Våren | 14

Sikkert som banken…..

Et forskningsstudie om informasjonssikkerhet i bank
av Marie Lahn Rømcke

MSAMAS, juni 2014

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I
SAMFUNNSSIKKERHET

MASTEROPPGAVE

SEMESTER: Vår 2014

FORFATTER:
Marie Lahn Rømcke

VEILEDERE:
David Häger og Annelin Thorkildsen

TITTEL PÅ MASTEROPPGAVE:
Sikkert som banken…
- Et forskningsstudie om informasjonssikkerhet i bank

EMNEORD/STIKKORD:
Informasjonssikkerhet, sikkerhetsstyring, bank, samfunnssikkerhet

SIDETALL: 67

STAVANGER **13.06.2014**

Sammendrag

Den teknologiske utviklingen har ført til endring i den norske bank- og finansnæringen sitt forretningsmønster. Dette har gjort informasjonssikkerhet til en større del av sikkerhetsarbeidet enn tidligere. Denne oppgaven har derfor som formål å kartlegge faktorer som er nødvendig for å oppnå god informasjonssikkerhet, samt forklare utfordringer med progresjon og modenhet i informasjonssikkerhetsarbeidet i norske banker. Problemstillingen for oppgaven er som følger; *Hvilke faktorer er nødvendige for å oppnå "god informasjonssikkerhet" i norske banker, og hvilke utfordringer har bankene for å oppnå videre progresjon og økt modenhet i informasjonssikkerhetsarbeidet?*

Studiet benytter eksplorativ kvalitativ metode, bestående av 14 intervjuer fra syv norske banker samt dokumentanalyse av både lovkrav, standarder og interne policydokumenter. Slutningene er tatt med bruk av både induktiv og abduktiv forskningsstrategi. Empirien er satt i sammenheng med sikkerhetsteori som omfatter *sikkerhetsstyring* (Perrow 1984, Weick 2001, La Porte 1996), *risikostyring* (Aven et al. 2004, Rausand 2009, Andersen & Häger 2010), *sikkerhetskultur og menneskelig faktor* (Reason 1997, Dekker 2006), *måling av informasjonssikkerhet* (Frost 2000, Von Solms 2001, Thomson 2006) og *Menneske-Teknologi-Organisasjonsperspektiv* (Bento 2001, Rollenhagen 1997).

Oppgaven har kartlagt samsvar mellom det lovkrav, sikkerhetsteorier og banknæringen mener er nødvendig for å oppnå "god informasjonssikkerhet". Utfordringene forbundet med progresjon og modenhet av informasjonssikkerhet i bank, er knyttet til faktorer som trekkes frem som utfordrende og sviktende, slik som klassifisering, helhetlig sikkerhetstilnærming og sikkerhetskultur.

Mangel på helhetlig og systematisk måling av informasjonssikkerhet, slik at bankene kan si noe om progresjon og modenhet, kan også forklares med at informasjonssikkerhet tradisjonelt har hatt en teknisk tilnærming. Dette gjelder også i bank. Ved å implementere en bevist Menneske-Teknologi-Organisasjonsperspektiv (MTO) til informasjonssikkerhet, vil man forenkle bankens helhetlige sikkerhetstilnærming og dermed løse utfordringer som er forbundet med videre progresjon og økt modenhet av informasjonssikkerhet i norske banker.

Innholdsfortegnelse

Tabelloversikt

Figuroversikt

Forord

Min motivasjon og inspirasjon for dette forskningsprosjektet kom etter å ha tatt emnene *infrastruktur og sårbarhet*, *risikobasert styring* og *styring av operasjonell risiko*. Etter finanskrisen i 2008 har bruken av risikostyring i bank- og finanssektoren økt, noe som krever mer forskning på området. Det samme gjelder knytningen mellom fagområdet informasjonssikkerhet med samfunnssikkerhet ettersom den teknologiske utviklingen har ført til nye trusler og risikoer både for virksomheter, men også for samfunnet i sin helhet. Jeg håper at denne oppgaven kan bidra positivt til faglitteraturen ved at den trekker linjer mellom etablerte sikkerhetsteorier og informasjonssikkerhetsarbeidet i norske banker.

Jeg vil takke alle mine 14 informanter som tok seg tid til å svare på mine spørsmål og at de delte velvillig sine kunnskaper, erfaringer, forståelser og forklaringer.

Takk til mine veiledere, David Häger og Annelin Thorkildsen, med deres gode innspill og tilbakemeldinger gjennom hele oppgaveprosessen.

Dessuten ønsker jeg å takke Marianne, Berit og Petter for korrekturlesing, gode tilbakemeldinger og kommentarer. I tillegg en stor takk til lillesøster Hedvig for estetisk utarbeidelse av figurer som er brukt i oppgaven.

Til slutt vil jeg takke Universitetet i Stavanger og professorene på masterstudiet i samfunnssikkerhet for deres kunnskapsdeling, smittende engasjement, involvering og motivasjon til å arbeide videre mot et sikrere samfunn!

Marie Lahn Rømcke

Stavanger, 13.06.2014

1 Innledning

Dette forskningsstudie vil omhandle samfunnssikkerhet[1] og kritiske samfunnsfunksjoner, nærmere bestemt bank- og finansnæringen. Denne industrien er en betydningsfull del av det moderne samfunn og i de siste årene har banknæringen endret sitt forretningsmønster. Det er i dag en økt forventning til teknologiske selvbetjeningsløsninger som mobil- og nettbank istedenfor de tradisjonelle bankkontorene.

Allerede i 2000 slo Sårbarhetsutvalget fast at dagens samfunn er mer sårbart enn før som følge av at avhengigheten av teknologien gjør at robustheten i det norske samfunn minker (NOU, 2000:24). Den komplekse IT-teknologien som benyttes av banknæringen i Norge byr på mange fantastiske muligheter, men dessverre bringer den økende bruken og avhengigheten også med seg ulike negative konsekvenser. Daglig leser og hører vi om kortsvindel, trojanere[2]/virus eller driftsproblemer i banker. Et driftsbrudd over lengre tid vil føre til en alvorlig krise både for privatpersoner og bedrifter. I 2003 opplevde Den Danske Bank (DDB) et driftsbrudd i fire dager, som omfattet alt fra selvbetjeningsløsninger, nettbank og minibanker. Dette resulterte i at sentralbanken i Danmark måtte forsyne DDB med penger og kostnaden etter denne krisen ble estimert til nærmere én milliard danske kroner (Daler, T. et al., 2010). For ikke å snakke om den personlige krisen mange av kundene og bedrifter opplevde. I tillegg ser man i Norge en økning av økonomisk kriminalitet og identitetstyveri som følge av endringsmønsteret i bank- og finanstjenestene (Finanstilsynet, ROS 2012). Dermed står bankene foran store utfordringer de neste årene for å minke gapet mellom truslene og sikkerhetstiltak.

I norske bank- og finansinstitusjonene kan man dele sikkerhetsarbeidet inn i to overordnede grupper; HMS[3] og informasjonssikkerhet. Denne oppgaven vil omhandle informasjonssikkerhet, som omfatter risikoer omkring virksomhetens informasjonsverdier og sikring av opplysninger i henhold til konfidensialitet, integritet og tilgjengelighet. Informasjonssikkerhet inngår i bankens styring av operasjonell risiko. Operasjonell risiko er

[1] **Samfunnssikkerhet** (St.meld. nr. 17. 2001-2002): ”Evnen samfunnet har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger.

[2] **Trojaner**: ”Ondsinnet program som utgir seg for å være noe annet enn det er. Når brukeren prøver å kjøre eller installerer dette programmet vil datamaskinen infiseres med ondsinnet kode som” for eksempel virus (Norsis leksikon).

[3] **HMS** vil i denne sammenhengen si fysisk sikring mot blant annet ran eller brann.

ifølge Basel II definert som ”*risikoen for tap som følge av utilstrekkelige eller sviktede interne prosesser eller systemer, menneskelige feil, eller eksterne hendelser*” (BCBS, 2006).

I mange rapporter, risikoanalyser, lovverk og krav som omfatter informasjonssikkerhet nevnes begrepet ”god eller tilfredsstillende informasjonssikkerhet”. Dette er begreper med stor tvetydighet. Denne oppgaven vil benytte disse to begrepene som ett, og mener at det å ha ”god informasjonssikkerhet” betyr det samme som å ha ”tilfredsstillende informasjonssikkerhet”. Begrepene uttrykkes som et mål av godheten til informasjonssikkerhetsarbeidet, dette kan skape forvirring om hvordan man kan oppnå målet. Allikevel vil det være viktig for alle bankene i Norge å oppnå ”god informasjonssikkerhet”. Denne oppgaven vil derfor forsøke å avdekke:
Hvilke faktorer er nødvendige for å oppnå ”god informasjonssikkerhet” i norske banker, og hvilke utfordringer har bankene for å oppnå videre progresjon og økt modenhet i informasjonssikkerhetsarbeidet?

For å besvare første del av problemstillingen vil oppgaven innledes med en analyse som kartlegger følgende delmål:

1. **Hva er ”god informasjonssikkerhet” i bank?**
2. **Hvilke faktorer trekker lovkrav og sikkerhetsteorier frem som nødvendige for å oppnå dette målet og hvordan samsvarer faktorer fra teorien og lovkrav med faktorer som bankene selv trekker frem som nødvendige for å nå ”god informasjonssikkerhet”?**

Ut i fra lover og standarder som omhandler informasjonssikkerhet i bank, og det tradisjonelle synet på informasjonssikkerhet, har hovedfokuset vært på de tekniske systemene som sikrer informasjonen. Eksempelet over med DDB viser hvor kritisk det er å ha pålitelige tekniske systemer, men til tross for gode systemer ser man at uønskede hendelser skjer. Teknologi er selve grunnmuren for informasjonssikkerhet, men truslene og sikkerhetsrisikoene har både tekniske og menneskelige opprinnelse. Dette vil legge føringer for oppgavens andre del av problemstillingen.

Et eksempel på en uønsket hendelse som oppstod i samspillet mennesket og teknologi er Nick Leeson i Barings Bank. Han hadde en dobbeltrolle som trader og sjef for oppstartsfasen for etableringen i Singapore for Barings Bank. Disse stillingene gav han flere tekniske tilganger enn det han burde hatt. Dessuten var det mangel på god sikkerhetskultur og internkontroll som tilsammen førte til at Barings Bank, som hadde eksistert siden 1762, kollapset i 1995

(Reason, 1997). De tekniske systemene for overvåkning og autorisert tilgang ville vært barrierer for å stoppe Leeson sine aktiviteter, dessuten ville strengere internkontroll kunne avdekket misligheten. Til slutt ville en god sikkerhetskultur gjort at de involverte følte seg trygge nok til å si ifra om feilene som var gjort. For å unngå slike uønskede hendelser må man se på informasjonssikkerhet som en helhetlig og integrert del av hverdagen til alle ansatte i bank. Dette har vært en utfordring for informasjonssikkerhetsarbeidet og Dhillon (2001) forklarer dette med;

> *"Solutions to the problem of managing information security in the new millennium hark back at shifting emphasis from technology to business and social processes. Although many researchers have placed calls for such an orientation, in practice over- formalized, acontextual and ahistorical solutions designed in a reactive manner still dominate"*

Derfor vil siste del av problemstillingen være knyttet til identifisering og forklaring av utfordringer for progresjon og modenhet i norske banker sitt informasjonssikkerhetsarbeid. Avslutningsvis vil oppgaven drøfte og avdekke om et Menneske-Teknologi-Organisasjonsperspektiv (MTO), som er en ledende tilnærmingen til sikkerhetsstyring i oljebransjen, kan være hensiktsmessig for norske banker. Etter å ha kartlagt delmål 1 og 2 vil oppgaven fortsette med å besvare følgende delmål:

3. **Hvilke utfordringer har bankene for å oppnå videre progresjon og økt modenhet av informasjonssikkerhet?**
4. **Kan et MTO-perspektiv brukes for å oppnå en progresjon i bankens modenhet av informasjonssikkerhet, og i så fall hvordan?**

1.2 Oppgavens struktur

Oppgaven begynner i kapittel 2 med å presentere nødvendige faktorer for å oppnå "god informasjonssikkerhet" fremhevet av lovkrav, standarder og *beste praksiser*.
I kapittel 3 vil relevant teori beskrives og satt i sammenheng med informasjonssikkerhet i bank. Deretter vil kapittel 4 gi en gjennomgang av metodikken som er benyttet i oppgaven. Etter det følger en presentasjon av funn og resultater i kapittel 5.
Både kapittel 2, 3 og 5 legger så føringer for kapittel 6 som drøfter foregående kapitler opp mot hverandre.
Kapittel 7 vil gi en konklusjon på både problemstillingen og de fire forskningsspørsmålene.

2 ”God informasjonssikkerhet”- beskrevet av lovkrav og *beste praksis*

2.1 Informasjonssikkerhetsrelaterte lovkrav

Lovverket for informasjonssikkerhet i bank vil i denne oppgaven bli avgrenset til *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT)* av 21. mai 2003 nr. 630 (Heretter IKT-forskriften) og *Lov om behandling av personopplysninger* av 14. april 2000 nr. 31 (Heretter Personopplysningsloven). Det finnes flere lover som direkte og indirekte legger føringer for informasjonssikkerheten i norske banker, men det er de overnevnte lovkravene som fastsetter de største delene av det regulatoriske rammeverket for informasjonssikkerheten i bankene.

Både Datatilsynet (2009) og Nasjonal Strategi for Informasjonssikkerhet (2012) er enige om at ”god informasjonssikkerhet” oppnås ved hjelp av planlagte, helhetlige og systematiske tiltak. I Personopplysningsloven *§ 13 informasjonssikkerhet* står det i tillegg at *”for å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene”*.

Videre presenteres kort de faktorer som overnevnte lovkrav påpeker som nødvendig for å sikre ”god informasjonssikkerhet” i norske banker.

Fysisk og logisk sikring

I paragraf *§5 Sikkerhet* i IKT-forskriften, settes det krav om utarbeidelse av fysisk beskyttelse for utstyr, systemer og informasjon av betydning. Dette kan være å låse eller skjerme utstyr ved å for eksempel lage en *sikker sone* med strenge krav til autorisasjon og tilgang av kritisk datautstyr. Logisk sikring kan bety sikring av digitale nettverk gjennom for eksempel brannmurer og anti-virus.

Rutiner og prosedyrer

Det skal foreligge prosedyrer og beskrivelse av alle prosesser og *”hvordan ansvaret for administrasjon, anskaffelse, utvikling, drift, systemvedlikehold, sikring av informasjon og avvikling utføres på en betryggende måte”* (IKT-forskriften *§2 Planlegging og organisering).*Ved utkontraktering skal egne retningslinjer og prosedyrer sikre leveranse. Personopplysningsloven *§ 13* legger opp til at det kan utarbeides forskrifter om informasjonssikkerhet av personopplysninger som vektlegger både organisatoriske og

tekniske sikkerhetstiltak, dette er gjort i *Forskrift om behandling av personopplysninger* av 15. desember 2000 nr. 1265 (heretter Personopplysningsforskriften).

Avvik- og endringshåndtering

Ifølge Personopplysningsforskriften *§2-6* er avvik definert som *"i strid med fastlagte rutiner, og sikkerhetsbrudd"*. IKT-forskriften *§9* omhandler avvik- og endringshåndtering; og der står det at avviksbehandling skal identifisere årsak til avviket, hindre gjentagelser og være en formell behandling av det. Prosedyrene i forbindelse med endringshåndtering skal gi en stabil, planlagt og forutsigbar drift.

Ansvarsfordeling

Både i *§2 og §3* av IKT-forskriften skriver at ansvaret og rollene for informasjonssikkerhet skal være klart definert i bankene. Dette skal dokumenteres og gjøres kjent for alle ansatte.

Internkontroll

I Personopplysningsloven *§14* settes det krav til internkontroll. Det vil si at den som har behandlingsansvaret skal ha kjennskap til gjeldene regler om behandling av personopplysninger og tilstrekkelig og oppdatert dokumentasjon for gjennomføring av de overstående rutiner.

Risikostyring

I IKT-forskriften *§3 Risikoanalyse* kreves det at det utarbeides risikovurderinger årlig, men også dersom det skjer endringer med betydning for informasjonssikkerheten i banken. I risikoanalysen skal bankene fastsette kriterier for akseptabel risiko som er forbundet med bruk av IKT-systemene.

Krav til underleverandører

For bankene i Norge settes det strenge lovkrav for kontroll av underleverandører. De må sette konkrete krav til underleverandører og forsikre seg om at arbeidet som gjøres er i henhold til avtale, aktuelle retningslinjer og regelverk (Finanstilsynet, 2011).

Kritiske komponenter

I IKT-forskriften sine paragrafer, *§ 3* (Risikoanalyse), *§ 10* (Krav til kontinuitet) og *§ 11* (Driftsavbrudd og katastrofeberedskap), stilles det krav om at bankene skal ha oversikt over alle kritiske komponenter i sitt IKT-infrastruktur. Det er i tillegg presisert at dette omhandler også de komponenter som blir behandlet av underleverandører (Finanstilsynet, 2011).

Kontinuitetsløsning og katastrofeplan

På bakgrunn av risikoanalyse skal bankene ha en oppdatert kontinuitetsplan. I IKT-forskriftskravet fastsettes det at det skal gjennomføres opplæring, øvelse og testing av reserveløsninger. Kun testene har lovpålagt dokumentasjon og resultatet skal vurderes i etterkant. Det skal fastsettes en plan som skal iverksettes i forbindelse med katastrofe, når IKT-driften ikke kan opprettholdes.

Sikkerhetskultur

Det finnes ingen lovkrav som omhandler sikkerhetskultur i bank. Finanstilsynet (2013) inkluderer kun ”myke faktorer” ved at de i veileder til IKT-forskriften anbefaler bankene å etablere en sikkerhetskultur som systematisk avdekker risiko og muligheter for forbedringer og at det utføres planmessig oppfølging av forbedringstiltak.

Alle lovkrav som er fremhevet er funksjonsbaserte krav, det vil si en regelverkstype som kun setter krav til forventet resultat og sier ingenting om hvordan resultatene skal oppnås. Det er dermed opp til virksomhetene selv å bestemme de løsningene som må til for å nå målene (Lindøe, 2012). Det er med andre ord opp til bankene å etablere egne løsninger for å oppnå ”god informasjonssikkerhet”.

2.2 Standarder og *beste praksiser*

I tillegg til myndighetskrav, benytter også mange banker etablerte standarder og *beste praksiser* for å sikre en systematisk tilnærming til informasjonssikkerhetsarbeidet. Faktorer som trekkes frem i disse vil være av en så generell karakter at de er gjeldene for enhver virksomhet, fra bank til kommune. Derfor går ikke oppgaven i svært detalj av disse *beste praksisene*. Isteden trekkes frem omfanget og hovedforskjellene mellom standardene og *beste praksisene* som kan brukes som en rettesnor for norske banker i sitt informasjonssikkerhetsarbeid.

ISO-27001 (2013) omfatter en del organisatoriske krav til virksomheter om hvordan informasjonssikkerhetsstyringssystemet (ISMS) i virksomheten bør implementeres, ivaretas og forbedres. I standarden omfattes alt fra sikkerhetspolicy, tilgangskontroll, vedlikehold og personellsikkerhet. Hendelseshåndtering vil også være en viktig del av å sikre åpenhet om hendelser og sårbarheter, samt etablere læring i virksomheten. En siste faktor som også påpekes er compliance; det å sikre at lover og regler er oppfylt.
ISO -27004 (2009) er en standard som omfatter måling av informasjonssikkerhet, og har som formål å effektivisere en etablert ISMS. Ettersom ingen banker i Norge er sertifisert i ISO-2700-serien vil ikke denne standarden være relevant for denne oppgaven.

Control Objective for Information and related Technology (COBIT) er en internasjonal standard for IT-revisjon som har som formål at IT-prosesser skal være styrt i henhold til *beste praksis*[4]. Den siste utgaven COBIT 5 Information Security[5] kan fungere som en sjekkliste for virksomheter og trekker frem faktorer som prosedyrer, rammeverk, adferd og holdninger, organisatoriske strukturer og prosesser, samt. infrastruktur (arkitektur). Finanstilsynet som har hovedansvaret for å sikre etterlevelse av blant annet IKT-forskriften i norske banker bruker tilpasset COBIT når de utøver tilsyn. De anbefaler også egenvurderingsskjemaer til bankene som også er basert på COBIT[6].

Information Technology Infrastructure Library (ITIL) skal sikre at informasjonsprosessene er nøyaktige, fullstendige og beskytter mot uautoriserte endringer. Service Level Agreement (SLA) er tjenesteleveranse gjort av eksterne og dette skal være en del av ITIL, der man sikrer leveranse, drift og support av IT-tjenester fra underleverandører.

Til forskjell fra lovkravene vil standarder gi en beskrivelse av mål i tillegg til å forklare hvordan de kan oppnås. En svakhet med standarder er at de kun gir generelle beskrivelser som passer til alle type virksomheter som for eksempel banknæringen, oljebransjen og offentlig forvaltning. Standardene og lovkravene til informasjonssikkerhet er overlappende og komplementære. Faktorer som er nødvendig for å oppnå ”god informasjonssikkerhet” som trekkes frem i lovkrav og standarder vil legge rammer for norske banker sitt informasjonssikkerhetsarbeid.

[4] **COBIT- offisielle hjemmeside**: http://www.isaca.org/cobit/pages/default.aspx
[5] **Introduksjon til COBIT 5**: http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf
[6] **Finanstilsynets egenevalueringsskjemaer**: http://www.finanstilsynet.no/no/Tverrgaende-temasider/IT-tilsyn/Egenevalueringssporsmal/

3 Teori

3.1 "God informasjonssikkerhet" – hva er det egentlig?

Informasjonssikkerhet består både av fysisk- og logisk sikring. Fysisk sikring vil si at informasjonen i IT-systemer eller papirform både er sikret mot naturkatastrofer og fysisk tilgang fra utenforstående, som for eksempel adgangskort og back-up i tilfelle lynnedslag. Logisk sikring er bevaring av konfidensialitet, integritet og tilgjengelighet av IT-systemer, der man sikrer seg mot blant annet hacking, virus og sabotasje (Slay et al., 2006). Den tekniske dimensjonen er omfattende og grunnmuren for informasjonssikkerhet i alle virksomheter. Informasjonssikkerhet er og vil alltid være en teknisk disiplin, og uten fokus på tekniske løsninger vil informasjonssystemene kollapse (Albrechtsen i Mjølsnes, 2012). Denne oppgaven vil allikevel avgrenses til å kun ha en overordnet tilnærming til den tekniske sikringen av IT-systemer og informasjon i bank. Den vil også avgrenses til kun å inkludere de delene av informasjonssikkerhet som norske banker har mulighet til å påvirke selv gjennom sikkerhetstiltak. Oppgaven vil sette den tekniske dimensjonen i sammenheng med de menneskelige og organisatoriske elementene av informasjonssikkerhet og beskrive det som en del av et sosio-teknisk system[7] (Albrechtsen, 2008).

Begrepet informasjonssikkerhet inneholder tre elementer som defineres i Nasjonal Strategi for Informasjonssikkerhet (2012:10) som:

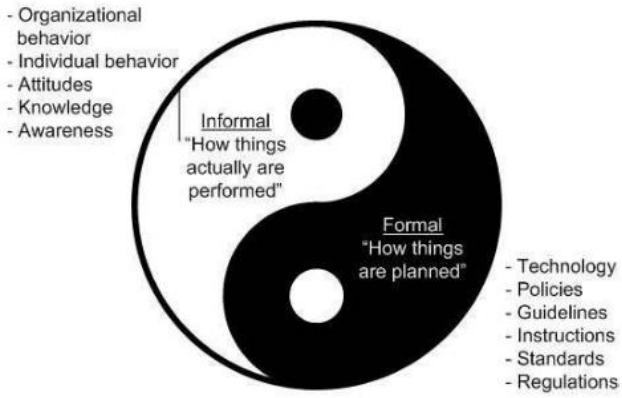
1. *Konfidensialitet* - Sikkerhet for at nærmere angitt informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til denne
2. *Integritet* - Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter
3. *Tilgjengelighet* – Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.

I oppgaven vil informasjonssikkerhet omfatte både fysisk- og logisk sikring og defineres som **sikring av konfidensialitet, integritet og tilgjengelighet for den informasjonen som behandles av bankens system og systemet i seg selv**. Ved å inkludere "systemet i seg selv" vil informasjonssikkerhet bli fremhevet som mer enn bare tekniske systemer.

Informasjonssikkerhetsstyring i bank og andre virksomheter vil være et sett av faktorer som har funksjonen å kontrollere trusler og sårbarheter, både gjennom formelle elementer og

[7] Et MTO perspektiv (menneske-teknologi-organisasjon) er ofte brukt som et synonym for sosio-teknisk systemer (Albrechtsen i Mjølsnes, 2012:203)

uformelle organisatoriske prosesser (Albrechtsen i Mjølsnes, 2012). Figur 1 forklarer hva som inngår i de formelle og uformelle prosessene i virksomheten.



Figur 1: illustrerer samspillet mellom det uformelle og formelle i en virksomhet (Albrechtsen i Mjølsnes, 2012:294)

En av utfordringene med informasjonssikkerhetsarbeidet i bank er at begrepet ”god informasjonssikkerhet” som er brukt i en rekke lover, veiledere, krav, standarder og interne sikkerhetspolicy er forbundet med tvetydighet. Ramirez (2000) skiller mellom ulike typer begreper og skriver at forskjellige mennesker ikke nødvendigvis mener det samme selv om de bruker samme uttrykk. Dermed kan det som beskrives som ”god informasjonssikkerhet” for enkelte tolkes annerledes av andre. Slike begrep er Ramirez (2000) kaller en blanding mellom ideologiske[8] og diffuse[9] begrep; *en ønsket og tiltenkt tilstand*. ”God informasjonssikkerhet” blir derfor et beskrivende mål som kan forstås forskjellig ut i fra hvilke aktører som bruker det og dermed vekker begrepet ulike meninger og assosiasjoner til mottaker av ordet.

3.2 Behov for et sosio-teknisk perspektiv?

Utviklingen av samfunnets syn på ulykker har utviklet seg fra å skylde på teknologien til et mer helhetlig perspektiv. Før mente man for eksempel at en fabrikkulykke oppstod som følge av usikre tekniske komponenter, mens med dagens kompleksitet og utvikling har man endret dette synet ved å gå dypere og avdekke direkte og indirekte årsaker til at uønskede hendelser og ulykker skjer. Ulykkesårsaker kan i dag bli forklart ut i fra samspillet mellom mennesker, organisasjon og teknologi (MTO) (Bento, 2001). Innenfor informasjonssikkerhetsarbeidet har det som nevnt tidligere tradisjonelt vært mest fokus på det teknologiske elementet. Følgelig har etableringen av sikre tekniske systemer vært hovedprioritet (Mjølsnes, 2012). Den

[8] **Ideologisk begrep** beskriver en ønsket tilstand.
[9] **Diffuse begrep** beskriver en forståelse eller håndtering av menneskelige situasjoner.

tekniske utviklingen har medført en endring i trusselbildet og risikoer forbundet med informasjonssikkerhet. Truslene og risikoene inkluder i større grad menneskelige faktorer, som brukere (ansatte og kunder) og trusselaktører, og organisatoriske faktorer, som prosedyrer og ansvarsroller. I Finanstilsynets årlige risiko og sårbarhetsanalyse (ROS) står det blant annet at *"Manglende forståelse og oppfølging kan føre til økt risiko. Det er derfor viktig at utviklingen [av risikobildet] følges for å sikre håndtering av en situasjon under endring"* (Finanstilsynet, 2013:6). Isolert sett er de tekniske IT-systemene i et informasjonssikkerhetssystem både pålitelige og robuste, men det er i samspillet mellom mennesket og organisasjon mange av de uønskede hendelsene oppstår (Perrow, 2007). Robusthet er linket med *"et systems evne til å opprettholde sin funksjon når det utsettes for påkjenninger"* (Aven et al., 2004:124). For å avverge uønskede hendelser og deres konsekvenser vil sikkerhetsstyring være nødvendig. Videre presenteres to ledende teorier for sikkerhetsstyring.

3.2.1 "Normal Accident Theory" og "High Reliability Organizations"

Perrow (1984) sin teori om "normal ulykker" mener at dersom det oppstår et misforhold mellom tette koplinger og høy kompleksitet i et sub-system[10] eller hele systemet[11], er ulykke eller systemsammenbrudd uunngåelige. I tilfeller der kun en del av sub-systemet eller systemet blir ødelagt kaller Perrow (ibid.) dette for en uønsket hendelse. Normal Accident Teorien (NAT) beskriver storulykker[12] og ble skrevet på bakgrunn av nesten-atomulykken på Three Mile Island i USA. Innenfor informasjonssikkerhet i bank vil ikke en storulykke per definisjon kunne oppstå. Men utviklingene av informasjonssystemene i bank blir i større grad enn tidligere mer høyteknologisk og tettere koplet. Dessuten kan de økonomiske konsekvensene ved brudd på informasjonssikkerhet i bank være så enorme at de tilsvarer en storulykke. Til tross for at et cyber-ran av penger eller internt bedrageri er svært ødeleggende, kan dette dekkes økonomisk i etterkant. Men om sensitiv informasjon lekkes ut til uvedkommende kan det vanskelig tas tilbake og føre til alvorlige konsekvenser for de bankkundene som er berørt. Så en "storulykke" for banker vil dermed i større grad enn tidligere linkes opp mot brudd på informasjonssikkerhet.

---

[10] **Sub-system:** samling av enheter som til sammen utgjør et system – f eks: operativsystem, web-server, applikasjonsserver, sertifikattjenester, nettverkstjenester som er nødvendig for å utføre elektroniske transaksjoner.

[11] **System**: det totale systemet – hele bankens virksomhet

[12] **Storulykker**: "en akutt hendelse, for eksempel et større utslipp, en brann eller en eksplosjon, som umiddelbart eller senere medfører flere alvorlige personskader og/eller tap av menneskeliv, alvorlig skade på miljøet og/eller tap av større økonomiske verdier" (Petroleumstilsynet 2013).

Som nevnt i innledningen er informasjonssikkerhet i bank en del av operasjonell risiko. Alle forretningsprosesser i norske banker er avhengig av IT, og mange av IT-systemene de bruker kan sammenliknes med det Perrow kaller et *tett koplet system*, fordi dersom en feil oppstår i en komponent av systemet vil det kunne påvirke for eksempel hele informasjon og transaksjonskjeden. En slik skjede er hovedsakelig et *lineært system* ved at det er automatiserte og forventede interaksjoner, men det vil allikevel inneholde *kompleksitet* ettersom det er mange distanser i prosessen der flere komponenter opererer samtidig eller veldig tett. Det kan derfor ofte være vanskelig for bankene å finne hvor feilen oppstår når det først skjer en uønsket hendelse i en transaksjonskjede. Dessuten øker kompleksiteten ved at bankene flere underleverandører, for desto flere aktører jo større sannsynlighet er det for at hull i systemet oppstår i skjæringspunktene mellom ansvarsområdene mellom aktørene. Et eksempel på det Perrow (ibid.) beskriver som ”normal ulykke” i sin teori oppstod i Norge i påsken 2011 da det ble utført en endring IT-systemene hos EDB ErgoGroup ASA (EDB) som fikk ringvirkninger for flere av bankens systemer. Endringen førte til en overbelastning av primærserveren. Sekundærserveren har da som funksjon å ta over og håndtere den ekstra belastningen, men var på grunn av feil ved en tidligere utført oppdatering svekket. Det førte til av hverken primær- og sekundærserverne klarte å dekke kapasitetsbehovet. Feilen fikk enorme konsekvenser for tilgjengeligheten og resulterte i et enormt driftsavbrudd med 140 000 berørte norske bankkunder. Driftsavbruddet varte i nesten en uke og førte blant annet til at minst 200 000 transaksjoner ble avvist og over 240 000 reservasjoner måtte slettes (Finanstilsynet, 2011). Perrow (1984) beskriver strategier for å avverge slike ulykker; ved at man redusere kompleksiteten og løsne koplingene i tett koplet system. Utviklingen for norske banker sine tekniske systemer er at de går motsatt vei enn det Perrow anbefaler ved å gjøre koplingene mer integrerte og tette, noe som gjør de mer effektive, men også svært sårbare.

Teknologiske systemer er ikke nødvendigvis det som representerer den største sikkerhetsmessige utfordringen til informasjonssikkerhet, det er heller menneskene som sitter med ansvaret for å forvalte informasjonen og som utfører saksbehandling daglig i banken (Daler T. et al., 2010). En mer optimistisk og komplementær sikkerhetsstyringsteori til NAT kalt ”High Reliability Organizations” (HRO) ble etablert av en rekke forskere ved University of California Berkeley (La Porte 1996, Weick 2001, m.fl). Teorien forklarer hvordan ulykker i komplekse og høyteknologiske systemer og organisasjoner kan forebygges og unngås. En HRO gjenkjennes ved at organisasjonen eller virksomheten har en godt utviklet sikkerhetskultur som gjør at de har færre uønskede hendelser enn hva andre virksomheter har. HROer opererer til enhver tid under komplekse og risikofylte forhold. Banker vil derfor kunne dra nytte av HRO-teorien da de gjerne er mer utsatt mot trusler og risikofylte forhold

for brudd på informasjonssikkerheten enn hos andre næringer og selskap ettersom den økonomiske gevinsten for inntrengere kan være stor. Selv om norske banker ikke nødvendigvis er HROer, vil teorien ha overførbare elementer ettersom bankene kan forvente å måtte håndtere alvorlige uønskede hendelser som følge av brudd på informasjonssikkerhet i fremtiden.

I en HRO prioriteres sikkerhet og produksjon likt gjennom hele organisasjonen. Dette motstrider NAT som mener at sikkerhet bare er et av mange konkurrerende mål i en virksomhet. Organisasjoner kan i følge HRO oppnå høy redundans mot menneskelige feil, ved å blant annet ha overvåking, overlapping av arbeidsoppgaver, effektive informasjons- og rapporteringssystemer og så videre (Rosness, 2004). Dette skaper læring, bevissthet og tilstedeværelse (*mindfulness*) når ansatte foretar arbeidsoppgaver og gjør at man fokuserer på sikkerhet i alle ledd (Weick, 2001). En stor del av det å oppnå redundans mot ulykker og god sikkerhetskultur er knyttet til å oppnå en økt bevissthet (*mindfullness*) blant de ansatte (ibid.). For å håndtere uønskede hendelser og kriser må alle ansatte ha klare roller og vite hva sitt ansvar er, dette er et element av krisehåndtering som Weick kaller *virtual role* (Weick, 1993). *Virtual role* gjør at ansatte kan simulere handlinger på forhånd fordi de er klar over sin rolle og andre sine roller i hendelsen, og dermed vil man få en mer forventet håndtering. Dette krever selvsagt at banken etablerer klare roller og øver på dette ofte. Slik vil organisasjonen minke usikkerheten og skape en robusthet i en krisehåndteringssituasjon (ibid.).

En fundamental del av en vellykket HRO er sikkerhetskulturen i virksomheten. Reason (1997) definerer sikkerhetskultur som: *"shared values (what is important) and beliefs (how things work) that interact with an organization´s structures and control systems to produce behavioural norms (the way we do things around here)"* (s. 192). I en moden og vellykket sikkerhetskultur vil man aktivt søke etter potensielle hendelser, lære av feil, være en åpen og informert organisasjon med fleksibilitet til å anpasse seg endringer (Reason, 1997). Tabell 1 illustrerer hvordan Westrum (1993) deler organisasjonskulturer inn i tre kategorier basert på hvordan de håndterer informasjon som omhandler sikkerhet.

Pathological	Bureaucratic	Generative
Don't want to know	May not find out	Actively seek information
Messengers are shot	Listened to if they arrive	Messengers are trained
Responsibility is shirked	Responsibility is compartmentalized	Responsibility is shared
Bridging is discouraged	Bridging is allowed but neglected	Bridging is rewarded
Failure is punished or covered up	Organization is just and merciful	Inquiry and redirection
New ideas are actively crushed	New ideas present problems	New ideas are welcome

Tabell 1: viser hvordan forskjellige organisasjonskulturer behandler informasjon (Westrum 1993 fra Rosness, 2004)

For eksempel er en rapporterende og lærende kultur en del av det å ha god sikkerhetskultur. Det vil si at organisasjonen er positiv til rapportering av avvik som vil føre til læring slik at det jobbes med å avverge at uønskede hendelser skjer igjen (Reason, 1997). Dersom banken ikke har en god sikkerhetskultur vil sannsynligvis ikke ansatte rapportere videre feil som for eksempel nedlasting av et infisert program eller en IT-arkitekt oppdager en feil i vedkommens design av IT-infrastrukturen. Uten sikkerhetskultur som omfatter informasjonssikkerhet, vil bankene få menneskelige feil som forplanter seg, det Reason (1997) kaller latente feil, i organisasjonen og lager sikkerhetshull som kan i verstefall føre til en ulykke senere.

En dårlig sikkerhetskultur kan både være en grunnleggende årsaksfaktor til en uønsket hendelse og en faktor som påvirker effektivitet av sikkerhetsbarrierer (Forelesning: Tungland, M., 21.10.2013). En barriere er en måte å beskytte et sårbart mål mot farer, som kan kontrollere, redusere eller stoppe farekilder fra å utvikle seg (Rosness, 2004). Tradisjonelt sett er banker allerede svært opptatt av sikkerhet i forhold til sikring av verdier gjennom fysiske sikkerhetsbarrierer som bankhvelv og brannsikring, men de elektroniske lagringssystemene av informasjon byr på andre og nye vanskeligheter. For banker vil derfor "informasjonssikkerhetskulturen" også bestå av for eksempel sikker bruk av e-post og internett, og bevissthet omkring phishing[13], trojanere og sosial manipulering. Dette er trusler som er i konstant endring og som lett kan føre til at ansatte lett gjør menneskelige feil. Det vil kreve en risikoforståelse og bevissthet både fra ansatte generelt og særlig hos de som arbeider spesifikt med informasjonssikkerhet i banken.

[13] **Phishing**: e-postsvindel for å samle inn personlige opplysninger, som f.eks. brukernavn og PIN-kode for å få tilgang til nettbank (Store norske leksikon, 2012).

3.2.2 Den menneskelige faktoren

Informasjonssikkerhet er tradisjonelt og hovedsakelig sett som et såkalt *security* felt der man arbeider med sikring mot intenderte og ondsinnede handlinger som med planlegging ønsker å forårsake et brudd på informasjonssikkerheten. Til forskjell fra *safety*, brudd som oppstår som følge av uintenderte menneskelige feil eller teknisk svikt (Albrechtsen i Lydersen et al., 2004). Denne oppgaven mener informasjonssikkerhet består av begge områdene, ettersom risikoer for brudd på informasjonssikkerhet vil tilfalle både planlagte (*security*) og tilfeldige (*safety*) hendelser. Men da det meste av forskning og fokus på informasjonssikkerhet omhandler *security* vil denne oppgaven særlig vektlegge *safety*-fagområdet i sammenheng med informasjonssikkerhet. Videre vil derfor teorier om uintenderte menneskelige feil (*safety*) presenteres.

Den menneskelige faktoren er sett på som den barrieren som er mest sårbar (Rasmussen, 1982). Ofte blir også menneskelige feil stadfestet som å være en dominant årsak til ulykker. Sidney Dekker (2006) argumenterer at under hver enkelt og åpenbare menneskelige feil er det en annen mer dyptgående historie. Dekker sin teori mener at feil kun er symptomer på noe som er galt innad i organisasjonen og som oppstår som følge av de betingelsene ansatte jobber under. Dette gjenspeiles også i Reason (1997) som skriver*" We cannot change the human condition, but we can change the conditions under which people work"* (s. 25). Reason definerer menneskelige feilhandlinger som svikt i planlagte handlinger, slik at man ikke når ønskede resultater. Reason deler slike feilhandlinger i to:

1. **Forsømmelser eller glipper** er det Reason (ibid.) kaller feil som blir gjort som følge av at mennesket ikke konsentrerer seg om jobben som skal gjøres. Man har en god planlegging, men man feiler å fullføre arbeidet.
2. **Intensjonelle feiltakelser** *(mistakes)* er når planen som blir laget ikke er god nok fordi til tross for at menneskene følger planen oppstår det feil. Reason (ibid.) deler dette igjen mellom regelbaserte feil og kunnskapsbaserte feil. Regelbaserte feil vil si at man benytter feil planer gjerne ved at det er innført nye eller endrede planer. Mens kunnskapsbaserte feil er når utførelsen er riktig, men som følge av lite kompetanse er planen ikke riktig.

Det er en rekke faktorer som påvirker sannsynligheten for feilhandlinger, som fysiske forhold, tids- og arbeidspress, kompetanse, opplæring og sikkerhetskultur. Til tross for at de menneskelige sikkerhetsbarrierene er sårbare, og menneskelige feilhandlinger er en fremtredende farekilde, så har mennesker i større grad enn teknologien evne til å oppdage og

korrigere avvik (Rausand, 2009). Det er et positivt menneskesyn som mener det er *"menneskelig å feile, men mer menneskelig å gjøre rett"* (Grimwall, 2009:313) .

3.3 Oppsummering

Sikkerhetsteorier som har blitt omtalt i dette delkapittelet vil ha overførbare elementer til informasjonssikkerhet i bank. Faktorer som er fremhevet av sikkerhetsteoriene for å oppnå høy sikkerhet vil være komplementære til de kriterier satt av lover og standarder og som ble trukket frem i kapittel 3. Alle faktorene trukket frem i både kapittel 2 og 3 er oppsummert i tabell 2.

Lovkrav	Sikkerhetsteori
Fysisk og logisk sikring	**Fysisk og logisk sikring**
Rutiner og prosedyrer	**Rutiner og prosedyrer**
Avviks- og endringshåndtering	**Hendelseshåndtering**
Ansvarsfordeling	**Ansvarsfordeling og organisasjonsstruktur**
Intern og ekstern kontroll	**Intern og ekstern kontroll**
Risikostyring	**Risikostyring**
Katastrofeplan	**Krisehåndtering**
Oversikt over kritiske komponenter	**Oversikt over alle komponentene**
Kontroll av underleverandører	
	Sikkerhetskultur
	Prioritering av sikkerhet

Tabell 2: Oppsummering av nødvendige faktorer for å oppnå "god informasjonssikkerhet" fremhevet i lovkrav og sikkerhetsteori

Tabellen viser at det i stor grad er samsvar mellom det lovkrav og sikkerhetsteori trekker frem som nødvendig for å oppnå god informasjonssikkerhet. Lovkrav trekker spesielt frem *kontroll av underleverandør* og dette omtales ikke direkte i sikkerhetsstyringsteori, men kan linkes til *oversikt over alle komponenter* i systemet og *sikkerhetskultur* som teoriene mener omfatter underleverandører også. Lovkrav omfatter ikke "myke" elementer av informasjonssikkerhet, men dette fremheves i teori (da særlig i teorien om HRO) som avgjørende faktorer for å oppnå god sikkerhet.

3.4 Måling– et hjelpemiddel for å oppnå videre progresjon og økt modenhet

"What you can't measure, you can't manage, and what you can't manage, you can't improve" - ISM3 v1.2

Måling av informasjonssikkerhet vil være nyttig for å fastsette fokusområder der man over tid avdekker progresjon og modenhet innenfor arbeidet. Dette referer til andre del av problemstillingen i denne oppgaven. Ved å benytte måling av informasjonssikkerhet vil bankene dessuten synliggjøre etterlevelse og dermed forenkle sitt etterlevelse av regelverk arbeid (compliance). I tillegg er det lovpålagt for banker i Norge med måling av informasjonssikkerhet ettersom det i IKT-forskriften *§5 Sikkerhet* står***:*** *"Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare"*. Finanstilsynet (2013) poengterer at målinger må være mest mulig automatiserte ved at de er integrert i systemene. I Personopplysningsforskriften *§2-3 sikkerhetsledelse* står det også at valg og prioriteringer innen informasjonssikkerhet skal beskrives i en sikkerhetsstrategi. Bruken av informasjonssystemet skal jevnlig gjennomgås for å avdekke om sikkerhetsstrategien i banken gir tilfredsstillende informasjonssikkerhet som deretter skal gi grunnlag til eventuelle endringer av sikkerhetsmål og strategi.

Uten måling vil ikke banken kunne si noe om de tiltak som foreligger faktisk utgjør en forskjell over tid (Frost, 2000). Det finnes en rekke metoder for å måle informasjonssikkerhet, men det viktigste er å sette konkrete definisjoner av hva som skal måles og hvordan det skal måles (Wang et al., 1997). Dessuten må målene samsvare med den overordnede informasjonssikkerhetsstrategien i banken. E. Powell utdyper dette: *"A strategy without metrics is just a wish. And metrics that are not aligned with a strategy are a waste of time"* (Powell i Frost, 2000:29). Målinger av informasjonssikkerhet bør være en sirkulær prosess som må forankres i ledelsen, med god dialog mellom dem og både myndighetene og ansatte i virksomheten. Målet skal være at man hele tiden skaper læring, videre progresjon og forbedring i virksomheten (SSØ, 2006). En generell målingsprosess forklares i figur 2:

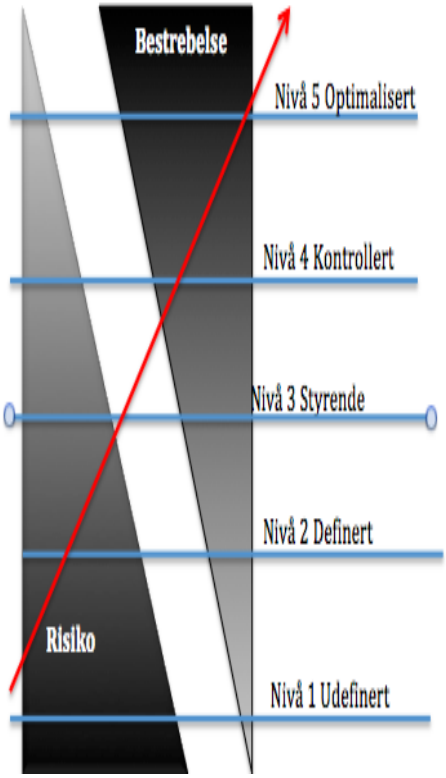
Steg 1: Målene og strategien er utgangspunktet for å definere hvilke resultater som skal måles og følges opp.
Steg 2: Styringsparametere beskriver direkte eller indirekte i hvilken grad virksomheten når sine mål.
Steg 3: Måling og vurdering av resultatene knyttet til de fastsatte styringsparametere indikerer om iverksatte tiltak er gode og hensiktsmessige, og om målene er nådd med effektiv ressursbruk.
Steg 4: Informasjon om resultater gir grunnlag for læring, slik at virksomheten løpende kan iverksette tilpasnings- og forbedringstiltak. En forutsetning for dette er at resultatene regelmessig rapporteres, formidles og drøftes.

Figur 2: Styringshjul for hvilke prosesser mål- og resultatstyring består av (SSØ, 2006:6).

Von Solms (2001) vektlegger at man i målinger av informasjonssikkerhet må benytte en multi-disiplinære tilnærmingen, som strategisk, organisatorisk, *beste praksis* osv. på lik linje med den tekniske dimensjonen. I tillegg til en måling av det tekniske systemet, muliggjør denne tilnærmingen en måling av individuelle og organisatoriske adferder. Det kan være måling av planlagt adferd og holdninger gitt prosedyrer og rutiner, og hva som faktisk blir gjort i virksomheten. Dessuten kan effektiviteten og kunnskapen i etterkant av holdningsskapende aktiviteter bli målt for å skape læring og forbedring av informasjonssikkerhetskunnskapen i virksomheten (Albrechtsen i Mjølsnes, 2012).

Von Solms og Thomson (2006) poengterer også at målinger vil gi en indikasjon på modenhet. Ved å benytte en metode som kalles *Information Security Competence Maturity Model* (ISMM) vil man avdekke om kriteriene satt av bankene for å nå ”god informasjonssikkerhet” har det fokuset det faktisk behøver (Thomson, 2006). En rekke modeller er etablert for å måle informasjonssikkerhet og de har forskjellige tilnærminger til modenhetsmålinger; COBIT som ble nevnt i forrige kapittel vektlegger etterlevelse (compliance), mens ISM3 konsentrerer seg om organisatorisk styring av informasjonssikkerhet. Det er den sistnevnte modellen som vil bli lagt vekt på i denne oppgaven ettersom det er en modell som muliggjør målinger av både tekniske og organisatoriske faktorer for informasjonssikkerhetsarbeid. Dessuten er den åpen for uformelle prosesser og ”myke faktorer”, som sikkerhetskultur. ISM3 ble presentert som en modenhetsmodell for informasjonssikkerhetsstyring i 2007. Den baserer seg på standardene (ISO-27001), rammeverkene (ITIL) og *beste praksis* som ble presentert i delkapittel 2.2 på side 6 og 7. Modellen deler modenhet inn i fem nivå som vist i figur 3 på neste side.

Generell sikkerhetsmodenhets modell	
Nivå 5: Optimalisert	Full implementering av policy og prosedyrer, jevne resultater og automatiserte sikkerhetskontroller.
Nivå 4: Kontrollert	Sikkerhetstesting, minske sårbarheter, informasjonsstyring og identifisere sikkerhets trusler.
Nivå 3: Styrende	Initiere sikkerhetsprogram, sikkerhetsarkitektur, strengere sikkerhetskontroller og organisatoriske policyer og prosedyrer.
Nivå 2: Definert	Oversikt av kritiske komponenter i organisasjonen, etablere et sikkerhetsteam, et viss nivå av tillit (confidence), sikkerhetspolicy og -prosedyrer.
Nivå 1: Udefinert	Fysisk sikkerhet, mangelfull tillit (confidence), basis IT og nettverksbeskyttelse.



Figur 3: Illustrasjoner av modenhetsnivåene i ISM3 basert på Lessing (2008) oversatt til norsk

Denne modellen kan benyttes av alle type virksomheter i forskjellige størrelser og er spesielt godt egnet for å måle organisatorisk og tekniske faktorer (Karokola, 2011). En svakhet er imidlertid at den ikke inkluderer det menneskelige aspektet.

3.5 MTO-perspektivet

Sikkerhetsarbeidet i den norske oljebransjen har i de siste tiårene vært påvirket av et MTO-perspektiv, dette vil si at man ser at *tekniske* systemer påvirkes av *organisatoriske* forhold og *menneskelige* prestasjoner. Når organisatoriske ulykker oppstår er det fordi forsvaret (barrierer) har blitt gjennomtrengt (Reason, 1997). Barrierer defineres som *"måter å separere sårbare mål fra en farlig energikilde"* (Rosness et al., 2004:16). Slike ulykker er sjeldne, men ofte katastrofale (Reason, 1997). På starten av 90-tallet fikk MTO-perspektivet fotfeste i flere bransjer fordi man så at ulykker generelt oppstod i samspillet mellom teknologien, mennesket og organisasjonen. Bento (2001) viser for eksempel til at 70 til 80 prosent av hendelser rapportert fra svensk luftfart til myndighetene relaterer seg til MTO-problemer.

MTO-området kan betraktes ut i fra et systemperspektiv; en helhetlig tilnærming til relasjoner mellom delsystemene mennesker, teknologi og organisatorisk istedenfor å kun ha fokus på delsystemene alene (Rollenhagen, 1997). Hovedhensikten med MTO er ikke å avdekke sårbarheter i et delsystem, men å fokusere på kombinasjonen av svakhetene i det tekniske-,

organisatoriske- og menneskelige systemet som en helhet. Det finnes en rekke etablerte bruksområder for MTO, og særlig blir den benyttes som granskningsmetodikk[14], men kan også benyttes i risikoanalyser (ibid.).

3.5.1 Risikoanalyser

Et helhetlig informasjonssikkerhetsarbeid vil være avhengig av risikostyring. Aven (2007) skriver at *"formålet med risikostyring er å sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap"* (s. 15). En del av risikostyring er risikoanalyser som avdekker risikoer knyttet til et analyse objekt, som kan for eksempel være en uønsket hendelse, et system eller en endring. Hensikten med risikoanalyser er å kartlegge mulige årsaker og konsekvenser knyttet til analyseobjektet og deretter danne grunnlag for at virksomheten kan ta de beste beslutningene som angår sikkerheten (Rausand, 2009). Risikoanalyser kan som vist i figur 4 deles inn i tre generelle trinn; 1) Årsaker/farekilder, 2) Kriseberedskap når en uønsket hendelse har oppstått og 3) Konsekvenser, som kan illustreres i et "bow-tie-diagram":

Figur 4: Risikoanalysene sine tre trinn som et "bow-tie-diagram", basert på Aven (2007)

Det finnes en rekke etablerte risikometoder og noen spesialiserer seg på årsaksanalyser, mens andre fokuserer på konsekvensene. Oppgaven vil fokusere på årsaksanalyser for hensikten med dem er å avdekker hva som gjør at brudd på informasjonssikkerhet oppstår. Avgrensningen er gjort med tanke på problemstillingen i oppgaven, fordi nødvendige faktorer for å oppnå "god informasjonssikkerhet" vil i hovedsak fungere som årsaksbarrierer for å unngå uønskede hendelser.

En populær risikometode for å avdekke årsaker er *feiltreanalyse*. Dette er et logisk diagram som avdekker årsakene til den uønskede hendelsen og finner sannsynligheten til denne

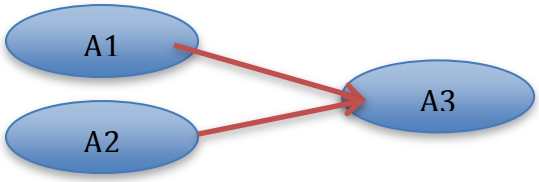
[14] Petroleumstilsynet benytter en bestemt MTO-metode for granskning av ulykker som er en presentasjon av hendelsesforløpet i en grafisk fremstilling i form av et flytskjema som er kombinert på en lineær tidslinje (Hovden 2004).

hendelsen. En svakhet med denne metoden er at den er best egnet for tekniske systemer og behandler ikke avhengige feil[15] (Rausand, 2009). Den vil derfor ikke vise hvordan elementer i virksomheten påvirker hverandre og den uønskede hendelsen. Et alternativ til feiltreanalyse er *bayesiansk nettverk* som i tillegg til tekniske og organisatoriske faktorer inkluderer det menneskelige. Ettersom et av forskningsspørsmålene i denne oppgaven ønsker å avdekke om et MTO-perspektiv er hensiktsmessig for informasjonssikkerhetsarbeidet i norske banker er det relevant å se nærmere på dette risikoanalyseverktøyet.

3.5.2 Bayesiansk nettverk i et MTO-perspektiv

Et bayesiansk nettverk (BN) er en grafisk nettverksmodell som visualiserer alle årsaksfaktorene til en uønsket hendelse, som er analyseobjektet. BN er bygget opp av ”noder” og ”linker”. Nodene er ovale og med en beskrivende tekst, mens linkene viser hvilke noder som er direkte påvirket av en annen (Rausand, 2009).

Den kvalitative analysen illustrerer hvordan nodene påvirker hverandre og kan dermed gi ideer til risikoreduserende tiltak. Erfaringer viser at den kvantitative analysen enkelt kan forstås av folk som ikke har detaljert kunnskap om hverken metoden eller analyseobjektet (Aven et al., 2008).



Den kvantitative analysen kan uttrykkes på følgende måte:

$$P\ (X) = \prod_{i=l} n\ \ P\ (Xi\ \mathrm{I}\ pa\ (Xi))$$

For node A3 (barnenode) med foreldrenodene A1 og A2 defineres en betinget sannsynlighetsfordeling. Variabler uten ”foreldrenoder” er gitt ubetinget sannsynlighetsdistribusjon. Modelleringen av et bayesiansk nettverk består både av statistiske data og ekspert kunnskap (Andersen & Häger, 2010). Historiske statistiske data vil kun si noe om fremtiden basert på fortiden, og kun med subjektive ekspertkunnskaper og

[15] **Avhengige feil (”Common cause failure”):** Feil på to eller flere (redundante) komponenter som har samme årsak, og som skjer innenfor et begrenset tidsintervall (SINTEF 2006).

scenarioanalyser vil man kunne kartlegge mulige fremtidige hendelser som ennå ikke har oppstått.

Tidligere forskning på risikoanalyseverktøy og deres praktiske benyttelse viser at *"bayesiansk nettverk skiller seg ut ved at en ved hjelp av metoden kan fokuserer på både M, T og O relaterte variabler, deres tilstand og innebygde avhengigheter"* (Hartvigsen, 2013:101). Et bayesiansk nettverk kan utføres på både små og store uønskede hendelser og viser avhengigheter som eksisterer i virksomheten og mellom de enkelte systemene.

En svakhet med bayesiansk nettverk er at det er svært ressurs- og tidkrevende, og variablene kan endres over tid. Det er derfor helt avgjørende at tilstandene i et bayesiansk nettverk oppdateres i henhold til ny kunnskap. Det gjør at risikostyringsverktøyet er dynamisk (Pearl & Russel, 2002). For informasjonssikkerhetsarbeidet i bank kan en slik risikometode være positiv ettersom trusselbilde og IT-løsninger er i konstant utvikling.

I neste kapittel beskrives metoden som er brukt for denne oppgaven og refleksjoner omkring valg som er tatt igjennom forskningsprosjektet.

4 Metode

4.1 Valg av metode

Kvalitativ metode gir kunnskap om noe særegent, mens kvantitativ metode er best for generalisering (Danemark, 1997). Fra tidligere forskning har kvantitativ metode vært den mest benyttede metoden for å forske på informasjonssikkerhet, og mye forskning er gjort på tvers av bransjer. En svakhet ved kvantitativ metode er at slike undersøkelser i hovedsak svarer på "Hva"-spørsmål, og vil gi en deskriptiv forståelse av fenomenet. For min problemstilling ville en slik forskningsmetode kun gi en overfladisk forståelse av informasjonssikkerhetsarbeidet i norske banker. Dessuten vil ikke en kvantitativ undersøkelse i like stor grad avdekke elementene eller vilkårene som trengs for å danne en "god informasjonssikkerhet" i bank samt forståelsen av informasjonssikkerhet blant de som arbeider med det i hverdagen. Tidligere forskning på området dreier seg hovedsakelig om en teknisk tilnærming til fenomenet, men hensikten med denne masteroppgaven er å avdekke om informasjonssikkerhet i større grad bør ses i et sosio-teknisk system. Et av formålene med oppgaven har vært å skape en forståelse av og forklare hva "god informasjonssikkerhet" innebærer, og deretter sette dette i relasjon med utfordringer forbundet med progresjon og modenhet. Derfor mener jeg det har vært hensiktsmessig å utføre en eksplorativ studie med kvalitativ metode bestående av semi-strukturelle intervjuer.

I forkant ble det utført en dyptgående dokumentanalyse av lovverk og standarder som omhandler krav til informasjonssikkerhet for norske banker. I tillegg fikk jeg fra enkelte banker tilgang til interne dokumenter som omfatter informasjonssikkerhet. Slik sett kan jeg argumentere for at metodetriangulering er benyttet ettersom både intervju og dokumentanalyse ble utført. Metodetriangulering vil si at man benytter to eller flere metoder i et studie av et enkelt problem. Styrken ved å benytte metodetriangulering er for å få flere perspektiver på samme fenomen og som et valideringsinstrument for å styrke funn (Ellefsen i Lorensen, 1998).

4.2 Forskningsdesign og -strategi

Forskningsdesignet i oppgaven har vært inspirert av Blaike (2009) som skriver at det er forskningsspørsmålene som danner utgangspunktet for videre valg av design. Både problemstillingen og forskningsspørsmålene har vært førende for valg av forskningsstrategi. Studiet har benyttet både induksjon og abduksjon for å trekke sine slutninger[16]. Induksjon

[16] **Slutning**: at man ut ifra noe drar konklusjoner fra noe annet (Danemark, 1997).

brukes for å teste hypoteser om hvilke faktorer som er nødvendig for å oppnå ”god informasjonssikkerhet ” (Thagaard, 2013). Hypotesene falsifiseres således ved at jeg benytter en komparativ analyse mellom lovverk, teoriene og svar fra intervjuer med banknæringen. Abduksjon vil ifølge Danemark (1997) bety at man tolker enkelte fenomener ut fra en sammenheng eller et mønster. Ettersom oppgaven kartlegger informasjonssikkerhetsarbeidet i flere norske banker, vil den kunne beskrives som sosialkonstruktivistisk, som vil si at den sosiale verden er tolket og opplevd fra innsiden. Ved å benytte en abduktiv forskningsstrategi vil jeg kunne trekke slutninger omkring mening, tolkning, motiver og intensjoner bak beslutninger som tas i forbindelse med informasjonssikkerhetsarbeidet i bankene. Kartleggingen og forklaringen av de nødvendige faktorene for å oppnå god informasjonssikkerhet i bank vil så legge grunnlaget for å forstå utfordringer forbundet med progresjon. Hypotesen og utfordringene forbundet med progresjon og økt modenhet vil bli satt i sammenheng og drøftes opp mot et MTO-perspektiv som en helhetlig tilnærming til informasjonssikkerhet.

Induksjon:

Hypotese: For å oppnå god informasjonssikkerhet må bankene ha følgende ……faktorer (fra lovverk og teori).

Bankene: Faktoren samsvarer/ det samsvarer ikke. Eventuelt legger og trekker fra faktorer som lovverk og teorien fremhever.

Abduksjon:

Sammenheng mellom hypotese og utfordringer.

Sammenheng mellom hypotese og MTO-perspektiv

4.3 Datainnsamling

4.3.1 Intervju

Kritikere av intervju som metode vil argumentere at mangel på standardisering av informasjonssituasjonen truer reliabiliteten, og man tar for stor høyde for subjektiviteten. Men i dette prosjektet vil det å benytte intervju for innhenting av empiri gi tilgang til observasjoner, innsikt, vurderinger og kunnskap som kvantitative spørreundersøkelser ikke fanger opp. Ifølge Weick (1989) vil kvaliteten på kvalitativ forskning avhenge mer av den analytiske strukturen i forskerens hode enn strukturen i selve datainnsamlingsprosessen (i Andersen, 2006). Problemstillingen og forskningsspørsmålene har naturlig nok lagt føringer for valg av teori og således for spørsmål i intervjuene.

Alle intervjuene ble utført ansikt-til-ansikt, noe som førte til mye reising over hele landet og til Sverige da informasjonssikkerheten i én av bankene blir styrt derifra. Det å velge en slik intervjusituasjon fremfor telefonintervju har hatt en positiv innvirkning på prosjektet fordi det muliggjør observasjon av kroppsspråk og signaler fra informanter. Informantene åpnet seg lett og enkelte gav meg muligheten til å observere sine systemer, policyer, rutiner og lignende som er sentrale deler av informasjonssikkerhetsarbeidet. Det ble utarbeidet en intervjuguide på bakgrunn av dokumentanalysen (vedlegg 1). Ettersom intervjuene var semi-strukturerte fungerte intervjuguiden til tider kun som en sjekkliste.

4.3.1.1 Utvalg

For å identifisere bankenes strategi og forståelse for informasjonssikkerhet, har det vært naturlig å intervjue sikkerhetsledere og IT-sjefer, samt enkelte ansatte som har ansvaret for informasjonssikkerheten i sin respektive bank. Utvelgelsen av informanter ble i stor grad gjort av ”snøballutvelgelsesmetoden”, der jeg tok kontakt med enkelte personer i hver bank som henviste meg videre til personer de trodde kunne komme med god kunnskap og innsikt omkring fenomenene (Grønmo, 2004). I tillegg sendte jeg ut generell henvendelse til ti banker. Jeg satte ikke et fast antall informanter på forhånd, men vurderte antallet i forhold til kvaliteten på dataen jeg fikk samlet inn. Når oppstod en ”metning”, som vil si at flere informanter ikke ville tilegne ny kunnskap og informasjon om fenomenet, var det ikke nødvendig å kontakte flere banker (Kvale et al., 2009) .

Det totalet antallet ble til slutt 14 informanter fordelt på syv norske banker, samt informanter fra Sparebank 1 Gruppen – avd. informasjonssikkerhet som ikke er en egen bank, men et team med spisskompetanse som jobber for 16 norske sparebanker. Utvalget inneholder tre banker fra Sparebank 1-alliansen, tre banker av liten, mellomstor og stor størrelse, samt en alliansebank med sentralstyring av informasjonssikkerhet for 75 små sparebanker på tvers av Norge. Dette gir et godt utgangspunkt fordi informantene kommer fra banker som varierer både i størrelse og lokasjon. Alle informanter har full anonymitet og dette ble de informert om både på forhånd og under intervjuet.

Følgende banker ble intervjuet:

- Sparebank 1 Gruppen – overordnet hovedansvar for informasjonssikkerheten for 16 sparebanker
- Sparebank 1 SR-bank - en del av Sparebank 1 gruppen
- Sparebanken Øst

- Eika Gruppen – overordnet hovedansvaret for informasjonssikkerheten for 75 sparebanker
- Sparebank 1 Oslo Akershus - en del av Sparebank 1 gruppen
- Nordea
- Skandiabanken
- Sparebanken Hedmark – en del av Sparebank 1 gruppen

Det ble foretatt et oppfølgingsintervju med én av bankene som bevisst benytter MTO i sitt informasjonssikkerhetsarbeid. Det ble etablert en egen intervjuguide til dette intervjuet (vedlegg 2) som kun omfattet valget og bruken av MTO-perspektivet i norske banker.

4.3.2 Dokumentanalyse

Dokumentanalyse kan være hjelpsomt både som et startpunkt for datainnsamling og som bakgrunn for utarbeidelse av intervjuguide. I tillegg kan det gi tilleggsopplysninger som er med på å verifisere og spesifisere data (Yin, 2014). I mitt prosjekt har det vært relevant å starte med en dokumentanalyse av interne dokumenter som omhandlet informasjonssikkerhetsarbeidet som jeg fikk tilgang til fra enkelte av bankene, samt standarder og lovkrav tilknyttet informasjonssikkerhet. Ettersom dette danner rammeverket for informasjonssikkerhetsarbeidet i norske banker fikk jeg en "førforståelse" for arbeidet som gjorde det lettere å lage relevante og gode spørsmål til intervjuene jeg foretok med banknæringen.

4.4 Validitet, generalitet, reliabilitet

En del utfordringer i all forskning, og da særlig ved bruk av kvalitative metoder, er relatert til validitet, generalitet og relabilitet. Derfor har det vært viktig å forstå disse elementene og hva de har å si for dette forskningsprosjektet.

Validitet: Ettersom det i mange forskningsprosjekter ikke er mulig å gjenta studiet på den eksakte samme måten, er validitet et stort metodisk problem. Årsaken til at man ikke kan gjenta studiet er fordi fenomenene forandrer seg og dessuten er forskningens resultater formet av forskerens subjektive fortolkninger og utvelgelse av empiri. Yin (2014) inndeler validitets utfordringer mellom konstruktiv, intern og ekstern.

- *Konstruktiv validitet*: Her er det elementært å skape troverdighet omkring datainnsamlingen og den empiri man finner.

- *Intern validitet*: Man ønsker å konstruere en årsakssammenheng i analysen der man mener at noen forhold fører til andre forhold (dette gjelder ikke eksplorative studier og er derfor irrelevant for dette prosjektet).
- *Ekstern validitet:* Denne typen peker på at man vil etablere funn som kan bli generalisert til andre lignende tilfeller.

En stor utfordring med oppgaven var tilknyttet ekstern validitet, nemlig det å skaffe nok informanter fra flest mulig banker slik at oppgavens validitet ble ivaretatt. Flere av bankene som fikk henvendelse fra meg ønsket ikke å delta med informasjon til dette prosjektet[17]. For å sikre ekstern validitet ville derfor en kvantitativ analyse i etterkant av kartleggingen av nødvendige faktorer med bruk av spørreskjema til alle norske banker vært den beste måten å sikre at funnene var gjeldene for alle banker i Norge.

Generalitet: Til tross for utfordringene knyttet til validitet har forskningsprosjektet etterstrebet det å oppnå det Grimen (2000) kaller *sosiologisk representativitet*. Det vil si at sentrale elementer og funn i oppgaven vil være mulig for andre banker i Norge å kjenne seg igjen i. Poenget vil da være å gjøre hendelsene forståelige, heller enn å kunne generalisere dem (Grimen, 2000). Her mener jeg at valget av de forskjellige bankene vil være med på å styrke prosjektets generalitet. Det vil være mulig for mange banker å kjenne seg igjen fordi empirien er hentet fra både store og små banker med forskjellige utgangspunkt, lokalitet og ressurser .

Reliabilitet: Det er avgjørende for forskningen at dataene er troverdige og at de lar seg bekrefte (Andersen, 2006). Igjen er dette ofte enklere i kvantitative metoder enn kvalitative metoder, men man kan allikevel gjøre visse grep for å øke troverdigheten. Et eksempel er at jeg har benyttet båndopptaker under alle intervjuene. Lydopptak er kun ment til denne oppgaven og vil slettes etter sensur er falt. Det er også benyttet intervjuguider (se vedlegg 1 og 2) som er brukt i semi-strukturerte intervjuer[18], slik at alle informanter har svart etter beste evne på fastsatte spørsmål. Formen på intervjuene har variert fra kun å være spørsmål og svar til at informanten har holdt foredrag om informasjonssikkerhetsarbeidet i sin bank, og da har intervjuguiden mer fungert som en sjekkliste slik at vi dekket alle spørsmål. Det har vært positiv at informantene selv bestemmer formen etter hva de føler seg komfortable med. Jeg mener dette har gjort at informantene har følt seg trygge og sikre nok til å svare veldig ærlig

[17] Se mer under 4.5 Utfordringer
[18] Intervjuguiden har fungert som en sjekkliste at alle spørsmål er besvart, men har variert i hvilken grad den er fulgt i samme rekkefølge.

på spørsmålene. Alle sitater som er brukt i oppgaven er også kontrollert ved at informantene har godkjent dem i ettertid.

4.5 Utfordringer

Opprinnelig skulle oppgaven være en komparativanalyse av modenheten og progresjonen til forskjellige norske banker basert på måling av informasjonssikkerhetsarbeidet. Det viste seg raskt, etter kun noen få intervjuer, at ingen av bankene foretok målinger på informasjonssikkerheten i sine respektive banker. Derfor endret problemstillingen seg til å forstå og avdekke utfordringene forbundet med modenhet og progresjonen av informasjonssikkerhet i norske banker.

En annen utfordring var å få nok informanter, ettersom mange banker ønsket kun å bidra dersom resultatet av oppgaven ble konfidensielt. Oppgavens problemstilling og spørsmål i intervjuguide omhandler ikke sensitiv eller konfidensiell informasjon. Derfor ble det besluttet å ikke samle inn data fra disse bankene, til tross for at spørsmålet om hvorfor disse bankene ønsker konfidensialitet vekker en ekstra nysgjerrighet hos meg.

5 Resultater

I dette kapitelet vil funn fra dokumentanalyse og intervjuene presenteres. Som nevnt i metodekapittelet, ble det intervjuet 14 personer som jobber som IT- og/eller sikkerhetssjefer fordelt på syv norske banker. Informantene sine svar vil settes i sammenheng med problemstillingen og de fire forskningsspørsmålene. De fire forskningsspørsmålene legger føringer for organiseringen av dette kapittelet ved at det begynner med å presentere kort det banknæringen mener er "god informasjonssikkerhet". Deretter vil faktorer de mener er nødvendige for å oppnå "god informasjonssikkerhet" presenteres. Så følger banknæringen sine forklaringer og forståelse for utfordringer med videre progresjon og økt modenhet av informasjonssikkerhetsarbeidet.

I flere avsnitt er direkte sitat fra intervjuene benyttet både for å understreke funnet og for å illustrere likhetene og forskjeller mellom bankene.

5.1 Hva er "god informasjonssikkerhet"?

Informantene sin definisjon av informasjonssikkerhet samsvarer med Datatilsynets elementer: konfidensialitet, integritet og tilgjengelighet, som også er grunnlaget for definisjonen brukt i denne oppgaven[19]. Gjennomgående uttrykker informantene at en klar definisjon er vanskelig, men at det hovedsakelig omhandler sikring av informasjon. "God informasjonssikkerhet" blir da som en informant sa at *"informasjonen kun er tilgjengelig for de som skal ha tilgang"* og det er en beskrivelse som mange mente var den viktigste delen av informasjonssikkerhet.

Over halvparten av informantene fremhever at den mest fremtredende assosiasjonen til informasjonssikkerhet er det tekniske, altså IT-sikkerhet, men noen trakk også frem den "myke" delen. En informant mener at informasjonssikkerhet er todelt, det ene er det systemtekniske og det andre er individene og de ansatte. En annen informant argumenterte også for at sporbarhet (traceability) var noe som i fremtiden ville bli inkludert i definisjonen av informasjonssikkerhet.

I det følgende presenteres faktorene som næringen selv trekker frem som nødvendige for å oppnå "god informasjonssikkerhet".

[19] Fra delkapittel 3.1: *"[God informasjonssikkerhet er] sikring av konfidensialitet, integritet og tilgjengelighet for den informasjonen som behandles av bankets system og systemet i seg selv"* (side 8).

5.2 Nødvendige faktorer i følge banknæringen

Fysisk og logisk sikring

Tekniske systemer er noe alle bankene som ble intervjuet prioriterer svært høyt og samtlige mener at banken sin har god teknisk sikkerhet. Teknisk sikring omfatter både fysisk og logisk sikring. Mange av informantene var også enige om at alle elementene av fysisk og logisk sikring fungerer som en avgjørende kjerne og er grunnmuren for informasjonssikkerhetsarbeidet i banken. En informant sa at;*" jeg mener at mange av disse tingene er egentlig bare basis ting som MÅ være på plass da som for eksempel sikring av de tekniske systemer, man kan ikke gjøre noe annet".*

Flere av IT-sjefene som ble intervjuet understreker at man kan gå mye mer i detalj når man snakker om de tekniske faktorer av informasjonssikkerhet i bank. Med tanke på oppgaven sin problemstilling og tidsramme vil en sammenfatning av teknisk sikkerhet til en overordnet faktor (*fysisk og logisk sikring*) være tilfredsstillende.

Kontinuitetsløsninger

Kontinuitetsløsninger bestående av reservesystemer og back-up var også prioritert høyt av informantene på grunn av at det sikrer tilgjengelighet av bankens systemer. For de mindre bankene vil tilgjengelighet av systemer ofte avhenge av underleverandører. En informant fortalte litt mer om hvorfor denne faktoren er viktig:

"Det med reserveløsninger. Vi er jo avhengig av noen samarbeidspartnere som sitter og håndterer selve kjernen innenfor banker. For oss så blir det Evry[20]. Vi er avhengig av at våre samarbeidspartnere har gode reserveløsninger så det er jo utrolig viktig".

Krav og kontroll til underleverandører

Alle bankene som ble intervjuet benytter seg av underleverandører som drifter deler av det tekniske systemet i banken. Dette genererer krav til underleverandører som skal sikre blant annet informasjonssikkerheten i disse tekniske systemene. Felles for de mindre bankene er at det meste av systemene og dermed informasjonssikkerhetsarbeidet er utkontraktert og banken sitter kun igjen med hovedansvaret for risikoene. Mye av tilgjengeligheten (*oppe-tid*) av systemene i disse bankene er derfor avhengig av kontroll av underleverandører og dette kan være utfordrende. En av informantene sa at *"alle har krav til leverandører…vi er kanskje litt dårlige der. Det blir alltid til at man mest kontrollerer dokumenter og sånn at jo vi har stilt krav"*. Det er en prøvelse å sikre "god informasjonssikkerhet" i leveransene fra underleverandører for alle bankene uansett størrelse på utkontrakteringen. For de mindre bankene som har utkontraktert de største delene av sine tekniske systemer vil sikring av

[20] **Evry** er et norsk informasjonsteknologiselskap (https://www.evry.no/bedrift/om-evry/)

avtalene være den største oppgaven for informasjonssikkerhetsarbeidet i banken. Noen informanter forteller at de har god oversikt over interne ansatte og oppfølging av rutiner, systemer og så videre, men å ha like god kontroll over underleverandører krever en del ressurser og da kan det skje svikt.

Sikkerhetskultur

Tradisjonelt er norske banker veldig sikkerhetsbevisste og flere av informantene poengterer at sikkerhetskulturen derfor allerede er godt etablert. En informant forteller at *"holdninger og adferd, der tror jeg banken generelt er ganske mye sterkere enn andre bransjer".* Men mye av den tradisjonelle gode sikkerhetskulturen i banker er forbundet med HMS ved at man har høy sikkerhetsbevissthet omkring sikring mot ran og brann. Informasjonssikkerhet kan by på nye og annerledes sikkerhetsproblemer. En av de mindre bankene uttrykker at*" bankene har vært veldig gode på fysisk sikring og det med ransikring. Så det er en sikkerhetskultur her, men kanskje ikke så mye på den logiske eller på informasjonssikkerhetssiden da"*. Dette mener informanten er mer gjeldene for små banker enn store, men intervjuene med de større bankene avdekker at de også ser på den teknologiske utviklingen som utfordrende for sikkerhetskulturen. Et eksempel som ble trukket frem i et av intervjuene med en av de største bankene var ansattes holdninger til bruk av data og mobiltelefoner. For eksempel dersom en bankansatt ikke er bevist på nedlasting av filer privat er det grunn til å tro at vedkommende ikke er bevist om dette på jobb heller, og dette kan derfor få negative konsekvenser for informasjonssikkerheten i banken.

Ettersom informasjonssikkerhet også innebærer informasjon som ikke er elektronisk så vil sikkerhetskultur være særlig viktig. Dette fordi sikring av informasjonssikkerheten på fysisk og muntlig informasjon må løses på andre måter enn tekniske sikkerhetstiltak. Et eksempel på brudd på informasjonssikkerhet kan da være når ansatte lar papirer med konfidensielt innhold ligge åpent på pulten. I en av bankene som ble intervjuet gjorde de stikkprøver på hvor utbredt dette er ved å gå runder etter arbeidstid for å se hva ansatte hadde liggende på pultene. Resultatet viste at flere ansatte lot konfidensielle dokumenter være lett tilgjengelig og synlig for andre medarbeidere på kontoret. Et klart brudd på informasjonssikkerheten.

Alle bankene som ble intervjuet driver jevnlig med informasjonssikkerhetsopplæring av ansatte, men dette utføres i hovedsak ved nyansettelse. Måten de fleste bankene øker ansattes bevissthet på informasjonssikkerhet er ved å benytte intranett. Fire av bankene fremhevet

også at de benytter NorSIS[21] sine årlige sikkerhetsmånedskurs i Oktober. Kun èn av bankene som ble intervjuet la særlig stor vekt på å tilpasse informasjonssikkerhetsopplæringen til de forskjellige enhetene i bankene: *"Vi kan ikke stå og ha en 'one-size-fits-all' presentasjon… Så du må situasjonsbetinge utdannelsen hele tiden. Du må finne former slik at det går 'inn i skallen' at dette her er viktig"*. Det gjør for eksempel at ansatte som jobber som forsikringsrådgiver vil få en litt annerledes innføring enn de som arbeider med lån. Således vil banken passe på at bevisstheten og opplæringen er mest mulig tilpasset hver enkelt ansatt sin hverdag.

Sikkerhetskultur er en faktor som prioriteres og arbeides med av alle bankene, men som samtlige uttrykker er vanskelig og at det til tider kan være utfordrende å sikre at det er en god sikkerhetskultur for informasjonssikkerhet i alle ledd i banken.

Intern og ekstern revisjon

Bankene informerer at de er veldig beviste på etterlevelse av lovkrav i sitt informasjonssikkerhetsarbeid, og flere henviste til IKT-forskriften og Personvernopplysningsloven. For å kvalitetssikre etterlevelse har alle bankene jevnlige intern og ekstern revisjoner. Denne faktoren har både høy prioritet og inntrykket er at samtlige mener det er godt nok. En informant forklarer at internkontroll *" skjer jo på flere måter, dels automatisk og dels via intern revisjon. Vi har et uttrykk at 'vi kan aldri erstatte interne kontroller med holdningen som her stoler vi på hverandre'".*

Bruk av *beste praksis*

Tre av bankene bruker også en egen versjon av ITIL som sikrer informasjonsprosessene, det vil si at de har utarbeidet *beste praksis* rammeverk som er tilpasset arbeidet i banken. En annen bank trekker frem at de bruker COBIT som en sjekkliste for å kvalitetssikre sitt informasjonssikkerhetsarbeid. Selv om ingen av bankene er sertifisert forteller fem av bankene at informasjonssikkerhetsarbeidet forsøker å gjenspeile standarder fra ISO-27000-serien. En bank forklarer også at de bruker ISO-27002 i sammenheng med ekstern revisjon;

> *"hvert år leier vi inn en ekstern revisor som foretar en sikkerhetsrevidering av arbeidet som settes opp mot den ISO-27002 standarden på sikkerhet. Der får vi enten grønt, oransje eller rødt lys på de her områdene og der skal vi aldri ha noen rød lys".*

Klassifisering

Noen få banker fremhevet klassifisering av systemer og informasjon som en viktig del av informasjonssikkerheten, ettersom man avgjør sikkerhetstiltaksnivå basert på sensitiviteten av

[21] **NorSIS** er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge.

informasjonen og systemene. Synonymt med klassifisering er lovkravet om *oversikt over komponenter*. For bankene betyr dette at de for eksempel må identifisere at komponent Z forsyner fem systemer så et brudd vil være kritisk for flere deler og muligens hele systemet, mens komponent Y operer alene og dermed er sårbarheten for systemet ved brudd av Y ikke like stor.

En av informantene forklarer klassifiseringen med *"hva er nødvendig og holdes hemmelig, hva må beskyttes fra innsyn, hva må beskyttes fra ødeleggelse, hva må beskyttes mot ….ja…i tilgjengelighetssammenheng"* og at svarene på disse spørsmålene vil således kreve forskjellige sikkerhetstiltak. Klassifisering vil kunne settes i sammenheng med to andre faktorer; *risikostyring* som kartlegger risikoene forbundet med informasjonssikkerhet, som således legges til grunn for *rutiner* for klassifisering av både informasjon og systemer.

Risikostyring

En annen avgjørende faktor som blir trukket frem er risikostyring. Alle bankene jobber risikobasert, men flere uttrykker at det kan være vanskelig. Én av de intervjuede bankene utmerker seg spesielt i sitt risikoarbeid. I denne banken er prioriteringen av risikostyring svært høy, og hele informasjonssikkerhetsarbeidet blir gjort på bakgrunn av dette. De bruker en modell fra Nasjonal sikkerhetsmyndighet (NSM) som illustrerer en generell risikostyring (Figur 5). Modellen viser hvordan risikostyring settes i sammenheng med en helhetlig sikkerhetstilnærming og at arbeidet er i kontinuerlig dynamisk progresjon. Når modellen benyttes i sammenheng med informasjonssikkerhet åpnes det opp for en *helhetlig sikkerhetstilnærming* som er en faktor som vil bli forklart i mer detalj avslutningsvis i dette delkapittelet.

Figur 5: Modellen for risikostyring som benyttes av én av bankene, basert på modell fra NSM.

Inntrykket og svarene fra intervjuene med de andre bankene (enn den nevnt over) er at deres informasjonssikkerhetsarbeid også følger en del eller alle trinnene fra modellen i figur 5. Forskjellen er at de andre bankene ikke på samme måte har en så systematisk tilnærming til

risiko- og informasjonssikkerhetsarbeidet. Alle bankene sier de utfører risikoanalyser jevnlig, minimum årlig, men også ved nye oppdateringer eller endringer i systemer. Hovedsakelig bruker norske banker en risikomatrise som sitt risikoverktøy. Denne faktoren mener derfor bankene er godt nok prioritert og implementert i sitt informasjonssikkerhetsarbeid.

Hendelses (avvik)- og endringshåndtering

Håndtering av uønskede hendelser eller endringer i systemene er også fremhevet som utfordringer i informasjonssikkerhetsarbeidet. Flere informanter forteller for eksempel at de tror mange hendelser fremdeles forblir urapportert.

- *"Det er litt i grenseland for hva oppleves som alvorlig nok hendelse. Det er kanskje litt lavt rapportert, en del type systemhendelser spesielt"*
- *" Der er en jobb å gjøre for å få alle bankene til å bli like flinke til å rapportere, men de har blitt flinkere og flinkere. I begynnelsen var det slik at 'nei det skjedde ikke noe i vår lille bank på landet', men det gjør det jo"*

Endringshåndtering var det kun én av bankene som trakk spesielt frem. De er svært opptatt av dette og har en veldig spesifikk rutine ved endringer som går igjennom flere instanser i banken. Rutinen tilsier at endringer kun er mulig dersom man kan vise at konsekvensene uten endring vil være så ødeleggende for det økonomiske, juridiske, sikkerhetsmessige og omdømme at endringene er helt nødvendige for banken. Det er usikkert om årsaken til at ikke flere bankene tar opp endringshåndtering som en faktor, men en mulig forklaring kan være at flertallet av bankene ikke ser det som et problem i forhold til informasjonssikkerhet.

Rutiner og prosedyrer

En organisatorisk faktor som alle informantene nevnte var rutiner som både indirekte og direkte omhandler informasjonssikkerhet. En informant sa følgende om hva som var viktig med rutiner: *"at man har tydelige, enkle og forståelige rutiner for den enkelte ansatte slik at det er lett å forholde seg til når man leser de så har man en sikkerhet i ryggmargen".* Rutiner og prosedyrer henger sammen med flere andre faktorer. De blir gjerne etablert og oppdatert på bakgrunn av risikoanalyser og etterlevelse blir sikret ved at bankene fortar intern og ekstern revisjon. Informantene er enige om at sikring og etterlevelse av rutiner ble godt nok gjennomført og høyt prioritert, men ettersom de vet at enkelte hendelser og avvik ikke blir rapportert kan det allikevel oppstå svikt.

Beredskapsplaner og øvelser

Alle bankene har interne sikkerhetsøvelser årlig, og selv om informasjonssikkerhet ikke alltid er hovedfokuset, vil det ofte være en indirekte del av øvelsene. Øvelser blir prioritet høyt og fører til at bankene oppdaterer beredskapsplaner jevnlig.

Ansvarsfordeling

Organiseringen av informasjonssikkerhetsarbeidet i bankene varierer veldig. For alliansebankene som ble intervjuet ligger hovedansvaret sentralt, et ansvar som i hovedsak omfatter de tekniske systemene og hendelseshåndteringen. Ansvarsrollene for informasjonssikkerhetsarbeidet i alle bankene som ble intervjuet var enten fordelt på IT-sjefer, sikkerhetssjefer eller egne fagavdelinger. For flertallet var arbeidet med informasjonssikkerhet lagt til en IT-avdeling. Ansvar for den daglige driften av informasjonssikkerhet og krisehåndtering må ikke forveksles med hovedansvaret for risikoene for informasjonssikkerhet. Hovedansvaret ligger på ledelsen og styret i bankene ettersom det er de som tar beslutninger og forankrer sikkerhetsstrategiene.

Ledelsesfokus

Gjennomgående i alle intervjuene får bankens ledelse ros for å ha høy fokus på informasjonssikkerhet og for å ta det på alvor. En av informantene mente det er en fremtredende faktor: ”*hva som er nødvendig for å oppnå god informasjonssikkerhet? Ja, det å ha god støtte fra ledelsen er jo veldig viktig”*. Alle informantene uttrykket at de fikk gjennomslag til alt de foreslo og dermed godt gehør fra ledelsen som har høy prioritet på informasjonssikkerhetsarbeid.

Ressurser

To av de mindre bankene trakk frem ressurser som en viktig faktor for deres informasjonssikkerhetsarbeid. I begrepet ressurs ligger både økonomi og menneskelig kompetanse. Det å ha nok ressurser innebærer både å ha økonomi til nødvendige tekniske løsninger og kompetente mennesker som kan jobbe med disse. For noen av bankene er det å ha tilstrekkelig menneskelig kompetanse innen informasjonssikkerhet vanskelig. De mindre bankene trakk dette frem som særlig faktor for å oppnå ”god informasjonssikkerhet”: ”*At [ansatte] hele tiden har tilstrekkelig kompetanse om sikkerhet når de gjør jobben sin. Så det å bevisstgjøre. At du tenker på det hele tiden”*. I disse mindre bankene er informasjonssikkerhet bare en del av ansvaret til IT-avdelingen og arbeidet med økt kompetanse og bevissthet for informasjonssikkerhet blant ansatte kan derfor bli nedprioritert. En av informantene fra en mindre bank fortalte at det var et ønske i fremtiden å få ressurser på området slik at de kunne ha interne som jobbet spesifikt med informasjonssikkerheten. På den annen side var økonomiske ressurser sett på som god nok, og ettersom ledelsen har høy fokus fikk informantene stor gjennomslag.

Helhetlig sikkerhetstilnærming

En av informantene poengterte at *"…til syvende og sist så er det den helhetlige sikkerhetstilnærmingen som er viktig"*. Informasjonssikkerhetsarbeidet i bankene er som nevnt organisert veldig forskjellig fra bank til bank, og dette gjør at det er stor forskjell på tilnærmingen til informasjonssikkerhet. For noen ligger arbeidet innbakt i IT, mens hos andre er ansvaret og styringen utarbeidet i en egen sikkerhetsavdelinger. Bare tre av bankene fremhevet helhetlig sikkerhetstilnærming som helt avgjørende faktor for å oppnå "god informasjonssikkerhet". En av informantene sa at *"målrettet og systematisk arbeid, det tar tid å få etablert det og vi har jobbet med det i mange år og vi er mye bedre nå enn det vi var for fem år siden og enda så har vi mye å gå på".* En informant fra en mindre bank fortalte at en helhetlig sikkerhetstilnærming byr på ekstra store utfordringer ettersom nesten alt av informasjonssikkerhetsarbeidet er utkontraktert til underleverandører.

5.2.1 Faktorer særegne for banknæringen

Mellom de norske bankene foregår det i dag et godt samarbeid på informasjonssikkerhetsområde. Dessuten benytter alle en del felles løsninger som for eksempel innlogging i nettbank med BankID[22]. I tillegg til dette blir samspillet med kundene også trukket fram som en særegen faktor. Dette blir fremhevet av alle informantene som en nødvendige og svært positive faktorer.

Bevissthet og risikoforståelse blant bankkunder

Mange bankkunder er naturlig nok like opptatt av sikkerhet som bankene ettersom det blant annet er deres informasjon som bankene disponerer. En av informantene mente at *"det er like viktig at våre kunder får kunnskap om sikkerhet som det er at ansatte får det"*. Enkelte banker jobber en del med å bevisstgjøre kundene på risikoer forbundet med informasjonssikkerhet, som for eksempel svindeleposter (phishing). Dette gjør de ved å legge ut tips og informasjons på sine nettsider.

Samarbeid mellom de norske bankene

Per i dag samarbeider bankene tett når det gjelder informasjonssikkerhet og trusselvurderinger, særlig for de mindre bankene er dette helt avgjørende for å holde seg oppdatert og tritt med risikoene. Samarbeidet omfatter også felles løsninger. *"I betalingsløsninger så er det kritisk at vi klarer å samarbeide godt og sånn som vi har det i*

[22] "BankID er en personlig og enkel elektronisk legitimasjon for sikker identifisering og signering på net" (BankID Norge)

dag er ingen konkurranse i sikkerhet". Alle informantene fra de mindre bankene, og særlig de uten allianse med andre banker, var spesielt opptatt av at dette samarbeidet er en vinn-vinn situasjon for alle banker og bankkunder i Norge.

5.2.2 Oppsummering

Tabell 3 oppsummerer alle faktorene som er trukket frem av informantene som nødvendig for å oppnå god informasjonssikkerhet.

Banknæringen		
Fysisk og logisk sikring	**Øvelser**	**Sikkerhetskultur**
Ledelsesfokus	**Beredskapsplaner**	**Endringshåndtering**
Rutiner	**Compliance**	**Ressurser**
Intern og ekstern kontroll	**Intern og ekstern kontroll**	**Klassifisering**
Bevissthet og risikoforståelse blant kunder	**Bruk av *beste praksis* og standarder: ITIL, COBIT og ISO-27001**	**Helhetlig og systematisk sikkerhetstilnærming**
Organiseringen i banken -ansvarsfordeling	**Risikostyring**	**Krav og kontroll til underleverandører**
Overvåking og logging	**Øvelser**	**Hendelseshåndtering**
Kontinuitetsløsninger	**Samarbeid mellom norske banker**	
Opplæring		

Tabell 3: illustrerer hva bankene uttrykker som nødvendige faktorer for å oppnå "god informasjonssikkerhet".

Fargekodingene er en illustrasjon av det bankene selv mener de er gode på og hvilke faktorer som er utfordrende.

Rød = Faktoren er ikke prioritert og arbeides ikke med av banken (**som tabell 2 viser er ikke dette gjeldene for bank, ettersom de inkluderer alle faktorene i varierende grad).**

Lilla = Faktoren har en viss prioritert, men bankene uttrykker at det er svakheter i arbeidet med denne faktoren.

Grønt = Faktoren har høy prioritert og blir jevnlig fulgt opp av banken.

Flertallet av faktorene prioriteres og anses som gode nok. Dette er faktorer som samsvarer både med lovkrav og sikkerhetsteori og omfatter både tekniske og organisatoriske faktorer.

Allikevel kommer det frem i intervjuene at noen områder er spesielt utfordrende og at svikt derfor skjer. Disse faktorene kan deles inn i "myke" faktorer:

- **Sikkerhetskultur**
- **Ressurser (menneskelig kompetanse)**

og faktorer som omhandler systematisk og helhetlig tilnærming til informasjonssikkerhetsarbeidet i bank:

- **Hendelses og endringshåndtering**
- **Klassifisering**
- **Krav og kontroll av underleverandører**
- **Helhetlig og systematisk tilnærming**

Dette er faktorer bankene mener er viktige, men som allikevel ikke fungerer optimalt i bankene. Når det gjelder de "myke" faktorene var det enkelte som fortalte for eksempel at det var vanskelig å finne ut om holdningsskapendearbeid hadde noen effekt. Dessuten var det noen få banker som uttrykket at de hvilte på den tradisjonelle sikkerhetskulturen som er veldig god, men dersom en uønsket hendelse skjer vil de måtte høyne fokuset på *informasjonssikkerhetskultur*. De "myke" faktorene varierte veldig fra bank til bank på lik linje med organiseringen av ansvar for informasjonssikkerhetsarbeidet. Dette er faktorer som er avhengig av at de med ansvar for informasjonssikkerhet setter fokus og prioriterer slikt arbeid. Når det gjelder faktorer som omhandler helhetlig tilnærming til informasjonssikkerhet så var dette faktorer som samtlige banker uansett størrelse og lokasjon så på som utfordrende. Med unntak av en bank som utmerket seg positivt. Noen av disse faktorene henger sammen med de "myke" ved at for eksempel hendelser er underrapportert og en årsaksforklaring kan være sikkerhetskulturen i banken og mangelfull menneskelige ressurser gjør at man ikke har nok kompetanse for å etablere en helhetlig og systematisk tilnærming, eller mulighet til å gå dypere inn (enn bare å sjekke dokumenter) for å kontrollere underleverandører.

5.3 Utfordringer for videre progresjon og økt modenhet

Et funn fra intervjuene var at ingen av bankene foretok helhetlige målinger av informasjonssikkerhet, som ville gi en indikasjon på progresjon og modenhet av hver bank. Antagelsen i forkant av prosjektet om at bankene foretok systematiske målinger på informasjonssikkerhet stammer fra IKT-forskriften *§ 5 Sikkerhet* der det står at: "*Kravene til IKT-sikkerhet skal så langt det er praktisk mulig være målbare*".

Mange av bankene fortalte at det gjøres målinger på tilgjengeligheten (*oppe-tid*) på tekniske systemer. Overvåking og statistikk over "innbruddsforsøk" som trojanertrusler og DDoS angrep[23] blir også trukket frem som målingsenheter. Alle bankene har også en form for

[23] **DDoS angrep**: lavintensitetsangrep fra eksterne aktører som i banksammenheng kan brukes som kamuflasje for svindel (IT-AVISEN 2013).

hendelseshåndteringssystem som behandler innrapporterte avvik. Dette kan gi et bilde på informasjonssikkerhetsarbeidet, ettersom man får statistikk over antall og omfang av uønskede hendelser relatert til informasjonssikkerhet. En svakhet med denne statistikken er at mange av bankene forteller at en del uønskede hendelser forblir urapportert. Ingen av bankene som ble intervjuet kunne fremvise en oversikt over informasjonssikkerhetsarbeidet eller vise til en kartlegging av informasjonssikkerhetens progresjon over en gitt periode.

5.3.1 Status på måling, progresjon og modenhet

For noen av bankene ble modenheten av informasjonssikkerheten sett i sammenheng med målsetninger og om de blir møtt. Målsetningene er satt i en strategi eller policy som er forankret på ledelsesnivået i banken. Informasjonssikkerhet er således en del av hovedmålene for det overordnede sikkerhetsnivået. Basert på svar fra intervjuene og funn i dokumentanalysen er det grunn til å tro at de fleste bankene arbeider likt når det gjelder målsetninger for informasjonssikkerhet.

En informant fortalte at banken vedkommende representerte jobber mot et helt konkret mål som omfatter informasjonssikkerhet og er målbart. Målsetningene er *"antall hendelser som resulterer i et direkte økonomisk tap for banken skal ligge på under 1 prosent av alle forsøk"*.

Risikostyring ble også trukket frem av et par banker som en måte å måle på. Det forklares med at man i en risikoanalyse kartlegger risikoene og tiltakene i banken og deretter kontrolleres det om dette samsvarer med de overordnende målene som er satt.

Intern og ekstern kontroll er noe alle bankene gjennomfører jevnlig. Revidering av rutiner, strategier, opplæring, øvelser og etterlevelse kan gi resultater der man får en indikasjon på hvilket modenhetsnivå informasjonssikkerhetsarbeidet i banken ligger. Enkelte banker bruker også ekstern revisjon med såkalt "trafikklys", rødt, gult og grønt, for å evaluere nivået på informasjonssikkerhetsarbeidet i banken.

Dette delkapittelet viser at dagens status på måling av informasjonssikkerhet i norske banker er variabel og at målinger på ingen måte blir gjort helhetlig og systematisk. Derfor kan ingen av informantene fortelle så mye om hverken progresjon eller modenhet av informasjonssikkerhetsarbeidet.

5.3.2 Utfordringene med videre progresjon og økt modenhet

Informantene poengterte at hovedutfordringen for måling og progresjon av informasjonssikkerhet er at det er vanskelig å måle noe konstant over tid. Mange av truslene mot informasjonssikkerhet er i konstant utvikling og det er derfor viktig at arbeidet er dynamisk og har en kontinuerlig progresjon, men å måle dette er ifølge bankene lettere sagt enn gjort. En informant brukte OL som metafor for å forklare utfordringene; *"selv om du er best i dag og vinner i dag så vinner du ikke neste OL hvis du ikke forbedrer deg på en rekke områder…og sånn er det hos oss også".*

En av informantene poengterte at dersom man skal måle informasjonssikkerheten i banken er det *"fordelaktig å gjøre det relativt enkelt…og så må du gjøre det på noe du faktisk kan forbedre"*. Mange var opptatt av at målinger ikke bare skal være tall og statistikk, ettersom det skaper mangelfull dynamikk og dermed kan målingen virke mot sin hensikt.

Videre i kapittelet som følger vil resultatene fra dette kapittelet drøftes opp mot lovkrav og sikkerhetsteori og dermed gi svar på problemstillingen og de fire forskningsspørsmålene i oppgaven.

6 Drøfting av funn

6.1 Hva er informasjonssikkerhet?

Alle bankene som ble intervjuet benytter elementene konfidensialitet, integritet og tilgjengelighet i sin offisielle definisjon av informasjonssikkerhet. Som nevnt i teorikapittelet er ”god informasjonssikkerhet” et begrep om en ønsket tilstand og blir et beskrivende mål som ligger til grunn for informasjonssikkerhetsarbeidet i enhver virksomhet. Dette delkapittelet vil svare på hva vil det si å ha ”god informasjonssikkerhet” i bank (forskningsspørsmål 1[24]).

Konfidensialitet

Flertallet av informantene svarte at informasjonssikkerhet er sikring av informasjon, slik at det kun er tilgjengelig for de som skal ha den. Dette vil være gjeldene både for interne ansatte og eksterne trusselaktører. I banksammenheng er det naturlig at konfidensialitet blir prioritert høyt, da kunder betror personlig og sensitiv informasjon til bankene. Av alle verstefallsscenarioer som kom frem fra intervjuene var tap av sensitiv informasjon noe samtlige trakk frem, da dette ikke like enkelt kan erstattes økonomisk. I tillegg vil det ha enormt ødeleggende konsekvenser for bankens omdømme.

Integritet

I tillegg til de tre veletablerte elementene mente en informant at også *sporbarhet* var et element som kom til å bli fremtredende for informasjonssikkerhet i fremtiden. Sporbarhet vil si at det går an å følge informasjonen og endringer til opprinnelsen eller endringsansvarlige. Ifølge definisjonen på integritet som er sikring av at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, vil sporbarhet kunne inngå under dette elementet.

Tilgjengelighet

En del av informantene fremhevet at kontinuitetsløsninger er nødvendig for å oppnå stabilitet og redundans. Dette er også et lovkrav. Ved å ha kontinuitetsløsninger som back-up og reservesystemer vil man sikre at informasjonen alltid er tilgjengelig ved behov både for ansatte og bankkundene. For sistnevnte vil kontinuerlig og ubegrenset tilgang til egne kontoer, forsikring og lån via selvbetjenteløsninger fortsette å ha høy betydning i fremtiden. Norske bankkunder forventer konstant tilgjengelighet til sin personlige informasjon som bankene besitter.

[24] Hva er ”god informasjonssikkerhet” i bank?

Helhetlige tiltak og sikkerhetskultur

En av informantene forklarte sin tilnærming til informasjonssikkerhet og mente at man ikke må ha en ensidig teknisk tilnærming. Informanten mener at menneskelige faktorene også bør tas til følge;

> *"Du har de tre begrepene, integritet, konfidensialitet og tilgjengelighet, som i utgangpunktet høres veldig teknisk ut. Det er ofte det man forbinder det med og så glemmer man ofte de andre faktorene rundt det med informasjonssikkerhet! Så informasjonssikkerhet for meg er; det systemtekniske og det er individene og ansatte".*

Den menneskelige faktoren inkluderes ved at banken oppnår en sikkerhetskultur der informasjonssikkerhet er en prioritert del av alle ansattes hverdag. Når sikkerhetskultur inkluderes i definisjonen for "god informasjonssikkerhet" vil det omfatte de uformelle og "myke" elementene; adferd, holdninger, kompetanse og bevissthet som er i banken. Det samsvarer med Albrechtsen (2012) som peker på at informasjonssikkerhetsstyring består både av formelle og uformelle elementer. Inkluderingen av både formelle og uformelle elementer i definisjonen gjør at man oppnår en helhetlig tilnærming til informasjonssikkerhet. Dette korrelerer derfor med Datatilsynet (2009) og Nasjonal Strategi for Informasjonssikkerhet (2012) som mener at "god informasjonssikkerhet" er planlagte, helhetlige og systematiske tiltak.

En grunnleggende del av informasjonssikkerhet er å inkludere all informasjonen i banken, dette innebærer også det som ikke er lagret elektronisk. I bank er dette særlig gjeldene og inkluderer fysiske dokumenter samt muntlig informasjon. Dessuten informasjon som finnes inne i hodene på de ansatte. Når man skal kartlegge faktorer som er nødvendige for å oppnå "god informasjonssikkerhet" er det derfor avgjørende å ikke ha et ensidig fokus på det teknologiske ettersom mye av informasjonen i bank ikke er elektronisk. Den informasjonen som ikke oppbevares elektronisk kan heller ikke beskyttes med tekniske systemer. Videre i neste delkapittel vil de nødvendige faktorene for å oppnå "god informasjonssikkerhet" i bank drøftes.

6.1.1 Oppsummerende delkonklusjon

Basert på drøftingene over om hvordan myndighetene, sikkerhetsteoriene og banknæringen definerer "god informasjonssikkerhet" vil en egnet definisjon være følgende:
"God informasjonssikkerhet" er **fysiske, tekniske og organisatoriske helhetlige tiltak som sikrer konfidensialitet, integritet og tilgjengelighet for den informasjonen som behandles i bankets system, samt en velfungerende informasjonssikkerhetskultur som**

gjennomsyrer hele virksomheten. Denne definisjonen vil omfatte all informasjon som finnes i bankets system, og det inkluderer både elektronisk, fysisk og muntlig informasjon.

6.2 Kartlegging av nødvendige faktorer

Informasjonssikkerhetsarbeid i bank er et kompleks sikkerhetsområde. Alle nødvendige faktorer trukket frem av lovverk, sikkerhetsteori og næringen for å oppnå "god informasjonssikkerhet" vil i dette delkapittelet bli drøftet opp mot hverandre (forskningsspørsmål 2[25]). I tillegg vil faktorene settes i sammenheng med definisjonen på "god informasjonssikkerhet".

Delkapittelet starter med tabell 4 som viser samsvar og mangel på samsvar mellom faktorene som trekkes fram av lovkrav, sikkerhetsteori og banknæringen. Fargekodingen korrelerer med tidligere tabeller:

Lilla = Faktoren har en viss prioritert, men bankene uttrykker at det er svakheter i arbeidet med denne faktoren.

Grønt = Faktoren har høy prioritert og blir jevnlig fulgt opp av banken.

Faktorer som samsvarer	Manglende samsvar	Faktorer som samsvarer, men som anses av bankene som utfordrende og sviktende
Fysisk og logisk sikring	**Prioritering av sikkerhet – Ledelsesfokus**	**Helhetlig sikkerhetstilnærming**
Rutiner og prosedyrer	**Samarbeid mellom norske banker**	**Klassifisering – oversikt over komponentene**
Overvåking og logging	**Bankkunder**	**Sikkerhetskultur**
Ansvarsfordeling	**Bruk av *beste praksis***	**Hendelses- og endringshåndtering**
Intern og ekstern kontroll		**Krav til underleverandører**
Risikostyring		
Krisehåndtering og beredskap		
Kontinuitetsløsninger		

Tabell 4: samsvar mellom nødvendige faktorer for å oppnå "god informasjonssikkerhet" fremhevet av lovverk, sikkerhetsteori og banknæringen.

[25] Hvilke faktorer trekker lovkrav og sikkerhetsteorier frem som nødvendige for å oppnå dette målet og hvordan samsvarer faktorer fra teorien og lovkrav med faktorer som bankene selv trekker frem som nødvendige for å nå "god informasjonssikkerhet"?

6.2.1 Faktorer som samsvarer

For å oppnå ”god informasjonssikkerhet” må man ha sikre tekniske løsninger. Både lovkrav, *beste praksis* og banknæringen fremhever dette som selve kjernen av informasjonssikkerhet. Alle faktorer som omfatter teknisk sikring samsvarer både med det lovkrav, sikkerhetsteori og banknæringer fremhever som nødvendig for å oppnå ”god informasjonssikkerhet”. Tekniske systemer gjør at banksystemene i dag og i fremtiden blir mer og mer komplekse. Perrow (2007) påpeker at tekniske informasjonssystemer isolert sett både er pålitelige og robuste, noe som stemmer overens med bankene sine informasjonssystemer som alle informanter opplever som svært gode.

Et eksempel på teknisk sikkerhet er når bankene foretar ***overvåking og logging*** som sikrer integriteten og konfidensialiteten av informasjonen bankene har fra trusler fra interne ansatte og eksterne trusselaktører. Når det gjelder eksterne trusselaktører må bankene kartlegge forsøk på penetrering i systemene og utviklingen av svindelmetoder. Dette er planlagte handlinger som tilfaller det såkalte ”security” feltet, som også kan omfatte ansattes handlinger, som interne misligheter. Men når det gjelder ansatte kan det også dreie seg om utilsiktede handlinger (*safety*) som fører til brudd på informasjonssikkerhet i banken. Det å skylde uønskede hendelser og ulykker på ansatte som brukere av systemet heller enn teknologien, har en lang tradisjon i analysering av årsakskilder til feil (Perrow, 2007). ”Operatør feil” var den mest vanlige tilskrivende årsak til storulykker som Three Mile Island, flyulykken på Tenerife i 1977 og kollapsen av Barings Bank. Men flere teoretikere (Perrow 1999, Reason 1990, Dekker 2006) spør seg heller: ”hva er det i systemet som gjør at det er enkelt for operatører eller brukere å gjøre feil?”. I følge Perrow sin teori ligger svaret i det som allerede har blitt diskutert med kompleksitet og tette koplinger i et teknisk system, mens Reason og Dekker mener hovedforklaringen er de organisatoriske vilkårene som ansatte arbeider under.

På lik linje med tekniske faktorer, er det også en del organisatoriske faktorer som samsvarer med det teoriene og bankene trekker frem som nødvendige. Både de organisatoriske og tekniske faktorene er beskrivende for den formelle strukturen av bankvirksomheten. Det er rammeverket og vilkårene som de ansatte i bankene jobber i. Som nevnt hevder en del sikkerhetsteorier at det er disse rammene som er den dyptgående årsaken til at uønskede hendelser og ulykker oppstår. En organisatorisk faktor som samsvarer er ***rutiner og prosedyrer*** som etablerers basert på antagelsen om at ansatte i bankene handler rasjonelt, men

ofte kan de organisatoriske rammene som for eksempel at flere rutiner utføres samtidig, gjøre at ansatte handler urasjonelt. Organisatoriske rammer kan gjøre at sikkerhet blir oversett av de ansatte i hverdagen ved at de tar snarveier utenom sikkerhetsrutiner. Slike "snarveier" kan skape rom for menneskelige feilhandlinger (Reason, 1997). Rutiner henger derfor i stor grad sammen med sikkerhetskulturen i banken. Sikkerhetskultur skal avverge feilhandlinger og ifølge HRO-teorien er bankene avhengige av at bankansattes holdning er at informasjonssikkerhet er viktig og at de handler deretter. Sikkerhetskultur vil bli diskutert i detalj i senere i delkapittel 6.2.3, side 49.

For å sikre kontinuitet og tilgjengelighet i driften er bankene nødt til å etablere ***beredskapsplaner*** og avholde jevnlige ***øvelser***. Øvelser og trening påpekes som viktig og avgjørende for en vellykket HRO. Alle bankene har øvelser årlig og informasjonssikkerhet er en indirekte del av dem alle, men det trenes sjelden kun på informasjonssikkerhets-scenarioer. Dette kan bankene bli flinkere på. Øvelser sikrer læring i organisasjonen og avdekker sårbarheter eller hull i planverk og rutiner som gjør at bankene hele tiden kan forbedre sitt informasjonssikkerhetsarbeid. Dette er faktorer som i sammenheng med ***ansvarsfordeling*** vil være svært viktig i en krisehåndteringssituasjon, fordi man skaper det Weick (1993) kaller en "virtual role". Det vil si at alle ansatte i banken er fullt klar over sitt ansvar og sin rolle i samspillet med andre ansatte, og det gjør at banken kan øke sannsynligheten for at håndteringen av en krisesituasjon vil bli utført på en forventet måte. Dessuten vil øvelser være med på å styrke ansatte sin risikoforståelse og bevissthet (*mindfullness*) for informasjonssikkerhet som de tar med seg i hverdagen. "*Jeg hører og jeg glemmer. Jeg ser og jeg husker. Jeg gjør og jeg forstår"* – Confucius **.** Bankansatte lærer og forstår bedre av praktisk læring enn fra å kun lese instruksjoner fra et dokument eller bli fortalt hvordan det bør gjøres.

6.2.2 Manglende samsvar

Banknæringen trekker frem noen organisatoriske forutsetninger for å oppnå "god informasjonssikkerhet" som ikke kan knyttes til definisjonen foreslått i delkapittel 6.1.1 og som heller ikke samsvarer med sikkerhetsstyringsteorier.

Ledelsesfokus trekkes frem som avgjørende for å få gjennomslag og forankring av informasjonssikkerhetsarbeidet. Dette genererer en annen faktor; ressurser, som gjør det mulig å investere i nødvendig teknisk utstyr og menneskelig kompetanse. De tre faktorene ledelsesfokus, ressurser og kompetanse samsvarer med det sikkerhetsteori skriver om

prioritering av sikkerhet. Men ifølge Normal Accident teorien er sikkerhet bare én av mange mål og prioriteringer i en organisasjon. Det gjør at virksomheter ikke legger like stor vekt på sikkerhet som det er behov for og at sikkerhet gjerne prioriteres først etter en uønsket hendelse har skjedd. Ofte er det ikke i lederne sin økonomiske interesse å prioritere sikkerhet (Perrow, 2007). I teorien om "High Reliability Organizations" (HRO) mener de at virksomheter bør prioritere sikkerhet høyest. Alle bankene forteller om stor støtte fra ledelsen, og alle informantene sier de får ressursene de trenger for å opprettholde et høyt sikkerhetsnivå. En forklaring på dette kan være at sikkerhet er avgjørende for bankenes forretningsdrift og for å sikre seg kundebeholdning. Funn viser derfor at samtlige av bankens ledere prioriterer sikkerhet høyt til tross for mange andre forretningsmål og denne faktoren samsvarer derfor ikke med Perrow. Det samsvarer heller ikke med HRO ettersom informasjonssikkerhet i bankene blir prioritert på lik linje med andre konkurrerende mål i bankene.

Hverken sikkerhetsteori eller lovverk omfatter bruk av *beste praksiser* og ettersom banknæringen i stor grad tar det i bruk vil dette være en faktor som ikke samsvarer mellom hva som fremheves som nødvendig. Bruk av *beste praksis* og standarder kan benyttes som verktøy og mal for organiseringen av informasjonssikkerhetsarbeidet. Det kan være god hjelp for norske banker i sitt arbeid. Finanstilsynet anbefaler bruk av ISO-27000-serien og flertallet av bankene som ble intervjuet uttrykker at de bruker standardene og "beste praksisene" som et rammeverk i sitt informasjonssikkerhetsarbeid.

De neste to faktorene som ikke samsvarer er fordi de er særegne for norske banker og blir derfor hverken nevnt i lovkrav eller sikkerhetsteori.
Den raske teknologiske utviklingen krever at bankene holder tritt med både ny teknologi og nye trusler og dette kan igjen føre til at forskjellene mellom de norske bankene øker. Lovkravene som omhandler informasjonssikkerhet er preget av å være funksjonsbaserte, slik at bankene selv står fritt til å utvikle og etablere løsninger selv. En svakhet ved dette er at det kan skape store forskjeller mellom de norske bankene der de små bankene henger etter. Det er derfor avgjørende for norske banker å ha et godt samarbeid. Per i dag er det et tett og positivt ***samarbeid mellom bankene*** innen informasjonssikkerhet, og dette er særlig viktig for de små bankene er samarbeidet nødvendig slik at de opprettholder en videre progresjon innenfor fagfeltet. Perrow (2007) viser til en casestudie av energiselskaper i USA der samarbeid innen næringen er positivt for å heve sikkerheten i hele den kritiske infrastrukturen. En av de største forskjellene mellom energiselskaper og norske banker er at energiselskapene i USA er

naturlige monopoler[26] og det er derfor ingen konkurranse, mens i norsk banknæring kan det å ha "god informasjonssikkerhet" bli et konkurransefortrinn. En slik utvikling kan være med på å ødelegge det gode samarbeidet som finnes per i dag. Både de norske bankene og myndighetene bør etterstrebe å bevare samarbeidet i fremtiden for å øke motstandsdyktigheten både i næringen og samfunnet generelt .

Som nevnt i innledningen har bankene sitt forretningsmønster forandret seg drastisk i løpet av de siste tjue årene. Brett King (2013) forklarer det godt i en setning: ***"Banking is no longer somewhere you go, it´s something you do".*** For bankene kan ***kunder*** sin bevissthet og risikoforståelse for informasjonssikkerhet både være en utfordring og et positivt bidrag. På den ene siden vil kundene sette større krav og ha høye forventninger til bankenes håndtering av informasjonssikkerheten. På den andre siden vil dialog med kundene og banken gi en utveksling av kunnskap og erfaring som begge parter kan utnytte for å skape bedre informasjonssikkerhet. Flere av bankene som ble intervjuet (samt andre norske banker) har etablert egne e-postadresser der kunder kan sende inn mistanke om svindel, videresende phishing-mailer og så videre. Dette gjør at banken tidlig kan avdekke svindelforsøk og dermed håndtere dem raskere. Dessuten kan bankene på lik linje med intern opplæring lære bort bevissthet og forståelse for informasjonssikkerhet til kunder. Denne interaksjonen mellom banker og kunder er en unik læringssløyfe. Få sikkerhetsteorier og annen forskningslitteratur skriver om slike læringssløyfer mellom organisasjoner og eksterne. Så det kunne vært spennende for fremtidige forskningsprosjekter å kartlegge slike unike læringssløyfer nærmere.

6.2.3 Faktorer som samsvarer, men som anses av bankene som utfordrende og sviktende

Bruken av ***underleverandørene*** gjør at bankens informasjonssystemer øker i kompleksitet. Flertallet av norske bankene benytter dessuten samme underleverandører, som for eksempel Evry. En feil hos dem kan forplante seg i hele den norske bank- og finansnæringen. Per i dag er feil hos Evry den største trusselen for brudd på tilgjengeligheten av informasjonssikkerhet fordi det vil kunne lamme hele den norske banksektoren og kan få negative følger for hele samfunnet. Dersom bankene heller fordeler ansvaret mellom flere underleverandører vil ikke den kritiske samfunnsfunksjonen være like sårbar og avhengig. Perrow (2007) poengterer at i den ideelle industrielle strukturen vil det være en rekke produsenter som bruker flere og forskjellige leverandører, slik at dersom én av dem feiler finnes det alternativer. Dette vil

[26] **Naturlig monopol**: beskriver et marked hvor det er samfunnsøkonomisk mest effektivt med bare en markedsaktør (Rosvold i Store norske leksikon 2010).

redusere bankenes avhengighet og gjøre samfunnet mer motstandsdyktig. DNB som er Norges største bank gikk nylig vekk fra en del kontrakter med Evry[27]. Dette setter press på underleverandøren til å levere mer stabile og sikre løsninger. Derimot kan det for små banker være vanskelig å sette slikt press på en så stor ekstern aktør. Det kan derfor være hensiktsmessig at norske myndighetene blir mer involvert i bruken av underleverandører i bank- og finanssektoren. For å evaluere mulige negative konsekvenser bruken av én eller få underleverandører kan føre til for den totale samfunnssikkerheten.

Det viktigste for bankene ifølge NAT er som nevnt å ha full oversikt over kompleksiteten i systemene og hvordan interaksjonen mellom hver komponent er koplet. Etter den nevnte EDB hendelsen i påsken 2011 innførte Finanstilsynet strengere krav som førte til et større ansvar på bankene for å ha bedre oversikt og kontroll av de systemer og komponenter som administreres av sine underleverandører (Finanstilsynet, 2011). Alle bankene som ble intervjuet foretar kontroller av underleverandører, men påpekte at det er en stor utfordring. Særlig ble det pekt på at dette krever mye ressurser og at det er mye enklere å kontrollere interne systemer og etterfølgelse av rutiner enn eksternt. Kontroll av underleverandører for bankene som ble intervjuet består i hovedsak av å kontrollere avtaler, dokumenter og systemer. Det kan være mangelfullt å kun kontrollere de formelle elementene av underleverandøren fordi bankene vil derfor ikke klare å sikre at rutiner *faktisk blir fulgt*. For å oppnå definisjonen på "god informasjonssikkerhet" i bank bør man ha en sikkerhetskultur som gjennomsyrer hele virksomheten og dette inkluderer utkontraktering (se 6.1.1, s. 41 og 42). Utkontraktering er en forlengelse av virksomheten og ikke et separat system eller enhet. For å inkludere dette i banken må man sikre at kompetansen og opplæringen på informasjonssikkerhet som gjøres innad i banken også utføres hos underleverandørene. Det var ingen av bankene som fortalte at de førte noe kontroll av sikkerhetskulturen til underleverandører.

En annen faktor som bankene også mener er viktig, men som mange bare nylig har begynt å prioritere høyere er ***Klassifisering.*** Det vil si at bankene kartlegger sårbarheten og sensitiviteten av både systemer og informasjon for å fastsette beskyttelsesnivået og sikre konfidensialiteten. Klassifisering vil også være med på å avdekke og etablere oversikt over alle komponenter og koplinger i systemene (IT-arkitekturen). Dersom bankene er suksessfulle i kartleggingen vil man kunne forenkle kompleksiteten og avverge for tette koplinger, og dermed vil man ifølge Perrow (1984) minke sårbarheter ved at man hindrer at feil får konsekvenser for hele systemet. Dette vil være like betydningsfullt for intern informasjon og

[27] VG (2013) *Evry mister kontrakt med DNB etter nettbanktrøbbel.*

systemer som det som blir behandlet av underleverandører. Enkelte systemer og informasjon har ulik betydning for bankene og derfor anbefaler Finanstilsynet (2013) at dette må sikres på ulike måter og nivåer gjennom klassifisering. Flere av bankene uttrykker at klassifisering er noe de kan bli flinkere på, særlig når det gjelder fysiske dokumenter som skal sikres mot innsyn. Siden klassifisering tilsvarer en oversikt over alle komponentene tilknyttet informasjonssikkerhet i bank kan en forklaring på at bankene mener dette er utfordrende være at de fleste bankene mangler en helhetlig og systematisk tilnærming til informasjonssikkerhetsarbeidet.

Når et brudd på informasjonssikkerheten oppstår i norske banker blir det registrert i et ***hendelseshåndteringssystem***. Flere banker trekker frem at en vellykket hendelseshåndtering er vanskelig fordi de er klar over at mange hendelser forblir urapportert og ofte kan det være utfordrende å håndtere hendelsene på en hensiktsmessig måte. Dessuten blir det ikke rapportert om nesten-ulykker som kan gi indikasjoner på sårbarheter i systemet. I hendelseshåndteringssystemer bør både nesten-ulykker, små og store hendelser rapporteres slik at man kan lære og rette opp sårbarheter som eksisterer i banken. En organisasjon med god sikkerhetskultur skal aktivt lete etter feil for å skape læring (Reason, 1997). Slik skaper man mer redundans i organisasjonen og blir mer motstandsdyktig mot brudd på informasjonssikkerheten. De fleste bankene etterspør ikke hendelser og avvik aktivt, og feil som oppstår blir hovedsakelig reparert ”lokalt”. Dette tilsvarer er såkalt byråkratisk type organisasjonskultur til motsetning fra den optimale generative kulturen der feil aktivt søkes og feil som oppstår fører til endringer i hele organiseringen eller organisasjonen (Westrum i Rosness, 2004).

I tillegg til hendelseshåndteringssystemer har alle bankene ***endringshåndteringssystemer*** som er avgjørende for sikring av nøyaktighet, stabilitet og tilgjengelighet av systemene. Dette omfatter både manuelle endringer som blir gjort i de tekniske systemene, som vedlikehold og omgjøring av forventet utfall (som sletting av godkjent transaksjon), samt introdusering av endringer i tekniske systemer. Bankene er også pålagt å ha kontroll over og delta i endringshåndteringen til underleverandører (Finanstilsynet, 2011). Det var kun én av bankene som trakk dette spesielt frem ettersom de operer med svært strenge rutiner på endringer. Flere av bankene som ble intervjuet brukte en tilpasset utgave av ITIL, *beste praksis* for endringshåndtering. Ettersom så få banker trakk endringshåndtering frem som en nødvendig faktor er det grunn til å tolke det som at de fleste aner denne faktoren som god nok i sin bank. Til tross for dette har endringer vært en direkte årsak på flere uønskede hendelser i bank- og

finanssektoren, som for eksempel fra introduksjonen med Den Danske Bank (DDB) og Goldman Sachs introdusering av ny Software som fører til at opsjonshandel løper løpsk[28]. For å kunne sikre seg mot at endringer resulterer i systemsvikt eller informasjon på avveie må bankene kartlegge hvilke konsekvenser endringene kan få og det kan også knyttes med to andre nødvendige faktor for å oppnå "god informasjonssikkerhet"; risikostyring og klassifisering. Dersom bankene har god klassifisering og dermed oversikt over alle systemer og informasjonen vil det forenkle endringshåndteringsarbeidet fordi man lettere skal kunne avdekke hvilke følger en endring får for hele systemet.

Både klassifisering, hendelses- og endringshåndtering er organisatoriske barrierer som har som funksjon å sikre banken mot sårbarheter, svikt og mulige menneskelige feilhandlinger.

For å oppnå "god informasjonssikkerhet" må bankene også inkludere de uformelle elementene i banken, det Albrechtsen (2012) beskriver som måten *ting faktisk blir gjennomført* i virksomheten. Det som kjennetegner lovkravene og banknæringen sin tilnærming til informasjonssikkerhet er at de har høy fokus på og prioritering av det formelle i virksomheten. Dersom de uformelle elementene nedprioriteres kan norske banker oppleve brudd på informasjonssikkerheten til tross for godt etablerte robuste tekniske systemer, jevnlige øvelser og gode skriftlige rutiner. For å sikre seg mot uønskede hendelser må bankene derfor etterstrebe en vellykket ***sikkerhetskultur.*** Elementer som inngår i en sikkerhetskultur er blant annet holdninger, adferd, risikoforståelse og –bevissthet, opplæring og kompetanse (Reason 1997, La Porte 1996, Weick 2001). Kun de små bankene som ble intervjuet påpekte kompetanse som en betydelig del av "god informasjonssikkerhet". En mulig forklaring på at ikke alle bankene påpekte dette kan være at de andre anser kompetanse på informasjonssikkerhet i sin bank som god nok og dermed ikke tenkt over viktigheten av å ha høy spisskompetanse, samt generell kompetanse blant alle bankansatte.

Rutiner og prosedyrer som er etablert for å avverge brudd på informasjonssikkerhet og som prioriteres høyt av bankene er helt avhengig av å ha en god sikkerhetskultur. En av informantene beskrev dette godt ved å si: *"Det som er viktig er jo atmosfæren, du kan jo ha så mye du orker av rutiner, men du er avhengig av at folk faktisk følger de, at de forstår at de er viktige"*. Sikkerhetskultur krever opplæring slik at bankansatte får en forståelse for truslene og dermed en holdning om at sikkerhet bør ha en høy prioritet. Bankene selv vet hvor avgjørende dette er og en av informantene forklarte at informasjonssikkerhet skal være like

[28] Bloomberg (2013). *Goldman Sachs Said to Send Stock-Option Orders by Mistake.*

naturlig og vanlig som å smøre en brødskive. Dersom man oppnår dette vil man få det Weick (2001) kaller økt bevissthet (*mindfullness*), som betyr at ansatte konstant er bevisst på at noe uforventet kan skje og at små feil blir håndtert raskt før de får utvikle seg. Feil og uønskede hendelser bør skape læringssløyfer og kunnskapsdeling med medarbeidere (og andre banker) for å øke kompetansen og bevisstheten rundt sårbarhetene innen informasjonssikkerhet. Bankene som ble intervjuet benytter hovedsakelig intranettet som en plattform for deling av slik læring blant sine ansatte. En svakhet med intranettet er at ansatte selv må aktivt inn for å innhente informasjon og kunnskap. Så jevnlig oppdatert informasjon som underbygger bevissthet og forståelse for informasjonssikkerhet i de fleste norske banker vil i stor grad være opp til den enkelte ansatt. Her kan bankene bli flinkere til å skape en bevissthet (*mindfullness*) ved at man har jevnlig opplæring, øvelser og kunnskapsdeling mellom alle ansatte, ledere og andre banker.

Alle bankene som ble intervjuet har fokus på sikkerhetskultur og mente at banker tradisjonelt sett har en god sikkerhetskultur. Samtlige jobber bevisst med å utvikle "mindfullness" blant sine ansatte slik at de ansatte tenker sikkerhet i alle ledd. Allikevel sa mange banker at en stor utfordring er at den teknologiske utviklingen går raskt. Dette berører alle bankansattes hverdag. Skille mellom privat- og arbeidsadferd viskes ut ettersom bankansatte gjerne bruker mobil og datamaskiner likt både privat og på jobb. Dersom en bankansatt ikke ser på det som alvorlig å laste ned programvarer privat kan dette gjøre at vedkommende tar dette med seg på arbeidsplassen, og uvisst (eller bevisst) tar i bruk infisert programvare på jobb. En av IT-sjefene sa litt ironisk at *"vi kan sikre oss mot veldig mye, men den adferden din den må du håndtere selv og vi får jo ikke installert noe anti-adferdsverktøy på [ansatte]….i utgangspunktet så er det kanskje den biten vi har en del å gå på da som jeg opplever rett og slett"*. Til tross for ironi illustrerer sitatet godt vanskeligheten bankene har med å sikre seg mot menneskelige feil som ikke kan løses på samme måte som de sikrer de tekniske systemene.

I banknæringen har det oppstått en rekke uønskede hendelser i forbindelse med brudd på informasjonssikkerhet som følge av menneskelige feil. Et eksempel som kan trekkes frem oppstod i én av bankene som ble intervjuet, der en bankansatt sendte ut en excel-fil til lokale bedriftsledere med sensitiv informasjon om rundt 11.000 kunder som lå gjemt under andre arkfaner. Informanten fra banken forklarte hendelsen på følgende måte:

"Tidlig i fjor fikk [vi] et brudd på håndtering av personopplysninger. Det var vanskelig for denne personen å oppdage at man gjør noe galt. Det var ikke sånn at han eller

hun sender ut noe som han eller hun burde vite er over streken. Da måtte vi se på rutinene rundt".

For å skape en organisasjon med høy redundans mener HRO-teorien at arbeidsoppgavene bør være overlappende og at man er observante ovenfor hverandres arbeid. Dersom en ansatt gjør en feil skal det bli oppdaget av andre før det kan utvikle seg til å bli en uønsket hendelse eller i verstefall en ulykke. For å muliggjøre dette må banken ha en høy toleranse for åpenhet og direkte kommunikasjon mellom ansatte slik at beskjeder er tydelige. I eksempelet over kunne en kvalitetssjekk fra en annenpart skapt den overlappen som HRO mener er nødvendig for å avverge feil som dette. Den uønskede hendelsen er et godt eksempel på en menneskelig feil som ved første øyekast kan virke som det Reason (1997) kaller en forsømmelse, men som viste seg å være en intensjonell feiltakelse ettersom ingen rutiner hindret den menneskelige feilhandlingen fra å skje.

Banken som opplevde sikkerhetsbruddet oppnådde elementer av det Dekker (2006) og Reason (1997) omtaler i sine teorier som en god sikkerhetskultur. Som følge av at banken gransket rutinene og arbeidsvilkårene istedenfor å jakte på en syndebukk. Ved at banken i dette tilfelle valgte å kartlegge de premissene som de ansatte arbeider under skaper de en rettferdig, åpen og lærende sikkerhetskultur. Dessuten vil feilen føre til endringer i rutiner og dermed organiseringen som gjenspeiles i det Westrum (1993) karakteriserer som generativ organisasjonskultur. Når banken er suksessfull i å etablere en slik kultur vil man unngå at ansatte er redd for å rapportere om egne menneskelig feil. Dersom ansatte oppfatter at banken forsøker å lære av feil og endrer på rutiner istedenfor å jakte på syndebukk vil det kunne skape en positiv sikkerhetskultur.

Bankene som ble intervjuet har som sagt fokus på sikkerhetskultur, men en del lener seg på tradisjonell sikkerhetstilnærming, som hovedsakelig omfatter uønskede hendelser som ran og brann. Informasjonssikkerhet derimot byr på nye type trusler og risikoer i ansattes arbeid. Det er derfor nødvendig at lovkravene og banknæringen også prioriterer de uformelle elementene og jobber mer med å skape en positiv informasjonssikkerhetskultur for å skape større samsvar med sikkerhetsteoriene som peker på at menneskelige faktorer er helt avgjørende for å avverge uønskede hendelser.

Alle faktorene som er fremhevet i tabell 4 på side 42 tilsvarer en ***helhetlig sikkerhetstilnærming***. Bankene uttrykker enighet om at helhetlig tilnærming er nødvendig, men forskjeller i organiseringen og størrelse kan gjøre det vanskelig for bankene å ha full oversikt. Særlig dersom store deler av informasjonssikkerhetsarbeidet er utkontraktert. På

grunn av at bankene går mot tettere koplinger og mer komplekse informasjonssikkerhetssystemer vil brudd på informasjonssikkerhet være uunngåelig (Perrow, 1984). Dette gjelder spesielt dersom lovkravene og banknæringens hovedfokus fortsetter å være på de tekniske og organisatoriske sikkerhetsløsninger. På den andre siden vil HRO-teorien mene at ulykker kan unngås ved at man etablerer god sikkerhetskultur (Reason 1997, Weick 1993). Dette må gjøres i tillegg til å ha full oversikt over kompleksiteten og koplingene både mellom de tekniske systemene og interaksjonen med menneskene. Det er kun med en helhetlig tilnærming til sitt informasjonssikkerhetsarbeidet at bankene vil klare å inkludere og prioritere alle faktorene som er kartlagt over som nødvendig for å oppnå "god informasjonssikkerhet".

6.2.4 Oppsummerende delkonklusjon

Alle tekniske faktorer samsvarer både med det lovkrav, sikkerhetsteorier og banknæringen mener er nødvendig for å oppnå "god informasjonssikkerhet". De fleste organisatoriske faktorer samsvarer også, som rutiner og ansvarsfordeling. Men med unntak av tre følgende organisatoriske faktorer:

- *klassifisering*
- *hendelses- og endringshåndtering*
- *krav til underleverandører*

Dette er faktorer som bankene også anerkjenner som viktige, men der det allikevel ikke er like høy prioritering. Dessuten uttrykker også banken at faktorene *sikkerhetskultur* og *helhetlig sikkerhetstilnærming* kan være vanskelig i sitt informasjonssikkerhetsarbeid. Utfordringene med disse fem faktorene er ofte den direkte årsaken til at svikt og dermed brudd på informasjonssikkerhet oppstår.

6.3 Utfordringer for progresjon og økt modenhet

Svarene fra de foregående delkapitlene på forskningsspørsmål 1 og 2 vil danne et grunnlag for å forklare utfordringene bankene har for å oppnå videre progresjon og økt modenhet av informasjonssikkerhet (forskningsspørsmål 3[29]) som vil bli drøftet i dette delkapittelet.

Hovedfunnet fra intervjuene med banknæringen var at ingen av bankene har en systematisk måling av informasjonssikkerhetsarbeidet og sammenligning mellom bankene og deres

[29] Hvilke utfordringer har bankene for å oppnå videre progresjon og økt modenhet av informasjonssikkerhet?

progresjon og modenhet blir derfor umulig. Modenhet av informasjonssikkerhet vil si bankens utviklingen fra kun å tilfredsstille lovbaserte krav med et minimum av sikkerhetstiltak til å arbeide helhetlig og proaktivt i tillegg til å etterleve lovkrav. Uten kartlegging av progresjon og modenhet vil man kun ha en informant beskriver som *"en subjektiv vurdering av hvordan man står da…i forhold til risikohåndtering og kompetanse på medarbeidere".* Av den grunn vil oppgaven skape en forståelse for utfordringene de norske bankene har med progresjon og modenhet av informasjonssikkerhet.

Ifølge teorier om sikkerhetsstyring ville prioritering av sikkerhet og ledelsesfokus kunne gi en forklaring på utfordringene forbundet med progresjon og modenhet av informasjonssikkerheten. Enten ved at sikkerhet bare er ett av flere konkurrerende mål og dermed ikke prioritert eller at sikkerhet alltid er prioritert og er hovedmålet for organisasjonen. Uten ledelsesfokus vil man ikke oppnå en forankring av mål- og resultatstyring (SSØ, 2006). Dette samsvarer ikke med funn fra intervjuene med banknæringen, for som nevnt i forrige delkapittel er informasjonssikkerhet høyt prioritert og har stort ledelsesfokus til tross for at det ikke er hovedmålet til banken. Derfor kan ikke denne faktoren forklare hvorfor banknæringen opplever utfordringer med progresjon og modenhet.

En alt for enkel forklaring (og unnskyldning) på at det er mangelfull måling i norske banker kan være at lovkravet, er for uklar ettersom det står at informasjonssikkerhet "*skal så langt det er praktisk mulig være målbare*" (IKT-forskriften, §5 *Sikkerhet*). Tvetydigheten kan utnyttes ved å påstå at det ikke er praktisk mulig å måle deler og helheten av informasjonssikkerhetsarbeidet. Videre vil det diskuteres hvorfor dette ikke er en god nok forklaring for å unngå måling av informasjonssikkerhet i bank.

Hensikten med måling av informasjonssikkerhet å skape læring, progresjon og forbedring i virksomheten (SSØ, 2006). Funn fra forrige delkapittel viser at det er mangel på helhetlig tilnærming på informasjonssikkerhet i bankene, og dette kan være en forklaring på at de ikke har en måling av progresjonen. Helhetlig sikkerhetstilnærming er en faktor som særlig trekkes frem i både NAT og HRO-teorien, men som kun noen få banker trakk frem som nødvendig. De som fremhevet faktoren mente det var utfordrende, men også at det var ønske om å arbeide videre med en helhetstilnærming slik at man ble flinkere på dette i banken. Som nevnt i 4.2 er det kun én av bankene som bevist hadde høy prioritet av arbeidet mot en mer systematisk og helhetlig tilnærming til informasjonssikkerhet. I tillegg hadde flertallet av bankene i den siste tiden begynt å prioritere klassifiseringsarbeid, men flere indikerte at her

var det en lang vei å gå. Uten helhetlig tilnærming og klassifisering vil ikke bankene ha oversikt over alle komponentene av informasjonssikkerhet. En høy modenhet av informasjonssikkerhetsarbeidet krever at bankene prioriterer disse faktorene høyt.

Slik det er i dag måler norske banker (dersom de i det hele tatt måler noe) utelukkende kun de tekniske informasjonssystemene, som for eksempel tilgjengelighet der man måler *oppe-tid*. En svakhet med dette er at målingen gir en liten del av hvordan informasjonssikkerheten i banken virkelig er. Her er noen eksempler på noen mulige målingsparametere som norske banker kan ha (listen er ikke uttømmende):

- **Brannmur** – antall stoppede forsøk på penetrering av systemet
- **Hendelseshåndtering** – antall uønskede hendelser som er rapportert og antall som har blitt håndtert
- **Holdningsskapende kampanje** – spørreundersøkelse som avdekker læring blant ansatte

Målinger er med på å styrke en helhetlig og systematisk styringen av informasjonssikkerheten i banker ettersom man jobber mot konkrete mål og ved at man etterhvert kan se en progresjon av modenheten til arbeidet. Som nevnt er de fleste modenhetsmodellene på informasjonssikkerhet basert på en teknisk tilnærming, men enkelte sier allikevel at man bør ha en multi-disiplinær tilnærming slik at det åpner opp for å inkludere mer enn bare den tekniske dimensjonen (Von Solms, 2001). Tabell 5 er en modifisert ISM3-modell for informasjonssikkerhet som vil kunne åpne opp for mer enn bare tekniske målenheter. Denne tabellen er en forklaring for hva som tilhører hvert nivå og som benyttes i den selvlagde figur 6 på neste side.

Informasjonssikkerhetsmodenhets modell	
Nivå 5: Optimalisert	Full implementering av policy og prosedyrer, jevne resultater, **gjennomsyrende sikkerhetskultur** og automatiserte sikkerhetskontroller.
Nivå 4: Kontrollert	Sikkerhetstesting, minske sårbarheter **(både tekniske, organisatoriske og menneskelige),** informasjonsstyring og identifisere sikkerhets trusler.
Nivå 3: Styrende	Initiere sikkerhetsprogram, **informasjonssikkerhetsopplæring,** sikkerhetsarkitektur, strengere sikkerhetskontroller og organisatoriske policyer og prosedyrer.
Nivå 2: Definert	Oversikt av kritiske komponenter i organisasjonen, etablere et sikkerhetsteam, et viss nivå av tillit (confidence), sikkerhetspolicy og -prosedyrer.
Nivå 1: Udefinert	Fysisk sikkerhet, mangelfull tillit (confidence), basis IT og nettverksbeskyttelse.

Tabell 5: Tilpasset sikkerhetsmodenhetsmodell basert på Lessing (2008)

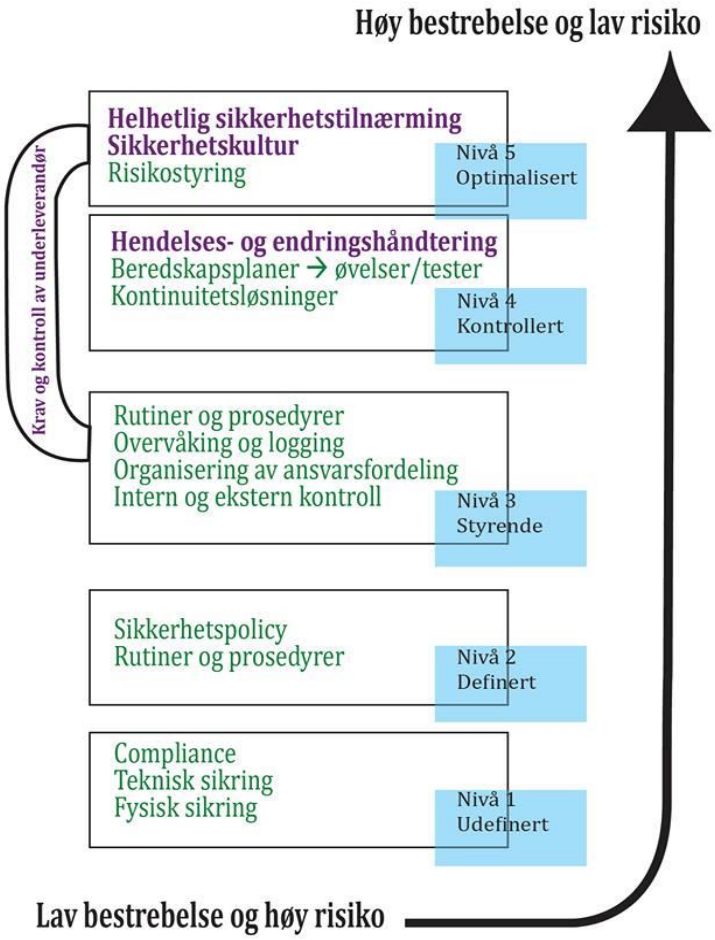
Nivåene beskrevet av Lessing (2008) er overlappende og bygger på hverandre slik at bankene ikke kan oppnå modenhet på nivå 5 uten at de har sikret at nødvendige faktorer som tilhører

lavere modenhetsnivå er implementert i bankens informasjonssikkerhetsarbeid. Denne generiske modenhetsmodellen er originalt lite egnet til menneskelige forhold, derfor er det lagt til menneskelige faktorer som oppgaven har avdekket er nødvendige faktorer for å oppnå "god informasjonssikkerhet" i bank. Dette er gjort med tanke på teori som mener at mennesker i større grad enn tekniske systemer kan handle fleksibelt og dermed oppdage og korrigere uventede feil (Rausand, 2009). Ettersom de fleste bankene har organisert ansvaret for informasjonssikkerhetsarbeidet i en IT-avdeling vil prioritering og fokus på den menneskelige dimensjonen ofte utebli. De norske bankene vil derfor ha store utfordringer i forbindelse med økt modenhet, fordi det krever en god sikkerhetskultur. Dessuten kan den menneskelige dimensjonen også omgjøres til måleparameter som kan gi en indikasjon på progresjon.

Ved å bruke tabell 4 presentert i forrige delkapittel 6.2 vil man kunne rangere de nødvendige faktorene for å oppnå "god informasjonssikkerhet" i bank inn i modenhetstabell basert på Lessing (2008).

Under illustrerer figur 6[30] dette. Fargekodene i denne figuren korrelerer med banknæringen sine svar på hvilke faktorer som er nødvendig for å oppnå "god informasjonssikkerhet" og i hvilken grad de prioriteres fra delkapittel 4.2.2, tabell 3 på side 36.

[30] Figuren er selvlagd og en modifisering av figur 3 (Lessing 2008) på side 36 i teorikapittelet og er tilrettelagt resultater som har kommet frem i oppgaven.



Figur 6: Nødvendige faktorer for å oppnå ”god informasjonssikkerhet” satt i modenhetsmodell for informasjonssikkerhet.

Lilla= Faktoren har en viss prioritert, men bankene uttrykker at det er utfordringer i arbeidet og til tider sviktende.
Grønt = Faktoren har høy prioritert og blir jevnlig fulgt opp av banken.

Informasjonssikkerhetsarbeidet må ha definerte mål som følges opp, deretter må det etableres styringsparametere som beskriver i hvilken grad bankene når disse målene. Faktorene trukket som nødvendig for å oppnå ”god informasjonssikkerhet” i delkapittel 6.2 kan for eksempel rangeres på følgene måte, ut i fra definisjonen og modenhetsnivå:

Integritet:
Nivå 1: Systemtilganger → sikrer at kun autoriserte personer kan gjøre informasjonsbehandlingen - administrasjonsrettigheter
Nivå 3: Overvåking og logging → Sporbarhet gjør at man kan følge informasjonen og endringer til dens opprinnelse eller endringsansvarlige.
Nivå 5: Sikkerhetskultur → sikrer at ansatte har samme sikkerhetsholdninger og verdier som banken og adferd som gjenspeiler dette.

Tilgjengelighet
Nivå 4: Kontinuitetsløsninger → sikrer stabilitet og motstandsdyktighet ved at man raskt kan komme tilbake til vanlig drift tross uønskede hendelser.

Konfidensialitet
Nivå 1: Logisk sikring → sikrer at eksterne trusselaktører ikke får tilgang til tekniske systemer.
Nivå 5: Sikkerhetskultur → sikrer at ansatte har samme sikkerhetsholdninger og verdier som banken og adferd som gjenspeiler dette.

Sikkerhetskultur og helhetlig tilnærming
Nivå 3: Sikkerhetsopplæring → sikrer at ansatte får kompetanse omkring informasjonssikkerhet
Nivå 5: Risikostyring → Målinger på selve resultatet av risikostyring for informasjonssikkerhet er meningsløst ettersom man vanskelig kan bevise at ingenting skjer på grunn av godt risikoarbeid, men man kan allikevel etablere måleparameter i banken som går på utførelsen og særlig oppfølgingen av risikostyringsarbeidet.
Nivå 3,4,5 (avhengig av banken): Krav og kontroll til underleverandører →*Nivå 3*: Sikrer at underleverandører følger kravene,
Nivå 4: Tester og øvelser på informasjonssystemene drevet av underleverandører,
Nivå 5: Sikring av ansatte hos underleverandøren har samme sikkerhetsholdninger og verdier som banken og adferd som gjenspeiler dette.

Noen faktorer som *rutiner* og *krav og kontroll til underleverandør* vil som vist i figur 6 side 55 tilhøre flere modenhetsnivåer ettersom innholdet i faktoren vil variere. Dersom banken kun kontrollerer ved å benytte en sjekkliste over dokumenter og kun de formelle elementene av underleverandørens levering vil man kunne overse kritiske faktorer. Modenheten vil da være på nivå 3. For å oppnå det optimaliserende nivå 5 må bankene sikre at det faktisk blir gjort på den måten som dokumentene tilsier. Dette vil være like relevant internt som eksternt med underleverandører. Det finnes flere måter å gjøre dette på, for eksempel kan man sikre tverrfaglig input ved at ansatte i sikkerhet, IT og representanter fra andre forretningsområder i banken gir tilbakemelding om hvordan det operasjonelle arbeidet gjennomføres (Dekker, 2006). Da vil man kartlegge og minske gapet mellom det som faktisk blir gjort, men det krever at banken har en god sikkerhetskultur som er preget av åpenhet, ærlighet og lyst til å lære.

Basert på denne modenhetsmodellen vil man allerede uten formell måling kunne utføre en subjektiv kartlegging av bankenes modningsnivå på informasjonssikkerhet. Som nevnt tidligere har norske banker tradisjonelt høy fokus på teknisk og fysisk sikkerhet, og innen informasjonssikkerhet samsvarer flertallet av det lovkrav, sikkerhetsteori og bankene selv fremhever som viktige faktorer. Dette gjør at ingen av bankene er på et lavere modenhetsnivå enn nivå 3. De minste bankene som utkontrakterer mesteparten av informasjonssikkerhet vil gjerne ha en modenhet som tilsvarer nivå 3, ettersom bankene har etablerte rutiner og gjennomfører både intern og ekstern kontroll. En del bruker *beste praksis* som mal, men allikevel bærer informasjonssikkerhetsarbeidet på dette modenhetsnivået preg av at det styres reaktivt og baserer seg i stor grad på lovverk. For å oppnå et høyere modningsnivå må bankene bestrebe større kontroll og oversikt over alle dimensjonene av

informasjonssikkerheten både i banken og hos deres underleverandører. Dessuten er små banker ofte avhengig av at underleverandørene har like stor eller høyere modenhet som dem når det gjelder informasjonssikkerhet. Nettopp derfor er også samarbeidet mellom bankene i Norge en viktig suksessfaktor for de bankene som befinner seg på et lavere modenhetsnivå, fordi det tillater dem å oppnå en videre progresjon og økt modenhet ved å lære av andre bankers erfaringer og kunnskap.

Flertallet av bankene som ble intervjuet befinner seg på nivå 4, fordi de arbeider proaktivt ved å søke etter sårbarheter for å lettere kontrollere informasjonssikkerheten. For eksempel ved å avholde omfattende øvelser og tester av informasjonssikkerheten vil banken avdekke sikkerhetshull i adferd, rutiner og tekniske systemer som man således kan arbeide med å tette. Det var kun én av bankene som skilte seg ut fra alle de andre bankene og for den banken vil modenheten ligge i mellomsjiktet nivå 4 og 5. Dette er banken som er trukket frem tidligere fordi den arbeider bevist mot en mer helhetlig, systematisk og risikobasert tilnærming til informasjonssikkerhet. En bank som ligger på modenhetsnivå 5 vil ha mange likhetstrekk med en HRO ved at man har et særlig høyt fokus på sikkerhetskultur, helhetlig oversikt og dynamiske arbeidsprosesser som hele tiden forbedrer informasjonssikkerheten i forhold til utviklingen innad i virksomheten og det eksterne trusselbilde. Det er ikke å si at det er kun de faktorene i øverste modenhetsnivå som er viktig, for det setter som premiss at de foregående faktorene i de tilhørende lavere modenhetsnivåene er vel integrert og har videre progresjon. For å oppnå økt modenhet må bankene bygge informasjonssikkerhetsarbeidet på det som allerede er god etablert slik som høy teknisk sikkerhet og dette må prioriteres minst like mye som etablering av helhetlig tilnærming.

På den annen side er det viktig å merke at målinger basert på KPIer[31] gir harde tall som ikke forteller den fulle sannheten, men at *"det på sitt beste kan utvikles trendindikatorer som sier noe om utvikling"* (FFI, 2007:16). Med bruk av målinger kan bankene kartlegge informasjonssikkerhetsarbeidet sin utvikling, avdekke svikt og prioriteringsområder, men målinger vil selvsagt ikke gi en garanti for at bankene oppnår en så "god informasjonssikkerhet" at ulykker aldri oppstår. Forklaringene for mangelfull måling var nettopp dette og informantene trakk frem at de ikke ønsket kun en statisk statistikk uten reel progresjon. Allikevel viser drøftingen over at det er mange parametere bankene kan benytte som skal kunne skape en indikasjon på videre progresjon, og dermed forenkle for eksempel

[31] **KPI (Key Performance Indicator)** er en av viktig måling som viser hvordan en situasjon er eller endrer seg over en gitt tid, som for eksempel hvor god økonomien, virksomheten eller et prosjekt gjør det eller hvordan ansatte jobber (Cambridge Business English Dictionary, 2014)

ressursstyring ved at banken avdekker sårbarheter i informasjonssikkerhetsarbeidet og hvilke områder som krever større prioritering over en gitt tid.

Forrige delkapittel viser at to av fem faktorene som ikke samsvarer mellom lovkrav, sikkerhetsteori og banknæringen er direkte eller indirekte knyttet mot den uformelle delen av bankvirksomheten. Som modenhetsnivåmodellen viser vil en prioritering av kun den formelle delen av banken føre til en lav modenhet av informasjonssikkerhet, ved at bankene overser interaksjonen mellom teknologi og menneske. Dette viser at det tradisjonelle synet om at teknologien er kjernen i informasjonssikkerhet er utdatert. For å oppnå ”god informasjonssikkerhet” er bankene avhengig av å inkludere og prioritere de ”myke faktorene” på lik linje med de tekniske og organisatoriske.

6.3.1 Oppsummerende delkonklusjon

Utfordringene forbundet med måling av progresjon og modenhet av informasjonssikkerhet i bank er knyttet til de faktorer som trekkes frem som nødvendig for å oppnå ”god informasjonssikkerhet” som ikke samsvarer mellom sikkerhetsteori og banknæringen. Slik som mangelfull *oversikt over alle komponenter*, *helhetlig sikkerhetstilnærming* og *sikkerhetskultur*. Det foregår noe måling av informasjonssikkerhet i banker i dag, men dette er hovedsakelig på de tekniske systemene og det vil kun gi en indikasjon på en liten del av hele informasjonssikkerhetsarbeidet. I dette delkapittelet er det foreslått flere mulige måleparameter som bankene kan benytte. Slike måleparametere skal sikre en helhetlig tilnærming til måling som inkluderer alle elementene i definisjonen for ”god informasjonssikkerhet” og som muliggjør bankene å følge arbeidets progresjon over tid.

6.4 MTO-perspektiv – en hensiktsmessig tilnærming?

De faktorene som er nødvendige for å oppnå god informasjonssikkerhet i bank, oppsummert i tabell 4 side 42, vil inkludere både de *tekniske* systemene som inneholder informasjon, det *organisatoriske* rammeverket som styrer behandlingen av informasjonen og *menneskene* som faktisk behandler informasjonen. Særlig utfordringen med helhetlig sikkerhetstilnærming skaper som vist i forrige delkapittel en hemming av videre progresjon og økt modenhet. Et Menneske-Teknologi-Organisasjonsperspektiv (MTO) kan skape rammene som åpner opp for en mer helhetlig tilnærming til informasjonssikkerhetsarbeidet i bank.

Informasjonssikkerhet inngår som nevnt i innledningen i banken sin operasjonelle risiko. Basel II definer operasjonell risiko som *"risikoen for tap som følge av utilstrekkelige eller sviktede interne prosesser (O) eller systemer (T), menneskelige feil (M), eller eksterne hendelser"* (BCBS 2006). Således kan et MTO-perspektiv i bank være hensiktsmessig fordi det omfatter alle de interne dimensjonene av operasjonell risiko. Funnene fra intervjuene med banknæringen viser at bankene har høy kvalitet og fokus på de tekniske systemene og bevaring av informasjonssikkerheten i disse. Arbeidet og sikkerhetsperspektivet for informasjonssikkerhet i bankene bærer derfor preg av en noe ensidig teknisk tilnærming. Oppgaven ønsker ikke å erstatte dette med noe nytt, men isteden diskutere om et MTO-perspektiv kan skape en forlengelse av den tekniske tilnærmingen slik at bankene lettere kan arbeide systematisk og helhetlig.

Et interessant funn fra intervjuene var at kun én av bankene brukte MTO-perspektivet bevist i hele sitt sikkerhetsarbeid. Ingen av de andre bankene kunne vise til at det ble benyttet et spesifikt eller bevist perspektiv for sikkerhet, og noen informanter forvekslet det med risikostyring. Dersom man har en MTO-tilnærming vil informasjonssikkerheten i bank være avhengig av:

- kvaliteten på det tekniske system
- kvaliteten i det organisatoriske system
- kvaliteten på det menneskelige system
- kvaliteten på relasjonene mellom elementene nevnt ovenfor (Rollenhagen, 1997:22).

Inntrykket fra intervjuene er allikevel at alle bankene arbeider ubevist med en MTO-tilnærming ettersom alle (i varierende grad) inkluderer de tre dimensjonene i sitt informasjonssikkerhetsarbeidet. En mangelfull systematikk omkring samspillet av de tre dimensjonene er gjennomgående for de aller fleste bankene som ble intervjuet.

Hovedstyrken til MTO-perspektivet er at det muliggjør en systematisk og helhetlig tilnærming til sikkerhetsarbeidet, som er overførbart til informasjonssikkerhetsarbeidet (Rollenhagen, 1997). MTO var et naturlig valg av sikkerhetstilnærming for informanten i banken som benytter perspektivet fordi det dekker skjæringspunktene mellom de tre dimensjonene. Skjæringspunktene kan være at det hjelper for eksempel ikke å ha gode tekniske systemer uten opplæring, eller opplæring uten rutiner. Man må inkludere alle tre dimensjonene i informasjonssikkerhetsarbeidet fordi samspillet mellom dem er uunngåelig. Informanten gir et godt eksempel på praktisk bruk av MTO i hverdagsarbeidet med informasjonssikkerhet: De skulle legge ut informasjon på intranettet om en trojanerhendelse,

ekstern trussel mot tekniske systemer (T), linket opp mot relevante rutiner og prosedyrer (O) og dette øker bevisstheten og forståelsen for informasjonssikkerhet hos den enkelte ansatt (M). Det var en fra IT-sikkerhetsavdelingen som publiserte innlegget og vedkommende glemte først å linke til rutiner. Umiddelbart ble vedkommende påminnet av en annen ansatt at det burde linkes til relevante rutiner. Dette ble gjort og viser at en bevissthet omkring MTO sikrer slikt arbeid. For uten å inkludere de organisatoriske rutinene kan det skapes sikkerhetshull ved at ansatte ikke kjenner til eller glemmer dem. Ved å ha MTO-perspektivet bevist i informasjonssikkerhetsarbeidet vil det sikre kvaliteten og prioriteringen av alle tre dimensjonene.

Som nevnt tidligere kan MTO også være en god tilnærming når man skal granske uønskede hendelser og ulykker (Bento ,2001). Eksempelet med hendelsen der sensitiv informasjon ble sendt via excel-fil viser at for å avdekke mer enn bare den direkte menneskelige feilen må man kartlegge de organisatoriske og tekniske dimensjonene for å se om de også kan være indirekte og dyptgående årsaker. Kun ved å forbedre de dyptgående årsakene vil man kunne avverge at lignende menneskelige feil oppstår igjen (Dekker, 2006). Man må forstå skjæringspunktene mellom det tekniske, menneskelige og organisatoriske for å tette mulige sikkerhetshull.

Ettersom et MTO-perspektiv gjør at bankene enklere kan jobbe helhetlig med informasjonssikkerhet vil de ifølge Figur 6 side 56, modenhetsmodellen, oppnå en økt modenhet. Dette fordi bankene lettere kan arbeide systematisk med interaksjonene mellom teknologi og mennesker. Funn fra forrige kapittel viser at en utfordring for måling av progresjon og modenhet av informasjonssikkerhet er knyttet til at det kun foretas få og varierte tekniske målinger. Dette illustrerer kun en liten del av det helhetlige arbeidet. Ved bruk av MTO på en bevist og systematisk måte vil målinger på informasjonssikkerhetsarbeidet naturlig nok inkludere alle tre dimensjonene og dermed avdekke progresjonen av hele arbeidet. Et MTO-perspektiv kan derfor være løsningen for å håndtere noen av utfordringene forbundet med progresjon og modenhet av informasjonssikkerhet.

En svakhet ved bruk av MTO-perspektiv i bank er at ansvaret for informasjonssikkerhet tradisjonelt har ligget hos IT mens andre sikkerhetsområder (som ranssikring) har tilhørt andre avdelinger. Slik er det for mange av bankene fremdeles, og det kan by på vanskeligheter ettersom skillene mellom informasjonssikkerhet og tradisjonelle

sikkerhetsområder i bank viskes ut og vokser sammen. For å benytte MTO i praksis, må man arbeide med å styrke koordineringen av flere miljøer og ansvarsroller i banken. Dette gjenspeiles i teorien om HRO, der organiseringen av ansatte er overlappende og at det eksisterer klare ansvarsroller slik at håndteringen av hendelser skjer på en forventet måte (Weick 1993, La Porte 1996).

En praktisk benyttelse av MTO-perspektivet i informasjonssikkerhetsarbeidet i bank kan også være å bevist benytte et risikoverktøy som på en god måte kan illustrere sammenhengene mellom alle dimensjonene. Informanten fra banken som bruker MTO-perspektivet forteller at MTO brukes i alle ledd av risikostyring. Forklaringen på at vedkommende foretrekker en slik anvendelse er at ofte vil en uønsket hendelse eller ulykke være et resultat av flere barrierebrister, og gjerne en kombinasjon av feil i det tekniske systemet, menneskelige samhandlinger og det organisatoriske rammeverket (Reason 1997, Rollenhagen 1997). Alle faktorene for å oppnå ”god informasjonssikkerhet” som er trukket frem i foregående delkapitler fungerer som sikkerhetsbarrierer. En vellykket barriere gjør at en feil vil avverges, isolert eller håndtert raskt slik at det ikke får forplante seg til en uønsket hendelse og ulykke.

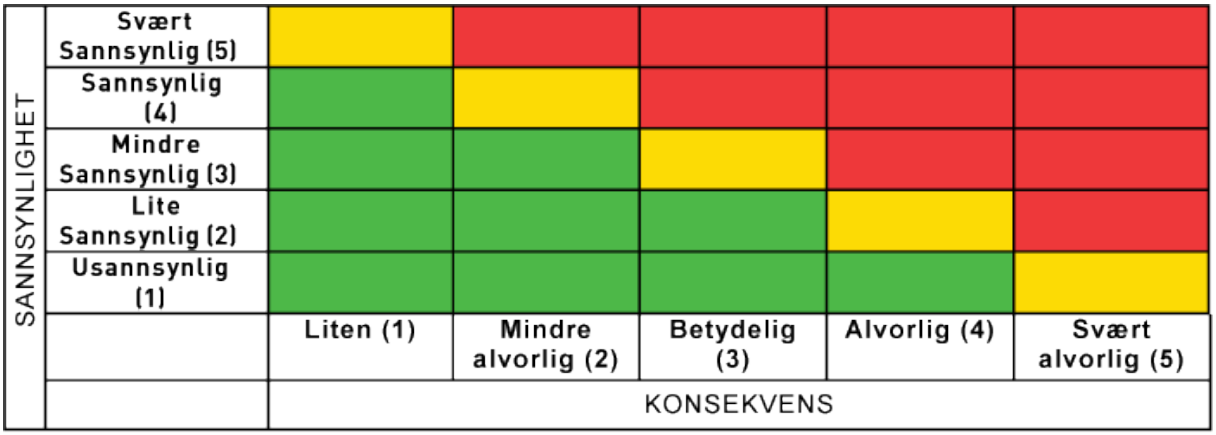
Figur 7 på neste side illustrerer barrierer i risikostyringssammenheng. Flere barrierer vil bety mer redundans i et system, men også mer kompleksitet (Perrow, 1999). Så en vellykket risikostyring skal kartlegge hensiktsmessige barrierer da både for få og for mange kan få negative konsekvenser.

Figur 7: Risikoanalysene sine tre trinn som et ”bow-tie-diagram” med barrierer, basert på Aven (2007)

Bankene vil øke motstandsdyktigheten mot brudd på informasjonssikkerhet dersom de etablerer sikkerhetstiltak som inkluderer både tekniske, organisatoriske og menneskelige elementer ettersom det utgjør overlappende barrierer som kan avverge eller begrense ulykker.

Hovedsakelig bruker norske banker en risikomatrise som sitt risikoverktøy. Dette er basert på at risiko er sannsynlighet ganger konsekvens. Alle bankene som ble intervjuet benyttet til

denne oppgaven benyttet i hovedsak risikomatrise. Utarbeidelse av risikomatrise vil enkelt forklart være at bankene lager scenarioanalyser der man kartlegger mulige hendelser. Deretter settes hendelsene inn i matrisen, som består av en fargekoding basert på akseptert risiko: Rødt betyr uakseptabel risiko, gul betyr i grenseland og bør gjøres tiltak mot, grønn betyr at risikoen er lav. Figur 8 viser et eksempel på hvordan en slik matrise kan se ut.



Figur 8: Eksempel på en risikomatrise (NOU 2012:4, s.22)

En svakhet er at denne risikoanalysemetoden sier mye om konsekvenser og lite om årsaker. Da bankene ble spurt om refleksjoner omkring bruken av en slik risikoanalysemetode var svaret at det er en enkelt å gjennomføre og forstå. Dessuten har det alltid har blitt utført på den måten. Det kan stilles spørsmålstegn om ikke bankene i større grad bør reflektere rundt bruken av forskjellige risikoanalysemetoder tilpasset forskjellige analyseobjekter og risikoer.

Derfor vil oppgaven i neste delkapittel utforske om en annen risikometode kan være mer fordelaktig for å inkludere et MTO-perspektiv enn en risikomatrise.

6.4.1 Bayesiansk nettverk

Et egnet systematiseringsverktøy som for banker som benytter et MTO-perspektiv som rammeverk er bayesiansk nettverk. Et bayesiansk nettverk vil visualisere årsakssamspillet og den gjensidige påvirkningen som mennesker, teknologi og organisasjon faktorer har på hverandre. Risikoanalysen passer derfor godt sammen med et MTO-systemperspektiv (Rollenhagen, 1997). Bayesiansk nettverk er spesielt godt egnet når det risiko forbundet med både høy kompleksitet og usikkerhet. Dessuten vil brudd på informasjonssikkerhet inkludere ”myke” årsaksfaktorer som menneskelig svikt. Risikomodellering for årsaksfaktorer for brudd på informasjonssikkerhet vil derfor for enkelte scenarioer kreve mer ekspertkunnskap enn

historiske data. Dermed kan bayesiansk nettverk være et godt egnet risikoverktøy for det forebyggende informasjonssikkerhetsarbeidet i norske banker.

Igjennom den kvantitative analysen vil et bayesiansk nettverk tillate en simulering av årsakenespåvirkninger for den uønskede hendelsen. Således vil man for eksempel avdekke om hacking av et teknisk system vil ha større påvirkning for den uønskede hendelsen enn brudd på en rutine. Selv komplekse systemer blir enkelt forklart visuelt og forstått i den kvalitative modelleringen av et bayesiansk nettverk (Andersen & Häger, 2010). Dette gjør at bankens ledelse vil ha et godt beslutningsverktøy som grunnlag for valg innenfor informasjonssikkerhetsområdet. Slik vil man forenkle ressursstyringen etter der det er størst behov. Et bayesiansk nettverk skal holdes oppdatert og dynamisk ved at det legges inn ny data og kunnskap etter at sikkerhetstiltak er utført (Pearl & Russel, 2002). Dersom bankene etablerer jevnlige helhetlige og systematiske målinger av informasjonssikkerhetsarbeidet vil det forenkle oppdateringen av det bayesiansk nettverket. Derfor vil man i motsetning til risikomatrise enkelt visualisere progresjonen og modenheten av arbeidet kvantitativt.

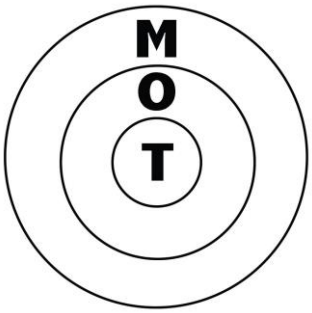
En av informantene mener at et bayesiansk nettverk er mest hensiktsmessig for komplekse situasjoner og enkelte topprisikoer, men at modelleringen er ytterst ressurs- og tidkrevende så for de fleste risikoene er en risikomatrise god nok. Derfor kan det for mange små banker være unødvendig å benytte dette verktøyet på alle risikoer forbundet med informasjonssikkerhet, men heller fokusere det mot de mest alvorlige slik at man skaffer seg fullstendig oversikt over årsaker til slike hendelser og dermed både forenkler og forbedrer forebyggingsarbeidet for brudd på informasjonssikkerhet.

Ettersom modellering av et bayesiansk nettverk er både enormt ressurs- og tidskrevende ble det ikke foretatt i forbindelse med denne oppgaven. Det bør gjøres mer forskning på risikostyring av informasjonssikkerhet, der man blant annet tester hypotesen presentert over: ”Bayesiansk nettverk er et godt egnet risikoverktøy for modellering av årsaker for brudd på informasjonssikkerhet i norske banker”.

6.4.2 Oppsummerende delkonklusjon

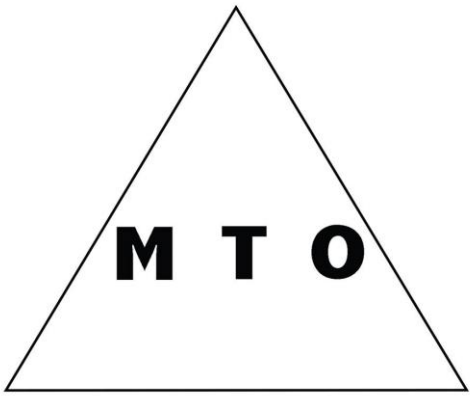
Norske banker kan og bør benytte et MTO-perspektiv i sitt informasjonssikkerhetsarbeid da dette vil gjøre det enklere å jobbe systematisk og helhetlig. MTO kan både brukes som en overordnet sikkerhetstilnærming, i risikostyring, granskning og praktisk utførelse av det daglige informasjonssikkerhetsarbeidet i banken.

Figur 9 illustrerer hvordan det tradisjonelle synet på de tre dimensjonene har vært (og fremdeles er) i flere norske banker:



Figur 9: Tradisjonell MTO-tilnærming i bank

Det tradisjonelle synet vil se på teknologi som selve kjernen, mens den organisatoriske og menneskelige dimensjonen tilrettelegges deretter og vil ikke være like viktig.
Funn i oppgaven viser at norske banker isteden bør prioritere de tre dimensjonene likt og at man er særlig oppmerksom på samspillet mellom alle tre. Dette illustreres i Figur 10:



Figur 10: Alle dimensjonene (MTO) bør prioriteres likt for å skape en helhetlig tilnærming til informasjonssikkerhet

Et bayesiansk nettverk kan være et godt egnet risikoverktøy for norske bankers informasjonssikkerhetsarbeid som styrker MTO-perspektivet. Det vil være et hjelpemiddel for å kartlegge de helhetlige årsakene til risikoene i banken som omfatter informasjonssikkerhet.

7 Konklusjon

”God informasjonssikkerhet” i norske banker **er fysiske, tekniske og organisatoriske helhetlige tiltak som sikrer konfidensialitet, integritet og tilgjengelighet for den informasjonen som behandles i bankets system, samt en velfungerende informasjonssikkerhetskultur som gjennomsyrer hele banken.** Denne definisjonen vil omfatte all informasjon som finnes i bankets system (samt deres underleverandører), og det inkluderer både elektronisk, fysisk og muntlig informasjon.

For å oppnå ”god informasjonssikkerhet” er norske banker avhengig av en rekke faktorer. Oppgaven har i tabell 4 kartlagt samsvar mellom det lovkrav, sikkerhetsteorier og banknæringen mener er nødvendig for å oppnå ”god informasjonssikkerhet”.

Faktorer som samsvarer	Manglende samsvar	Faktorer som samsvarer, men som anses av bankene som utfordrende og sviktende
Fysisk og logisk sikring	Prioritering av sikkerhet – Ledelsesfokus	Helhetlig sikkerhetstilnærming
Rutiner og prosedyrer	Samarbeid mellom norske banker	Klassifisering – oversikt over komponentene
Overvåking og logging	Bankkunder	Sikkerhetskultur
Ansvarsfordeling	Bruk av ”beste praksis”	Hendelses- og endringshåndtering
Intern og ekstern kontroll		Krav til underleverandører
Risikostyring		
Krisehåndtering og beredskap		
Kontinuitetsløsninger		

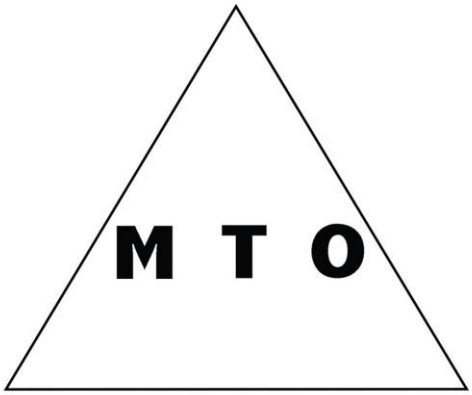
Tabell 4[32]: samsvar mellom nødvendige faktorer for å oppnå ”god informasjonssikkerhet” fremhevet av lovverk, sikkerhetsteori og banknæringen.

Utfordringene forbundet med videre progresjon og økt modenhet av informasjonssikkerhet i bank er knyttet til faktorer som trekkes frem som utfordrende og sviktende. Det foregår noe måling av informasjonssikkerhet i banker i dag, men dette er hovedsakelig på de tekniske systemene og det vil kun gi en indikasjon på en liten del av hele informasjonssikkerhetsarbeidet.

Mangel på helhetlig og systematisk måling av informasjonssikkerhet, slik at bankene kan si noe om progresjon og modenhet, henger også sammen med den tradisjonelle tilnærmingen til informasjonssikkerhet. Det tradisjonelle synet mener at teknologi er selve kjernen, mens den

[32] **Lilla** = Faktoren har en viss prioritert, men bankene uttrykker at det er svakheter i arbeidet med denne faktoren.
Grønt = Faktoren har høy prioritert og blir jevnlig fulgt opp av banken.

organisatoriske og menneskelige dimensjonen tilrettelegges deretter og vil ikke være like viktig. Funn i oppgaven illustrert av figur 10 viser at for at norske banker skal oppnå en videre progresjon og økt modenhet bør de prioritere de tre dimensjonene likt og at de er særlig oppmerksom på samspillet mellom alle tre.



Figur 10: Alle dimensjonene (MTO) bør prioriteres likt for å skape en helhetlig tilnærming til informasjonssikkerhet

Ved å implementere en bevist MTO-perspektiv til informasjonssikkerhet vil bankene forenkle sitt helhetlige sikkerhetstilnærming og dermed løse en del utfordringer som er forbundet med videre progresjon og økt modenhet av informasjonssikkerhet i norske banker.

8 Referanser

Albrechtsen, E. (2008). *Friend or foe?: information security management of employees* (Vol. 2008:101). Trondheim: Norges teknisk-naturvitenskapelige universitet.

Andersen, L. B., & Häger, D. (2010). Contributions to Bayesian network model design for operational risk in the financial industry (Vol. Vol. 1, pp. s. 41-48).

Andersen, S. (2006). Aktiv informantintervjuing. *Norsk vitenskaplig tidskrift, 22*, 278-298.

Aven, T. (2007). *Risikostyring: grunnleggende prinsipper og ideer*. Oslo: Universitetsforl.

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget.

Aven, T., Røed, W., & Wiencke, H. S. (2008). *Risikoanalyse: prinsipper og metoder, med anvendelser*. Oslo: Universitetsforlaget.

ITAvisen. (2013). Bruker DDoS til å kamuflere banksvindel. Hentet10 mars, 2014, fra http://www.itavisen.no/nyheter/bruker-ddos-til-%C3%A5-kamuflere-banksvindel-90002

BankID Norge. *Dette er BankID*. Hentet 15.april 2014, fra https://www.bankid.no/Dette-er-BankID/)

Bakås, T. H. (2005). *God praksis for måling av informasjonssikkerhetsnivå*. Gjøvik: Høgskolen i Gjøvik.

Bento, J.-P. (2001). Menneske - teknologi - organisasjon. Veiledning for gjennomføring av MTO-analyse.

Blaikie, N. (2009). *Designing social research: the logic of anticipation*. Cambridge: Polity Press.

Bloomberg (2013). *Goldman Sachs Said to Send Stock-Option Orders by Mistake.* Hentet 1.juni 2014, fra http://www.bloomberg.com/news/2013-08-20/goldman-says-exchanges-working-to-resolve-options-order-mishap.html

Daler, T., Gulbrandsen, R., Høie, T. A., & Sjølstad, T. (2010). *Håndbok i datasikkerhet: informasjonsteknologi og risikostyring*. Trondheim: Tapir akademisk.

Danemark et al. (1997). Generalisering, vetenskapliga slutledningar och modeller för forklarande samhällsvetenskap *Att förklara samhället*. Lund: Studentlitteratur.

Datatilsynet. (2009). *En veiledning om internkontroll og informasjonssikkerhet*. Oslo, Norge.

Dekker, S. (2006). *The field guide to understanding human error*. Aldershot: Ashgate.

Departementene. (2012). *Nasjonal Strategi for Informasjonssikkerhet*. Oslo, Norge. Hentet 15. januar 2014, fra http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf

Dhillon, G. (2001). *Information security management: global challenges in the new millennium.* Idea Group Publishing, PA, USA.

Ellefsen, Bodil. (1998) *Triangulering - eller hvorfor og hvordan kombinere metoder?*, fra Lorensen,M. (red.) Spørsmålet bestemmer metoden. Forskningsmetoder i sykepleie og andre helsefag. Universitetsforlaget, Oslo, Norge. .

Finanstilsynet. (2011). *Økte krav til bankene i lys av driftsproblemene i påsken 2011*. Oslo, Norge.

Finanstilsynet. (2013a). *Risiko- og sårbarhetsanalyse (ROS) 2012*. Oslo, Norge.

Finanstilsynet. (2013b). *Veileder til IKT-forskriftens §5 "sikkerhet"*. Oslo, Norge.

Finanstilsynet. (2013c). *Veiledning til IKT- forskriftens § 5 "Sikkerhet"*. Oslo, Norge.

Finanstilsynets egenevalueringsskjemaer. Hentet 21. januar 2014, fra http://www.finanstilsynet.no/no/Tverrgaende-temasider/IT-tilsyn/Egenevalueringssporsmal/.

FOR 2003-05-21-630 *Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT).*

FOR-2000-12-15-1265 *Forskrift om behandling av personopplysninger* (personopplysningsforskriften).

Frost, B. (2000). *Measuring performance: using the new metrics to deploy strategy and improve performance*. Measurement international, Dallas, USA.
Glendon, A. I., & Stanton, N. A. (2000). Perspectives on safety culture. *Safety Science, 34*(1–3), 193-214. doi: http://dx.doi.org/10.1016/S0925-7535(00)00013-8
Grimen, H., Ugelvik, I. L., & Jåsund, K. K. (2000). *Samfunnsvitenskapelige tenkemåter*. Universitetsforlaget, Oslo, Norge
Grimvall, G. (2009). *Risks in technological systems*. Springer, London, England.
Grønmo, S. (2004). *Samfunnsvitenskapelige metoder*. Fagbokforlaget, Bergen, Norge.
Hartvigsen, T. (2013). *Er det behov for nytenkning og utvikling av nye risikoanalysemetoder for å håndtere risiko i det moderne informasjonssamfunn?* (Masteroppgave).
Hovden, J. (2004). *I etterpåklokskapens klarsyn: gransking og læring av ulykker*. Tapir, Trondheim, Norge
Introduksjon til COBIT 5 Informasjonssikkerhet. Hentet 21. januar 2014, fra http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf.
Justisdepartementet (2012) NOU 2012:4 *Trygg hjemme. Brannsikkerhet for utsatte grupper.* Oslo, Norge.
Karokola, G., Kowalski, S., & Yngström, L. (2011). *Towards an information security maturity model for secure e-government services: a stakeholders view.* Paper presented at the Proceedings of the 5th HAISA2011 Conference, London, England.
King, B. (2013). *Bank 3.0: why banking is no longer somewhere you go, but something you do*. Wiley, Singapore.
KPI. Cambridge Business English Dictionary (2014) Hentet 6.juni 2014, fra http://dictionary.cambridge.org/dictionary/business-english/key-performance-indicator#
Kvale, S., Brinkmann, S., Anderssen, T. M., & Rygge, J. f. (2009). *Det kvalitative forskningsintervju*. Gyldendal akademisk, Oslo, Norge.
La Porte, T. R. (1996). *High Reliability Organizations: Unlikely, Demanding and At Risk.* Journal of Contingencies and Crisis Management, *4*(2), 60-71. doi: 10.1111/j.1468-5973.1996.tb00078.x
Lessing, M. M. (2008). *Best Practices Show the Way to Information Security Maturity*. Retrieved 26 Februar, 2014
Lindøe, P., Kringen, J., & Braut, G. S. (2012). *Risiko og tilsyn: risikostyring og rettslig regulering*. Universitetsforlaget, Oslo, Norge.
LOV-2000-04-14-31*Lov om behandling av personopplysninger* (personopplysningsloven).
Lydersen, S., Albrechtsen, E., Hovden, J., & Sklet, S. (2004). *Fra flis i fingeren til ragnarok: tjue historier om sikkerhet*. Trondheim: Tapir akademisk forl.
Mjølsnes, S. F. (2012). *A multidisciplinary introduction to information security*. CRC Press, Florida, USA.
Offisiell hjemmeside om COBIT. Hentet 20. januar 2014, fra http://www.isaca.org/cobit/pages/default.aspx.
Om Evry. Hentet 6. juni 2014, fra https://www.evry.no/bedrift/om-evry/
Om NorSIS. Hentet 19.mai 2014, fra https://norsis.no/om-norsis/.
Pearl, J. R., S. (2002). Bayesian networks. In E. M. A. Arbib (Ed.), *The Handbook of Brain Theory and Neural Networks* (pp. side 157-160). MIT Press, Cambridge, MA, USA.
Perrow, C. (1999). *Normal accidents: living with high-risk technologies*. Princeton University Press, Princeton, N.J., USA.
Perrow, C. (2007). *The next catastrophe: reducing our vulnerabilities to natural, industrial, and terrorist disasters*. Princeton University Press, Princeton, N.J., USA.
Petroleumstilsynet. *Tema: Storulykke* (2013). Hentet 30. januar 2014, fra http://www.ptil.no/artikler-i-sikkerhet-status-og-signaler-2012-2013/tema-storulykke-article9140-1094.html.

Phishing. (2012, 4. januar). I Store norske leksikon. Hentet 19. mai 2014 fra http://snl.no/phishing.
Politidepartementet (2000). *NOU 2000: 24. Et sårbart samfunn - Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Oslo, Norge.
Politidepartementet (2001-2002). *Samfunnssikkerhet - Veien til et mindre sårbart samfunn*. Oslo, Norge.
Ramirez, J. L. (2000). *Socialplaneringens verktyg*. Regionplane- och trafikkkontoret. Nordregio, Stockholm, Sverige.
Rasmussen, J. (1982). *Human errors: A taxonomy for describing human malfunction in industrial installations*. Journal of Occupational Accidents, *4*, 311-335.
Rausand, M. (2009). *Risikoanalyse: teori og metoder*. Tapir akademisk forlag, Trondheim, Norge.
Reason, J. (1997). *Managing the risks of organizational accidents*. Ashgate, Aldershot, England.
Rollenhagen, C. (1997). *Sambanden menniska, teknik och organisation -en introduksjon*. Lund, Sverige.
Rosness, R. (2004). *Organisational accidents and resilient organisations: five perspectives* (Vol. STF38 A04403). Trondheim: Stiftelsen for industriell og teknisk forskning ved Norges tekniske høgskole.
Rosvold, K. A., 29. november). Naturlig Monopol. I Store norske leksikon. Hentet 28. april 2014 fra http://snl.no/naturlig_monopol.
SINTEF. (2006). *Uavhengighet av sikkerhetssystemer offshore – status og utfordringer*. Hentet 19.mai 2014, fra http://www.sintef.no/upload/Teknologi_og_samfunn/Sikkerhet og p%C3%A5litelighet/Rapporter/STF50 A06011.pdf
Basel Committee on Banking Supervision (2006). *Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version.* Hentet 14.januar 2014 fra http://www.bis.org/publ/bcbs128.pdf
Thagaard, T. (2013). *Systematikk og innlevelse: en innføring i kvalitativ metode*. Bergen: Fagbokforlaget.
Thomson, K.-L., & Von Solms. (2006). Towards an Information Security Competence Maturity Model. *Computer Fraud & Security*, *2006*(5), 11-15. doi: http://dx.doi.org/10.1016/S1361-3723(06)70356-6
Trojaner. Norsis leksikon. Hentet 19.mai 2014 fra https://admin.norsis.no/leksikon/t/Trojansk_hest.html.
VG (2013) *Evry mister kontrakt med DNB etter nettbanktrøbbel.* Hentet 20.april 2014 fra http://www.vg.no/nyheter/innenriks/evry-mister-kontrakt-med-dnb-etter-nettbanktroebbel/a/10133477/
Von Solms. (2001). *Information Security — A Multidimensional Discipline*. Computers & Security, 20(6), 504-508. doi: http://dx.doi.org/10.1016/S0167-4048(01)00608-3
Wang, C. (1997). A framework for security measurement. *NISSC*.
Wang, e. a. (1997).
Weick, K. E. (1993). The Collapse of Sensemaking in Organizations: The Mann Gulch Disaster. *Administrative Science Quarterly*, *38*(4), 628-652.
Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected: assuring high performance in an age of complexity*. San Francisco, Calif.: Jossey-Bass.
Woodhouse, S. (2008, 8-11 July 2008). *An ISMS (Im)-Maturity Capability Model.* Paper presented at the Computer and Information Technology Workshops, 2008. CIT Workshops 2008. IEEE 8th International Conference on.
Yin, R. K. (2013). *Case study research: design and methods*. SAGE, Los Angeles, Calif., USA.

Vedlegg 1

Intervjuguide

Generelt

1. Hva er din stilling og hva innebærer det?

God informasjonssikkerhet

1. Hva er informasjonssikkerhet?
2. Hvordan jobber banken med at alle ansatte skal ha innsikt i risikoene som er forbundet med informasjonssikkerhet?
3. Kjenner du til om det finnes noen overordnet policy om informasjonssikkerhet på ledelsesnivå? – Hva synes du om den og hvordan er den brukt i sikkerhetsarbeidet i banken?
4. Hvordan tar ledelsen informasjonssikkerhet på alvor? *Be om konkrete eksempler på sikkerhetstiltak.*
5. Hvorfor er et fokus (fra ledelsesnivå) på informasjonssikkerhet er viktig banken?
6. Hva er det verste som kan skje dersom det skjer brudd på informasjonssikkerhet?
7. Hva mener du er nødvendig for å nå "God informasjonssikkerhet" i din bank?
8. Hvordan blir "godheten" av informasjonssikkerhetsarbidet målt i banken?
9. Er banken ISO-27001 sertifisert, eller bruker den andre standarder i sitt arbeid eller måling?
10. Hva kan være gode målenheter å benytte for å oppnå god informasjonssikkerhet?

Faktorer for å nå god informasjonssikkerhet

1. Hva er de største utfordringene forbundet med å oppnå "God informasjonssikkerhet"?
2. Hvordan går dere frem for å avgjøre hvilke faktorer som er viktige for å oppnå god informasjonssikkerhet? – verktøy og metodikk
3. Hvor ofte blir risikoanalyser for informasjonssikkerhet utført?
4. Hvilke metoder mest brukt i risikoanalyse, og er det noe diskusjon omkring metodikk?
5. Dersom det ikke foreligger en risikoanalyse – hvordan blir sikkerhetsarbeidet for informasjonssikkerhet utført?
6. Dersom det har oppstått feil og uønskede hendelser relatert til informasjonssikkerhet hva skal man som ansatt/leder i banken gjøre?
7. Føres det statistikk over slike hendelser i banken?
8. Blir slike feil/hendelser tatt alvorlig? -Hva er konsekvensene etter at feil er rapportert? (Fører det til tiltak og oppfølging?) *Be om konkrete eksempler på dette.*
9. Hvordan er fokuset på informasjonssikkerhet på din arbeidsplass?
10. Er det gjennomført holdningsskapende aktiviteter i banken rettet mot informasjonssikkerhet?
11. Hvordan blir slike kampanjer tatt imot? Måler man utfall i etterkant?
12. Benytter banken en bestemt metode/tilnærming/perspektiv i sitt informasjonssikkerhetsarbidet? Hvilket og hvorfor? (eks. Menneske-Teknologi-Organisasjon (MTO))
13. Tror du det er forskjeller i modenheten av informasjonssikkerhet mellom norske banker? Hvorfor, hvorfor ikke?
14. Hva er nødvendig for å forbedre informasjonssikkerhetsnivået i banken evt. opprettholde dagens nivå dersom det er høyt?
15. Dette er noen faktorer som står beskrevet i teorien og i lovkrav som viktige faktorer for informasjonssikkerhet, hvilke av disse mener du er viktigst, velg gjerne flere og utdyp valgene.
16. Er det noen faktorer du savner eller er det noen faktorer som du mener ikke er nødvendig?

- Sikre tekniske systemer:
    - Digitale nettverk
    - Autorisasjon og tilgangskontroll
    - ”Back-up” og reserveløsninger
    - Kryptering
    - Overvåking og logging
    - Brannmurer
    - Anti-virus programmer
- Krav og kontroll til underleverandører (SLA)
- Organisering i banken– ansvarsfordeling
- Rutiner og prosedyrer
- Risikostyring
- Håndtering og gransking av uønskede hendelser
- Oppfølging av sikkerhetstiltak
- Krav og kontroll til underleverandører
- Atmosfære (sikkerhetskultur)
- Risikoforståelse og bevissthet
- Håndtering og gransking av uønskede hendelser
- Holdninger & adferd
- Helhetlig sikkerhetstilnærming
- Ressurser
- Fokus (prioritering av informasjonssikkerhet)
- Etterlevelse av regelverk - Compliance
- Beredskapsplaner
- Øvelser
- Intern og ekstern kontroll

Vedlegg 2

Intervjuguide om MTO-perspektiv på informasjonssikkerhet

Valg av perspektivet og refleksjoner omkring det

1. Hvorfor har dere valgt å bruke et MTO-perspektiv på sikkerhetsarbeidet her i banken?
2. MTO-perspektivet er vel etablert i oljebransjen, men ganske ny i banknæringen, hvorfor tror du det er slik?
3. Hva kan et MTO-perspektiv tilføre banker i deres informasjonssikkerhetsarbeid?
4. MTO ligger i Basel II sin definisjonen for Operasjonell risiko der informasjonssikkerhet i bank inngår :"*risikoen for tap som følge av utilstrekkelige eller sviktede interne prosesser (O) eller systemer (T), menneskelige feil (M), eller eksterne hendelser*", så hvorfor tror du ikke flere banker bruker et MTO-perspektiv på informasjonssikkerhet?
5. Rollenhagen bruker MTO-området blant annet i et systemperspektiv.
   Er dette en synsvinkler som dere i banken bruker? Hvorfor, hvorfor ikke?

Praktisk bruk av perspektivet

6. Hvordan brukes MTO-perspektivet i informasjonssikkerhetsarbeidet i banken?
7. Hva er styrkende med å benytte et MTO-perspektiv?
8. Hvilke utfordringer er det med et MTO-perspektiv, og hvordan jobber dere i banken med disse?
9. Dersom en norsk bank skal starte opp med et systematisk MTO-perspektiv på sitt informasjonssikkerhetsarbeid, hvordan bør de gå frem?
10. Hva tror du er grunnen til at ikke flere banker benytter MTO bevist og systematisk?

Risikostyring og MTO

1. Benyttes MTO-perspektivet i sammenheng med risikostyring i banken?
   Hvordan…hvorfor ikke?
2. Tror du et bayesiansk nettverk kan være et egnet risikoverktøy for å modellere MTO-aspektet av informasjonssikkerhet? Hvorfor, hvorfor ikke?
3. Kan det være andre risikoverktøy som er mer egnet enn bayesiansk nettverk? Hvilke, og hvorfor…hvorfor ikke?