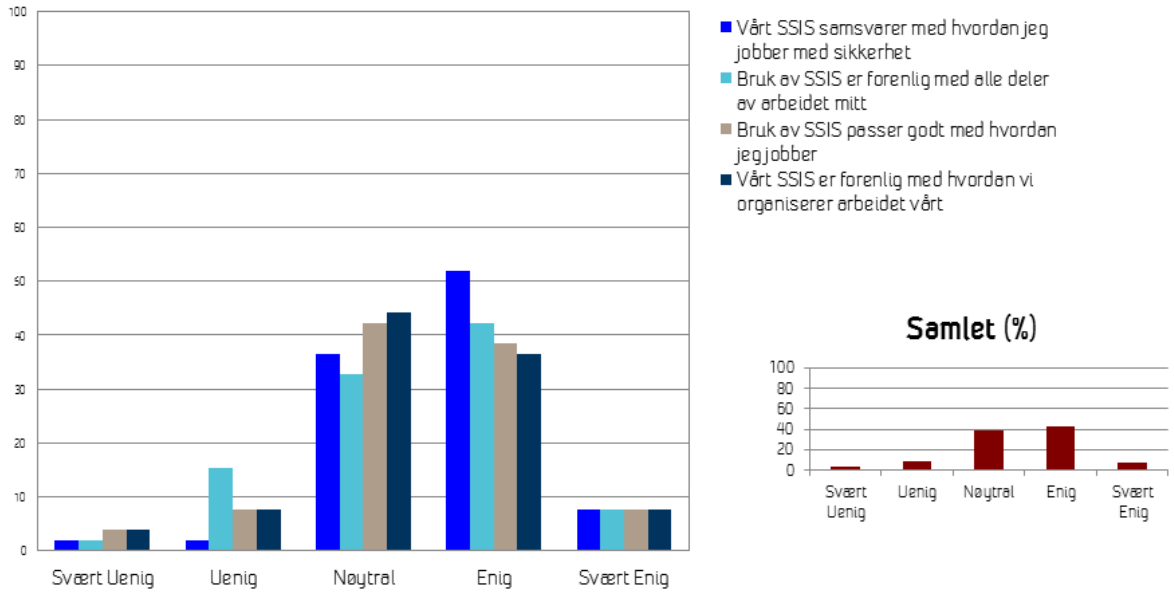
Figur 6. Opplevd nytte

På oppfattet brukervennlighet (se Figur 7) var flesteparten nøytrale, men her var det også mange som mente at SSIS var lite brukervennlig. Spesielt var det mange som mente at SSIS krever mye tankearbeid for å kunne bruke.



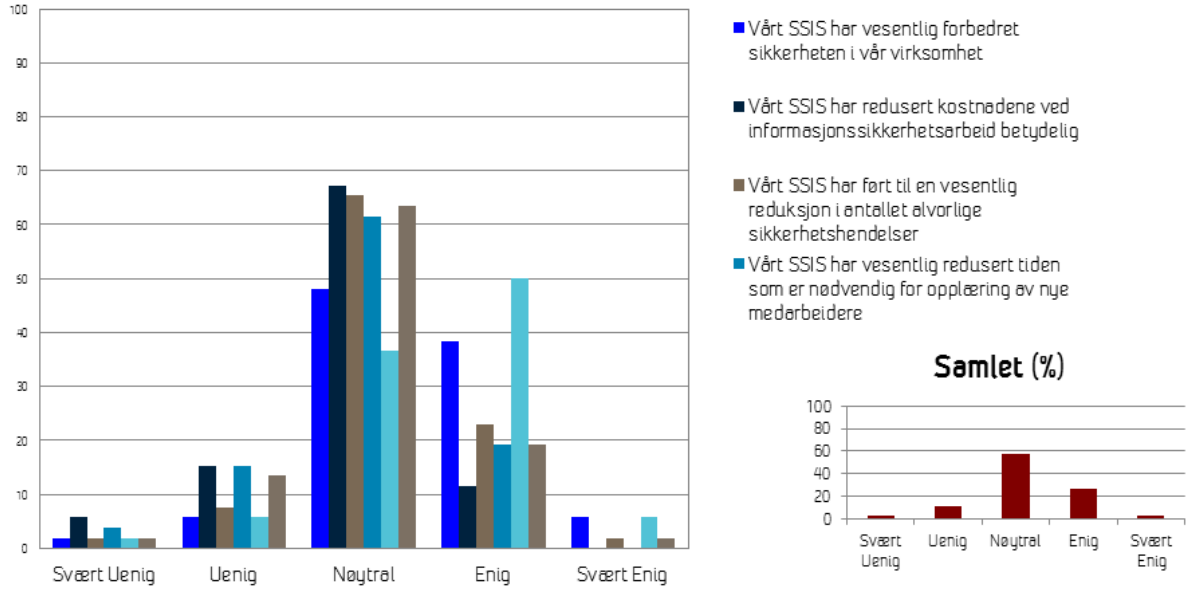
Figur 7. Oppfattet brukervennlighet

Når det gjelder opplevd kompatibilitet (se Figur 8), var de fleste av deltakerne nøytrale eller enige til påstandene i spørreskjemaet. Det virker som om deltakerne var enige om at SSIS stort sett er i samsvar med hvordan den enkelte jobber med informasjonssikkerhet. En mulig forklaring kan være at mange av deltakerne har vært med og produsert SSIS. Resultatene fra fokusgruppene viser imidlertid at det ofte er manglende samsvar mellom styringssystemet og det som faktisk skjer i organisasjonen.



Figur 8. Opplevd kompatibilitet

På området opplevd ytelse (se Figur 9) har de fleste ingen mening om hvordan SSIS påvirker deres prestasjoner. En mulig årsak til den store andelen nøytrale svar, kan være at informasjonssikkerhet oppleves som vanskelig å måle. Hele 50% mener imidlertid at SSIS har gjort det enklere å jobbe sammen om informasjonssikkerhet.



Figur 9. Opplevd ytelse

B.4 Test av hypotesene

Tabell 4 viser inter-korrelasjoner mellom variablene fra det konseptuelle rammeverket (Figur 1). Av 15 korrelasjoner mellom variablene, har fem en korrelasjonskoeffisient som er større enn eller lik 0,5. Den høyeste korrelasjon (0,63) er mellom opplevd nytte og intensjon om fremtidig bruk. Figuren viser at alle bivariate sammenhenger mellom hver av de fire uavhengige variablene og de to avhengige variabler, dagens system bruk og intensjon om fremtidig bruk i, er signifikant (i fet skrift), som strekker seg fra r=0,307 (p <0,05).

Tabell 4. Korrelasjonsmatrise

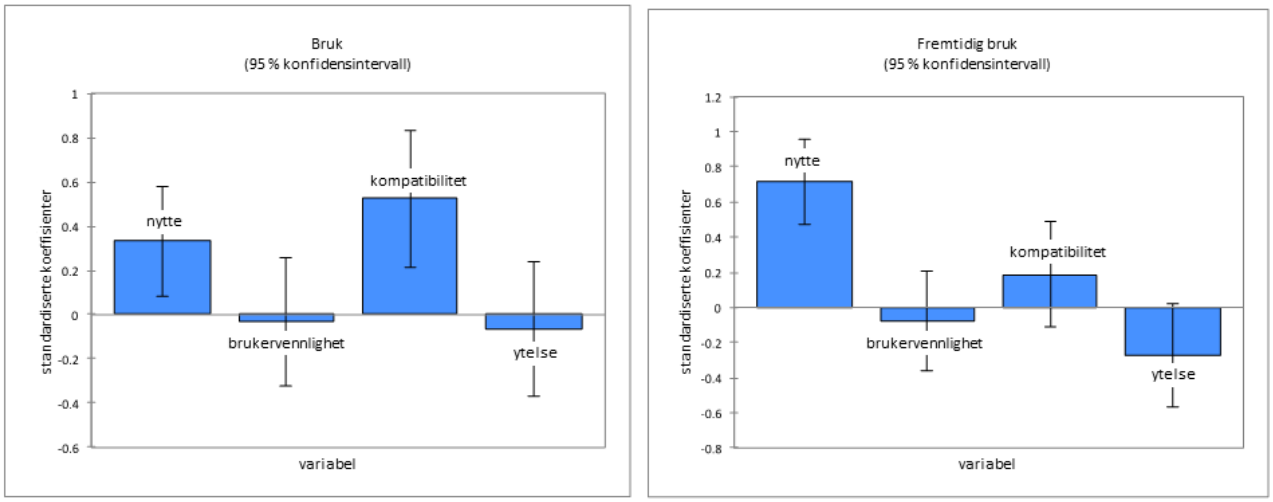
	Bruk av SSIS	Framtidig bruk	Opplevd nytte	Brukervennlighet	Samsvar	Ytelse
Bruk av SSIS	**1**					
Framtidig bruk	**0.496**	**1**				
Opplevd Nytte	**0.455**	**0.630**	**1**			
Brukervennlighet	**0.357**	0.126	**0.334**	**1**		
Samsvar	**0.568**	0.195	**0.307**	**0.594**	**1**	
Ytelse	**0.379**	0.103	**0.424**	**0.526**	**0.608**	**1**

Uthevede verdier er forskjellige fra 0 med et signifikansnivå alpha=0,05

Figur 10 viser hvordan variablene forklarer de to avhengige variablene: 1) dagens bruk av SSIS (CU), og 2) intensjon om fremtidig bruk (FU). Opplevd nytte (korrelasjon 0.48) er en sterk og betydelig faktor i å forklare dagens bruksnivå. Det som overrasket var at kompatibilitet har en enda sterkere sammenheng enn opplevd nytte (korrelasjon 0.67) når det gjelder dagens bruk av SSIS. Den justerte R-kvadrat var 0,36, noe

som forklarer 36% av variansen i dagens bruk.

Tilsvarende resultater for sannsynligheten for framtidig bruk, antyder at den eneste relevante faktoren er opplevd nytte (korrelasjon: 0,8). Denne faktoren forklarte 40% av variansen i intensjon om fremtidig bruk av SSIS.



Figur 10. Koeffisienter for dagens bruk av SSIS og fremtidig bruk av SSIS

Ut fra resultatene finner vi sterk støtte for hypotese 1, moderat støtte for hypotesen 3 og ingen støtte for hypotese 2 og 4, se Tabell 5. Disse funnene står i noe kontrast til et funn fra fokusgruppene (funn nr. 9) som sier at brukervennlighet er viktig om SSIS skal bli tatt i bruk ut over i organisasjonen. En årsak til at brukervennlighet ikke er en viktig faktor ut fra resultatene fra spørreundersøkelsen er at de som har svart på spørreundersøkelsen har en spesiell rolle knyttet til informasjonssikkerhet, og at mange av dem har vært med på å utarbeide SSIS.

Tabell 5. Støtte for hypoteser

Nr.	Hypotese	Resultat
H1	*Opplevd nytte av SSIS er positivt assosiert med bruk av SSIS og intensjon om fremtidig bruk.*	Aksepter
H2	*Opplevd brukervennlighet av SSIS er positivt assosiert med bruk av SSIS intensjon om fremtidig bruk.*	Forkast
H3	*Opplevd kompatibilitet til SSIS er positivt assosiert med bruk av SSIS og intensjon om fremtidig bruk.*	Aksepter for nåværende bruk. Forkast for fremtidig bruk
H4	*Den opplevde ytelsen ved hjelp av SSIS er positivt assosiert med bruk av SSIS og intensjon om fremtidig bruk.*	Forkast

B.5 Oppsummering

Det har blitt gjennomført en kvantitativ undersøkelse for å undersøke de faktorer som påvirker bruken av SSIS blant de som jobber med informasjonssikkerhet i offentlige norske virksomheter. Resultatene viste at

opplevd nytte er en sterk og meget betydelig faktor for dagens bruk av SSIS og intensjon om fremtidig bruk. Dette var som forventet og i samsvar med tidligere studier. En vellykket innføring av SSIS vil bli alvorlig svekket dersom SSIS ikke anses som nyttig av brukerne. Videre viste resultatene at opplevd kompatibilitet er sterkt korrelert til nåværende bruk av SSIS.

Resultatene fra undersøkelsen kan oppsummeres som følger: Jo mer nyttig SSIS oppfattes jo, mer sannsynlig at systemet vil bli akseptert. På samme måte, hvis SSIS er kompatibelt med hvordan informasjonssikkerhetsansvarlig utfører sitt arbeid, jo mer nyttig synes de SSIS er og jo mer vil de bruke SSIS. Opplevd brukervennlighet forklarer ikke dagens bruk eller intensjon om fremtidig bruk. Dette skyldes trolig at 65% av de som svarte har vært med på å definere SSIS i sin virksomhet. Siden de da kjenner SSIS inngående, anser de ikke brukervennlighet som viktig for egen bruk av styringssystemet.

Økt forståelse av de faktorer som bestemmer dagens bruk og fremtidig bruk setter virksomhetene i stand til å innføre tiltak for å få tatt SSIS mer i bruk. En nøkkel i en vellykket utvikling og innføring av SSIS er å involvere sentrale interessenter i virksomheten når SSIS utvikles og forbedres. Da vil det enklere oppnås kompatibilitet med eksisterende verdier og arbeidsrutiner. Hvis kun den som er ansvarlig for informasjonssikkert er involvert i arbeidet med å etablere og forbedre SSIS, blir innføringen vanskelig. Hvis etablering av SSIS blir motivert ut fra hva tilsynsmyndigheter krever, og ikke en virksomhets reelle behov, vil SSIS få lavere kompatibilitet med virksomhetens verdier og arbeidsrutiner noe som igjen gir lav faktisk bruk.

Forholdet mellom faktorer som påvirker bruk og fremtidig bruk av SSIS, som vist i denne studien, gir innsikt til ledere i statlige virksomheter og Difi i hva som kreves for en vellykket innføring av SSIS.

C Spørreskjema

Spørreundersøkelse: **Bruk og nytte av styringssystemer for informasjonssikkerhet**

Hva er din nåværende stilling? _____
Hva er din høyeste fullførte utdanning?

☐ Bachelorgrad eller tilsvarende ☐ Mastergrad eller tilsvarende ☐ Doktorgrad
☐ Annet:_____

Hvor mange års erfaring har du fra arbeid med informasjonssikkerhet? _____
Hvor lenge har du jobbet i din nåværende organisasjon?_____

Styringssystem for informasjonssikkerhet (SSIS) kan defineres slik:

De prosesser, prosedyrer, dokumenter, o.l. som skal sikre ledelsen styring, kontroll og kontinuerlig forbedring av virksomheten innen informasjonssikkerhet. (Difi-rapport 2012:15)

Et SSIS kan inneholde prinsipper, retningslinjer og rutiner knyttet til informasjonssikkerhet. Videre kan SSIS beskrive ansvar og ressurser, risikostyringsaktiviteter, mål for informasjonssikkerhetsarbeidet, og hvordan måle effekten av informasjonssikkerhetsarbeidet.

Har du vært med å utarbeide SSIS i din organisasjon?_____
Hvis ja: hvor lenge har du jobbet med utarbeidelse av SSIS i din organisasjon?_____

For hvert av utsagnene under, hak av i den boksen som passer best med din oppfatning.

1. Hvordan vil du vurdere din bruk av SSIS i dag i dine aktiviteter?	Ikke brukt	Brukt noen ganger	Jevnlig bruk i noen få aktiviteter	Jevnlig bruk i de fleste aktiviteter	Jevnlig bruk i alle aktiviteter
Arbeid med tekniske sikkerhetstiltak	☐	☐	☐	☐	☐
Arbeid med organisatoriske sikkerhetstiltak	☐	☐	☐	☐	☐
Rapportering av sikkerhetsarbeidet til toppledelse	☐	☐	☐	☐	☐
Bevisstgjøringsaktiviteter i organisasjonen	☐	☐	☐	☐	☐
Prioritering av sikkerhetsarbeidet	☐	☐	☐	☐	☐
Planlegging og organisering av sikkerhetsarbeidet	☐	☐	☐	☐	☐
Håndtering av sikkerhetsproblemer	☐	☐	☐	☐	☐

2. Intensjon om framtidig bruk	Svært uenig	Uenig	Nøytral	Enig	Svært enig
Jeg kommer til å *øke* min bruk av SSIS i arbeidet mitt framover	☐	☐	☐	☐	☐
Jeg kommer til å *bruke* SSIS i arbeidet mitt framover	☐	☐	☐	☐	☐
Om jeg kunne velge, ville jeg foretrekke å *ikke bruke* SSIS i framtidig arbeid	☐	☐	☐	☐	☐
Jeg ønsker å *bruke* SSIS framover	☐	☐	☐	☐	☐

3. Opplevd nytte	Svært uenig	Uenig	Nøytral	Enig	Svært enig
Jeg opplever at SSIS er nyttig i jobben min	☐	☐	☐	☐	☐
Bruk av SSIS forbedrer min arbeidsprestasjon	☐	☐	☐	☐	☐
Bruk av SSIS øker produktiviteten min	☐	☐	☐	☐	☐
Bruk av SSIS øker kvaliteten i arbeidet mitt	☐	☐	☐	☐	☐
Bruk av SSIS gjør det enklere å gjøre jobben min	☐	☐	☐	☐	☐
Fordelene med å bruke SSIS oppveier ulempene	☐	☐	☐	☐	☐

4. Opplevd brukervennlighet					
Jeg synes vårt SSIS er klart og forståelig	☐	☐	☐	☐	☐
Bruk av SSIS krever ikke mye tankearbeid	☐	☐	☐	☐	☐
Jeg synes SSIS er lett å bruke	☐	☐	☐	☐	☐
Vårt SSIS er ikke tungvint å bruke	☐	☐	☐	☐	☐
Bruk av SSIS tar ikke for mye tid fra mine vanlige arbeidsoppgaver	☐	☐	☐	☐	☐

5. Opplevd samsvar					
Vårt SSIS samsvarer med hvordan jeg jobber med sikkerhet	☐	☐	☐	☐	☐
Bruk av SSIS er forenlig med alle deler av arbeidet mitt	☐	☐	☐	☐	☐
Bruk av SSIS passer godt med hvordan jeg jobber	☐	☐	☐	☐	☐
Vårt SSIS er forenlig med hvordan vi organiserer arbeidet vårt	☐	☐	☐	☐	☐

6. Opplevd ytelse					
Vårt SSIS har vesentlig forbedret sikkerheten i vår virksomhet	☐	☐	☐	☐	☐
Vårt SSIS har redusert kostnadene ved informasjonssikkerhetsarbeid betydelig	☐	☐	☐	☐	☐
Vårt SSIS har ført til en vesentlig reduksjon i antallet alvorlige sikkerhetshendelser	☐	☐	☐	☐	☐
Vårt SSIS har vesentlig redusert tiden som er nødvendig for opplæring av nye medarbeidere	☐	☐	☐	☐	☐
Vårt SSIS har gjort det betydelig enklere å jobbe sammen om informasjonssikkerhet	☐	☐	☐	☐	☐
Vårt SSIS har vesentlig forbedret vår generelle ytelse	☐	☐	☐	☐	☐

Gi en kort beskrivelse av din virksomhets styringssystem for informasjonssikkerhet?

D Intervjuguide

1. Innledning
    a. Velkommen v/DIFI
    b. Kort om opplegget og om hvordan data vil bli behandlet
    c. Kort presentasjonsrunde (rolle i organisasjonen, arbeidsoppgaver, bakgrunn, forventninger til dagen)
2. Idemyldring med bruk av gule lapper
    a. Hva fungerer bra i arbeidet med informasjonssikkerhet hos dere?
    b. Hva er utfordrende med informasjonssikkerhet i din arbeidshverdag?
3. Kultur og forankring
    a. Hva er sikkerhetskultur?
    b. Hvorfor er det utfordrende å skape en god sikkerhetskultur?
    c. Hvordan er sikkerhetsarbeidet forankret i organisasjonen?
    d. Hvordan får du støtte til arbeid med oppgaver og problemstillinger knyttet til informasjonssikkerhet?
4. Styringssystemer og risikovurderinger
    a. Presentasjon og diskusjon av resultater fra spørreundersøkelsen (kun en gruppe)
    b. Hvordan få nytte av et styringssystem for informasjonssikkerhet?
    c. Hvilke utfordringer opplever de når det gjelder risikovurderinger – i planlegging, gjennomføring og bruk i etterkant?
    d. Hvordan gjør man vurderinger knyttet til akseptabel risiko – er ledelsen involvert?
    e. Hvordan opplever de nytteverdien av å gjøre risikovurderinger knyttet til informasjonssikkerhet?
    f. I hvilken grad vurderes risiko knyttet til IT-systemene opp mot risikovurderinger gjort på andre områder?
5. Krav, utvikling, forvaltning (kun tre av gruppene)
    a. I løpet fra utlysning/krav, utvikling til forvaltning av IT-systemer, hvor og hvordan er sikkerhet involvert? (tegne et løp på tavla, finne aktiviteter de er med på. Vi dekker følgende faser: *Løsningsbeskrivelse, Utvikling, Test, (Mottak/Beredskap), Forvaltning*)
        i. Hvem er med på å lage sikkerhetskrav?
        ii. Er sikkerhetskrav viktig?
        iii. Diskusjoner rundt hvordan sikkerhet oppleves opp mot andre egenskaper som f.eks. brukervennlighet, ytelse og pris.
        iv. I hvilken grad er dere (informasjonssikkerhetsansvarlige) involvert?
        v. Hvor viktig er krav til sikkerhetskompetanse i valg av leverandør?
        vi. Hvordan samarbeider man med leverandører om sikkerhetsaktivitetene som er identifisert? (kontrakter)
        vii. Gjøres det risikovurderinger i forbindelse med utvikling og forvaltning?
6. Oppsummering
    a. Ble forventningene til dagen møtt?

Teknologi for et bedre samfunn

www.sintef.no