Modell for analyse av IT risiko i bank

Master i Økonomi og Administrasjon

Annelin Thorkildsen
17.06.2013

Universitetet i Stavanger

DET SAMFUNNSVITENSKAPELIGE FAKULTET,

HANDELSHØGSKOLEN VED UIS

MASTEROPPGAVE

STUDIEPROGRAM: **Master i Økonomi og Administrasjon**	OPPGAVEN ER SKREVET INNEN FØLGENDE SPESIALISERINGSRETNING: **Risikostyring** ER OPPGAVEN KONFIDENSIELL? **Nei** (**NB**! Bruk rødt skjema ved konfidensiell oppgave)

TITTEL:

Modell for analyse av IT risiko i bank

ENGELSK TITTEL:

Model for the analysis of IT risks in banking

FORFATTER		VEILEDERE:
Studentnummer: **108332**	Navn: **Annelin Thorkildsen**	**David Häger** **Lasse Berg Andersen**

OPPGAVEN ER MOTTATT I TO – 2 – INNBUNDNE EKSEMPLARER

Stavanger, ……/…… 2013 Underskrift administrasjon:……

Sammendrag

IKT (Informasjons- og kommunikasjonsteknologi) har forandret risikobildet for finansielle institusjoner dramatisk, fra å behandle kontanter over skranke til elektronisk overføring av penger via smarttelefoner. Utviklingen skjer raskt og bankenes utvikling med hensyn til nye produkter er i stor grad teknologidrevet. IT gjør det mulig å flytte store beløp uten at angriper er fysisk i nærheten av banken eller nettbankkundene som rammes. Endringer i kildekode eller implementering av ondsinnet programvare gjør det mulig å stjele mange små beløp fra et stort antall kontoer nærmest ubemerket, eller et stort beløp der hvor kontroller for beløpsgrense mangler eller er satt ut av drift.

IT er ikke bare en risiko med hensyn til direkte økonomisk tap som følge av urettmessig tilgang, men innebærer også risiko for kritiske systemfeil som kan føre til tap av data eller system utilgjengelighet over lengre tid. Avisene forteller stadig om mer eller mindre alvorlige hendelser hvor nettbank eller kortbetaling er satt ut av drift både for private kunder og bedrifter.

IT svikt er en del av operasjonell risiko (oprisk). Med reguleringene i soliditetsverket Basel II ble bankene pålagt å måle operasjonell risiko på lik linje med kredittrisiko og markedsrisiko. Men, det å identifisere og måle operasjonell risiko, som IT risiko er en del av, har vist seg å være vanskelig. Bankenes metoder for kvantifisering av kredittrisiko og markedsrisiko har vært brukt som utgangspunkt, men har vist seg å ikke være egnet for oprisk. Oprisk som faget er i utvikling og det samme er metodene for oprisk styring og kvantifisering. Det er behov for økt kunnskap omkring styring av IKT-risiko og verktøy for kvantifisering av risikoeksponeringen. I denne oppgaven vil forfatteren prøve å gi et bidrag på det området.

Problemstillingen i oppgaven er å utarbeide en kvantitativ modell for analyse og måling av IKT-risiko på AMA-nivå, herunder beregning av økonomisk tap. For å kunne utarbeide en modell var det nødvendig å kartlegge bankenes rammebetingelser for IKT-styring og informasjonssikkerhet, samt å identifisere de mest kritiske IKT-hendelsene i banknæringen.

De mest kritiske IKT-relaterte initierende hendelsene er identifisert og en kvantitativ modell for analyse og måling av IKT risiko er utarbeidet. Funnene i denne oppgaven viser at Bayesianske nettverk er velegnet til formålet. BN som risikostyringsverktøy gir beslutningsstøtte på essensielle spørsmålene som; er risikoen er høy eller lav, hvilke påvirkende faktorer er mest kritiste, hva forskjellen er i risikoeksponering med hensyn til ulike løsninger og i tillegg hvilken risikoreduserende effekt som kan oppnås ved ulike risikoreduserende tiltak.

BN vil på en god måte kunne håndtere både de tekniske og menneskelige aspektene ved styring og måling av IKT-risiko.

Forord

Jeg vil gjerne takke personer som har vært viktige i prosessen og til stor nytte for resultatet.

Takk til;

- David Häger og Lasse Berg Andersen (Universitetet i Stavanger) som har vært til stor inspirasjon. Dere har også gitt meg veldig god og konstruktiv veiledning.
- Stian Ruud Larsen (Sparebank 1 SR-Bank) for informasjon og tilrettelegging.
- Deltakerne som brukte tid i ekspertpanelet for å dele sin kunnskap og erfaring.
- Lars Erik Fjørtoft (Bankenes Standardiserings Kontor – BSK) for engasjement og diskusjon samt innspill på årsakssammenhenger.
- Jeg vil også takke Edouard, Tonja og Torunn som har lest oppgaven og kommet med gode tilbakemeldinger på oppgavens struktur og skriftlige fremstilling

Annelin Thorkildsen

16.06.2013

INNHOLDSFORTEGNELSE

Figurliste

1. INNLEDNING

1.1 Innledning

IKT-risiko (Informasjons- og Kommunikasjons Teknologi risiko) og operasjonell risiko har fått økende oppmerksomhet de senere år ettersom systemene har blitt mer omfattende i bruksomfang og kompleksitet. Samtidig har vi sett en økende grad av eksterne dataangrep. Mange studier innenfor IKT risiko fokuserer i stor grad på ulike typer tekniske angrep, nye former for ondsinnet programvare, DDoS eller trojanere. Det finnes derimot ikke så mange studier som fokuserer på hva som er konkrete IKT tapshendelser for banker i Norge. Internasjonale studier gjelder i stor grad banker av en helt annen størrelsesorden og dette risikobildet er ikke like relevant for mindre banker i Norge. Finanstilsynet, som har tilsyn med bankene, gjør en årlig risiko- og sårbarhetsstudie av norske finansinstitusjoners bruk av IKT. Forfatteren av denne studien har bl.a. konsultert Finanstilsynets rapport i starten av analysen. Denne oppgaven baseres også på et samarbeid og intervju med en lokal bank for å få konkretisert hendelser. I tillegg har vi hatt tilgang til en hendelsesdatabasen fra 6 norske banker. Finanstilsynets ROS-rapport identifiserer generelle risikoområder som finnes gjennomgående hos norske finansinstitusjoner. Funnene og anbefalingene må inkluderes i bankenes risikovurderinger, men det er ikke spesifikt eller håndgripelig nok for vår lokale bank til å jobbe videre med i sitt risikostyringsarbeid. Denne undersøkelse har som formål å konkretisere tapshendelser for norske banker omfattet av Basel II reguleringene. For å analysere og modellere årsakssammenhengene er viktig å ha en klar forståelse av begrepene, og å skille på hva som er årsaker, konsekvenser, influerende faktorer og hendelser.

Arbeidet med denne oppgaven starter med å gjøre rede for bakgrunnen for operasjonell risiko og reguleringen av bankene. Deretter følger strukturen i oppgaven en generell risikostyrings prosess med identifikasjon av tapshendelser, forklaring av årsakssammenhenger og risikoanalyse. Barrierer og kontroller forklares. Det gjøres videre rede for tilgjengelige hjelpemidler på dette området i form av standarder og beste praksis innenfor informasjonssikkerhet, IT-styring og internkontroll. Hver bank må naturligvis vurdere sitt behov for kontroller i forhold til risikoeksponeringen, men mye kan læres fra standarder og rammeverk som har vært utviklet over mange år. Videre vil oppgaven beskrive kvantifiseringen av risikoeksponeringen.

1.2 Operasjonell risiko bakgrunn

Operasjonell risiko var ikke et begrep bankene opererte med før det ble introdusert av baselkomiteen i 2001. Banker og finansinstitusjoner har tradisjonelt vært mest opptatt av kredittrisiko og markedsrisiko. Men, som følge av alvorlige hendelser som terrorangrepet 11.

september, og enorme økonomiske tap i Société Générale og Barings bank som følge av uautorisert handel, har forståelsen for risikobegrepet endret seg. Det er for snevert av bankene å begrense risiko til utelukkende å omfatte til kreditt- og markedsrisiko. Risikostyring må også omfatte operasjonell risiko.

Den operasjonelle risikoeksponeringen har vært økende på grunn av utviklingen i produktene og metodene tatt i bruk i de internasjonale finansielle markedene (Bodur, 2012). Den teknologiske fremgangen de siste 25 årene har vært drivende for utviklingen i de finansielle markedene. Innføringen av derivater som finansielle instrumenter, samt endringen fra manuell til elektronisk handel har ført til økt kompleksitet og versatilitet. I samme periode har det også vært en betydelig deregulering og globalisering av finansmarkedene. Fra 2000-tallet har det vært stor turbulens i markedene og press på bankene.

Flere hendelser med påfølgende store økonomiske tap de senere år har vist oss viktigheten av styring av operasjonell risiko. Société Générale var en av Frankrikes eldste og mest prestisjefylte banker før katastrofen inntraff. I januar 2008 ble det klart at en enkeltstående finansmegler hadde påført banken et tap på 4,9 milliarder euro. Han hadde gått utover sitt mandat og arrangert flere store transaksjoner i 2007-2008 som kom ut av kontroll og endte med et historisk stort tap for denne type handel. For å kunne gjennomføre svindelen ble det påstått at megleren hadde forfalsket dokumenter og lagt inn falske data i datasystemene, men Jérôme Kerviel selv hevdet at banken var klar over hans handlinger og stilletiende godtok det så lenge resultatet var skyhøy inntjening for bankens del.

Barings Bank var Englands eldste handelsbank etablert i 1762. Banken hadde overlevd både depresjonen og to verdenskriger. Banken kollapset likevel i 1995 etter at en megler påførte banken et tap på 827 millioner pund som følge av uautorisert derivat handel ved bankens avdeling i Singapore. Megleren, Nick Leeson, prøvde å dekke inn tap han tidligere hadde påført banken ved å ta enda større risiko i nye transaksjoner, noe som viste seg til slutt å gå forferdelig galt. I ettertid har det kommet frem at Nick Leeson hadde rollen både som leder for meglerne på avdelingen og samtidig var ansvarlig for å overholde korrekt regnskap. Vanligvis ble disse to stillingene besatt av 2 forskjellige personer for å sørge for en ryddig deling av funksjoner og ansvar. I dette tilfellet både kontrollerte og godkjente Nick Leeson sine egne transaksjoner. Det manglet med andre ord både internrevisjon og risikostyring.

Operasjonell risiko defineres iht. til Baselkomiteen som ”Risikoen for tap som følge av utilstrekkelige eller sviktende interne prosesser eller systemer, menneskelige feil, eller eksterne

hendelser" (Finanstilsynet, 2008). Definisjonen inkluderer juridisk risiko, men ekskluderer strategisk risiko samt omdømme risiko.

Definisjonen inkluderer svikt i interne systemer. Informasjons og kommunikasjons teknologi (IKT) har fått en stadig økende betydning for de fleste finansinstitusjoner ettersom skranke og kontanter er blitt erstattet med elektroniske transaksjoner. Satt på spissen kan man si at bankene kun har noen få fysiske produkter, som bankkort og kredittkort, resten er IKT systemer. Milliarder av kroner ligger på en harddisk og skal være tilgjengelig 24/7 for kundene. På bakgrunn av den teknologiske utviklingen har IT-sikkerhet fått et kontinuerlig økende fokus. Med god grunn fordi bankene og den nye teknologien er et yndet mål for mennesker som urettmessig prøver å tilegne seg andres penger. Systemsvikt kan oppstå både som følge av planlagt svindel fra eksterne eller interne ressurser, eller utilsiktede systemfeil som kan oppstå som følge av manglende rutiner og internkontroll.

IT svikt kan lede til betydelige tap. En relativt ny hendelse som eksemplifiserer dette er hentet fra finansselskapet Knight Capital. Knight Capital er et amerikansk globalt finansselskap. Selskapet fikk smertelig erfare konsekvensene av IKT-risiko i august 2012 etter at bedriften hadde installert et nytt «trading software», en såkalt aksjerobot. Programvaren fikk utilsiktede virkninger på den måten at applikasjonen igangsatte hundrevis av feilaktige kjøps- og salg transaksjoner. Før selskapet fikk stoppet de automatiske transaksjonene og ryddet opp, førte feilen til et tap på 440 millioner dollar. Selskapets aksjeverdi sank med 53% fra den ene dagen til den andre.

Et annet eksempel på operasjonell risiko som følge av svikt i IT-systemer er fra United Airlines i 2007. Selskapet opplevde avbrudd i et forretningskritisk system som førte til en kansellering av mer enn 20 avganger og forsinkelser i 250 avganger. Til sammen medførte svikten et tap på over 10 millioner dollar (Goldstein, Chernobai, & Bernaroch, 2011).

Som en konsekvens av store tap utløst av operasjonell risiko innførte baselkomiteen krav til kapitalavsetning for risiko. Dette ble gjort for å sikre bankenes soliditet og stabilitet. Basel II er en internasjonal standard og veiledning som danner grunnlaget for implementering av nasjonale krav til kapitaldekning og risikostyring i bank. I Basel II ble bankene pålagt å holde kapital for operasjonell risiko på lik linje med kredittrisiko og markedsrisiko. EUs direktiv for kapitaldekning ble innført i Norge fra 1. januar 2007.

Denne studien omhandler IKT-risiko innen bank og finans, og er en del av et større forskningsprosjekt ved Universitetet i Stavanger. Forskningsprosjektet " Operasjonell Risiko i Bank og Finansindustrien (oprisk)" ved UIS var opprinnelig finansiert og drevet av en samling av seks norske banker, Finanstilsynet, UIS og Norges Forskningsråd. Prosjektet var motivert av de nye

kapitaldekningsreglene. Forskningsprosjektet søker å gi økt kunnskap omkring emnet operasjonell risiko samt verktøy for beregning og styring av operasjonell risiko. Prosjektet hadde oppstart i 2007 med varighet til 2011. Prosjektet er nå videreført inn i en fase 2 med varighet til 2014.

1.3 Mål

Formålet med denne oppgaven er å utarbeide en modell for kvantitativ analyse av IKT risiko som også støtter risikoidentifikasjonsprosessen. Modellen skal i tillegg fungere som beslutningsstøtte for risikostyring og skal tilfredsstille kravene til "Advanced Measurement Approaches" (AMA) som er anbefalt av Baselkomiteen. Modellen skal være et verktøy i bankens daglige risikostyrings- og beslutningsprosesser ved at den reflekterer effekten av barrierer og alternative løsninger, og i tillegg benyttes til å beregne regulatorisk kapital. Det er et poeng i seg selv at det er samsvar mellom den løpende vurderingen og håndteringen av operasjonell risiko og beregnet regulatorisk kapital.

Videre er hensikten med denne studien å beskrive årsakssammenheng samt influerende faktorer på det som oppfattes som de mest kritiske IKT-relaterte initierende hendelsene. Oppgaven skal også resultere i en modell som skal kvantifisere potensielle IKT-tap.

Konkret skal denne oppgaven:

- Kartlegge bankenes rammebetingelser for IKT-styring og informasjonssikkerhet (regelverk og standarder)
- Kartlegge kritiske IKT-hendelser i banknæringen
- Utarbeide en kvantitativ modell for analyse og måling av IKT-risiko på AMA-nivå, herunder beregning av økonomisk tap

Proaktiv risiko styring gjøres best ved en detaljert forståelse for forretningsprosessene, visualisert ved detaljerte kausale modeller (Häger D. , Andersen, Aven, & Bø, 2007). For å få en best mulig forståelse for forretningsprosessene samt årsakssammenhengene baserer forfatteren av denne studien modelleringen av de mest kritiske initierende IKT-hendelsene på informasjon fra et samarbeid med en lokal bank. Modellen er generisk i sin utforming ved at forfatteren tatt utgangspunkt i "beste praksis" og etablerte standarder for IKT-risikostyring og internkontroll.

1.4 Omfang

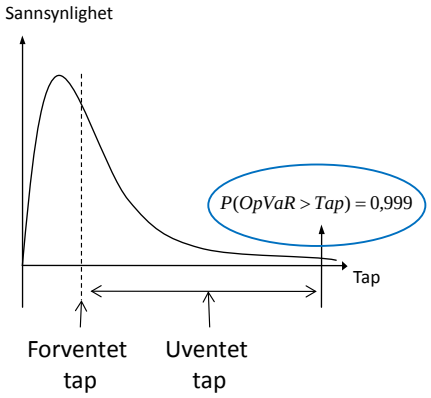
IKT-risiko innenfor bank og finans er et omfattende emne. Under arbeidet med oppgaven har forfatteren fått forståelse for at området er mer utstrakt enn først antatt. Det ville for eksempel være

mulig å skrive en oppgave utelukkende om bankenes betalingssystemer. Denne oppgaven forsøker å dekke operasjonell risiko generelt for alle bankens IKT systemer som har betydning for viktige forretningsprosesser. Allikevel er det er nok betalingssystemene som har fått størst fokus i oppgaven gitt at de utgjør størst risikoeksponering. Betalingsformidling rangeres av bankene selv som den høyest prioriterte prosessen å få tilbake i drift ved en eventuell systemutilgjengelighet. Bankenes IKT-systemer er nært knyttet til leverandørers systemer ved integrasjon, det er derfor naturlig i denne sammenheng å se på den helhetlige risiko dette utgjør. En svikt hos leverandøren vil gi direkte konsekvenser for bankens egne systemer.

Forfatteren har valgt å ekskludere «misbruk av informasjon» i denne oppgaven. Oprisk definisjonen omfatter heller ikke omdømme risiko eller strategisk risiko.

1.4.1 Lav frekvente tap med høy tapsalvorlighet

De fleste operasjonelle tapene innenfor både IT og andre operasjonell risiko kategorier forekommer ofte og fører til begrensede økonomiske tap (Hinz, 2005). Se figur 1. Eksempler på dette kan være mindre systemfeil som fører til utilgjengelighet i betalingssystemene i kortere perioder.



Figur 1 Tapsfordeling – forventet tap og uventet tap.

Figur hentet fra forelesningspresentasjon MOS140 Styring av operasjonell risiko, februar-2012.

Denne oppgaven vil imidlertid fokusere på lav-frekvente tap som potensielt kan lede til store økonomiske tap. Beregningene i modellen for IKT oprisk kapital skal innbefatte forventningen til uventet tap. Lav-frekvente tap med høy tapsalvorlighet kjennetegnes ved at finnes lite historiske data både internt og eksternt, følgelig er det derfor en større utfordring å beregne sannsynlighet for disse hendelsene.

1.5 Videre kapittelinndeling

Oppgaven er strukturert på følgende måte;

Kapittel 2, introduserer rammebetingelsene for bankene. Først overordnet mht. soliditetsverk for operasjonell risiko, Basel II og AMA, så i forhold til informasjonssikkerhet ved IKT-forskriften.

Kapittel 3, omhandler IKT spesifikk operasjonell risiko. Litteraturgjennomgangen tar for seg hva som er gjort tidligere mht. å kvantifisere IKT risiko. Kapittelet forklarer hva informasjonssikkerhet er og hvordan det kan styres. Anerkjente standarder for IT styring (governance) og informasjonssikkerhet presenteres.

Kapittel 4, tar for seg risikoidentifikasjons prosessen.

Kapittel 5, introduserer bayesiansk nettverk som valgt metode.

Kapittel 6, modellering for kvalitativ og kvantitativ analyse, forklaring av modell og diskusjon, eventuelle svakheter i modellen introduseres. Kapittelet omhandler følgelig sannsynlighetsfordeling og tapsprediksjon. Videre gjennomgås validering av modellen.

Kapittel 7, konklusjon

Kapittel 8, forslag til videre arbeid.

2. REGULATORISKE KRAV

2.1 Soliditetsregelverk for banker

For å styrke stabiliteten i det finansielle system har myndighetene lovpålagt finansinstitusjoner bedre risikostyring og kontroll samt nye kapitalkrav. «The Basel Committee on Banking Supervision» er et organ for globalt samarbeid om banktilsyn. Komiteen består av representanter fra sentralbanker og tilsynsmyndigheter fra medlemslandene globalt. Komiteen har ikke overnasjonal myndighet, men jobber for en global standard for tilsyn (Basel Committee on Banking Supervision, 2009). Retningslinjene fra Baselkomiteen har etter hvert dannet grunnlag for bankreguleringen i store deler av verden, deriblant Norge. Baselkomiteen introduserte sitt første forslag til en harmonisert internasjonal standard for kapitaldekningsregler for banker (The Basel Capital Accord) i 1988, Basel I. Den internasjonal standarden hadde også som formål å oppnå like konkurransevilkår. Komiteen ga videre ut den reviderte versjonen Basel II i 2004. De nye kapitaldekningsreglene for finansinstitusjoner trådte i kraft i Norge fra 1. januar 2007.

Reguleringene er basert på ett EU-direktiv som ble innført i Norge gjennom EØS-avtalen. Regelverket fører til større samsvar mellom hvordan myndighetene setter krav til kapitaldekning i finansinstitusjonene, og metodikken finansinstitusjonene benytter når de beregner kapitalbehovet. Basel II innebærer krav til risikostyring og internkontroll, herunder krav til interne prosesser for vurdering av risikoeksponering og kapitalbehov (ICAAP - Internal Capital Adequacy Assessment Process). Foretak som er underlagt kapitaldekningsregelverket skal i tillegg til å oppfylle minstekrav til ansvarlig kapital etter pilar 1, regelmessig gjennomføre en intern kapitalvurderingsprosess ICAAP, pilar 2, for å ta stilling til kapitalbehov. Basel II "Capital Accord" åpnet for er et mer risiko sensitivt rammeverk enn tidligere, og gir flere muligheter for måling av operasjonell risiko. Rammeverket har til hensikt å motivere banker til å jobbe for en kontinuerlig forbedring av risikostyring samt evnen til å måle risikoeksponeringen på en slik måte at kapitalavsetningen er mer i tråd med risikoeksponeringen.

Basel II og Basel III er et risikobasert soliditetsregelverk, som stiller krav til integrasjon mellom bankenes strategier, forretningsplaner, risikostyring og kapitalstyring. De består av 3 pilarer som omfatter:

- Pilar 1: minimumskrav til soliditet
- Pilar 2: Krav til risikostyring og internkontroll, herunder krav til interne prosesser for vurdering av risikoeksponering og kapitalbehov (ICAAP)
- Pilar 3: krav til offentliggjøring av informasjon

De tre pilarene utgjør regelverket bankene må forholde seg til mht. operasjonell risiko. Basel II stiller krav til en gitt minimumskapital i forhold til sin eksponering for operasjonell risiko. Kravet til kapital kan beregnes enten etter standardiserte modeller (basis- og sjablonmetoden), eller mer avanserte, intern utviklede modeller (AMA-modeller).

Basel III vil bli innarbeidet i EUs kapitaldekningsdirektiv (CRD IV) som vil bli gjennomført i norsk lov. Planen var at CRD IV skulle gjelde fra årsskiftet 2012/2013. På nåværende tidspunkt er ikke Basel III innført i norsk lovgivning. Finansdepartementet foreslo i mars 2013 nye lovregler som innebærer økte minstekrav til kapital i finansinstitusjoner og verdipapirforetak og nye bufferkrav for banker og verdipapirforetak m.fl. Finansdepartementet foreslår at reglene skal gjelde fra 1. juli 2013 (Finansdepartementet, 2013). Basel III vil på lik linje som Basel II være et risikobasert soliditetsverk, og innebærer ikke endringer i kapital krav knyttet til operasjonell risiko sammenlignet med Basel II.

2.1.1 Avanserte målemetoder (AMA)

Reguleringene i Basel definerer 3 metoder for beregning av kapitalkrav for operasjonell risiko. De aktuelle metodene er; basismetoden, sjablongmetoden og avanserte målemetoder (AMA), hvorav sistnevnte AMA i størst grad sikrer samsvar mellom risikoeksponering og kapitalavsetning.

Metoden for beregning av kapitalkrav og styring av operasjonell risiko iht. AMA metoden skal godkjennes av myndighetene for hver bank før de evt. kan tas i bruk. Det stilles flere krav til metoden for at den skal bli godkjent. Kravene innebærer blant annet at aktuelle banker må ha implementert sunne prinsipper for risikostyring. Det må videre være et styre- og ledelses engasjement. Banken må også ha en uavhengig risikostyringsfunksjon og foreta en omfattende og systematisk tapsregistrering og registrering av nesten hendelser. Banken må utover dette ha minimum 5 års datahistorikk av denne type hendelsesrapportering. Et AMA system for måling og styring av operasjonell risiko skal fange opp og ta hensyn til alle forventede og uventede tapshendelser for virksomheten over en ettårs periode innenfor et konfidensintervall på 99,9%. Det vil si at det skal være mindre enn 0,1 % sannsynlighet for at det skal påløpe samlede operasjonelle tap i løpet av ett år som overstiger det kapitalkrav som beregnes og settes av etter en AMA modell. AMA metoden skal også reflektere endringer i risikoeksponeringen som følge av daglig risikostyringsarbeid. Det er også et krav til AMA metoden er at den er basert på 4 informasjonskilder:

- Eksterne data
- Interne data
- Forretningsmiljø og interne kontroll faktorer
- Scenario analyse

I tillegg så stilles det krav til ”use test”. Dette innebærer at bankens rammeverk for styring av oprisk skal være integrert i bankens daglige risikostyrings- og beslutningsprosesser. Det fordrer at risikomåling integreres med den løpende risikostyringen slik at risikomåling gir en læringssløyfe tilbake til forretningsområdene og utgjør reell beslutningsstøtte i virksomheten. Måling skal være integrert med daglig risikostyring fremfor å være en isolert prosess knyttet til beregning av regulatorisk kapital.

Retningslinjene for AMA (Basel Committee on Banking Supervision , 2011) fastsetter derimot ikke hvilken metode som skal benyttes for å oppfylle retningslinjene, men viser til at operasjonell risiko er et fag under utvikling og det samme er metodene for beregning av risikosensitiv kapital. Hvordan man skal kombinere de ulike informasjonskildene i beregningene er i liten grad redegjort for. Det

sies heller ikke noe om hvordan risikoeksponeringen basert på de ulike kildene skal vektes i forhold til hverandre. De mest brukte kvantitative metodene hittil har fokus på objektive risikotall og baserer seg på teknikker fra forsikringsbransjen samt metoder benyttet for å beregne markedsrisiko og kredittrisiko.

2.2 IKT forskriften

IKT-forskriften fordrer at finansinstitusjoner fastsetter kriterier for akseptabel risiko forbundet med bruk av IKT-systemene og at bankene foretar en årlig risikoanalyse. Vi finner en del sammenfallende punkter angående IT-styring og informasjonssikkerhet fra standardene som beskrives i kapittel 3.3 i denne oppgaven. Det er derimot verdt å trekke frem spesifikasjonene som kom i tillegg i et rundskriv fra Finanstilsynet 2011. Her setter Finanstilsynet økte krav til bankene. Bakgrunnen for kravene var driftsproblemene som bankene opplevde i påsken 2011, som synliggjorde sårbarheter i transaksjonskjeden, og viste nødvendigheten av at bankene tar tydeligere ansvar for den delen av transaksjonskjeden som driftes av eksterne leverandører (Finanstilsynet, 2011).

Bankene plikter å gjøre en helhetlig kartlegging av kritiske komponenter i IKT-infrastrukturen som representerer kritiske funksjoner slik at betalingssystemer og kundereskontrovirksomheten har tilstrekkelig tilgjengelighet.

Bankene skal også sikre samordnet beredskap mellom banken og leverandøren, inkludert gjennomføring av øvelse.

Bankene skal også gjøre rede for hvordan den enkelte bank vil sikre seg en mer direkte deltakelse i endringshåndteringen hos leverandøren. Dette gjelder der bankenes løsninger er direkte berørt i endringene, og for kritiske komponenter som direkte kan berøre bankenes betalingssystemer og/eller kunde-/reskontroområdet.

Ellers så er viktige punkter i IKT-forskriften det som omhandler kontinuitetsplaner. Forskriften stiller krav til en kontinuitetsplan med bakgrunn i risikoanalysen. Dette innebærer at hvis risikoen endrer seg, må man vurdere på nytt påvirkningen på kontinuitetsplanen. IKT-forskriften stiller krav til dokumentert katastrofeplan, samt at det minst en gang årlig gjennomføres opplæring, øvelse og test i et omfang som gir tilstrekkelig trygghet for at katastrofeløsningen virker som forutsatt. Det er derimot ikke spesifisert hva som menes med tilstrekkelig.

Et annet punkt som bør trekkes frem er det forskriften sier om utkontraktering. Bankene har ansvar for at IKT-virksomheten oppfyller alle krav som stilles etter denne forskrift. Dette gjelder også der hele eller deler av IKT-virksomheten er utkontraktert. Skriftlige avtaler skal sikre dette og avtaler skal sikre innsyn og mulighet til å kontrollere leverandørens aktiviteter tilknyttet avtalen. Avtaler må også omfatte håndtering av taushetsbelagt informasjon. Bankene må også sikre at organisasjonen selv eller i formelt samarbeid med andre enn IKT-leverandøren, besitter tilstrekkelig kompetanse til å forvalte utkontrakteringsavtalen.

I Rundskriv 14/2010 om "Utflytting av bankenes IKT-oppgaver", legger Finanstilsynet til grunn klare begrensninger i utkontraktering til områder som betegnes som høyrisikoområder.

For å begrense omfanget av denne oppgaven er ikke «Lov om betalingssystemer m.v.» (betalingssystemloven), heller ikke «Lov om behandling av personopplysninger» (personopplysningsloven) redegjort for i oppgaven. Dette er også reguleringer som er som bankene må rette seg etter og som har betydning for sikkerhetsarbeidet.

3. OPERASJONELL RISIKO OG IKT

I henhold til Basel II reguleringene så er finansinstitusjoner pliktet til å overvåke og måle sin operasjonelle risikoeksponering innenfor 7 tapshendelseskategorier (Kredittilsynet, 2007).

Svikt i IT systemer utgjør kun en del av operasjonell risiko, men som tabellen viser så kan IT tapshendelser gjøre seg gjeldende i alle de definerte Basel tapshendelseskategoriene (Goldstein, Chernobai, & Bernaroch, 2011). De fleste arbeidsprosesser vi finner i bankene skjer ved bruk av IKT-systemer.

Basel tapshendelseskategorier	Definisjon (ifølge norsk forskrift)	Eksempler på operasjonell risiko knyttet til IT hendelser
Internt bedrageri	Tap som følge av handlinger med sikte på uberettiget å tilegne seg midler eller omgå lovgivning eller virksomhetens mål unntatt hendelser knyttet til forskjellsbehandling.	Ansatt som selger konfidensiell eller sensitiv informasjon. Megler som utfører uautorisert handel ved å utnytte smutthull i IT systemet for å skjule tap.
Eksternt bedrageri	Tap som følge av handlinger som har til hensikt å bedra, uberettiget tilegne seg midler eller omgå lovgivningen, begått av en tredjepart.	Hackere som får tak i sensitiv data til tusener av kunder. Data virus/orm som angriper telefon, internett, og nettbank som fører til driftsavbrudd i tjenester.
Ansettelsesvilkår og sikkerhet på arbeidsplassen	Tap som følge av hendelser som er i strid med lovgivning, forskrifter og avtaler om arbeidsmiljø, utbetaling av erstatninger som følge av personskade	Ansatt tar med seg verdifull kunde-opplysninger før han/hun slutter og begynner i en konkurrerende bedrift.

	eller andre forhold.	
Kunder, produkter og forretningspraksis	Tap som følge av utilsiktede handlinger eller unnlatelser som medfører manglende oppfyllelse av en forpliktelse overfor bestemte kunder (herunder tillits- og egnethetskrav), eller som følge av produktets art eller utforming.	Meglerhus overtrer lovreguleringer på grunn av systemfeil. Bank mislyktes i å implementere systemer i samsvar med lovreguleringer mot hvitvasking.
Skade på fysiske eiendeler	Tap som følge av skade på, eller tap av, fysiske eiendeler i naturkatastrofer eller andre begivenheter.	Brudd i fiberkabel i nettverket fører til utilgjengelighet i nettbank.
Avbrudd i drift og/eller systemer	Tap som følge av driftsavbrudd eller systemfeil.	En tastefeil gir en innledende børsnotering (IPO) av en multi-million aksje på Nasdaq til $0,01 pr aksje i stedet for original prisen på $19,50 pr aksje.
Oppgjør, levering og annen transaksjonsbehandling	Tap som følge av utilstrekkelig eller sviktende transaksjonsbehandling eller systemer for transaksjonsbehandling med handelsmotparter og leverandører.	Mangelfull overholdelse av regler for personvern iht. personopplysningsloven på grunn av systemfeil som gjorde at sensitive opplysninger ble sendt til feil mottaker. Dette er konsesjonsbelagt for bankene, og mislighold kan føre til tap av konsesjon.

Tabell 1: Basel grupperinger operasjonell risiko.

IKT operasjonell risiko defineres motsatt av informasjonssikkerhet dvs. IKT risiko er alle trusler som kan føre til svikt i konfidensialitet, integritet og tilgjengelighet av informasjons og kommunikasjons ressurser (Goldstein, Chernobai, & Bernaroch, 2011).

3.1 IT risikostyring - litteratur gjennomgang

IT risikostyring har sin bakgrunn i amerikansk militære og etterretningstjeneste på 70-tallet, og ulike standarder ble utviklet med tanke på informasjonssikkerhet. Utgangspunktet både i «Security controls for computer systems» fra Defense Science Board som ble publisert i 1970, og National Institute of Standards and Technology (NIST) fra 1983 var data sikkerhet og konfidensialitet. Det var mindre fokus på stabilitet og tilgjengelighet. Da ISO standarden kom i 1999 var fremdeles fokus sikkerhetsaspekter som konfidensialitet, integritet og tilgjengelighet. Senere ble risikostyring innenfor IT-prosjekter mye diskutert i litteraturen, med forskjellige metodikker for utvikling og implementering (Hinz, 2005).

Gjennomgang av eksisterende litteratur viser at det derimot har vært lite fokus kvantifisering av IT risiko.

Standarden ITIL (The Information Technology infrastructure Library) som lansertes på 1980-tallet introduserer et nytt element «IT Service Continuity Management» (ITSCM). Hensikten med ITSCM er å støtte bedriftens generell kontinuitetsplaner ved å sikre at nødvendige IT tekniske og

service fasiliteter (nettverk, applikasjoner, helpdesk etc.) er tilbake i drift innen fastsatt ramme. ITSCM fokuserer på katastrofe hendelser, og for hver forretningsenhet gjøres det en «Business Impact Analysis» (BIA) for å kvantifisere hva tapet av IT-tilgjengelighet vil ha på virksomheten (Guo, Zhan, Wang, & Zhao, 2012). Tapet kan måles enten i økonomisk tap, tap av relasjoner eller tap av konkurranseevne. Risikoeksponeringen fra en trussel er et produkt av sannsynligheten for at et angrep vil inntreffe, sannsynligheten for påvirkende faktorer, og kostnaden av at et angrep lykkes. I denne sammenhengen sees IT risiko som en integrert del av bedriftens totale risikoeksponering, en bør unngå silo tankegang som ser på risiko adskilt pr avdeling. En vurderer det slik at IT påvirker alle prosesser i bedriften. Systemene blir stadig mer integrert i motsetning til tidligere da det var mer vanlig med frittstående applikasjoner. IT risiko hendelser har utviklet seg fra å være marginale tekniske problemer, til å bli mer og mer et forretningsproblem som kan påvirke bedriftens konkurranseposisjon og strategiske mål (Spremic, 2012). Evalueringsmodeller som for eksempel fra NIST (National Institute of Standards and Technology) benyttes til å kalkulere tekniske tiltak for risiko, men målet bør i stedet være å evaluere den mulige påvirkningen trusselen har på bedriftens prosesser eller evne til å nå sine mål (Spremic, 2012). Dette kan gjøres bl.a.ved «Business Impact» analyser.

Det er flere som taler for at IT risiko burde bli inkludert i en helhetlig risikovurdering av virksomheten. IT risiko må løftes utover prosjekt nivå. IT strategisk risiko sier noe om IKT's evne til å påvirke virksomhetens evne til å implementere strategi for å nå bedriftens overordnede mål (Ginzberg & Moulton, Information Technology Risk Management, 1990). IKT-styring bør sikre at IKT tilfører verdi med hensyn til å nå virksomhetens strategiske mål, at infrastrukturen er hensiktsmessig og at risikoeksponeringen ved valg av ulike alternativer er akseptabel. Til tross for at bankenes transaksjoner blir mer og mer automatiserte og avhengigheten av informasjonsteknologi øker, så er forskningen på identifisering og minimering av operasjonell risiko innenfor IT relativt begrenset. Dette etterlater IT-ledere med minimalt med beslutningsstøtte for dette området (Hinz, 2005).

Utviklingen av verktøy for beslutningsstøtte og å kvantifisere IT risiko er i større grad relevant i takt med utviklingen av CIO'ens rolle fra levering av bits og bytes til å levere forretningsverdi. IKT er en integrert del av alle funksjoner og avdelinger. Bankenes utvikling fremover mht. nye produkter og tjenester vil sannsynligvis være teknologi drevet eller teknologi tilrettelagt. Denne utviklingen innebærer at risikostyring som kompetanse bør styrkes i IT-avdelingene. IT strategi bør forstås som kryss-funksjonell ved at den omfatter produkter, prosesser og menneskelige ressurser og er sammenfallende med bedriftsstrategien (Öbrand , Augustsson, Holmström, & Mathiassen, 2012).

3.2 Informasjonssikkerhet

Dette kapittelet har til hensikt å definere hva informasjonssikkerhet er, og hvilken betydning det har for IKT-risikoeksponeringen.

Økt bruk av IKT gjør at bankene blir mer sårbare. Truslene mot IKT-systemene øker, og angrepene blir stadig mer avanserte. For dagens virksomheter er operasjonell risiko i stor grad knyttet til IT-systemene. Dette henger sammen med at de fleste forretningsprosesser er helt avhengig av IT. Med informasjonssikkerhet mener vi at informasjonen er beskyttet mot uønsket innsyn, at den er tilgjengelig når den trengs, og at den er beskyttet mot uønskede endringer.

Bankene er avhengige av tillit fra næringslivet, private kunder og samfunnet for øvrig for å bevare sitt omdømme og muligheten til å drive forretning. Det er essensielt at bankenes nettverk og systemer er sikre og stabile til enhver tid slik at de digitale tjenestene fungerer. Betalingsformidling og betalingstjenester utgjør en betydelig del av samfunnets kritiske infrastruktur og funksjoner (Finanstilsynet, 2012). Den teknologiske utviklingen og finanssektorens innføring og bruk av mer komplekse tjenester gjør arbeidet med risiko mer krevende både for den enkelte virksomhet og for myndighetene. Ny teknologi inneholder ofte ukjente sårbarheter som i en tidlig fase både kan utnyttes av kriminelle og føre til feilsituasjoner (Finanstilsynet, 2012).

IKT-sikkerhet er et stort område, og det er ikke alle sikkerhetsbrudd som leder til økonomiske tap. Bankenes forretningsidé er i stor grad å tjene penger på å ta risiko. Noe risiko må en med andre ord være villig til å ta. For å være konkurransedyktige så må bankene tilby kundene den funksjonalitet og de produktene som etterspørres, følgelig blir IKT-sikkerhet en avveining mellom risiko og graden av brukervennlighet. Det må være en riktig balanse mellom sikkerhet og kostnader. For at en skal vite hvor det er mest hensiktsmessig å sette inn sikkerhetstiltak, dvs. hvor hver krone investert gir mest effekt i form av forhindret økonomisk tap, så må en vite noe om hva som er de mest kritiske IKT risikoene. Hvilke hendelser er det som potensielt kan utløse et økonomisk tap? For å være orientert mot fremtiden og fremtidige hendelser, bør en ikke bare se på historiske data og anta at fremtiden vil se lik ut. Analysen bør også ta i betraktning utviklingstrekk i samfunnet generelt samt den teknologiske utviklingen..

Akseptabelt risikonivå kan ikke oppnås ved utelukkende å ivareta den systemtekniske sikkerheten. Informasjonssikkerhet krever tiltak på mange fronter både når det gjelder teknologi, retningslinjer, holdninger og kultur (Datatilsynet, 2012). Det er et tverrfaglig felt som omfatter både teknisk kunnskap om maskinene og systemene, i tillegg til eksempelvis psykologien omkring svindel.

Ofte kan trusselen komme innenfra i form av dårlig kultur. I denne sammenhengen er det viktig å ha ansvarsdeling, gode retningslinjer og en god risikokultur og risiko bevissthet i organisasjonen. Holdningene og bevisstheten blant de ansatte har stor betydning for informasjonssikkerheten. Man kan si at menneskene og deres oppførsel faktisk betyr mer for informasjonssikkerheten enn alle mulige tekniske løsninger. Avgjørende for kvaliteten på styringssystemet for informasjonssikkerheten er etterlevelse og kultur. Her har ledelsens handlinger eksempelets makt.

En studie med data fra 1980-2005, på hva som var avgjørende faktorer for operasjonell risiko i amerikanske finansielle institusjoner viser at de fleste operasjonelle tapene kan spores tilbake til svakheter og mangler i internkontrollen (Chernobai, Jorion, & Yu, 2011).

Som beskrevet i ISO 27002 seksjon 0.2 så er mange informasjonssystemer ikke laget med spesielt fokus på å være sikre. Det er også slik at sikkerheten som kan oppnås gjennom tekniske virkemidler er begrenset. Sikkerhetsarbeidet bør derfor også være støttet av hensiktsmessig ledelse og rutiner (NS-ISO/IEC, 2005).

Informasjonssikkerhet betyr at virksomheter skal sikre opplysninger med hensyn til konfidensialitet, integritet og tilgjengelighet (Datatilsynet, 2012). Det kontinuerlige og systematiske sikkerhetsarbeidet er en del av virksomhetens internkontroll. ”IT Governance” eller god IT-styring og kontroll på norsk er et rammeverk for å styre virksomhetens bruk at IT (Standard Norge, 2009). God IT-styring og kontroll skal sørge for at bedriften ivaretar både det administrative og det operative, det forretningsorienterte og det prosessorienterte, så vel som det teknisk og ikke-tekniske. God styring med informasjonssikkerhet følger ofte den sekvensielle prosessen; styringssignal fra ledelsen, informasjonsidentifisering, risikovurdering og valg av sikringstiltak. Solid IT ”governance”, risikostyring og ”compliance” vil gjøre det mulig for bankene å redusere den økonomiske kapitalavsetningen ved å minimere risikoeksponeringen. I et langsiktig perspektiv kan det utgjøre et konkurransefortrinn.

3.3 Standarder for IT-styring og informasjonssikkerhet

Standarder for informasjonssikkerhet og IT-styring gir en innføring i «beste praksis» og er veiledning i relevante barrierer og generelt aksepterte sikringstiltak. Det er mye kunnskap å hente mht. hvordan oppnå et effektivt fungerende kontrollmiljøet.

Arbeidet med IKT-risikostyring krever at man kjenner til årsaker til operasjonell risiko, og at man kjenner til de sikringstiltak/risikoreduserende tiltak som kan minimere bankenes risikoeksponering.

Solid IT-styring (IT-governance) danner grunnlaget for god risikostyring. For å forstå hva som ligger i IKT-sikkerhet og IT-governance vil forfatteren av denne oppgaven gå igjennom ”de facto” rammeverk og standarder på området, i tillegg til IKT-forskriften. Hensikten er å sikre at oprisk modellen har generisk/generell anvendelse og dermed kan benyttes av banker med ulik risikoeksponering. Det vil også sikre at modellen inkluderer de mest kritiske barrierene bankene bør ha implementert, og at den innbefatter effekten de har på risikoeksponeringen (iboende risiko og gjenværende risiko/residual risk).

Informasjonssikkerhet spiller en viktig rolle for å beskytte bankenes kapital og sensitiv informasjon. Det finnes ingen enkel formel som kan garantere for 100% sikkerhet, derfor er det behov for ”beste praksis” og allment godkjente standarder for å sikre at en har et tilfredsstillende sikkerhetsnivå. Lovverket gir også føringer for informasjonssikkerhet og risikostyring via IKT-forskriften og Basel reguleringene. Jeg vil presentere noen av de globalt anerkjente rammeverkene og standardene for informasjonssikkerhet. Standardene forfatteren vil gjennomgå er

- COBIT (Control Objective for Information and related Technology).
- ISO/IEC 27001-27002 (Informasjonsteknologi - Sikkerhetsteknikk Administrasjon av informasjonssikkerhet)
- ITIL rammeverk (Information Technology Infrastructure Library)
- IKT-forskriften.

COBIT er et rammeverk for IT-styring som skal sikre at;

- IT er i henhold til forretningsmessige behov og mål
- IT maksimerer forretningsfordeler ved effektiv og innovativ bruk av IT
- IT ressurser utnyttes ansvarlig, og
- IT risikoer er håndtert på en skikkelig måte

NS-ISO/IEC 27001-27002 er en internasjonal standard for styring av informasjonssikkerhet i organisasjoner.

ITIL er et rammeverk for IT service ledelse. Rammeverket skal sørge for kvalitetssikring av leveranse, drift og support innen IT-sektoren.

Generelt kan man si at COBIT og NS-ISO/IEC 27001-27002 hjelper med å definere hva som skal gjøres, og ITIL beskriver hvordan for service ledelse. COBIT kan benyttes på det høyeste nivå av

IT styring, og gir et overordnet kontrollrammeverk basert på en IT prosess modell som er generisk nok til å passe alle bedrifter. Det er også behov for et mer detaljert praktisk rammeverk. Rammeverket ITIL og standarden NS-ISO/IEC 27002 dekker spesifikke områder og kan sammenstilles med COBIT rammeverket noe som gir et hierarki i veiledningsmaterialet (ITGI, 2008). Disse ulike standardene er alle utviklet på bakgrunn av "Beste praksis". ISO 27001/2 (2005) og ITIL v3 komplementerer hverandre. ITIL fokuserer på serviceledelse beste praksis. ISO 27001 og ISO 27002 fokuserer på informasjonssikkerhet bestepraksis. (Warren, 2010). Den delen av ITIL som omhandler sikkerhetsstyring "ITIL Security Management" er basert på ISO/IEC 27002.

Implementerte tiltak skal føre til at restrisikoen blir redusert til et akseptabelt nivå. Standarden anbefaler at ressursene som brukes på sikringstiltak, må veies opp mot de mulige skadene ved sikkerhets svikt, altså en kost/nytt avveining.

Standarder for sikkerhet skal understøtte virksomhetens strategi og være et virkemiddel for risikostyring og kontroll med risiko i virksomheten. Det er også viktig å være klar over at lover og forskrifter stiller konkrete krav til sikkerhet, jfr. For eksempel IKT-forskriften, personopplysningsforskriften og Basel II som gir føring for risikostyring.

IKT-forskriften stiller blant annet krav til risikoanalyse ved at foretakene skal fastsette kriterier for akseptabel risiko forbundet med bruk av IKT-systemene. Når det gjelder kvalitet så skal foretakene ha prosedyrer for oppfølging av fastsatte kvalitetsmål. Med hensyn til sikkerhet så skal foretakene utarbeide prosedyrer som skal sikre beskyttelse av utstyr, systemer og informasjon av betydning for foretakets virksomhet.

Når risikovurderinger er foretatt samt risikohåndtering besluttet, så må egnede kontroller defineres og implementeres. Ut i fra en risikovurdering defineres egnede kontrolltiltak som tiltak for å sikre at forretningsmålene blir nådd og at uønskede hendelser unngås (Information Systems Audit and Control Association (ISACA), 2009). Kontrolltiltak besluttes med utgangspunkt i nevnte rammeverk og standarder. Kontrolltiltak kan deles inn i to hovedgrupper:

- Generelle IT kontroller som er innebygget i prosedyrer og rutiner innenfor; anskaffelse og systemutvikling, endringshåndtering, tilgangsstyring og IT-drift.
- Applikasjonskontroller dvs. kontroller som er implementert i applikasjonene som skal sikre fullstendighet, nøyaktighet, gyldighet, autorisasjon og arbeidsdeling.

Gode kontrolltiltak må både være design effektive og operasjonelt effektive. Med design effektive menes at kontrolltiltak faktisk kontrollerer det de skal kontrollere. Med operasjonelle menes at de

utføres slik de er beskrevet (Standard Norge, 2009). Det må systematiske tiltak til for å undersøke om sikringstiltakene blir etterlevd, om de fungerer som forutsatt og om de over tid er dekkende for endringer i risikobildet.

Operasjonell risiko kan reduseres og/eller elimineres ved å implementere kontroller og risikoreduserende tiltak. Å visualisere årsakssammenhengene i et BN nettverk mht. hvor ting kan gå galt, og hvordan tapshendelser kan oppstå bil gi beslutningsstøtte mht. hvor tiltak bør implementeres. På bakgrunn av analysen av årsakssammenhengene samt beste praksis mht. informasjonssikkerhet er kontroller/barrierer modellert i nettverket. Modellen skal gjenspeile effekten av implementerte kontroller på risikoeksponeringen basert på kontrollenes tilstand og bedriftsspesifikke forhold.

Standardene er for omfattende til å gjengi i denne oppgaven, men hoved retningslinjene, de mest relevante risikoreduserende tiltakene, er inkludert i modellen som barrierer/kontroller i BN nettverket.

4. RISIKOIDENTIFIKASJON

De mest kritiske IKT-relaterte hendelsene for en lokal bank er kartlagt basert på all tilgjengelig informasjon. All informasjon i denne sammenheng omfatter gjennomgang av oprisk prosjektets (forskningsprosjekt ved UIS) hendelsesdatabase (tapshendelser fra 6 banker for flere år tilbake), fag litteratur, egne erfaringer fra arbeid med IKT rådgiving i 10 år, samt en formell risikoidentifikasjons prosess hos en lokal bank. Ut i fra dette har forfatteren kommet frem til hva banken opplever som de mest kritiske IKT-relaterte hendelsene.

Risikoidentifikasjonen ble gjennomført med et ekspertpanel fra en lokal bank. Forfatteren av denne oppgaven sammen med to av de ansvarlige i Oprisk forskningsprosjektet gjennomførte møtet. Fremfor å benytte tradisjonelle sjekklister og/eller risikomatriser, valgte vi en ny måte å gjennomføre den på. Hensikten var å oppnå at deltakerne ikke ble fastlåst i å tenke bare på hva som har skjedd tidligere, men i stedet å oppnå engasjement og kreativitet. Risikoidentifikasjonen bør være framoverskuende og dekke alle vesentlige risikoer. Man bør ta utgangspunkt i all tilgjengelig informasjon, og sette sammen et ekspertpanel med personer fra ulike deler av organisasjonen med ansvar for ulike fagområder, for å få frem ulike perspektiv. Dersom man kun baserer seg på erfaring og historikk vil man kun identifisere hendelser som har inntruffet tidligere. Som vi ser det er faren

med sjekklister at deltakerne blir passive og svarer ja eller nei på spørsmål om risikoer som allerede er kjente, det oppfordrer ikke til å tenke «ut av boksen».

Før risikoidentifikasjonen kan starte, bør det avklares hva analyse objektet er. Dette for å vite helt konkret hva vi analyserer, hvilke hendelser er vi ute etter å identifisere, og hvordan skal vi identifisere disse hendelsene? Analyseobjektet sees i sin kontekst. Vårt utgangspunkt for identifikasjonen er sparebank alliansen og dens underleverandører av IKT-tjenester.

Risikoidentifikasjons møtet ble gjennomført med en bank som Universitetet i Stavanger har opparbeidet relasjoner til tidligere i forbindelse med forskningsprosjektet «Operasjonell Risiko i Bank og Finansindustrien (Oprisk)». Banken har høy fokus på risikostyring og var derfor interessert i å bidra på dette møtet for selv å lære mer. Innkallingen til møtet skjedde gjennom kontaktpersonen i banken, som lettere kan få de ulike deltakerne til å bruke tid på IKT risikoidentifiseringsprosessen. Personene som vi ønsket skulle delta på møtet har en travel timeplan, men det var viktig at alle vi hadde tenkt å inkludere kunne delta samtidig. Deltakerne ble plukket ut fordi de jobber med et bestemt fagområde deres unike erfaring og synspunkter er viktige å ha med i undersøkelsen. Deltakerne bestod av 6 personer fra banken. Kontaktpersonene i banken er Risk Manager og har ansvar for operasjonell risiko. Neste deltaker er leder for IT-drift som selvfølgelig har nær kjennskap til hva som kan gå galt mht IKT. Han er ansvarlig for sikker og stabil drift. Den tredje deltakeren er leder for Løsningsutvikling. Han er ansvarlig for alle nye produkter som lanseres fra banken. Her kommer avveiningen mellom risiko og brukervennlighet/service inn. Den fjerde personen er leder for betalingsformidling. Dette området er kanskje det området som er mest utsatt mht. misligheter og svindel forsøk. Den teknologiske utviklingen skjer også raskt og medfører hyppige endringer, derfor vil hans vurderinger være av stor betydning. Den femte deltakeren er leder for prosess. Han representerer et litt mer overordnet syn, og tenker hele prosessflyten. Og, den sjette deltakeren er Sikkerhetssjef, dvs. overordnet ansvarlig for sikkerhet fysisk og på andre måter for banken. Sikkerhetssjefen og hans medarbeidere har gjort bla. ”business impact” studier av forskjellige risiko scenario for banken.

I forkant av møtet forberedte vi et forslag til årsakssammenhenger, visualisert i et enkelt nettverk med noder og piler. Dette for å få deltakerne til å tenke prosess, og kjenne seg igjen i sine fagområder. Forslaget ble utarbeidet på bakgrunn av Finanstilsynets årlige ROS analyse av finansforetakenes bruk av IKT, bankenes tapshendelsesdatabaser samt standarder for informasjonssikkerhet og IKT styring. Erfaringene vi gjorde oss var at denne fremgangsmåten er et godt utgangspunkt for å få i gang diskusjoner. Visualiseringen av årsaker, influerende faktorer og årsakssammenhenger og konsekvenser fanget interessen, og det var lett for ekspertpanelet å «ta tak

i» og kommentere. Visualiseringen av årsakssammenhengene oppfordrer til å tenke igjennom hva som kan skje dersom ulike hendelser inntreffer. Denne måten å gjennomføre prosessen på førte til at gjennomgangen fulgte en viss struktur, men allikevel oppfordret til kreativitet og meningsutveksling bland de ulike deltakerne.

Vi opplevde at det var en veldig åpen kultur i banken mht. å snakke fritt om hva som kunne gå galt og om ting som hadde gått galt. Man kan tenke seg at når det gjelder å snakke om ting som går galt så vil gjerne ansatte dekke over egne feil, og skyve ansvaret over på andre. Men, vi oppfattet ikke dette som er problem i det hele tatt. Det kan skyldes at banken har hatt fokus på risikostyring lenge og innførte rapportering av uønskede hendelser for flere år siden. De har dermed utviklet en god rapporteringskultur og holdning til risikostyring.

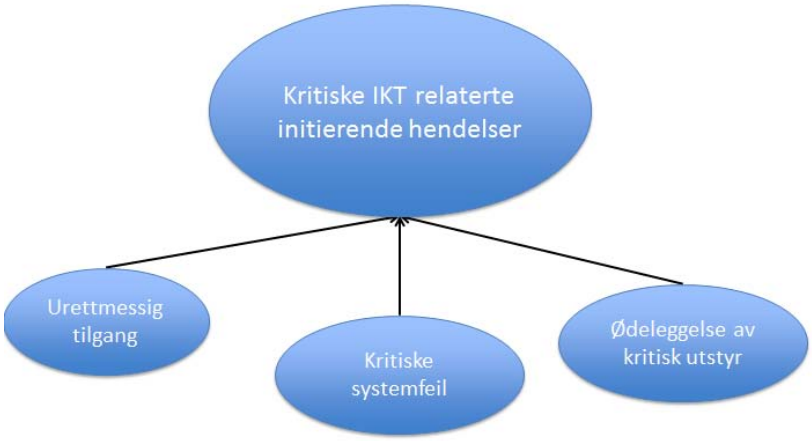
Det som ble identifisert som de mest kritiske hendelsene er;

- urettmessig tilgang
- kritiske systemfeil
- ødeleggelse av kritisk utstyr

Kritiske IKT-relaterte initierende hendelser forstås som de faktiske hendelser eller episoder som initierer risiko. Det er ikke et risikoområde eller årsaker, men en konkret hendelse som initierer et potensielt tap. Denne begrepsavklaringen gjør risikoidentifiseringen og dermed risikoarbeidet håndgripelig, og viser med tydelighet hvor sikkerhetsfokus bør konsentreres. Risikoidentifiserings prosessen klargjorde at det dette er de tre mest kritiske IKT-relaterte hendelsene. Andre faktorer kan i relasjon til disse hendelsene defineres som årsaker, influerende faktorer og konsekvenser.

Kritisk i sammenhengen kritiske systemfeil og kritisk utstyr, defineres som hendelser som kan føre til system nedetid dvs. utilgjengelighet i lengre enn 1-3 dager i systemer som er sentrale for verdiskapningen i bedriften. Og/eller hendelser defineres også som kritiske dersom de potensielt kan medføre et tap på 50 millioner eller mer.

Figuren under viser på et overordnet nivå de viktigste kritiske IKT relaterte initierende hendelsene. Ved å se nærmere på undergrupper og konsepter forklares årsaker og influerende faktorer.



Figur 2: Kritiske IKT-relaterte initierende hendelser.

5. METODE

Metoden for denne oppgaven skal dekke både kvalitativ analyse samt kvantitativ måling. Begrepene sannsynlighet og usikkerhet kan forstås på ulike måter, og av den grunn redegjøres det her for hvilken forståelse som legges til grunn i denne oppgaven. Deretter forklares Bayesianske nettverk som er benyttet for modelleringen.

5.1 Bayesiansk metode

Bayesiansk statistisk metodelære er oppkalt etter den engelske presten og sannsynlighetsteoretikeren Thomas Bayes som ble født 1702 og døde i 1761. Hans statistiske metodelære skiller seg fra klassisk statistisk metode spesielt i vurdering av innsamlet data og sannsynlighetsberegninger. Klassisk statistikk og hypotesetestingsteori er først og fremst egnet til å teste data i de tilfellen hvor det er store mengder historiske data, hvor en har mulighet for å ekskludere andre påvirkningsfaktorer og kan gjenta et eksperiment uendelig mange ganger under like omstendigheter. Slike eksperiment kan oppnås i et laboratorie, men det er ofte ikke mulig med hensyn til operasjonell risiko. Klassisk hypotesetestingsteori er ikke særlig egnet for å danne grunnlag for beslutninger under usikkerhet. I dissse tilfelle ville det være lite hensiktsmessig ikke å ta hensyn til godt skjønn i tillegg til mer konkrete data. For eksempel en lege som vurderer om en pasient skal gjennomgå en hjerteoperasjon, bør ikke bare basere seg på generelle estimater for slike operasjoner er vellykket. Legen må også til dels skjønnsmessig ta hensyn til pasientens fysiske og psykiske helsetilstand. Bayesiansk metode er utviklet for å ta hensyn til ekspert vurderinger og skjønn på en måte som er konsistent med sannsynlighetsregningens regler og er derfor særlig velegnet i forbindelse med beslutninger under usikkerhet (Natvig, 1997).

Kombinering av ulike datakilder og andre typer informasjon blir stadig viktigere i ulike typer analyser. Bayesianske tilnærminger har vist seg særdeles nyttige i slike sammenhenger. Generell Bayesiansk teori, og bruk av Bayesianske metoder for en formell utnyttelse av både (ekspert) kunnskap om den aktuelle problemstillingen og observerte data. Beregning av à posteriori fordelinger via Bayes' formel.

5.2 Sannsynlighet og usikkerhet

På lik linje med markedsrisiko og kreditt risiko så er finansielle institusjoner ifølge Basel II reguleringene pålagt å gjøre kapitalavsetninger for operasjonell risiko. Basert på erfaring bankene har mht. teknikker for måling av markeds- og kredittrisiko ønskes det på tilsvarende måte å oppnå objektive risikotall for operasjonell risiko. Det å oppnå objektive risikotall har vært ansett som svært viktig. På en annen side kan det stilles spørsmål ved om disse metodene, som opprinnelig er basert på forsikringsmatematikk, er egnet til å gi beslutningsstøtte i forhold til operasjonell risiko. Er det rimelig å anta at objektive risiko tall i det hele tatt finnes mht operasjonell risiko? I så fall, hva uttrykker usikkerheten knyttet til risikotallene? Det er ikke en klar felles forståelse for hva som menes med objektivitet. Andersen og Häger i (Andersen & Häger, Objectivity and the Measurement of Operational Risk, Reconsidered, 2011) hevder at det ikke finnes objektive risikotall for operasjonell risiko. De fremhever også at datadrevne modeller ikke er egnet som verktøy på grunn av at de ikke gir noe informasjon om årsakene til at risikoeksponeringen er høy eller lav, forhold som bør fremkomme for å kunne iverksette effektive tiltak for å minimere risikoeksponeringen. Datadrevne analyser utelukkende basert på historiske data ekskluderer viktig kunnskap, og gir ikke nødvendigvis relevant informasjon om hva som vil skje i fremtiden, resultatene kan i verste fall være misvisende. Karakteristikken av data fra oprisk hendelser er anderledes enn hendelser fra markeds- og kreditt risiko eller forsikringsoppgjør. I motsetning til feks tapshendelser innenfor forsikring, kjennetegnes oprisk av få hendelser med potensielt store konsekvenser. Hendelsene er avhengige av omstendighetene og disse endres stadig. Oprisk hendelser som eksempelvis fallet av Barings Bank eller de enorme tapene i Société Générale kunne aldri vært forutsagt eller forventet basert på analyse av historiske data.

Objektivitet kan i en risikostyrings kontekst forstås på to måter. Den ene er at objektivitet forstås som sanne risikotall avledet fra en korrekt eller sann sannsynlighet. Usikkerhet er i denne sammenheng avvik fra en korrekt risikoverdi uttrykket med et konfidensintervall. Den andre forståelsen er at objektivitet er målet på i hvilken grad resultatene er basert på fakta, upåvirket av følelser og/eller personlige fortolkninger.

Men, en statistisk analyse av operasjonell risiko med liten poulasjonen, vil nødvendigvis være preget av antagelser, tolkninger og personlige meninger. Anaylyseresultater med disse forutsetningene kan ikke kommuniseres som objektive. Klassisk sannsynlighetsforståelse forutsetter at hendelser skjer under identiske forhold, at omstendighetene er de samme. Men, i virkeligheten fungerer banker og finansinstitusjoner i et læringsmiljø som gjør at bankene får kunnskap om hvordan de kan unngå hendelser i fremtiden ved å undersøke historiske hendelser. Det er derfor urimelig å anta at det finnes en objektiv sannsynlighet for operasjonell risiko kvantifisering.

Kriteriene for godkjenning av AMA-modeller iht. Basel II setter krav til modellens nøyaktighet, men regelverket spesifiserer ikke nøyaktighet iforhold til hva. Modellen skal også ha et et konfidensintervall på 99,9% over en ettårs periode. Skal konfidensintervallet være et uttrykk for usikkerhet i risiko tallene? I såfall, usikkerhet iforhold til hva? Det kan tyde på at Basel kommitteen henstiller til at det finnes en korrekt eller sann verdi på risiko, og i såfall at konfidensintervallet uttrykker avvik iforhold til den sanne eller korrekte risiko verdi. I kontrast til dette setter Basel II krav til at risikotallene fra AMA modeller ikke bare skal være basert på historiske data, men også scenarioanalyse data og hver enkelt bedrifts forretningsmiljø og interne kontroll faktorer. Begge disse to datakildene er basert på ekspertkunnskap som er subjektiv. Datadrevne modeller er i liten grad egnet til denne type data. Datadrevne modelleringsteknikker gir like informasjon omkring årsaker til at risikoen er høy eller lav noe som er hensikten med risikoanalysen for å kunne iverksette tiltak for å redusere risikoeksponeringen enten ved å fjerne årsakene til risiko eller redusere konsekvensene (Andersen & Häger, Objectivity and the Measurement of Operational Risk, Reconsidered, 2011). For å sikre nytteverdi av modellene så foreslår Andersen og Häger at modeller skal gi verdifullt bidrag til den daglige risikostyringsarbeidet og utgjøre grunnlaget for kapitalavsetning. Det er derfor nødvendig å inkludere informasjon utover historiske tap. Objektivitet er derfor hverken riktig eller ønskelig mht kvantifisering av operasjonell risiko.

5.3 Risikoperspektiv

Denne oppgaven baseres på en subjektiv forståelse av sannsynlighetsbegrepet. I en subjektiv forståelse er sannsynlighet et uttrykk for subjektiv vurdering, eller grad av tro (Neapolitan, 2003). Denne graden av tro er betinget på kunnskapen til den som angir sannsynligheten. Subjektiv sannsynlighet tillater å inkludere all tilgjengelig kunnskap. Sannsynligheten i denne forstand er et uttrykk for usikkerhet knyttet til hva som vil skje i fremtiden. Det finnes ikke en sann eller korrekt verdi. Bakgrunnen for å hevde dette baseres på at fremtidige hendelser ansees for ikke å være uavhengige av hva som har skjedd tidligere, som de for eksempel vil være i monte carlo

simuleringer. Hendelsene skjer derimot i et læringsmiljø og organisasjonene lærer av tidligere hendelser. Dersom en gitt type tapshendelse rammet en bank, så ville det umiddelbart bli iverksatt tiltak mot denne type hendelser for å forhindre at noe tilsvarende skulle skje igjen. Subjektiv sannsynlighet kan sees som et forsøk på å overfører kunnskap om hva som har skjedd tidligere til noe som ligger fremover i tid. Usikkerheten er blant annet et resultat av at fremtiden ikke kan antas å være en direkte gjentakelse av historien. I subjektiv tolkning og modellering vil en bryte ned hendelser i årsaker noe som bidrar til å gjøre det mulig å samle inn og systematisere all tilgjengelig informasjon.

Subjektiv fortolkning av sannsynlighetsbegrepet står i motsetning til den tradisjonelle fortolkningen av sannsynlighetsbegrepet som er basert på ”de store talls lov”. Dersom en gjentar et forsøk uendelig mange ganger så vil vi få en korrekt eller sann verdi på sannsynlighet. De store talls lov fungerer utelukkende under bestemte forhold, for eksempel ved monte carlo simuleringer i et laboratorium eller et casino. Eksempelvis er sannsynligheten for å få et terningkast seks med en korrekt terning 1/6. Usikkerheten ut i fra et objektiv perspektiv defineres som et gap mellom estimert verdi av sannsynlighet og sann, eller korrekt verdi. I virkeligheten er forholdene sjeldent identiske fra gang til gang. Eksempelvis i en bank hvor det skjer rask utvikling med ny teknologi, nye produkter etc. Operasjonell risiko i bank kjennetegnes av små populasjoner, sjeldne hendelser med store konsekvenser. Bankene rapporterer hendelser og iverksetter tiltak i en kontinuerlig prosess, de fungerer i et læringsmiljø. En ren statistisk analyse av små populasjoner

Motivasjonen for å velge Bayesianske Nettverk (BN) som metode for denne oppgaven er at forfatteren anser den som mest egnet til å dekke kravene i Basel II avanserte målemetoder (AMA). Bayesianske nettverk kombinerer på en god måte kvalitativ og kvantitativ informasjon. Modellen vil være et verktøy for identifisering av risiko samt kvantifisering og vil kunne brukes i det daglige risikostyringsarbeidet. Basel II for avanserte målemetoder (AMA) stiller krav til at modellen skal kunne benyttes i bankens jevnlige risikostyringsarbeid i henhold til «use test». Erfaring fra risikostyringsarbeid fra andre bransjer som olje & gass tilsier at modeller for analyse av operasjonell risiko bør tilstrebe å gi beslutningsstøtte ved å besvare følgende spørsmål (Neil, Häger, & Andersen, 2009);

- Er risikoen høy eller lav, er den akseptabel?
- Hvilke påvirkende faktorer er mest kritiske?
- Hva er forskjellen i risikoeksponering med hensyn til ulike løsninger?
- Hvilken risikoreduserende effekt kan oppnås ved ulike risikoreduserende tiltak?

En kausal modell i et bayesiansk nettverk (BN) har sin styrke i at den er en intuitiv visuell modell som gir forståelse for årsakssammenhengene og konsekvenser. Det muliggjør diskusjoner omkring risiko på tvers av faggrupper hvor alle vil kunne bidra med sin ekspertkunnskap på egne fagområder. Modellen som verktøy vil fremme fruktbare diskusjoner om organisasjonsspesifikke problemstillinger som for eksempel tilstanden på internkontrollmiljøet og organisasjonskultur (Häger & Andersen, A knowledge based approach to loss severity assessment in financial institutions using Bayesian networks and loss determinants, 2010). Bayesiansk nettverksmodellering gir også et solid matematisk grunnlag for kvantitative beregninger.

5.4 Bayesianske nettverk

Et bayesiansk nettverk (BN) kan sies å bestå av to hoved elementer. En kvalitativ del bestående av en grafisk struktur med noder eller variabler og piler som definerer avhengigheter og uavhengigheter. Og, en kvantitativ del som viser styrken til avhengighetene gitt ved betinget sannsynlighet (Häger, MOS140 Introduksjon til bayesianske nettverk, 2011). BN er grafiske probabilistiske modeller som anvendes til å resonnere under usikkerhet. Modellen i denne oppgaven har nettopp det formål å gi beslutningsstøtte under usikkerhet. Modellen skal som eksempel vise endringen i risikoeksponeringen ved valg av ulike alternative løsninger. Nodene i nettverket representerer variabler som kan være diskre eller kontinuerlige, og pilene representerer koblingene mellom dem (Korb & Nicholson, 2004).

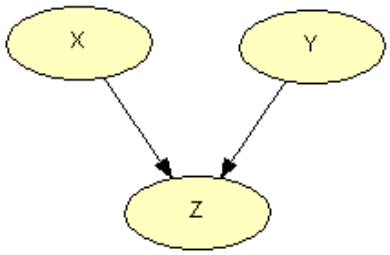
Bayesianske nettverk benyttes til å kalkulere nye sannsynligheter gitt ny informasjon (Jensen, 2001). Bayesianske nettverk er probabilistiske modeller som baseres på Bayes teorem og muliggjør slutninger (inferens) basert på observasjoner eller bevis. Probabilistisk vil si at modellene viser sannsynligheter under gitte betingelser og under usikkerhet. Bayes teorem gir en matematisk regel for hvordan en oppdaterer sannsynligheter i lys av nye bevis (Pearl & Russell, 2001). BN er altså et rammeverk for å resonnere kvantitativt om usikkerhet gitt observasjoner. Ulike fageksperters vurderinger benyttes for å gi input til årsakssammenhenger og sannsynligheter. Et BN er sammensatt av en grafisk struktur med noder og piler som beskriver årsaker og konsekvenser og avhengighet og uavhengighet. Styrken i avhengighetene er gitt ved betinget sannsynlighet. For hver node A, med foreldrenode $B_1 \ldots B_n$ defineres en lokal betinget sannsynlighetsfordeling $P(A| B_1 \ldots B_n)$. Hver variabel har et endelig sett med tilstander og en sannsynlighetstabell (Node Probability Table – NPT) knyttet til seg.

Variablene sammen med pilene utgjør sammen en rettet asyklisk graf eller på engelsk en «directed acyclic graph» (DAG) (Jensen, 2001). Den matematiske betegnelsen er en rettet graf, og den er asyklisk dersom den ikke har noen løkker. I et bayesiansk nettverk representerer nodene tilfeldige

variabler, og retningsbestemte koblinger/piler som representerer betingede avhengigheter mellom dem. Nodene i modellen for IKT-risiko representerer årsaker, influerende faktorer, barrierer, hendelser og konsekvenser. En probabilistisk modell gir en oversikt på den sammensatte sannsynlighetsfordelingen (joint distribution) dvs. sannsynligheten for alle mulige hendelser som er definert av verdiene fra alle variablene. Dvs. når vi har behov for å se på sammenhengen mellom to eller flere hendelser.

$$P(X_1,...,X_n) = \prod_{i=1}^{n} P(X_i \mid pa(X_i))$$

For tre variabler X, Y og Z sammensatt i en DAG, som vist i figuren under, så betyr den grafiske fremstillingen at sannsynligheten for at Z skal inntreffe avhenger av at X og Y inntreffer. Vi kan si at X og Y er årsaker til Z (Andersen & Häger, 2009).



Figur 3: Directed Acyclic Graph (DAG).

I Bayesianske nettverk så brukes betegnelsene «barn» og «foreldre» for å beskrive forholdet mellom nodene. I figur n over så er Z barnet av foreldrene X og Y. Den sammensatte sannsynlighetsfordelingen i dette tilfellet er:

$$P(X, Y, Z) = P(Z|X,Y)P(X)P(Y)$$

Marginal fordelingen gir sannsynligheten for en variabel når en ser bort i fra påvirkningen fra en annen variabel/hendelse. Dersom vi ønsker å si noe om hvordan A og B varierer for seg, når du bare ser på en av dem om gangen. Vi kan si at vi fjerner innflytelsen av en eller flere hendelser.

$$P(A) = \sum_{B} P(A \mid B)P(B)$$

I eksempelet fra figur 1, dersom vi ønsker å se på marginalfordelingen til Z, så kan vi få frem dette ved å marginalisere ut X og Y på følgende måte:

$$P(Z) = \sum_{X,Y} P(Z \mid X,Y)P(X)P(Y)$$

Bayesianske nettverk behøver ikke være kausale, men i denne oppgavens sammenheng så tar forfatteren utgangspunkt i kausale modeller. Kausale modeller viser som beskrevet årsakssammenhenger, influerende faktorer og konsekvenser. Lenkene i kausale bayesianske nett representerer direkte influerende faktorer. Når vi beskriver relasjonene i en rettet graf så brukes begrepene foreldre og barn. Par av noder i bayesianske nett som er lenket sammen består av en forelder node (årsak) og en barn node (konsekvens). Sannsynlighetene i nettverket er altså betingede sannsynligheter av verdiene, gitt verdien av foreldre nodene (Neapolitan, 2003). Dette gjelder alle tilfeller bortsett fra tilfeller av røtter, dvs. noder uten foreldre der fordelingen er gitt apriori eller der det gis bevis.

Noder i et nettverk er enten avhengig eller uavhengig av andre noder i nettverket. Linken mellom to noder er enten betinget avhengig eller betinget uavhengig av den andre noden og dens etterkommere. Kausale nettverk kan brukes til å følge hvordan endring i sannsynlighet for en variabel kan endre sannsynligheten for en annen variabel. Ved å introdusere bevis i en variabel så vil en kunne avgjøre for alle par av variabler om de er uavhengige gitt beviset som er introdusert. Dette avgjøres ved regelen om d-separasjon. Dersom to sett av noder X og Y er d-separert i nettverket av et tredje sett med variabler Z, så er X og Y betinget uavhengige gitt variablene i Z. Dette innebærer at hvis A og B er d-separert så vil endringer i sannsynligheten for A ikke ha noen effekt på sannsynligheten for B. D-separasjon er et kriterium for å beslutte, fra en gitt kausal graf, om et sett X av variabler er uavhengig av et annet sett av variabler Y, gitt ett tredje sett Z. Ideen er å assosiere avhengighet med tilknytning og uavhengighet med adskilthet.

Kausale grafer er antatt å være komplette i en gitt betydning og ikke i en annen. Dvs. under gitte forutsetninger eller omstendigheter. De er ufullstendige mht. at de ikke nødvendigvis inkluderer alle årsakene for hver variabel i systemet. En kausal graf er i tillegg antatt å være komplett i den betydning at alle de kausale relasjonene mellom de spesifiserte variablene er inkludert i grafen.

Den fundamentale regelen for sannsynlighets regning er;

$$P(A|B)P(B) = P(A, B)$$

Hvor P(A, B) er sannsynligheten for både A og B gitt at vi vet sannsynligheten for at B inntreffer.

Bayes teorem brukes til å oppdatere bevis i et nettverk. Essensen av bayesiansk tilnærming er å gi en matematisk regel som forklarer hvordan du skal endre eksisterende oppfatninger i lys av nye

bevis. Med andre ord, så muliggjør det å kombinere nye data med eksisterende kunnskap og ekspertise.

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)}$$

Bayesianske nettverk er i de senere år anbefalt som metode av flere for å måle og styre operasjonell risiko i finansielle institusjoner. Oprisk skiller seg fra tradisjonell kredittrisiko og markedsrisiko ved at det er lite historisk data. Det anbefales derfor å ta i bruk menneskelig vurdering og ekspert kunnskap (Sanford & Moosa, 2012). BN er ikke i seg selv ikke en ny metode, den har eksistert i over 20 år. BN kan anvendes på flere ulike områder, men det som kjennetegner tidligere anvendelser er modeller for å resonnere under usikkerhet.

6. MODELLERING FOR KVANTITATIV ANALYSE AV IKT-RELATERTE HENDELSER

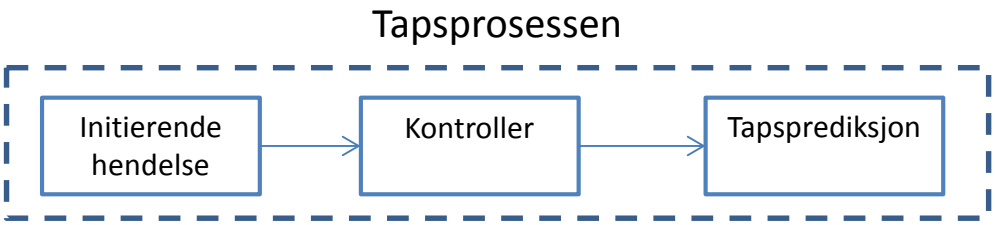
6.1 Modellering introduksjon

Dette kapittelet gir en beskrivelse av nettverket og modelleringen utført i et bayesiansk nettverk. Beskrivelsen er delt opp og forklarer årsaker og årsakssammenhenger for hver av de mest kritiske hendelsene; urettmessig tilgang, kritiske systemfeil og ødeleggelse av kritisk utstyr.

Den kvalitative delen av nettverket forklares ved gjennomgang av årsaksbildet, med forklaring av årsaker og årsakssammenhenger. Den kvantitative delen av nettverket beskrives nærmere i delkapittel 6.6, kvantitativ tapsprediksjon. Den kvantitative delen omfatter også styrken til avhengighetene mellom nodene som er definert i nodesannsynlighetstabellene (Node Probability Table - NPT) i nettverket.

Hendelser modelleres med tanke på hva som kan skje og hvorfor. Hvilken kjede av hendelser er det som må inntreffe, og hvilke kontroller må feile for at en tapshendelse skal kunne utløses? Hvilke kontroller har banken implementert for å unngå hendelser og i verste fall å oppdage hendelser når de har skjedd? Modellen skal også si noe om hvorfor og hvordan kontroller kan feile. Samlet viser modellen årsakssammenhengen og forklarer hvordan tap kan skje.

I modelleringen av en prosess eller et fagområde innenfor bank og finans, må utvikleren ta stilling til hvilket detaljnivå som er hensiktsmessig. Detaljnivået henger sammen med hvordan modellen skal brukes for eksempel i risikoidentifisering prosessen, analysen og muligheten for eksperter å kunne si noe om sannsynligheter i input nodene. Detaljene bør være på et slikt nivå at det gir mening for eksperter å gi sin vurdering av sannsynligheter for sitt fagfelt. Samtidig må ikke modellen være så omfattende at den mister fordelen av å gi oversikt og intuitiv forståelse. Modellen skal også gi beslutningsstøtte ved vurdering av ulike alternativer, og effekten av kontrolltiltak.



Figur 4: Tapsprosessen for alvorlige tapshendelser.

(figur hentet fra forelesningsnotat MOS140 «Styring av Operasjonell risiko», UIS 21.03.2011)

BN modellering av alvorlige tapshendelser tar utgangspunkt i tapsprosessen med initierende hendelser og kontroller som er iverksatt for å forhindre eventuelle tap, se figur 4. Samlet gir dette en tapsprediksjon fra modellen.

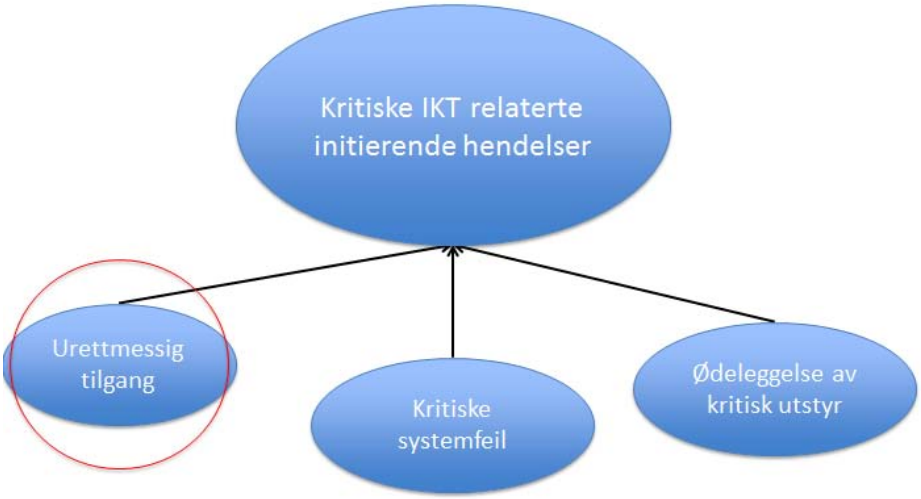
Bayesianske nettverk (BN) benyttes til å systematisere all tilgjengelig informasjon. Bayesianske nettverk gir struktur på informasjonen ved at informasjonen blir sortert etter hva som er årsaker, konsekvenser og tapshendelser. Den grafiske visualiseringen gir en helhetlig oversikt over risikodrivere og årsakssammenhengene. Den vil også vise konsekvensene av eventuelle svakheter i kontrollmiljøet. Det er mulig å teste effektene av ulike influerende faktorer. Ut ifra et BN vil en kunne se hvor det har størst effekt å sette inn tiltak, og en vil på denne måten kunne gjøre en kost/nytte vurdering av ulike tiltak opp mot hverandre.

Som forfatteren av denne oppgaven også har opplevd så vil gir BN kunne gi merverdi både i risikoidentifiseringsprosessen og som risikostyringsverktøy. For gjennomføring av risikoidentifiseringsprosess så er det en fordel å ha et utgangspunkt for diskusjonen. Tidligere erfaringer, kunnskap fra forskning, hendelsesdatabaser kan modelleres i forkant av møtet med kunden. Det kan også være nyttig å inkludere informasjon «beste praksis» enten fra standarder eller bransjepraksis når en modellerer kontrollmiljøet. Det vil kunne gi innspill til diskusjoner med kunder.

6.2 Urettmessig tilgang

Den første av de mest kritiske IKT relaterte initierende hendelsene som vil bli gjennomgått er urettmessig tilgang.

Urettmessig tilgang viser til all systemtilgang til bankens IKT-systemer eller kunders nettbank som er oppnådd på urettmessig vis med den hensikt å tilegne seg informasjon, penger eller på annen måte skade banken.

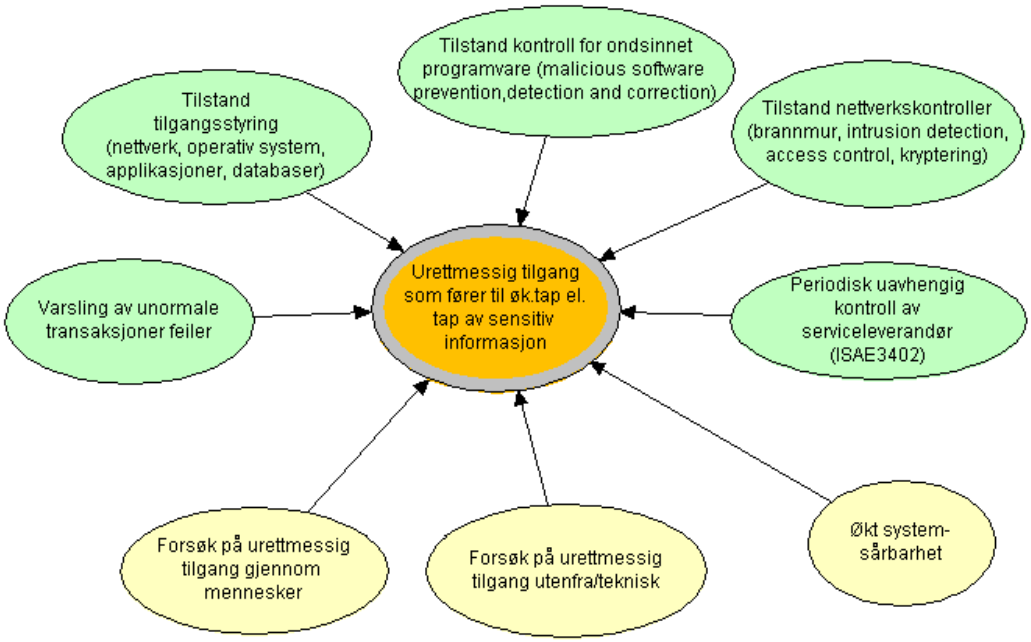


Figur 5: Kritiske IKT-relatert initierende hendelser – urettmessig tilgang.

Angrep utenfra kan komme fra hacking ved bruk av trojanere. Det finnes ulike typer trojanere og det kommer stadig nye. Phishing er en digital måte å tilegne seg informasjon som for eksempel passord til kunders nettbank. Dette kan betegnes som en form for sosial manipulering. En annen type sosial manipulering er for eksempel å utgi seg for å være en leverandør for å få tilgang til bankens systemer.

Både internt ansatte og eksterne kan være motivert ved penger eller utpressing. Evne, motivasjon og mulighet må inntreffe samtidig for at en ansatt skal være utro. Manglende styring og kontroll enten internt eller med underleverandør av IT-tjenester kan også være en årsak til at noen kan oppnå urettmessig tilgang enten ved tekniske angrep eller via mennesker. Hva som menes med *kritisk* hendelse har partisipantene fra banken gitt uttrykk for er hendelser som kan utløse et potensielt tap på 50 millioner eller mer. Dette enten ved direkte økonomisk tap eller andre konsekvenser som stans i forretningsdrift, tap i omdømme, tap av konsesjon, tap av sensitiv informasjon (personopplysninger), tap av konfidensiell informasjon (bedriftshemmeligheter), urettmessig pengeoverføring og erstatningsansvar.

Som vist i figur 6 under, skilles det i nettverket mellom to hovedtyper årsaker til urettmessig tilgang; forsøk på urettmessig tilgang gjennom mennesker, og forsøk på urettmessig tilgang utenfra/teknisk. En viktig influerende årsak både for risikoen for urettmessig tilgang og systemfeil er økt system sårbarhet. Bankene kan oppleve økt systemsårbarhet i perioder med organisatoriske- eller systemendringer. Risikoreduserende kontroller er også modellert inn, her merket med grønt.

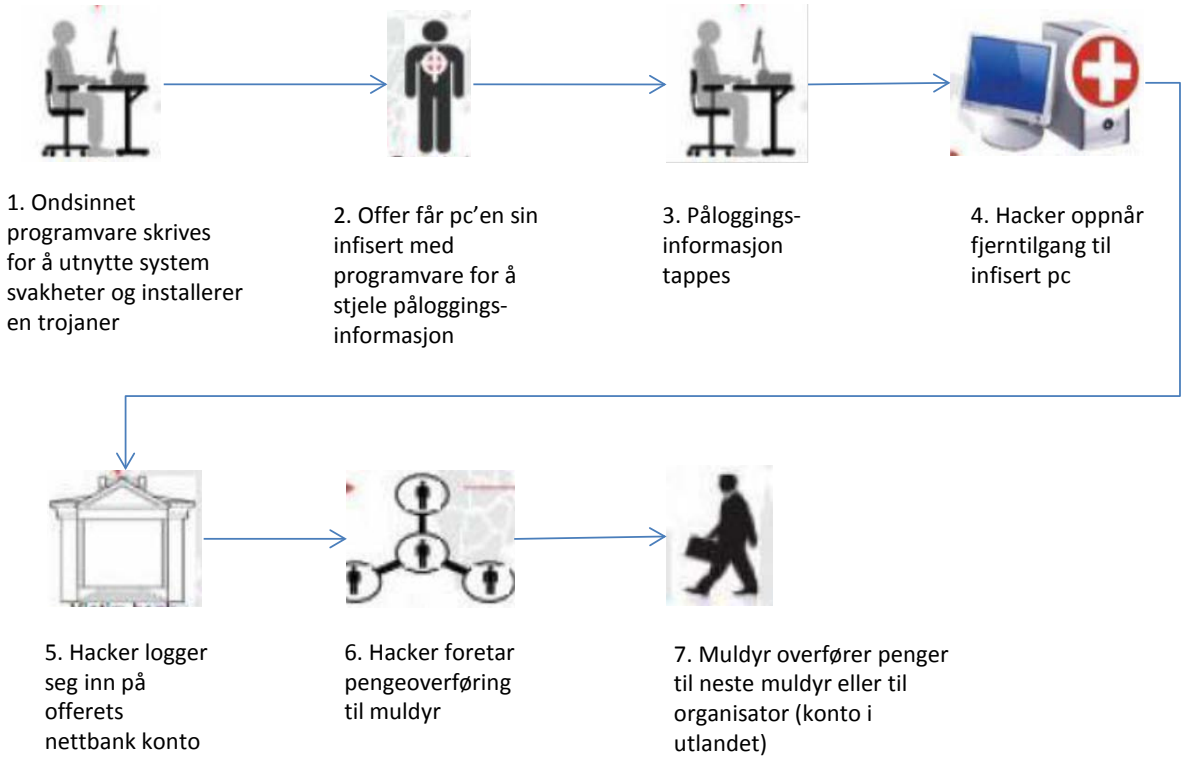


Figur 6: Urettmessig tilgang, årsaker og kontroller/barrierer.

6.2.1 Årsaker til urettmessig tilgang gjennom mennesker

Ansattes og kunders bruk av private mobile enheter og sosiale medier kan være årsaker til at ansatte eller kunder får sin pc infisert av ondsinnet kode programmert for å stjele offerets påloggingsinformasjon.

Et eksempel på urettmessig tilgang kan tenkes å ha følgende hendelsesforløp:



Figur 7: Eksempel på hendelsesforløp for urettmessig overføring av penger.

(figur hentet fra «Top Security Threats to Banks in 2013, av ISACA,2012).

Manglende bevissthet omkring informasjonssikkerhet

Holdningen og bevisstheten blant de ansatte har stor betydning for informasjonssikkerheten. Det vil ha påvirkning på hvordan ansatte forholder seg til bruk av private mobile enheter, bruk av sosiale medier på jobb pc-er, samt internett bruk. Gode rutiner for hendelsesrapportering og generell fokus på risikostyring vil være med å skape gode holdninger og bevissthet.

Ansattes bruk av mobile enheter (BYOD)/sosiale medier

Det å ha ansatte utgjør i utgangspunktet en stor trussel. Ansatte må nødvendigvis ha tilgang til IT systemer og sensitiv informasjon for å gjøre jobben sin. En annen trussel er ansattes bruk av mobile enheter («Bring you own device - BYOD») og bruk av sosiale medier. I utgangspunktet så burde organisasjoner ha formelle retningslinjer for ansattes bruk av denne type kommunikasjon.

Phishing/vishing

Phishing eller nettfisking er en metode svindlere bruker for å lure informasjon fra datamaskinbrukere for å kunne misbruke tilgang og tappe kontoen din for penger eller misbruke kredittkortet ditt. Phishing-ordet kommer fra engelsk «fishing», med f-en byttet ut med "ph", men det uttales «fishing». Svindlerne er ute etter sensitiv informasjon og benytter seg gjerne av e-post som ser ut som den kommer fra banken din eller andre pålitelige kilder. E-posten opplyser gjerne om at det er problemer med noen kreditt kort, en betaling, eller andre ting og ber deg derfor registrere dine opplysninger på ny. Eller e-posten sier kanskje at banken har innstallert nye sikkerhetstiltak og ber deg derfor registrere på ny. Brukeren bes deretter å trykke på en link til en nettside som ser ut som det er bankens nettside, og det føles derfor trygt, men det er en falsk nettside. Her ber de deg registrere personlige opplysninger, brukernavn, kontonummer og passord etc. Dersom svindlerne lykkes med å få tak i denne type informasjon vil de bruke den til å misbruke kreditkortet ditt, eller tappe bankkontoen din for penger.

Sosial manipulering

Sosial manipulering (på engelsk social engineering) er en teknikk for å skaffe seg informasjon og tilgang ved hjelp av sosiale ferdigheter. Man kan si at det er en form for hacking ved at mennesker bruker sosiale evner til å få tak i informasjon, påloggingskoder etc. Et eksempel er at en angriper utgir seg for å være en IT-konsulent som skal utføre vedlikehold på brukerens datamaskin, og dermed lurere til seg brukernavn og passord.

Botnet

En «bot» er et nettverk av kompromitterte datamaskiner som kriminelle kan kontrollere eksternt. Begrepet «bot» er en forkortelse av robot. Datamaskiner som det er tatt kontroll over og som er en del av et botnet kalles ofte zombier. Et botnet er en samling «boter» som blir kontrollert av én person eller datamaskin. Datamaskinene som blir kapret har i utgangspunktet vært sårbare for skadelig programvare. Et bot-program på en bot åpner en kanal (port) mot omverdenen der den mottar instruksjoner. Det kan være instruksjoner på å sende ut virus, e-postreklame (spam), eller delta i tjenestenektangrep. Til enhver tid er flere millioner datamaskiner over hele verden med i aktive botnet uten at eierne er klar over det (NorSIS Norsk senter for informasjonssikring, 2013). Pc-er kan bli infisert med små script eller programsnutter som lastes inn i pc-en din når du besøker infiserte nettsider. Programmene åpner «bakdører» i datamaskinen og gjør at din pc kan bli en del av et nettverk av datamaskiner som kan styres fra sentralt hold. Hensikten med botnet er å tjene penger, de som eier nettverket selger informasjonen som de får tak i, for eksempel kredittkort-informasjon. Det kan også som nevnt brukes til DDoS angrep. På denne måten kan botnet også

benyttes til utpressing, at de kriminelle truer med å sette systemene ut av spill ved å utføre et distribuert tjenestenekt (DDoS) angrep, men kan la være å gjøre det mot en sum penger.

Person plantet i organisasjonen

En risiko som kanskje vil være økende i fremtiden er risikoen for at organiserte kriminelle «planter» en person i organisasjonen. I stedet for å eksternt prøve å hacke seg inn i banken, så vil det kanskje være bedre å lære opp noen for videre å få de ansatt i organisasjonen, for eksempel i IT avdelingen som database administrator (Webber, 2013).

Økt systemsårbarhet

Økt systemsårbarhet kan oppstå i forbindelse med at organisasjonen opplever IT strategiske endringer eller organisasjonsendringer. Dersom en bank har store endringer i systemene kan dette i en periode lede til at det er usikkerhet omkring rutinene, eller usikkerhet omkring funksjonalitet. De ansatte har kanskje ikke like mye oversikt som de ville hatt over systemer som de kjenner godt og har lang erfaring med. På samme måte kan organisasjonsendringer mht. ressurser gi økt sårbarhet i en periode. Dersom for eksempel nøkkelpersonell slutter og tar med seg verdifull kunnskap som ikke er videreført i organisasjonen. Eller at for eksempel banken utkontrakterer ny aktiviteter eller til en ny leverandør. Dette kan på ulike måter føre til endringer som påvirker stabiliteten i kontrollmiljøet.

6.2.2 Årsaker til urettmessig tilgang utenfra/teknisk

Hackerangrep og «muldyr»

Hacking er et fellesbegrep for det å bryte seg inn i datamaskiner og nettverk uten tillatelse. Trojanere, ondsinnet programvare («malware»), virus, orm, sql injection og phishing er ulike former for hacking.

Hackerangrep mot nettbankkunder i Europa er i ferd med å bli et stadig større problem. I 2011 stjal hackere 700 000 fra norske nettbankkunder ved hjelp av trojanere og virus. I disse tilfellene blir som regel beløpet overført til kontoen til et «muldyr». Et «muldyr» er en person som stiller sin nettbankkonto til disposisjon for innskudd, for deretter å overføre penger til ukjente personer mot en avtalt provisjon. (Hardware.no, 2012). Erik Moestue i Kripos, forklarer i et innlegg i ABC Nyheter i fjor, (ABC Nyheter, 2012) at oppgaven til muldyr er å transportere pengene for bakmenn. Muldyr kan gjerne være norske personer. De mottar instruksjoner fra bakmenn, via e-postadresser som gjerne er fiktive, om hvem som skal motta pengene. Muldyrene overfører pengene ved hjelp av tjenester som Money Gram hvor det er mulig å sende penger uten annet enn et navn og mottaker

land. Når pengene er tatt ut på «muldyrets» konto er det elektroniske sporet brutt. Mottakeren er gjerne også et «muldyr» som sender pengene videre. Muldyrene blir som regel alltid tatt, men det er vanskelig å få tak i bakmennene. Kripos samarbeider med politimyndigheter i andre land.

DN skriver onsdag 9. januar at kriminelle gjorde fire ganger så mange forsøk på å trenge inn I norske nettbanker I 2012 som året før. Kriminelle rekrutterer mellommenn via datingtjenester og jobbannonser for tjenester som muldyr.

Trojaner angrep

Trojaner angrep er en annen metode hvor kriminelle forsøker å få kontroll over datamaskiner ved å utnytte sårbar programvare. Kriminelle vil på denne måten vanligvis forsøke å overføre penger til utenlandske konti. Spredningen av trojanere kan skje ved å få brukere til å klikke på lenker som dermed installerer skadelig programvare eller gjennom kompromittering av vanlige nettsider (Dagens Næringsliv, 2013).

Kriminelle prøver å logge inn i nettbanker fra pc-er som er infisert med en trojaner. Den som styrer trojaneren vil vil verste fall kunne utføre banktransaksjoner i ditt navn. Det utvikles stadig nye trojanere ettersom bankene setter inn mottiltak. Den årlige ROS rapporten fra Finanstilsynet (Finanstilsynet, 2013) viser at bruken av trojanere for å misbruke nordmenns nettbanker er et økende problem. Også Kripos varsler om at svindelforsøkene mot norske nettbanker er økende. Misbruket skjer ved at nettsteder angripes av hackere, og infiseres med ondsinnet kode som installerer virus og trojanere på PC-en din om du besøker nettstedet. Trojanere kan overvåke kundens aktivitet og tilegner seg innloggingskoder eller introduserer falske transaksjoner mens den rette brukeren er pålogget.

Ondsinnet programvare (malware)

Et skrekkscenario er å oppdage at alt data er fjernet fra jobb pc'en. Ikke bare fra din pc, men fra alle kollegaene sine også. Det var akkurat dette som hendte hos det statseide Saudi Arabiske oljeselskapet Aramco (Saudi Arabian Oil Company) så sent som i august i fjor. Alle data var fjernet fra pc'ene og erstattet med et brennende amerikansk flagg (Bank Info Security, 2013). 30.000 pc'er ble ødelagt. Målet var å stoppe produksjonen av olje og gass. Saudi Aramco står alene for leveransen av en tiendedel av verdens olje eksport. Angriperne mislyktes i å stoppe oljeproduksjonen, men utførte det mest alvorlige IT sabotasje angrepet noensinne (Reuters, 2012).

Viruset som ble kalt Shamoon var designet for å gjøre to ting; erstatte data på harddisker med et bilde av et brennende amerikansk flagg og rapportere ip adressene til infiserte pc-er, som en skryteliste. Viruset kan ha blitt installert ved at en medbrakt USB minnepinne er satt i en av

bedriftens pc-er. Det er ikke klart om data som ble slettet var data lagret lokalt på pc-ene, eller om også sentrale servere ble rammet.

Vi vet ikke nok om Aramcos modenhets nivå mht. risikostyring, eller sikkerheten av Aramcos IT-systemer. Sannsynligvis var det en eller flere på innsiden med administrator rettigheter som var medvirkende. Vi kan ikke anta at det samme kunne skjedd i banknæringen i Norge. Sannsynligvis er sikkerheten og overvåkningen betydelig sterkere i banknæringen. Men, det åpner øynene for tenkelige scenario, og viser hvor omfattende et slikt angrep kan være om angriperne lykkes.

DDoS angrep

Et DDoS-angrep, eller distribuert tjenestenekt angrep, forekommer når et datanettverk utsettes for et bombardement av kommunikasjonsforespørsler, gjerne fra mange datamaskiner eller botnett. Dette ender ofte med at serverne ikke takler det massive presset, og dermed blir slått ut av spill. I praksis fortoner dette seg som siruptrege nettsider eller tjenester, eller at de ikke er tilgjengelige i det hele tatt. Angriperne bruker gjerne store nettverk av kaprede pc-er, såkalte ”bot-net” eller zombier. Eierne av pc-ene vet typisk ikke at de er infisert av ondsinnet programvare som bruker dem i slike angrep. Slike zombiehærer kan man nå leie, og programvare for massive angrep skal være både brukervennlig og kan komme med brukerstøtte.

Danske banker, deriblant Nordea og Danske Bank ble til eksempel utsatt for et DDoS-angrep i april i år. Angrepet førte til at kunder i perioder ikke kunne logge seg på nettbankene. Politiet behandler nå en sak der DNB, Norsk Tipping, PST, IT-avisen og en rekke andre nettsteder i fjor ble senket av et massivt tjenestenekt-angrep

Internasjonale medier bekrefter inntrykket av at DDoS-angrep er økende også i andre deler av verden. Information Week Security skriver at amerikanske banker og finansinstitusjoner har sett en dobling av nedetid sammenlignet med for bare et år siden. Den økte nedetiden skyldes i hovedsak DDoS-angrep som gjør nettsidene utilgjengelige for kundene i perioder (InformationWeekSecurity, 2013). Angrepene mot amerikanske organisasjoner kan ha politiske årsaker og noe kan spores tilbake til islamistiske protester mot den omstridte mohammed-filmen «Innocence of Muslims» som skapte protester blant muslimer over hele verden i.

Trenden er at angrepene blir mer sofistikerte og organiserte. Man mistenker at organisert kriminell aktivitet eller til og med stater kan stå bak angrepene. Men, dette er ikke blitt bekreftet eller avkreftet ennå. Man har også sett mange angrep uten åpenbar hensikt bortsett fra å skape kaos eller å søke å finne svakheter. Det man frykter er at slike angrep ikke bare skal skape treghet i systemet, men at det skal bli brukt som en distraksjon, for å skape forvirring og styre oppmerksomheten bort

fra andre nettangrep som finner sted. For eksempel tyveri av penger eller informasjon. Det kan være storstilt operasjon med tåkelegging for å skjule et reelt angrep. Dette har man sett tegn på, men ikke funnet bevis for enda (Dagens IT, 2013).

Operational Risk & Regulation ranker IT sabotasje på topp i sin vurdering av topp 10 operasjonell risiko for 2013 (Operational Risk & Regulation, 2012). Internettangrep kan utvikle seg fra å være en mindre trussel på organisasjonsnivå, til å bli en samfunnsmessig trussel ved å true stabiliteten i det finansielle system.

6.2.3 Risikoreduserende kontroller

Internkontroll eller barrierer har til hensikt å fjerne eller redusere risiko. Kontrollene omfatter kontroller på selskaps-/konsernnivå som relaterer seg til IT-virksomhetsstyring og IT-kontrollmiljø. IT-kontroller for informasjonssikkerhet kan både være manuelle, automatiserte applikasjonskontroller, eller en kombinasjon av begge deler. De risikoreduserende kontrollene er modellert inn på et overordnet nivå. Totalt antall kontroller, som banken sannsynligvis har implementert og som er anbefalt av anerkjente standarder, er så omfattende at det ikke ville vært hensiktsmessig å ha alle detaljene i modellen.

De fleste kontroller i nettverket er konfigurert med de mulige tilstandene; Effektiv, ikke effektiv eller med svakheter. Tilstandene er hentet fra revisjonsstandard, og er i IT-revisjon vanlig for å avdekke om kontroller er operasjonelt effektive, om de ikke er operasjonelt effektive (ikke utføres som forutsett/ ikke fungerer som forutsatt) eller om det er funnet svakheter/mangler i kontrollene.

I henhold til IT-revisjon praksis testes kontroller først for design for så å vurdere om de er operasjonelt effektive. Design vurdering utføres med tanke på om kontrollen er hensiktsmessig utformet for å kunne fjerne evt. redusere risikoen den er rettet mot. Operasjonell effektivitet testes ved å sjekke om kontrollene faktisk blir utført på den måten de er beskrevet, dvs. at de er implementert.

Ved bruk av modellen vil bankene kunne benytte seg av en uavhengig part for eksempel internrevisjon eller ekstern revisjon for å angi tilstandene objektivt i risikostyringsmodellen. I motsetning til om risikostyringsansvarlige eller IT-avdelingen selv skulle vurdere effektiviteten av egne kontroller, så vil en uavhengig part være mer tillitsvekkende. Det vil bidra til å øke troverdigheten omkring risikoeksponerings tallene.

Varsling av unormale transaksjoner feiler

Manuelle eller automatiske kontroller som skal avdekke unormale transaksjoner. Det kan være transaksjoner som skiller seg ut på forskjellige måter enten i beløpsstørrelse, hyppighet eller annet.

Tilstand tilgangsstyring

Kontroller med hensikt å sikre at at tilgang til programmer og data er rettmessig. Kontrollene skal redusere risiko for uautorisert/urettmessig tilgang til bankens systemer. Kontrollere må være implementert for alle relevante applikasjoner, operativ system, databaser, nettverk, mobile løsninger. Kontroller vil omfatte;

- kontroll av IT sikkerhets policy
- tilgangsstyring (rutiner for søking om tilgang, godkjenning, oppretting, endring av tilgang, avslutting)
- brukergrupper/rolledeling (SOD - Segregation of Duties),
- identifisering og autentisering (bruker ID og passord krav, logisk tilgang, lengde, varighet, kompleksitet etc.) Hvem er jeg og hva har jeg tilgang til.
- begrensning av brukere med utvidede rettigheter (superbrukere med admin rettigheter)
- monitorering av brukere (en oppdagende periodisk kontrollen som tester om eksisterende brukeres tilganger er autorisert og rettmessig tildelt)

Tilstand kontroller for ondsinnet programvare

Kontroller med hensikt å forebygge, oppdage og korrigere evt. ondsinnet programvare. Implementere forebyggende, oppdagende og korrigerende tiltak. Tiltak i form av oppdaterte sikkerhetsoppdateringer og virus kontroll for å beskytte IT system og teknologi fra ondsinnet programvare som for eksempel viruser, ormer, spyware og spam.

Tilstand nettverkskontroller

Kontroller med hensikt å ved hjelp av sikkerhetsteknikker og styringsrutiner å kontrollere tilgangen til og informasjonsflyten fra og til nettverk. Eksempel på slike sikkerhetsteknikker er brannmurer, sikkerhetsapparater, nettverk segmentering, «intrusion detection» verktøy.

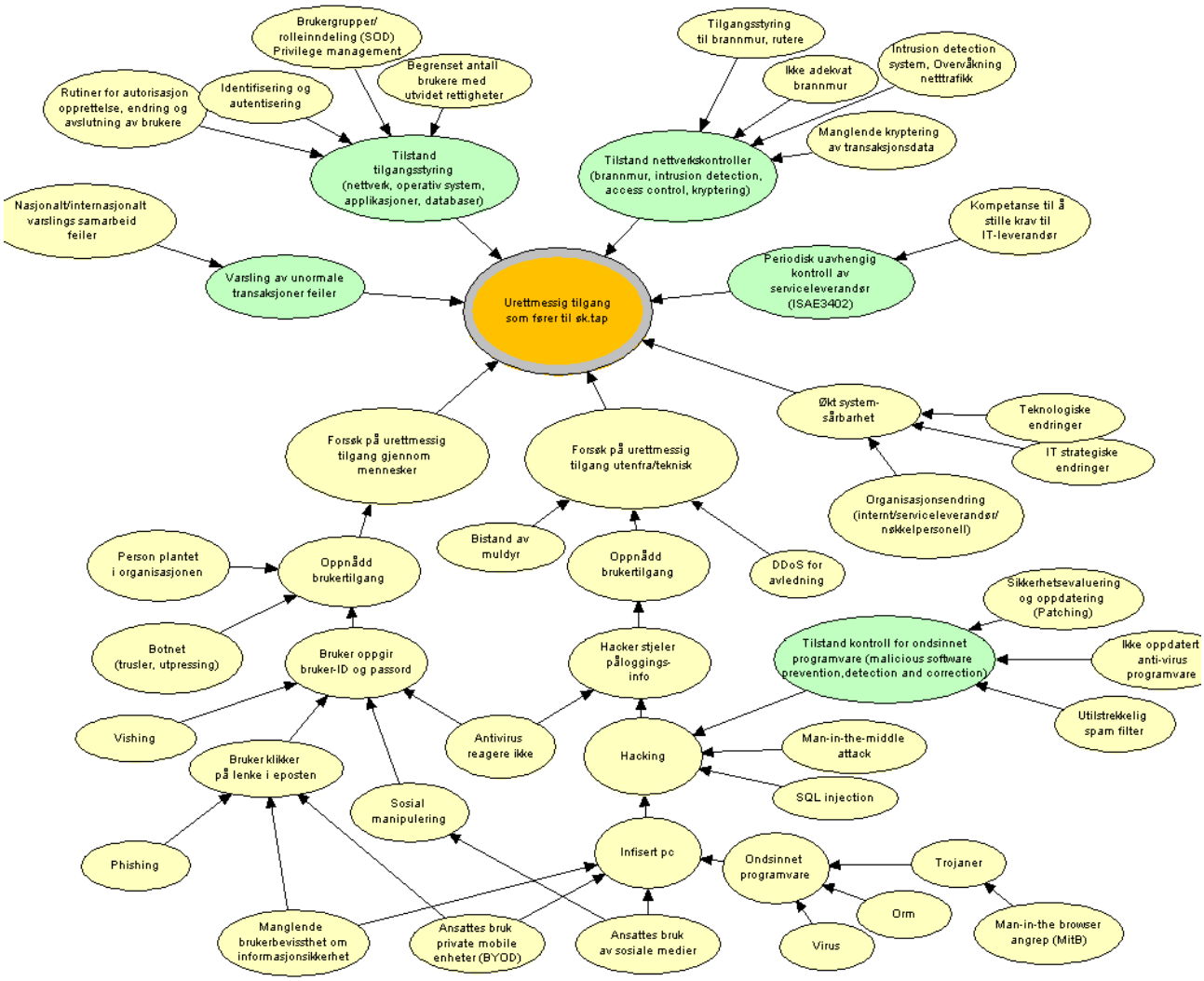
Tilstand uavhengig kontroll av serviceleverandør (ISA3402)

Attestasjonsuttalelser om kontroller hos en serviceorganisasjon. Benyttes for å vurdere om serviceleverandører har nødvendige rutiner og kontroller for å ivareta internkontroll og risikostyring for å holde risiko på et akseptabelt nivå. Type 2 rapport kontrollerer at kontrollene fungerer effektivt i hele den spesifiserte perioden. ISAE3402 er en internasjonal og norsk revisjonsstandard. Hensikten med rapporten er at serviceorganisasjonen gir en beskrivelse av relevante kontroller de

har implementert og at de fungerer effektivt. Kontroller som sikrer kvaliteten i en serviceorganisasjons drift.

Oversikt modell for urettmessig tilgang

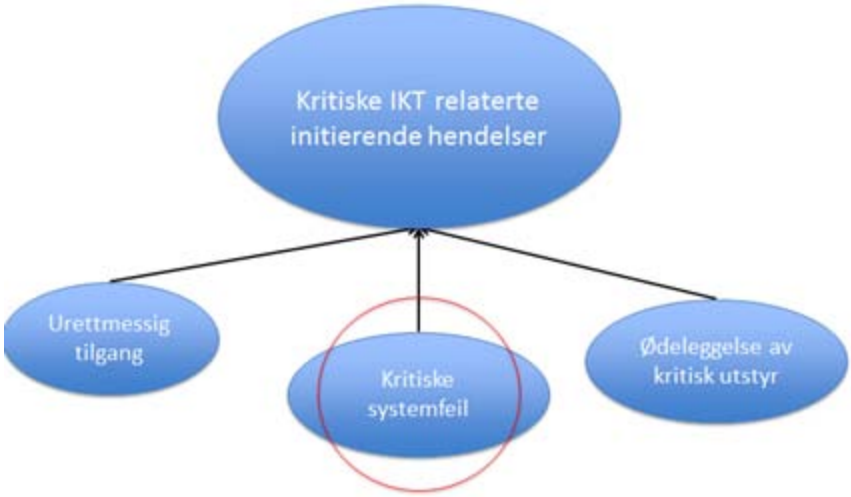
Modellen på neste side, figur 8, viser årsakssammenhenger og betingede og ubetingede avhengigheter for både forsøk på urettmessig tilgang gjennom mennesker og forsøk på tilgang utenfra/teknisk.



Figur 8: Urettmessig tilgang - årsaker og influerende faktorer til oppnåelse av urettmessig tilgang.

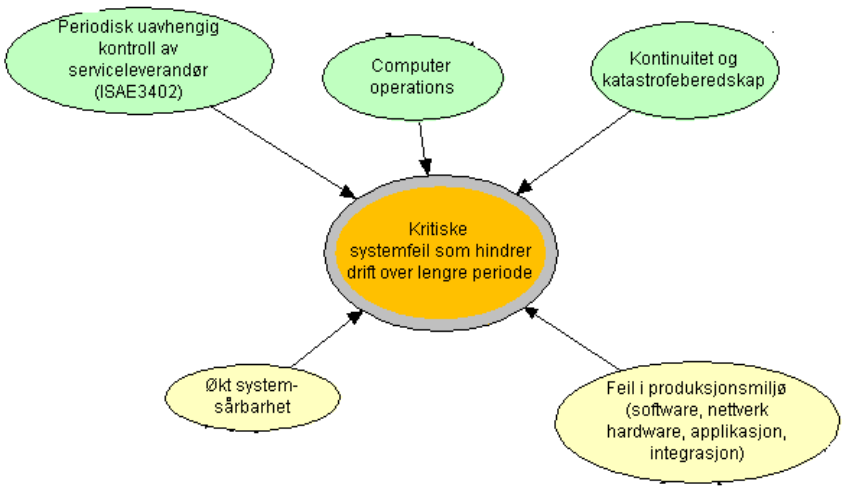
6.3 Kritiske systemfeil

Den andre identifiserte hovedkategorien IKT hendelser er kritiske systemfeil.

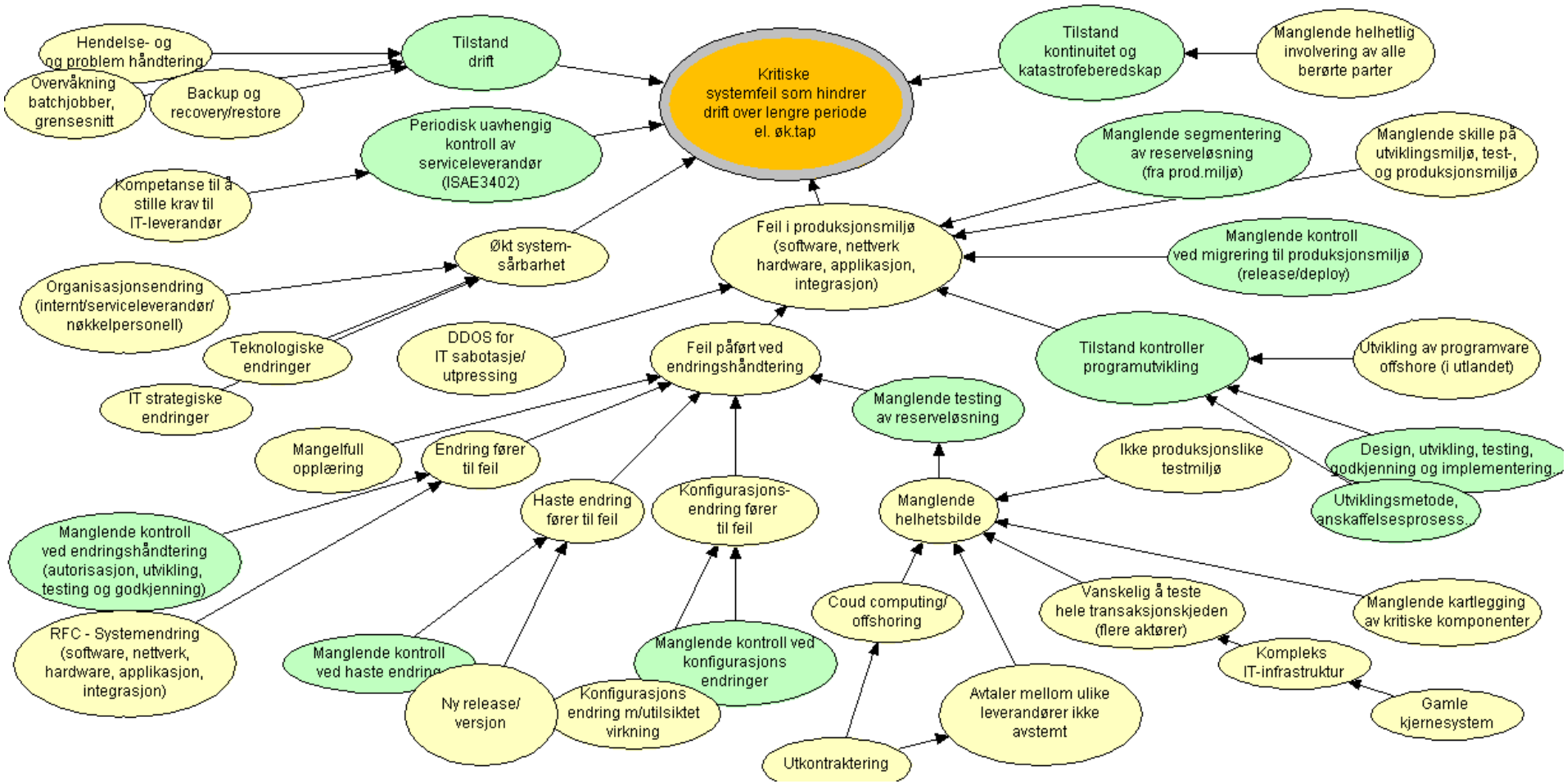


Figur 9: Kritiske IKT-relaterte initierende hendelser. Kritiske systemfeil.

Stans i forretningsdriften kan gi erstatningsansvar, tap av omdømme og i verste fall tap av konsesjon. Andre konsekvenser av systemfeil kan være er urettmessig pengeoverføring og direkte økonomisk tap. Kritiske systemfeil kan oppstå på flere punkter i bankens IKT-systemer og generelt kan man si at dersom en feil oppstår er det stor fare for følgefeil i andre systemer. Bankenes infrastruktur er svært kompleks, noe som både er en barriere for forsøk på hacking, men også en faktor til økt risiko og sannsynlighet for kritiske systemfeil.



Figur 10: Kritiske systemfeil – overordnet nivå.



Figur 11: Kritiske systemfeil- årsaker og influerende faktorer.

6.3.1 Årsaker til feil i produksjonsmiljø

Systemfeil kan gi stans i forretningsdriften. Det anses som kritisk dersom stansen vedvarer i 2 dager eller mer. Systemfeil kan også gi feil i data eller tap av data. Omdømme risiko omhandles ikke spesielt i denne oppgaven, men det bør nevnes at hyppig eller langvarig driftsstans vil kunne påvirke bankens omdømme.

Kritiske systemfeil skyldes feil i ulike deler av IKT nettverket. Det kan være applikasjonsfeil, feil i infrastruktur, konfigurasjonsfeil, feil i integrasjon og/eller feil i nettverkskomponent. En eller flere feil kan inntreffe samtidig, noe som kan utvikle seg til å bli enda mer kritisk dersom reserveløsningen ikke fungerer som den skal. Som vist i figur 11 over er det mange ulike årsaker til at feil kan inntreffe. Bankenes teknologiske infrastruktur er svært kompleks, og en feil ett sted kan også lede til feil andre steder i integrerte systemer.

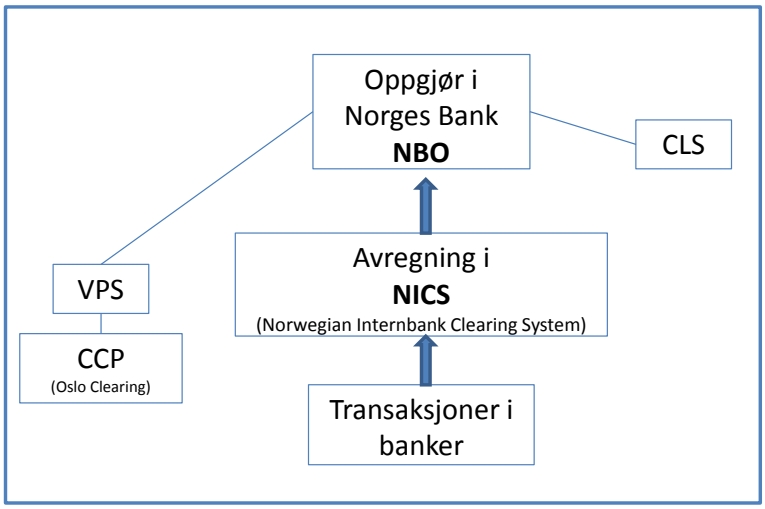
Gamle kjernesystem

De fleste bankene i Norge benytter kjernesystemer for kontoavregning og inn- og utbetalinger som er teknologisk gamle (Finanstilsynet, 2013). Koden til disse systemene ble utviklet på 80- og 90 tallet. Utviklingen har vært på utsiden av disse kjernesystemene, nye brukergrensesnitt er bygget på utsiden av det opprinnelige. Gamle IT systemer sys sammen med nye forretningsapplikasjoner og det legges nye moderne brukergrensesnitt i frontsystemene som for eksempel i nettbank. Å gjøre endringer og oppdateringer er blitt mer risikofylt på grunn av denne systemarkitekturen. Kompetansen på disse gamle systemene begynner også å bli mangelfull. Personene som i sin tid utviklet systemene og som har en oversikt over helheten er snart gått av med pensjon.

Kompleks IT infrastruktur

Bankenes IT infrastruktur er svært kompleks bestående av mange ulike komponenter og flere aktører involvert med ansvar for ulike deler av den elektroniske infrastrukturen. Systemet som er felles for alle bankene i Norge er interbanksystemet. Interbanksystemet er et system for avregning, oppgjør og overføring av penger mellom banker. Interbanksystemet er kjernen i den finansielle infrastrukturen. Norges Bank er konsesjonsmyndighet for interbanksystemer.

Norges Banks oppgjørssystem (NBO) ble etablert for å sikre effektiv og sikker håndtering av oppgjør. Avregningene av transaksjonene som inngår i nettooppgjørene i Norges Bank, gjøres hos NICS (Norwegian Interbank Clearing System).



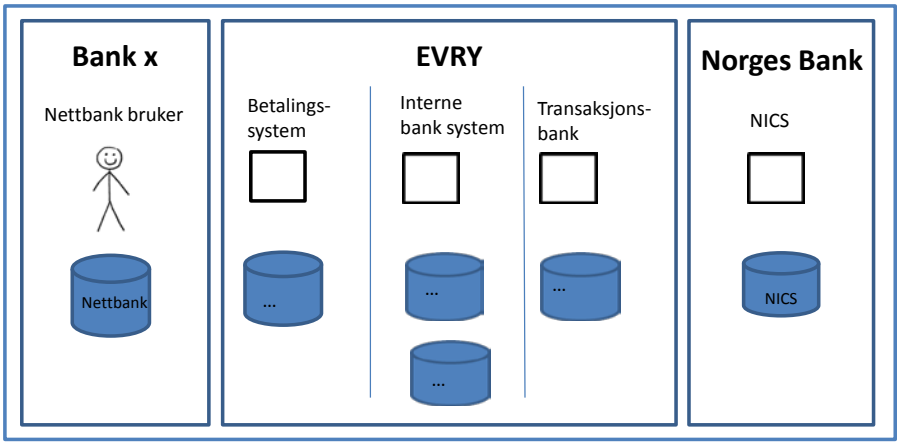
Figur 12: Norges interbanksystem, hentet fra "Årsrapport om betalingssystem 2011", Norges Bank.

Norges Bank tar i mot avregninger fra NICS og Verdipapirsentralen (VPS). Også bankenes pengeposisjoner fra handel med derivat gjennom Oslo Clearing (CCP) gjøres opp i Norges Bank.

Norges Bank deltar også i sentralbankenes overvåkning i det internasjonale valutaoppgjørssystemet (CLS) (Norges Bank, 2012).

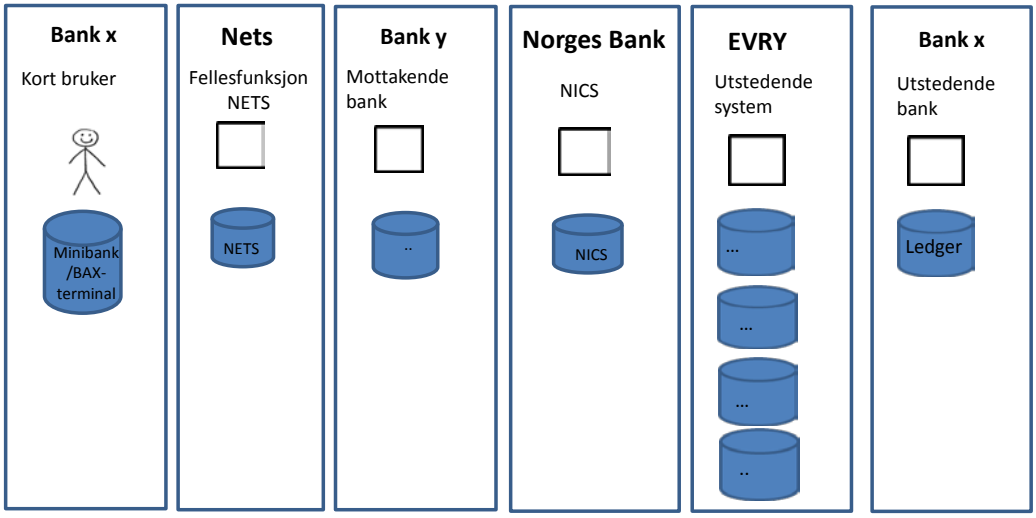
NICS er bankenes felles avregningssystem for norske kroner og benyttes av alle banker som deltar i banknæringens felles infrastruktur for betalingsformidling. Banker skal benytte NICS for utveksling av transaksjoner som inngår i banknæringens felles infrastruktur og som påvirker en banks posisjon i Norges Banks Oppgjørssystem (NBO). NICS driftes av Nets Infrastruktur AS.

Når en nettbank bruker foretar en betaling fra sin nettbank til en leverandør, går transaksjonen elektronisk gjennom flere systemer og aktører. Bankene er gjerne ansvarlige for egne nettbank-løsninger, men har utkontraktert andre deler av it-systemene. Se eksempelet i figuren under.



Figur 13: Komponenter i privat betaling nettbank.

Figur 14 under viser transaksjonskjeden for betaling med BankAxept-kort i kortterminal. Transaksjonen starter ved at kunder handler med bankkort. Autorisasjons- forespørsel og validering går gjennom alle systemer før selve transaksjonen utføres og oppdateres i mottakende- og utstedende bank samt kortholders konto. Avregning mellom ulike banker skjer gjennom NICS.



Figur 14: Betaling privat og bedriftskunder med bankkort.

Den norske felles kortinfrastrukturen består av systemene BALTUS og Best BDM. Baltus (Bankenes onLine Transaksjons Utvekslings System) er on-line dekningskontrollsystem hvor det er mulig å dekningskontrollere konti i alle banker for alle typer betalingsoppdrag, enten ved elektronisk forespørsel eller ved muntlig telefonkontakt. Bankenes Standardiseringskontor (BSK) eier programvaren. Best BDM er felles programvare for mottak av kortautorisasjoner fra Nets (BankAxept). BDM er en av IT serviceleverandøren EVRY's kritiske komponenter for å støtte bankenes kortkunder ved betaling med BankAxept-kort.

Systemarkitekturen er etter hvert blitt svært kompleks, og feil i deler av et system vil kunne få følger for hele systemet. Det kan også føre til mer ustabilitet på helheten og kan gi sikkerhetshull

Vanskelig å teste hele transaksjonskjeden/manglende helhetsbilde

På grunn av den komplekse teknologiske infrastrukturen, mange aktører involvert og mange ulike systemer som er integrert medfører at det er vanskelig å teste hele transaksjonskjeden.

Ikke produksjonslike testmiljø

Kompleksitet i IT-arkitekturen gjør det mer komplisert å ha full oversikt og oppdaterte testmiljø for alle applikasjoner. Dersom testmiljøene og evt. utviklingsmiljøene er forskjellige fra produksjonsmiljøet, kan endringer som testes i testmiljøet oppføre seg annerledes enn det de vil gjøre i produksjonsmiljøet. Dette kan føre til at endringer migreres til produksjon og gir utilsiktede virkninger som ikke er blitt oppdaget i test.

Bankens IT-infrastruktur - konsentrasjonsrisiko

Modellen for IT-risiko er med utgangspunkt i risikobildet for en enkeltstående bank allianse. Men, på grunn av at IT-infrastrukturen er så sammensatt, er det nødvendig at bankene skaffer seg et helhetlig bilde av arkitekturen og tilhørende risiko. Selv om banken har full kontroll på egne IT-systemer, er ikke det tilstrekkelig. Bankenes ulike IT-systemer er integrert med hverandre og underleverandørers IT-systemer. Flere aktører er involvert og har ansvaret for ulike deler av den digitale infrastrukturen. Dersom en komponent feiler ett sted, så kan dette få følger for hele infrastrukturen. Bankenes IT-risiko påvirkes med andre ord også av eksterne aktører og må derfor sees på som et analyseobjekt i et helhetlig risikoperspektiv.

Teknologisk utvikling har gjort det mulig å effektivisere IT-systemene ved at grensesnitt er bygget og systemene er blitt integrert med hverandre. På denne måten unngår en manuelt arbeid som å taste inn den samme informasjonen flere ganger i ulike system. Systemene «snakker» sammen og man oppnår en sømløs integrasjon. Transaksjoner føres elektronisk gjennom hele infrastrukturen uten manuelle inngrep. Dette er selvfølgelig en fordel, men det medfører også økt risiko. Feil i tjenesten ett sted kan føre til svikt i hele transaksjonskjeden. Man kan se på konsentrasjonsrisikoen som to delt. Det ene problemet er at den integrasjonen mellom tjenestene, det andre er at svært mange banker benytter seg noen få aktører. Dvs. at dersom en aktør, for eksempel Evry ASA har problem så rammer dette svært mange banker samtidig. Samfunnsmessig er sistnevnte et problem. Men, når vi ser på operasjonell risiko for en bestemt bank, så er ikke det like relevant. Et eksempel på en stor aktør er Nets. Nets forvalter og drifter både BankAxept, BankID og avregningssystemet NICS. BankAxept–kortet er det med brukte kortet i Norge. Over 8 av 10 kortbetalinger i Norge er med BankAxept (Finanstilsynet, 2013). Evry ASA er også en stor aktør. De fleste bankene utkontrakterer større eller mindre deler av IT-oppgaver til denne leverandøren.

Utkontraktering «Outsourcing»

Utkontraktering av IKT-tjenester er blitt mer vanlig. Dette drives frem av ønsker om å spare kostnader og tilgangen på kompetanse. Men, utkontraktering er også forbundet med risiko. Risiko omkring kvaliteten på IT-tjenestene, mangelfulle kontrakter og uklare ansvarsforhold mellom partene. Det kan være mangelfullt samarbeid mellom kunden og leverandøren, liten kontroll med leverandørens sikkerhetsregime, internkontroll og sikkerhetskultur. Det er derfor viktig at bankene setter konkrete krav til leverandøren og deres arbeid, gjennom aktiv styring og kontroll med leveransene.

Som vist i modellen har ansattes bevissthet omkring informasjonssikkerhet, bruk av sosiale medier samt bruk av private mobile påvirkning på risikoeksponeringen. Man kan anta at dersom banken har et tett samarbeid med leverandører over lengre tid og for eksempel ved at leverandørens ansatte

sitter i bankens lokaler, så vil bankens kontroll over leverandørens organisasjonskultur være betydelig større enn tilfellet vil være dersom leverandøren har kontorer i utlandet.

Utkontraktering til utlandet «cloud computing»

Det som beskrives som internetts største bankran utspant seg i februar i år. En organisert gruppe hadde planlagt et kupp i mange måneder. Hackere klarte å hacke seg inn på databaser i USA og midtøsten, og stjal kontonummer og pinkoder fra forhåndsbetalte betalingskort. Debetkort er forhåndsbetalt bankkort med et gitt beløp som kan brukes til betaling. De brukes for eksempel som gavekort, eller til å utbetale penger til personer som ikke har bankkonto. De stjålne opplysningene ble brukt til å kode magnetstripene på falske «dummy» kort. Det forhåndsbetalte beløpene som satte grensen for uttak på kortene ble endret til i praksis ubegrenset beløp. Prosjektet gikk under navnet «Unlimited Operation». I henhold til nøye planer ble så uttak fra forskjellige minibanker over hele verden foretatt av koordinerte medlemmer på samme tidspunkt. Ranerne hadde med seg ryggsekker og gikk fra minibank til minibank og tok ut kontanter. Til sammen ble kontanter for 45 million dollar, cirka 260 millioner kroner, tatt ut i USA, Japan og 24 andre land i løpet av noen få timer. Det blir sagt at operasjonen hadde en kirurgisk presisjon i forhold til tidsbruk, hvilke minibanker skulle ranes og hvor mye de kunne ta ut i hver uten å bli stoppet av automatiske grenser (IKT nytt.no, 2013). To arabiske banker ble rammet, henholdsvis National Bank of Ras Al-Khaimah PSC («Rakbank») i De forente Arabiske Emirater og Bank of Muscat i Oman. Men, det var ikke bankenes systemer som ble hacket. Bankene benyttet seg av underleverandører som hadde ansvaret for overføring av transaksjoner mellom kundene og banken. Svakhetene lå ikke hos bankene, men hos mellomleddet som sørger for at transaksjonene foretas. I dette tilfellet var det to indiske selskaper ElectraCard Systems og EnStage som var ansvarlige for de forhåndsbetalte kortene. Men, i Vesten generelt er det ikke vanlig å bruke denne type kort, og det er verdt å merke seg at kortene det dreide seg om ikke hadde brikke, bare magnetstripe.

Hendelser som dette gjør av det settes spørsmålstegn ved sikkerheten av lagring av sensitiv informasjon i utlandet (cloud computing) og sikkerheten generelt i indiske utkontrakterings selskaper. Dagens Næringsliv skriver at Finanstilsynene i Storbritannia og Sveits har kritisert sikkerheten som eksisterer ved indiske oursourcing selskaper som håndterer transaksjoner på vegne av britiske og sveitsiske finansinstitusjoner. Det advares spesielt om hvordan rekrutteringen av ansatte i India foretas. Det er ofte store mangler i CV-ene og heller ikke mulig å snakke med referanser (Dagens Næringsliv, 2013).

Utvikling i utlandet («Offshoring»)

Det kan utgjøre en risiko for bankene at utviklingen av programvare skjer i utlandet, såkalt «offshoring». Bankene bruker leverandører som har avdelinger i utlandet. For eksempel EVRY som er serviceleverandør for bl.a. Sparebanken 1 og DNB Nor har datterselskapene Infopuls i Ukraina og Span InfoTech i India. Selskapene driver både utvikling og driftsstøtte. Det er en reell mulighet at koden utviklet hos underleverandører inneholder bakdører eller ondsinnet kode (Ellison & Woody, 2010), (Zadeh & De Volder, 2007). Selv om bankene har rutiner for testing og validering av koden, så kan koden inneholde uoppdagede svakheter som kan utnyttes i ettertid. Offshoring/nearshoring kan gi kostnadsbesparelser og tilgang til ressurser, men det må tas forhåndsregler.

Korrupsjon kan være en større utfordring i andre land. På transparency.org sin oversikt for 2012 så ligger Ukraina på nivå med Den Sentral Afrikanske Republikk, Kongo og Syria med hensyn til korrupsjon (Transparency International, 2013). Dette er vesentlig mer enn India. På en skala fra 0-100 hvor 0 er verst, så er Ukraina på nivå 26, India 36 og Norge til sammenligning 85.

Det er av betydning hvilken utviklingsmetodikk som anvendes, hvilken sikkerhetskultur og holdninger de ansatte har, hvor lang erfaring har utviklerne, om det er høy turnover og hva lokale lover sier om intellektuell eiendomsrett og datapersonvern (Frank, 2005). Misbruk av kildekode enten ved ulovlig salg eller mangler i koden vil være ekstremt uheldig for banker å oppleve. Avstand og kulturelle forskjeller kan gjøre kommunikasjonen vanskeligere samt evnen til å innføre gode rutiner og internkontroll. Det innebærer også mindre kontroll med nevnte kritiske faktorer som; hvem som velges ut som programmerere, hvor lang erfaring de har, og hvor stor turnover det er i bedriften (Matloff, 2005). IT driftspraksis, kultur og lederskap vil påvirke graden av effektiv styring og kontroll.

Manglende kartlegging av kritiske komponenter

IKT-forskriften pålegger bankene å gjøre en kartlegging av kritiske komponenter både internt i organisasjonen, og hos serviceleverandørene. I tillegget til IKT-forskriften som kom i et rundskriv fra Finanstilsynet juni 2011, påpekes det at bankene er ansvarlige for å ha en samordnet beredskap med leverandører som står for drift/tjenester som involverer kritiske ikt komponenter.

Systemendring/haste endring/konfigurasjonsendring

Endringer utgjør alltid en risiko for å rokke ved stabiliteten i systemet. En enkelt endring testes gjerne for akkurat det den er tenkt å forbedre eller oppdatere, men kan kanskje påvirke andre ting som ikke er kjent i forkant eller testet for. Endringer som ikke er tilstrekkelig testet vil kunne medføre feil i produksjonsmiljøet. Manglende prosedyrer på for eksempel at all utvikling skal skje i

et separat utviklingsmiljø og testet i et separat testmiljø før det godkjennes og migreres (oversettes til et annet format, eller til en annen lagringsenhet) til produksjonsmiljøet (det miljøet som brukes for alle reelle transaksjoner). Utilsiktede konsekvenser av endringer kan medføre feil og evt. nedetid for å finne feilen og implementere korreksjoner eller reversere endringer.

Det bør finnes formelle prosedyrer for alle endringsforespørsler («RFC – Request for change»), inkludert vedlikehold og «patches», haste endringer og konfigurasjonsendringer.

Autorisasjon av system, applikasjon og infrastruktur endringer på hensiktsmessig nivå av forretnings og IT ledelse i forkant av utvikling bidrar til å forsikre at endringer vil møte brukerkravene og at de implementeres på en sikker måte. Se risikoreduserende kontroller for endringshåndtering forklart i neste avsnitt.

6.3.2 Risikoreduserende kontroller

Tilstand endringshåndtering

Endringshåndtering kontroller er nødvendige for at ikke større eller mindre systemendringer (driftsendringer og applikasjonsendringer) skal føre til systemfeil. Endringshåndteringskontroller har til hensikt å forsikre at rutiner er etablert for å sikre at endringer i eksisterende systemer/applikasjoner er autorisert, testet, godkjent, riktig implementert og dokumentert. Kontrollene vil typisk omfatte kontroller for;

- autorisasjon, utvikling, testing og godkjenning
- adskilte miljø for utvikling, test og produksjon
- migrering til produksjonsmiljø
- konfigurasjons endringer
- haste endringer

Endringer blir utført både av bankene selv og av IT-tjeneste leverandør. De fleste feil skjer i forbindelse med en endring. Bankene skal også ha kontroll med at leverandøren(e) har en tilfredsstillende endringshåndteringsprosess. Dette skal inngå som en del av kontrollene i en uavhengig periodisk kontroll av serviceleverandøren (se kapittel 7.1.3 – tilstand uavhengig kontroll av serviceleverandør ISAE3402).

Tilstand kontroller for programutvikling

Kontroller som skal sikre at programutvikling skjer i henhold til fastsatte rutiner for autorisasjon, testing, godkjenning, riktig implementering og dokumentering. Sikre at forretningsbehov blir dekket i tråd med overordnet IT strategi, risikoprofil etc. Sikre «fallback/backout» plan.

- Metode for utvikling/anskaffelse
- Design, utvikling, testing, godkjenning og implementering
- Data migrering til produksjon (deployment)

Manglende segmentering av reserveløsning

Reserveløsninger må være tilstrekkelig både fysisk og virtuelt adskilt fra produksjonsmiljøet. Dersom systemfeil oppstår i produksjonsmiljøet så må dette ikke påvirke reserveløsninger. Det kan være vanskelig å gjennomføre på grunn integrasjoner mellom flere systemer. Det er kanskje ikke alle deler av systemene som har ulike miljø for utvikling, testing og produksjon.

Manglende kontroll ved migrering til produksjon

Dette er en viktig kontroll ved endringshåndtering, den endelige godkjenningen av endringer eller oppdateringer før de settes i produksjon. Skal sikre at rutiner i endringshåndteringsporsessen er fulgt, og endringer følgelig trygt kan foretas i produksjonsmiljøet.

Tilstand drift («computer operations»)

Kontroller som skal sikre at system/applikasjons data prosessering. Kontroller for å forhindre ufullstendig overføring, duplisering etc.

- Overvåkning av on-line transaksjoner, batch jobber, integrasjoner
- Backup og recovery prosedyrer
- Incident og problem håndterings prosedyrer

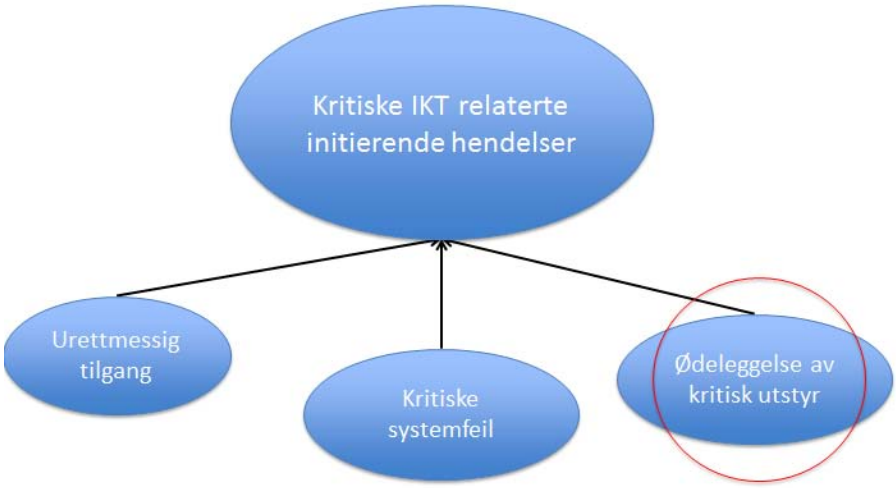
Tilstand kontinuitet og katastrofeberedskap

Kontinuitet og katastrofeberedskap. Kontroller for å sikre at dersom avbrudd eller alvorlige feil inntreffer, så blir det håndtert på en slik måte at kritiske forretningsprosesser blir gjenopprettet innen rimelig tid. IKT-forskriften stiller krav til dokumentert katastrofeplan, samt at det minst en gang årlig gjennomføres opplæring, øvelse og test i et omfang som gir tilstrekkelig trygghet for at katastrofeløsningen virker som forutsatt.

En årsak til svikt i kontinuitetsløsninger kan være manglende helhetlig involvering av alle berørte parter i IT-verdikjeden. På grunn av at flere aktører er ansvarlig for ulike deler av infrastrukturen, får en ikke testet alt samtidig. Man oppnår ingen ”tilstrekkelig” trygghet for at katastrofeløsningen virker dersom ikke alle er med og tester.

6.4 Ødeleggelse av kritisk utstyr

Den tredje hovedkategorien av kritiske IKT relaterte initierende hendelser er ødeleggelse av kritisk utstyr. Kritisk utstyr som data servere kan bli ødelagt enten bevisst av mennesker som ønsker å skade banken, eller ved ulykker. Beredskapsplaner, vedlikehold og internkontroll er viktig for å forebygge denne type kritiske hendelser. Ødeleggelser kan skyldes naturkatastrofer, sabotasje og hærverk, tyveri, brann, vannlekkasje, graving, strømbrudd og manglende vedlikehold. Alle de ulike årsakene kan inntreffe både lokalt, sentralt og hos underleverandør.



Figur 15: Kritiske IKT-relaterte initierende hendelser. Ødeleggelse av kritisk utstyr.

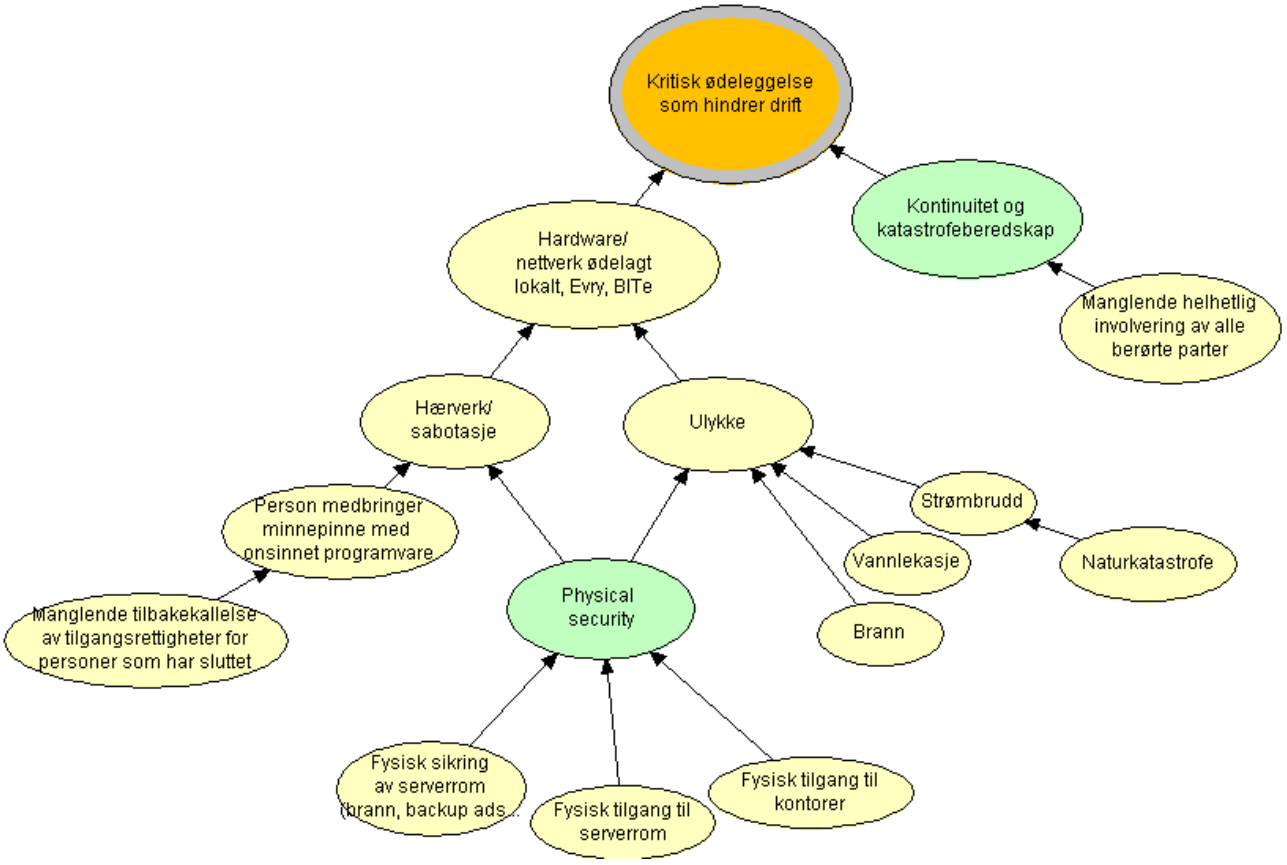
6.4.1 Årsaker til ødelagt hardware/nettverk

Naturkatastrofer

Et eksempel på hvilke situasjoner som kan oppstå ved naturkatastrofer er stormen «Sandy» som herjet USA og spesielt New York i fjor høst. Storbyens så kjente «skyline» så ut som en mørk spøkelsessilhuett etter at Sandy hadde truffet Manhattan med voldsom kraft. Uværet medførte at strømmen ble kuttet for anslagsvis 6,5 millioner mennesker over flere steder i USA.

Figur 16: Manhattan skyline etter strømbrudd.

En enkelt eksplosjon i et elektrisk anlegg nær 14th Street på Manhattan slo ut strømmen for 250.000 mennesker i byen. Strømleverandøren er ikke helt sikre på hva som forårsaket eksplosjonen, men at det er mulig vrakrester kan ha vært årsaken. Store vannmasser og kraftig vind førte til store skader (Aftenposten, 2012).



Figur 17: Kritisk ødeleggelse av utstyr

Sabotasje/Hærverk

Med tanke på hendelser som beskrevet i angrepet mot oljeselskapet Aramco, så er det nærliggende å tenke på hvor lett det vil være for personer som ønsker å skade banken av ulike grunner å medbringe en minnepinne med ondsinnet programvare å få den satt i en av bankens pc'er. Det kan

det tenkes at tidligere ansatte eller for eksempel konsulenter som har vært innom banken ikke har fått sin tilgang til lokalene trukket tilbake da oppdraget var ferdig vil utgjøre en trussel i denne sammenheng.

6.4.2 Internkontroll (kontroller/barrierer)

Det er to hovedkontroller (merket i grønt) for å minimere risikoen for ødeleggelse av kritisk utstyr. Den første er «fysisk sikring» og den andre «kontinuitet og beredskap», som er forklart tidligere i oppgaven under kritiske systemfeil. Fysisk sikring består av ulike preventive kontroller, mens kontinuitet og beredskap er kontroller som trer i kraft dersom en ulykke eller sabotasje skulle inntreffe.

Fysiske tilgangskontroller innebærer tilgangsstyring til serverrom og til kontor lokalene generelt. Kontrollene skal sikre at ikke urettmessig tilgang forekommer. Tilgang til serverrom bør til eksempel begrenses med fysisk sikring med lås og kode, og kun et fåtall ansatte bør ha kjennskap til koden. Serverrom bør være et brannsikkert rom, backup lokasjon bør være fysisk adskilt fra primær serverrom etc.

Prosedyrer for å innvilge, begrense og trekke tilbake tilgang til kontorlokaler og serverrom. Tilgang bør være behovsprøvd, autorisert, logget og overvåket. Dette bør gjelde alle som har tilgang til lokalene inkludert, ansatte, midlertidig ansatte, kunder, leverandører gjester og andre eksterne parter.

6.5 Helhetlig modell

Som nevnt tidligere i oppgaven viser erfaringer fra andre bransjer som olje & gass at modeller for analyse av operasjonell risiko bør kunne gi beslutningsstøtte ved å svare på spørsmålene om risikoen er høy eller lav og hvilke påvirkende faktorer er mest kritiske. Modellen bør også kunne svare på hva forskjellen er i risikoeksponeringen mht. ulike løsninger, og hvilken risikoreduserende effekt kan oppnås ved ulike risikoreduserende tiltak (Neil, Häger, & Andersen, 2009).

Kausale modeller modellert på et detaljert nivå vil fange opp effektene av daglige risikostyrings aktiviteter. Det grafiske aspektet ved Bayesianske nettverk (BN) oppfordrer til konstruktive diskusjoner rundt hendelser og årsakssammenhenger ved å visualisere mekanismene i tapsprosesser. Det visuelle aspektet gjør det også lettere å kommunisere informasjon omkring risikodrivere og risikoreduserende tiltak også til ansatte som ikke jobber med risikostyring til daglig. Det gjør informasjonen lettere tilgjengelig for alle enn avanserte statistikker som kun forstås av statistikere. BN gir troverdighet omkring resultatene med en gjennomsiktig og intuitivt strukturert kvantitativ

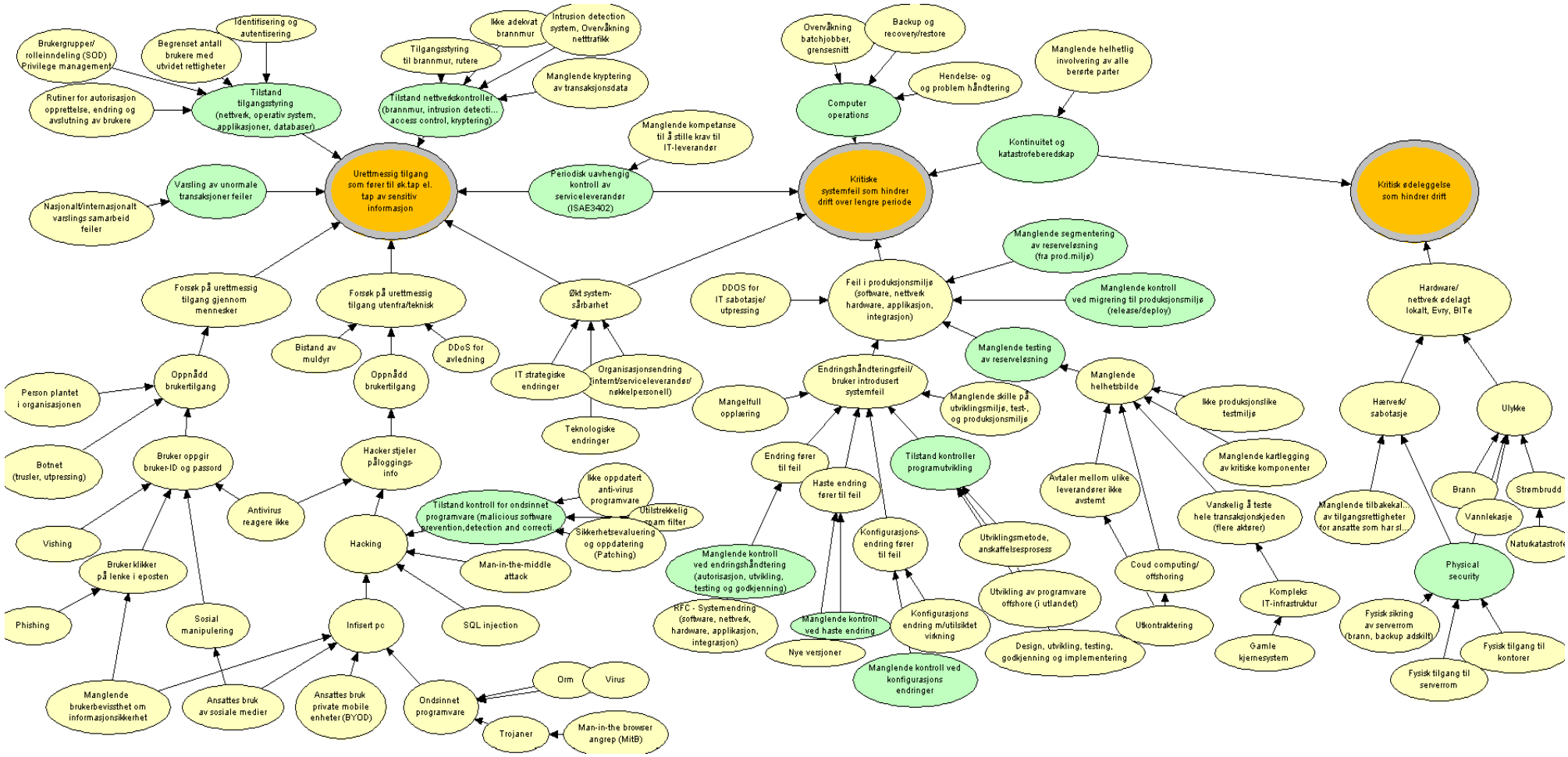
modell (Andersen & Häger , Modelling for the Analysis of Operational Risk - The Advanced Measurement Approach Reconsidered, 2012).

Modeller som skal møte kravene på AMA-nivå for operasjonell risiko iht. Basel II reguleringene skal produsere kvantitativ måling av den operasjonelle risikoen som reflekterer bankens individuelle risikoeksponering. Måling skal reflektere endringer i risikodrivere, som for eksempel svakheter i kontroller og/eller økt kompleksitet i aktivitetene etc. (Andersen & Häger , Modelling for the Analysis of Operational Risk - The Advanced Measurement Approach Reconsidered, 2012).

Tradisjonelle datadrevne modeller basert på historiske data vil i liten grad fange opp ”hale hendelser”. Hale hendelser er sjeldne hendelser med potensielt store konsekvenser. AMA forutsetter at hale hendelser fanges opp. Bayesianske nettverk baseres på all tilgjengelig kunnskap og har derfor muligheten til å fange opp ekstremhendelser. Risikostyring basert på all tilgjengelig kunnskap gir en framoverskuende og proaktiv holdning i stedet for å basere seg utelukkende på historiske data. Problemet er at operasjonell risiko skiller seg fra disse andre typene risiko ved at hendelsene er sjeldne og kan gi potensielt store tap, såkalte halehendelser. Det er vanskelig å basere fremtidig tapsforventning på historiske data. Det er også derfor AMA stiller krav til bruk av de 4 informasjonskildene.

På bakgrunn av dette så er det behov for nye metoder for kvantifisering av operasjonell risiko og metoder med en subjektiv forståelse av risikobegrepet. Som Andersen og Häger (Andersen & Häger, Objectivity and the Measurement of Operational Risk, Reconsidered, 2011) diskuterer så kan det settes spørsmålstegn ved om det er relevant å tilstrebe objektive risikotall med hensyn til operasjonell risiko. Kvantifiseringen bør i stedet ta utgangspunkt i all tilgjengelig kunnskap for å vurdere det reelle risikobildet. Organisasjoner lever i et læringsmiljø og vil hele tiden forbedre risikostyringen og tiltak basert på egne erfarte hendelser eller andre bankers historikk. Som Andersen og Häger hevder så er Bayesiansk nettverksmodellering en relevant metode for å modellere tapshendelser i henhold til en kunnskapsbasert tilnærming. For denne oppgaven er det derfor hensiktsmessig å benytte kausale nettverk som gjenspeiler årsaker og konsekvenser gjennom betingede sannsynligheter og bruken av Bayes teorem. Bayesianske nettverk er en metode som gjør det mulig å kombinere både observasjoner av historiske data samt relevant kunnskap og erfaring i scenario analysene. Dette gir en systematisk analyse av risiko.

En datadreven modell som utelukkende er basert på historiske data vil ikke gi svar på hvilke faktorer som er mest kritiske, hvilken risikoreduserende effekt tiltak har eller hva alternative løsninger har å si for risikoeksponeringen.



Figur 18: IKT-risiko i bank, BN

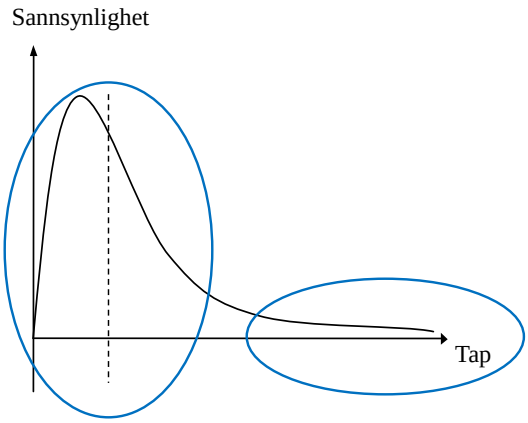
6.6 Beregning av økonomisk tap

Det endelige utfallet av modellen for tapsprosessen er tapsprediksjon.

Måling av operasjonell risiko er en utfordrende oppgave. Karakteristikkene til oprisk er avgjørende forskjellig fra både kredittrisiko, markedsrisiko og forsikringsrelaterte tap. På tross av dette har metodene for kvantifiseringen av risikoeksponeringen vært de samme. Men, dette et område under utvikling, og man søker å komme frem til metoder som er bedre egnet for oprisk.

Det som har utviklet seg til å bli «Beste praksis» for måling av operasjonell risiko for AMA er LDA «Loss Distribution Approach»). LDA er basert på historiske tapshendelser hvor en ser på tapsalvorlighet dvs. tapsbeløp og frekvens, dvs. hvor ofte en hendelse antas å inntreffe innenfor en gitt periode. Dette gir til sammen akkumulert tapsbeløp som kalles «Operational Value at Risk» (OpVaR). Metoden har som formål å beregne aggregert tap over en ettårs periode innenfor et konfidensintervall på 99,9%. Beregningsmetoden har sitt utspring i forskningsbransjen (Accumulated Claims Process) og aktuarisk matematikk (Andersen & Häger , Modelling for the Analysis of Operational Risk - The Advanced Measurement Approach Reconsidered, 2012). LDA knyttes normalt til datadrevne modeller. Det oppstår derfor problemer når denne metoden skal benyttes for å beregne «halehendelser» dvs. hendelser som inntreffer svært sjeldent med katastrofale tap (Häger & Andersen, A knowledge based approach to loss severity assesment in finance using Bayesian networks and loss determinants, 2009). Tradisjonelle datadrevne modeller viser ikke linken til årsakene til hvorfor risikoeksponeringen er høy eller lav.

Fordelen med Bayesianske nettverk er at man viser årsakene til risikoeksponeringen og at man kan inkludere data fra ulike kilder, ikke utelukkende historisk data. AMA stiller krav til bruk av data fra alle de fire datakildene; scenario genererte data, intern- og eksterne data, samt forretningsmiljø og interne kontrollfaktorer (BCEIF). Med hensyn til forventede tap som består av høyfrekvente tap med lav tapsalvorlighet så er datadrevne modeller velegnet. Mens scenariobaserte data og BCEIF («Business Environment and Internal Control Factors») data basert på ekspertkunnskap krever en annen tilnærming. Resultat fra de ulike datakildene skal også kombineres på en god måte.



Figur 19: Tapsfordeling høyfrekvente tap og lavfrekvente tap.

Vanligvis så er det slik at bankene har tilstrekkelig interne- og eksterne data av høy frekvente tap med lave tapsbeløp. Historiske data kan altså benyttes for å beregne forventet tap. Med denne metoden ser man tilbake i tid for å finne ut hva som kan komme til å skje igjen. Men, nå det gjelder halehendelser så finnes det lite både interne- og eksterne data tilgjengelig. Dette har ført til at man bruker scenariodata. Scenarioer er basert på ekspertkunnskap og bankenes eget forretningsmiljø og interne kontroll faktorer. Dette gir kvalifiserte forventninger til hva som kan skje i fremtiden. Scenario genererte data og historiske observasjoner gir parameter input til en LDA modell bestående av tapsalvorlighet og frekvens som igjen gir total tapsprediksjon. Kombinert vil frekvens og tapsalvorlighet vise fordelingen av de totale tap i hver at de kritiske hendelsene.

Det endelige utfallet av modellen for tapsprosessen er tapsprediksjon.

Totale tap beregnes av antall tapshendelser og tap generert av en enkelt hendelse.

$$L_t = \sum_{i=1}^{N_t} X_i$$

Lt = totale tap, per hendelseskategori eller totalt
Nt = antall tapshendelser på tidspunkt t (tapsfrekvens) inntruffet i intervallet 0-t sannsynligheten for at hendelsen inntreffer
Xi = tap generert av en enkelt hendelse, tapsalvorlighet = varighet * kostand per tidsenhet (tapsalvorlighet)

De enkelte utfall av en tilfeldig variabel kan ikke forutsies, men sannsynlighetsfordelingen vil beskrive sannsynligheten for at hvert mulige utfall vil inntreffe, og hvordan verdiene i et større utvalg normalt vil fordele seg.

Sannsynlighetsfordelingen for aggregert tap:

$$L_t = P(N=1)F_{X_1} + P(N=2)F_{X_1+X_2} + \ldots + P(N=n)F_{X_1+\ldots+X_n}$$

6.6.1 Sannsynlighetsfordeling - urettmessig tilgang

Når det gjelder urettmessig tilgang så kan vi si noe om antall angrep *n* i løpet av en bestemt tidsperiode for eksempel ett år, og vi har en sannsynlighet *p* for om angrepene lykkes. Usikkerhet mht. antall hendelser urettmessig tilgang antas å ha en binomisk fordeling bin(n, p).

Dersom vi gjør et forsøk *n* ganger, og det er samme sannsynlighet for suksess (sannsynlighet for urettmessig tilgang) *p* hver gang, så har vi et binomisk forsøk med sannsynlighetsfordelingen gitt ved:

$$P(X=x) = \binom{n}{x} p^x(1-p)^{n-x} \qquad \text{der } x = 0, 1, 2, \ldots, n .$$

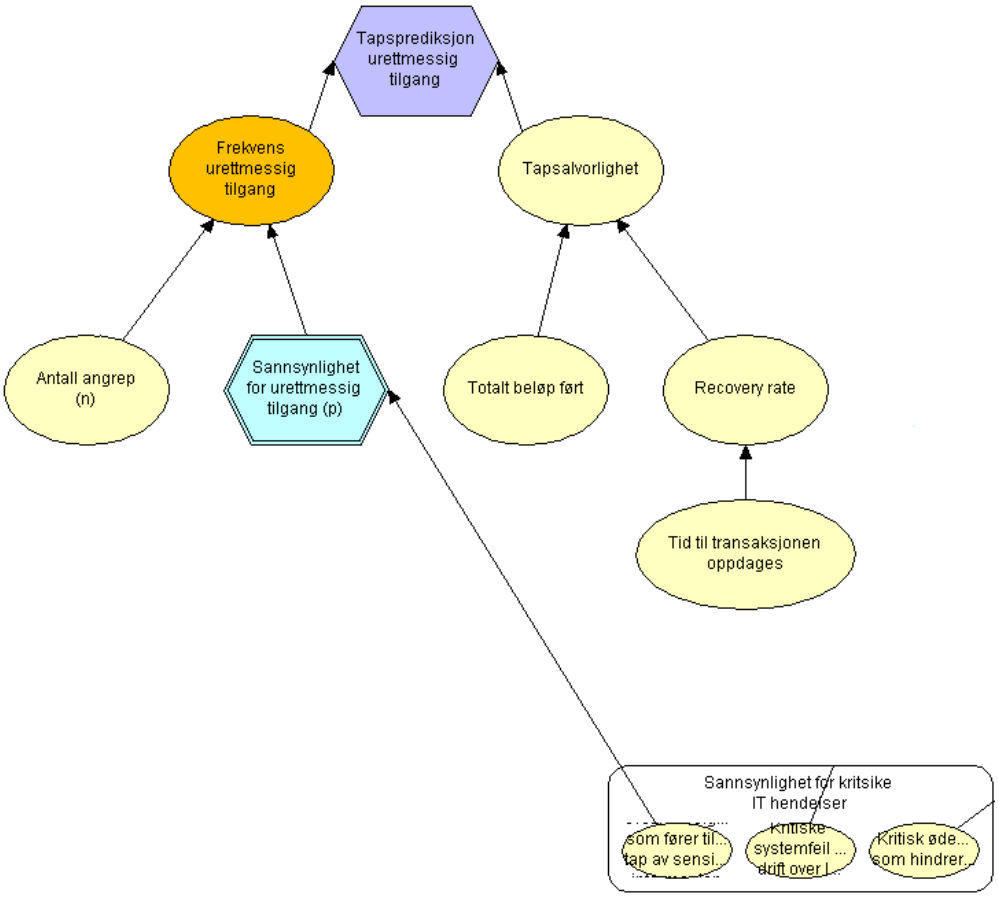
n = antall angrep
p = sannsynligheten for urettmessig tilgang
x = antall gunstige utfall

En binomisk fordeling er en diskret fordeling. Man deler populasjonen i to deler og sier at den ene hendelsen skjer med sannsynlighet p og den andre tingen skjer med sannsynligheten q og vi har p + q = 1. Myntkast er et eksempel på binomial fordeling. Sannsynligheten for å få en kron eventuelt mynt er p = 1/2. Sannsynligheten for at hendelsen skal inntreffe er den samme i alle forsøk. Hvert forsøk er uavhengige av det foregående slik at resultatet fra et forsøk ikke virker inn på det neste.

Dersom X er binomisk fordelt med sannsynlighet *p* for suksess i hvert delforsøk, så er forventningsverdien gitt ved:

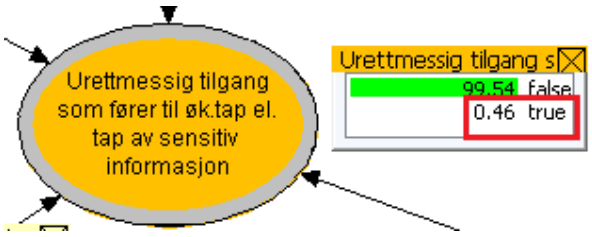
$E(X) = n \times p$

Sannsynlighetsfordelingen til den totale tapsprediksjonen fremkommer ved å kombinere hendelse frekvensen og tapsalvorlighetsfordelingen.



Figur 20: Tapsprediksjon urettmessig tilgang.

Usikkerheten rundt frekvensen for urettmessig tilgang er angitt med en binomisk fordeling (*n*, *p*). Antall angrep *n* i løpet av et år er angitt med en poisson fordeling. Sannsynligheten *p* for om angrepene lykkes er hentet fra modellens output node for hendelsen urettmessig tilgang som leder til tap, se figur 21. En output node er en node som inneholder delresultat som brukes som input til modellelementet som beskriver tapsprediksjonen til hendelsen, se figur 20.



Figur 21: Output node med sannsynlighet p for urettmessig tilgang.

Tapsalvorligheten er en funksjon av totalt beløp ført *a* og tilbakeført rate *r* «recovery rate» (beløp gjenvunnet av banken fra eventuelle tap). Tapsalvorlighet = *a* * (1-*r*).

Totalt beløp ført har en normalfordeling med intervall 1-10 millioner med forventet beløp satt til 1 million og varians til hundre tusen. Variansen beskriver forholdet mellom årsak og konsekvens, dvs.

dersom samtlige årsaker er i tilstand «true» hvor sikre er vi da på at også konsekvensen er i tilstand «true». Recovery rate avhenger av tid til oppdagelse. Dersom tap fra urettmessig tilgang oppdages tidlig, er gjenvinningsraten høyere enn dersom det oppdages sent.

Tapsprediksjonen for urettmessig tilgang er aggregert beregning av frekvens og tapsalvorlighet. Tapsprediksjonsmodellen er for øvrig basert på teori som fremkommer fra det tidligere beskrevne forskningsprosjektet «Operasjonell Risiko i Bank og Finansindustrien (oprisk)» ved Universitetet i Stavanger. Tapsprediksjonsmetoden er hentet fra teorien rundt modelleringen av urettmessige transaksjoner i det prosjektet.

6.6.2 Sannsynlighetsfordeling – nedetid (kritiske systemfeil)

Systemfeil kan føre til at større eller mindre deler av den teknologiske infrastrukturen blir berørt og kan være utilgjengelig for en periode. Avhengig av type feil og type system kan de ha ulik gjenopprettingstid. Dersom et IT-system er utilgjengelig over et lengre tidsrom, medføre dette at forretningsprosessene som er berørt ikke kan utføres. Det kan være for eksempel betalingsformidling eller finansiering. Dersom nettbanken er utilgjengelig pga. driftsproblemer vil ikke privat kunder eller bedriftskunder kunne utføre betalingene som vanlig. Låneformidling vil ikke være mulig dersom systemene for finansieringsprosessen er utilgjengelig. Tjenestene vil ikke kunne utføres noe som kan lede til økonomisk tap. På bakgrunn av dette definerer vi den største driveren av økonomisk tap fra kritiske systemfeil som nedetid (system utilgjengelighet).

System nedetid antas å ha en poisson-fordeling. Poisson-fordeling brukes dersom vi har hendelser som fordeler seg tilfeldig over for eksempel et bestemt tidsintervall. Forutsetningene for en poisson fordeling er at antall hendelser er uavhengige av hverandre, og forventet antall hendelser pr tidsenhet er konstant. Hendelser kan heller ikke inntreffe flere ganger helt samtidig/ oppå hverandre. Dette blir eksempler på stokastiske eller tilfeldige prosesser. Poissonfordelingen bestemmes av en parameter lambda (λ) som er forventet verdi, gjennomsnitt eller forventede hendelser per tidsenhet

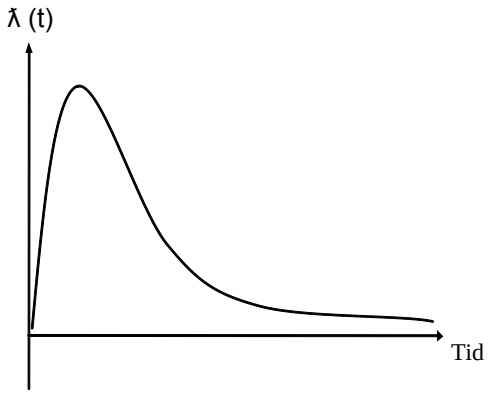
$$P(X=x) = \frac{\lambda^x}{x!}e^{-\lambda} \qquad x = 0, 1, 2, \ldots(\infty)$$

Formelen viser sannsynligheten for at faktoren som måles, antall systemfeil som gir nedetid X, inntreffer x antall ganger i løpet av et gitt tidsintervall.

x = antall ganger hendelen inntreffer i et gitt tidsrom
λ = forventet antall feil/nedetid pr. tidsenhet

I vårt eksempel erλ feilraten, eller nedetid -raten for IT-systemene. Fra bankens interne data kan vi finne den historiske feilraten. Vi ønsker videre i BN modellen å beregne nedetid-raten fremover i tid, den prediktive raten. Den prediktive feilraten er basert på både historiske data, ekspertkunnskap, organisasjonsspesifikk input og årsakssammenhengene i BN modellen. Det operasjonelle miljøet er i stadig forandring med teknologisk utvikling, nye produkturer og nye systemer. Som årsakssammenhengene i modellen viser, er det mange faktorer som påvirker eventuelle systemfeil og eventuell nedetid. Noen av bankens systemer, kjernesystemene, begynner å bli teknologisk gamle samtidig som personene med kompetanse på disse systemene har begynt å gå av med pensjon. Intensiteten av feil i kjernesystemene kan være voksende på grunn av aldringsfeil. På bakgrunn av endringene i det operasjonelle miljøet bør vi med fortrinn benytte oss av all tilgjengelig informasjon, i motsetning til utelukkende å se på historiske tall. Dette vil gi et mer troverdig risikobilde og en mer korrekt tapsprediksjon.

Utover antallet feilhendelser, er varighet av nedetid avgjørende for tapsprediksjonen. Tapsalvorlighet er proporsjonalt økende med nedetidens varighet.



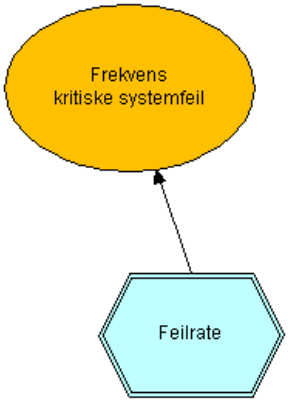
Figur 22: Nedetid fordeling.

$$f(x) = \frac{(\lambda \cdot t)^x}{x!} e^{-\lambda \cdot t}$$

Bruk: X er antall “hendelser” i et tidsintervall med lengde *t* (konstant feilrate, forventet antall hendelser per tidsenhet er λ).

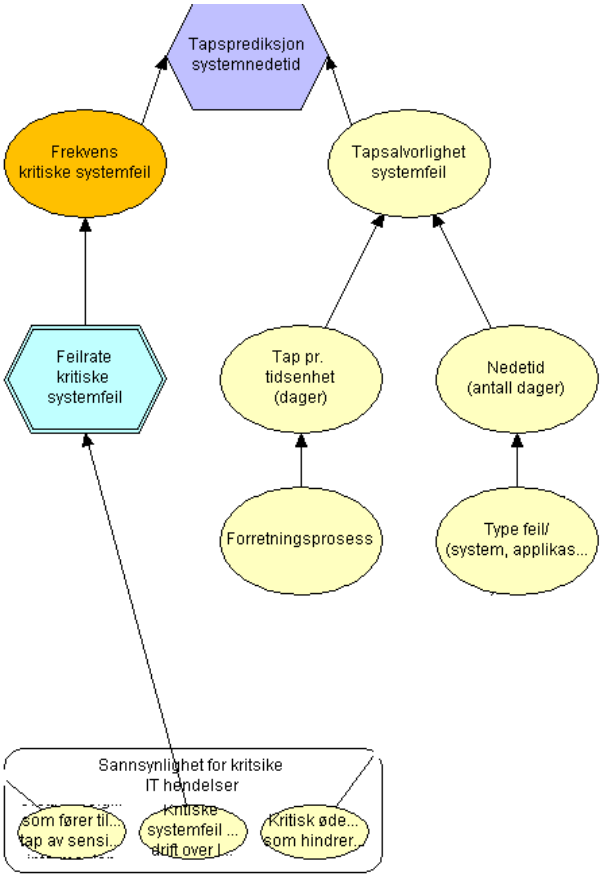
Forventningsverdi $E(X) = \lambda \cdot t$

Varians $Var(X) = \lambda \cdot t$



Figur 23: Frekvens kritiske systemfeil

Feilraten (λ) fremkommer av årsaksmodellen, med andre ord sannsynligheten som beregnes i outputnoden - kritiske systemfeil.



Figur 24: Tapsprediksjon kritiske systemfeil.

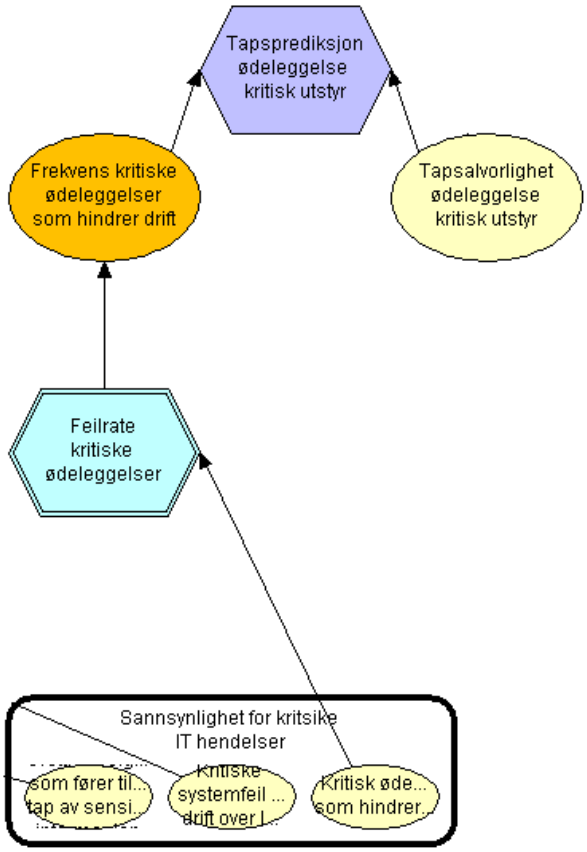
Tapsalvorlighet for kritiske systemfeil beregnes ut i fra en frekvens (feilrate) * tapsalvorlighet. Tapsalvorligheten er basert på tap pr tidsenhet (pr. dag), og nedetid (antall dager).

Tap pr. tidsenhet (pr. dag) varierer basert på type forretningsprosess. Bakgrunnen for det er «impact studier» gjort av banken som viser hvilke forretningsprosesser som er mest kritisk og hvordan det

eventuelt vil påvirke banken økonomisk. Nedetid (antall dager) varerier med om feilen gjelder en kritisk komponent eller en ikke-kritisk komponent.

6.6.3 Sannsynlighetsfordeling – ødeleggelse av kritisk utstyr

Ødeleggelse av kritisk utstyr innebærer fysisk skade på kritisk utstyr og evt. nedetid dersom beredskap og kontinuitetsløsninger ikke fungerer som forutsatt. Bankene er lovpålagt å ha redundante løsninger for kritiske systemer, men det kan måtte påregnes noe gjenopprettingstid. Det kan diskuteres om tapsalvorlighet bør beregnes basert på nedetid, eller økonomisk tap som følge av ødeleggelse av fysisk utstyr på hardware, kabler etc. Dette er relativt enkle endringer å gjøre i modellen, og bør drøftes i detalj med bankene for å komme frem til den beste løsningen. I denne oppgaven er det valgt å beregne potensielt tap ut i fra fysisk skade på utstyr. Tanken bak det er at dersom noe fysisk utstyr er ute av drift, så vil det være umiddelbar aktivitet for å bytte ut skadet utstyr, evt. gå over på reserveløsning. Dersom reserveløsning fungerer som forutsatt, vil det økonomiske tapet være det fysiske utstyret. Ved en kritisk systemfeil så er situasjonen annerledes, sannsynligvis pga. kompleks infrastruktur så vil en måtte lete etter hvor feilen er og hva som forårsaker den, det vil så bli iverksatt arbeid med å korrigere feilen, teste korreksjoner i testmiljø iht til prosedyrer for så å migrere (overføre) rettelsen til produksjonsmiljøet. I det tilfellet så er det nedetid som er tapsdriveren.



Figur 25: Tapsprediksjon ødeleggelse av kritisk utstyr.

Feilraten for ødeleggelse av kritisk utstyr antas å ha en poisson-fordeling.

6.7 Sensitivitetsanalyse

Valideringen av modellen gjøres ved sensitivitetsanalyse. Ytterkant scenarioer benyttes for å se om modellen responderer som forutsatt og gir resultater som er troverdige. Modellen i denne oppgaven er en kunnskapsbasert modell og har til hensikt å vekke tillitt omkring resultatene. Nettverket er basert på subjektiv vurdering og metoden for validering baseres derfor på begrunnelse for årsakssammenhenger, grunnlag fra fag litteratur og ulike eksperters vurderinger av årsaker og sannsynlighet.

For å validere modellen, så må vi også se på hva som er hensikten med modellen. Målet for modellen er at den skal være et verktøy for beslutningstøtte i risikostyringsarbeidet, og i tillegg benyttes for kvantifisering av risikoeksponeringen. Den skal oppfylle kravene til AMA-modeller som bl.a. innebærer «use test».

Stegene for validering:

1) Oppnå troverdighet gjennom diskusjon og bidrag fra ulike eksperter
2) Sensitivitetsanalyse, kalibrering av modell ved ulike scenario, best case, worst case scenario
3) Vurdering av om modellen tilfredsstiller kravene til AMA-modeller, use-test etc.

6.7.1 Vurdering og bidrag til modell fra ulike eksperter

Som tidligere nevnt så ble risikoidentifikasjonen foretatt med en gruppe eksperter bestående av 6 personer hos en lokal bank. Modelleringen av årsakssammenhengene er i tillegg basert på fag litteratur, tapshendelse databasen fra 6 banker, samt egne erfaringer.

For å få en vurdering og bidrag fra en person med høy kompetanse innen teknologi og risikostyring utenfor banken, kontaktet vi daglig leder i BSK (Bankenes Standardiserings Kontor). BSK er eid av norske banker, og har ansvaret for å ivareta forvaltning og videreutvikling av norske bankstandarder innen betalings- og informasjonsformidling i bankenes felles infrastruktur (Bankenes Standardiserings Kontor (BSK), 2013) . BSK er også ansvarlige for sikkerheten i de standardiserte norske løsningene. BSK samarbeider både med bankene, FNO og Finanstilsynet, vi anser derfor organisasjonen som særdeles relevant i vurderingen av årsaksbildet til norske bankers risikoeksponering og utviklingen i teknologiske løsninger fremover.

Møtet ble avholdt i Oslo på BSK's kontorer med daglig leder. BN nettverket ble gjennomgått og årsaker med årsakssammenhenger ble diskutert, og nye faktorer ble introdusert. Et viktig innspill som daglig leder kom med var i forhold til hva som var analyse objektet. Daglig leder påpekte at bankene i dagens infrastruktur og med store deler av IT-virksomheten utkontraktert var svært avhengig av eksterne parter og at risikoanalysen burde omfatte alle aktørene som er involvert i hele transaksjonsprosessen. Dette har forfatteren tatt til etterretning og følgelig identifisert aktørene som i hovedsak er involvert i betalingsprosessene. Som nevnt tidligere i oppgaven er bankenes teknologiske infrastruktur svært kompleks noe som i høyeste grad har påvirkning på risikoeksponeringen.

6.7.2 Kalibrering av modell - scenario analyse

Kalibrering av modellen har til hensikt å vurdere modellens egnethet eller relevans. Dette gjøres ved å vurdere modellens evne til å reflektere påvirkende faktorer på risikoeksponeringen. Ved å se på hvordan modellen oppfører seg under ulike scenarioer, beste case, nøytralt og verste case scenario om resultatet virker troverdig.

Scenario – urettmessig tilgang

Urettmessig tilgang					
Best Case - sannsynlighet for at hendelsen inntreffer	0,49 %	**Nøytralt Case - sannsynlighet for at hendelsen inntreffer**	74,80 %	**Worst Case - sannsynlighet for at hendelsen inntreffer**	100,00 %
Uventet tap 99,9% (NOK mill.)	2,00	**Uventet tap 99,9% (NOK mill.)**	10,60	**Uventet tap 99,9% (NOK mill.)**	11,68
Kontroller:	**Tilstand**	**Kontroller:**	**Tilstand**	**Kontroller:**	**Tilstand**
Varsling unormale transaksjoner	Effektiv	Varsling unormale transaksjoner	No evidence	Varsling unormale transaksjoner	Ikke effektiv
Tilstand tilgangsstyring	Effektiv	Tilstand tilgangsstyring	No evidence	Tilstand tilgangsstyring	Ikke effektiv
Tilstand kontroll for ondsinnet progra	Effektiv	Tilstand kontroll for ondsinnet progra	No evidence	Tilstand kontroll for ondsinnet progr	Ikke effektiv
Tilstand nettverkskontroller	Effektiv	Tilstand nettverkskontroller	No evidence	Tilstand nettverkskontroller	Ikke effektiv
Periodisk uavhengig kontroll	Effektiv	Periodisk uavhengig kontroll	No evidence	Periodisk uavhengig kontroll	Ikke effektiv
Årsaker:		**Årsaker:**		**Årsaker:**	
Phishing	No evidence	Phishing	No evidence	Phishing	No evidence
Vishing	No evidence	Vishing	No evidence	Vishing	No evidence
Trojaner	True	Trojaner	True	Trojaner	True
Virus	No evidence	Virus	No evidence	Virus	No evidence
Orm	No evidence	Orm	No evidence	Orm	No evidence
DDoS	No evidence	DDoS	No evidence	DDoS	True
Bistand av muldyr	No evidence	Bistand av muldyr	No evidence	Bistand av muldyr	True
Manglende brukerbevissthet	False	Manglende brukerbevissthet	No evidence	Manglende brukerbevissthet	True
Ansattes bruk av sosiale medier	False	Ansattes bruk av sosiale medier	No evidence	Ansattes bruk av sosiale medier	True
Ansattes bruk av private mobile enhe	False	Ansattes bruk av private mobile enhe	No evidence	Ansattes bruk av private mobile enh	True
Anitvirus reagerer ikke	False	Anitvirus reagerer ikke	No evidence	Anitvirus reagerer ikke	True
Sosial manipulering	No evidence	Sosial manipulering	No evidence	Sosial manipulering	No evidence
Bruker klikker på lenke	No evidence	Bruker klikker på lenke	No evidence	Bruker klikker på lenke	No evidence
SQL injection	No evidence	SQL injection	No evidence	SQL injection	No evidence
Man-in-the-middle attack	No evidence	Man-in-the-middle attack	No evidence	Man-in-the-middle attack	No evidence
Man-in-the-browser attack	No evidence	Man-in-the-browser attack	No evidence	Man-in-the-browser attack	No evidence
Botnet	No evidence	Botnet	No evidence	Botnet	No evidence
Økt system sårbarhet	False	Økt system sårbarhet	No evidence	Økt system sårbarhet	True
Person plantet i organisasjonen	False	Person plantet i organisasjonen	No evidence	Person plantet i organisasjonen	True

Figur 26: Scenario analyse, urettmessig tilgang.

Alle tre scenario tar utgangspunkt i at vi er sikre på at det eksisterer et forsøk på urettmessig tilgang. Type forsøk er satt til trojaner, det kunne også vært satt bevis for en annen type forsøk. Grunnen til at det er satt bevis for forsøk, er at vi ikke kan måle ytelsen til kontrollene dersom det ikke er forsøk på urettmessig tilgang.

Best case tilsvarer input "effektiv" for kontroll noder «false» mht. variabler som gjelder internt regulerbare faktorer som henger sammen med organisasjonskulturen eller interne retningslinjer.

Scenario 1: Best case

Et slikt tap virker fornuftig, da det fortsatt kan inntreffe urettmessig tilgang. Men ved å redusere sannsynligheten for urettmessig tilgang bankene bli påført et betydelig mindre tap.

Scenario 2: Nøytralt case

Virker rimelig å anta et relativt høye tapstall fordi en i dette caset ikke vet om kontrollene fungerer eller ikke, og samtidig har høy sannsynlighet for eksterne og interne forsøk på urettmessig tilgang. I nøytralt case er input nodene normalisert dvs. at sannsynlighet er lik for alle tilstander. For boolske input noder betyr det at true/false har samme sannsynlighet, altså 50 %.

Scenario 3: Worst case

Hendelsen inntreffer med 100% sannsynlighet pga. en antar at ingen kontroller fungerer effektivt og flere påvirkende faktorer inntreffer samtidig. Det er samtidig en usunn organisasjonskultur angitt ved manglende brukerbevissthet omkring informasjonssikkerhet. På samme tid er organisasjonen i en sårbar posisjon ved at det pågår organisasjonsendringer og/eller systemendringer.

Dette scenariet viser at urettmessig tilgang ser ut til å være en betydelig risiko, potensielt tapsbeløp er i denne modellen vurdert til å bli betraktelig høyere enn ved kritiske systemfeil eller ødeleggelse av utstyr. Dette kan stemme med utviklingen vi har sett med stadig mer avanserte angrep sammen med rask teknologisk utvikling, så er det en utfordring for bankene å være i forkant og stadig oppdatere barrierene.

Scenario – kritiske system feil

Kritiske systemfeil					
Best Case - sannsynlighet for at hendelsen inntreffer	0,00 %	**Nøytralt Case - sannsynlighet for at hendelsen inntreffer**	43,00 %	**Worst Case - sannsynlighet for at hendelsen inntreffer**	83,00 %
Uventet tap 99,9% (NOK mill.)	0,01	**Uventet tap 99,9% (NOK mill.)**	3,45	**Uventet tap 99,9% (NOK mill.)**	4,93
Kontroller:	**Tilstand**	**Kontroller:**	**Tilstand**	**Kontroller:**	**Tilstand**
Tilstand periodisk uavhengig kontroll	Effektiv	Tilstand periodisk uavhengig kontroll	No evidence	Tilstand periodisk uavhengig kontrol	Ikke effektiv
Tilstand computer operations (drift)	Effektiv	Tilstand computer operations (drift)	No evidence	Tilstand computer operations (drift)	Ikke effektiv
Tilsand kontinuitet og katastrofebere	Effektiv	Tilsand kontinuitet og katastrofebere	No evidence	Tilsand kontinuitet og katastrofebere	Ikke effektiv
Manglende segmentering av reservel	False	Manglende segmentering av reservel	No evidence	Manglende segmentering av reserve	True
Manglende kontroll ved migrering til	Effektiv	Manglende kontroll ved migrering til	No evidence	Manglende kontroll ved migrering til	Ikke effektiv
Tilstand kontroll programutvikling	Effektiv	Tilstand kontroll programutvikling	No evidence	Tilstand kontroll programutvikling	Ikke effektiv
ikke produksjonslike testmiljø	False	ikke produksjonslike testmiljø	No evidence	ikke produksjonslike testmiljø	True
Årsaker:		**Årsaker:**		**Årsaker:**	
Mangelfull opplæring	No evidence	Mangelfull opplæring	No evidence	Mangelfull opplæring	No evidence
DDoS for sabotasje/utpressing	No evidence	DDoS for sabotasje/utpressing	No evidence	DDoS for sabotasje/utpressing	No evidence
Utkontraktering	No evidence	Utkontraktering	No evidence	Utkontraktering	No evidence
Endring med utilsikted feil	True	Endring med utilsikted feil	True	Endring med utilsikted feil	True
Hasteendring med utilsikted feil	No evidence	Hasteendring med utilsikted feil	No evidence	Hasteendring med utilsikted feil	No evidence
Konfigurasjonsendring med utilsikted	No evidence	Konfigurasjonsendring med utilsikted	No evidence	Konfigurasjonsendring med utilsikte	No evidence
Økt system sårbarhet	False	Økt system sårbarhet	No evidence	Økt system sårbarhet	True
Manglende kartlegging av kritiske kon	False	Manglende kartlegging av kritiske kon	No evidence	Manglende kartlegging av kritiske ko	True
Manglende skille på utviklingsmiljø, t	False	Manglende skille på utviklingsmiljø, t	No evidence	Manglende skille på utviklingsmiljø,	True
Kompleks IT-infrastruktur	No evidence	Kompleks IT-infrastruktur	No evidence	Kompleks IT-infrastruktur	No evidence
Gamle kjernesystem	No evidence	Gamle kjernesystem	No evidence	Gamle kjernesystem	No evidence

Figur 27: Scenario analyse, kritiske systemfeil.

Scenario 1: Best case

Det kan tenkes at effektive kontroller vil kunne begrense tapet nesten til null. Det er angitt bevis for at systemfeil inntreffer, men effektive kontroller reduserer sannsynligheten for kritiske systemfeil til tilnærmet lik 0%. Det er verdt å merke seg at dersom beløpsintervallene er angitt med en finmasket diskretisering, så bidrar det til bedre å få frem nyansene i tapsbeløp ved mindre prosentuelle endringer i sannsynlighet.

Scenario 2: Nøytralt case

Virker rimelig å anta et relativt høye tapstall fordi en i dette caset ikke vet om kontrollene fungerer eller ikke, og samtidig har høy sannsynlighet for at systemfeil kan inntreffe. I nøytralt case er input nodene normalisert dvs. at sannsynlighet er lik for alle tilstander. For boolske input noder betyr det at true/false har samme sannsynlighet, altså 50 %. Det er med andre ord stor sannsynlighet for alle årsaker å inntreffe.

Scenario 3: Worst case

Hendelsen inntreffer med 83% sannsynlighet pga. en antar at ingen kontroller fungerer effektivt og flere påvirkende faktorer inntreffer samtidig. Tapet kan bli relativt høyt.

Scenario - ødeleggelse av kritisk utstyr

Ødeleggelse av kritisk utstyr					
Best Case - sannsynlighet for at hendelsen inntreffer	0,30 %	**Nøytralt Case - sannsynlighet for at hendelsen inntreffer**	9,00 %	**Worst Case - sannsynlighet for at hendelsen inntreffer**	90,00 %
Uventet tap 99,9% (NOK mill.)	0,16	**Uventet tap 99,9% (NOK mill.)**	0,39	**Uventet tap 99,9% (NOK mill.)**	0,85
Kontroller:	**Tilstand**	**Kontroller:**	**Tilstand**	**Kontroller:**	**Tilstand**
Tilstand kontinuitet og beredskap	Effektiv	Tilstand kontinuitet og beredskap	No evidence	Tilstand kontinuitet og beredskap	Ikke effektiv
Physical security	Effektiv	Physical security	No evidence	Physical security	Ikke effektiv
Årsaker:		**Årsaker:**		**Årsaker:**	
Brann	True	Brann	True	Brann	True
Strømbrudd	No evidence	Strømbrudd	No evidence	Strømbrudd	No evidence
Vannlekasje	No evidence	Vannlekasje	No evidence	Vannlekasje	No evidence
Manglende tilbakekallelse av tilangsti	No evidence	Manglende tilbakekallelse av tilangst	No evidence	Manglende tilbakekallelse av tilangs	No evidence
Naturkatastrofe	No evidence	Naturkatastrofe	No evidence	Naturkatastrofe	No evidence

Figur 28: Scenarioanalyse, ødeleggelse av kritisk utstyr.

Scenario 1: Best case

Ved effektive kontroller, er det rimelig å anta at sannsynligheten vil bli svært lav og følgelig øavt potensielt økonomisk tap.

Scenario 2: Nøytralt case

I nøytralt case er det ikke gitt bevis for at kontrollene fungerer men med tanke på at man har både preventive kontroller og beredskap i etterkant burde ikke tapene bli så store.

Scenario 3: Worst case

Tapsprediksjonen for verste scenario er ikke høy sammenlignet med kritiske systemfeil eller urettmessig tilgang, argumentasjonen for det er selv om en naturkatastrofe inntreffer og ødelegger mye utstyr, så vil det allikevel være mulig for banken å være tilbake i drift på relativt kort tid. Bankens data og systemer er speilet eller det finnes backup på fysisk separate lokasjoner, som sikrere dette. Tapsbeløp i fysisk utstyr er sannsynligvis ikke kritisk.

Det er ikke gjort beregninger av verdien for et eventuelt tap av sensitiv informasjon. Det er vanskelig å beløpsfeste, det ville i høy grad hatt påvirkning på bankens omdømme. Omdømme risiko er ikke omhandlet i denne oppgaven.

6.7.3 Sensitivitetsanalyse

Formålet med sensitivitetsanalysen er å vurdere hvorvidt modeller gir resultater som samsvarer med tilgjengelig kunnskap og observerte data. Testen skal gi et bilde av hvordan forskjellige input variabler er vektlagt i forhold til hverandre i modellen. Dette for å avdekke de årsakene som har størst effekt på risikoeksponeringen. Nodene rangeres i forhold til påvirkningskraft ved å angi bevis på en og en node og lese av resultatet i output noden.

Når påvirkningskraften til nodene testes, er det valgt å sette bevis på at det er observert den dårligste tilstanden pr hver enkelt input node. Ved testingen av påvirkningskraften til enkeltvis variabler forutsettes «nøytral» tilstand for de øvrige input variablene (se forklaring under nøytralt case).

Endringen i (p) er målt mot sannsynligheten i nøytralt case med bevis for at det er satt bevis for inntruffet forsøk på urettmessig tilgang (trojaner). Bevis er satt på trojaner, det kunne også vært en annen type forsøk på urettmessig tilgang. Bevist som settes i testen i forhold til forsøk på urettmessig tilgang (i dette tilfellet trojaner) bør settes slik at en får testet effekten av alle kontroller etc., at ikke beviset forskyver sannsynligheter på en uhensiktsmessig måte.

Figuren under viser rangeringen av årsakene til urettmessig tilgang.

Ranering av input noder	Navn på input node	Sannsynlighet (p) for urettmessig tilgang	Endring i (P) for urettmessig tilgang gitt dårligste tilstand i input noden
1	Person plantet i organisasjonen	85,97 %	11,17 %
3	Anitvirus reagerer ikke	83,54 %	8,74 %
4	Varsling unormale transaksjoner	83,21 %	8,41 %
5	DDoS	79,59 %	4,79 %
6	Bistand av muldyr	78,00 %	3,20 %
7	Bruker klikker på lenke	77,42 %	2,62 %
8	Tilstand tilgangsstyring	77,39 %	2,59 %
9	Tilstand kontroll for ondsinnet programva	77,39 %	2,59 %
10	Periodisk uavhengig kontroll	77,39 %	2,59 %
11	Tilstand nettverkskontroller	77,39 %	2,59 %
12	Botnet	76,78 %	1,98 %
13	Manglende brukerbevissthet	76,30 %	1,50 %
14	SQL injection	76,16 %	1,36 %
15	Man-in-the-middle attack	76,16 %	1,36 %
16	Økt system sårbarhet	75,91 %	1,11 %
17	Phishing	75,40 %	0,60 %
18	Ansattes bruk av private mobile enheter	75,10 %	0,30 %
19	Trojaner	74,86 %	0,06 %
20	Virus	74,86 %	0,06 %
21	Orm	74,86 %	0,06 %
22	Man-in-the-browser attack	74,80 %	0,00 %
23	Ansattes bruk av sosiale medier	74,41 %	-0,39 %
24	Vishing	74,30 %	-0,50 %
25	Sosial manipulering	73,95 %	-0,85 %

Figur 29: Rangering påvirkningsfaktorer, urettmessig tilgang.

Som vi kan se av rangeringen i tabellen så ville en hendelse med at en person blir plantet i organisasjonen være årsaken med høyest påvirkning. Det er også en årsak som det kanskje er vanskelig å beskytte seg mot. En vil for eksempel ikke finne noen anbefalinger for kontroller rettet mot denne type risiko i noen standarder for styring av IT-risiko eller informasjonssikkerhet. Det er ikke modellert inn kontroller spesifikt for å sikre seg mot dette i nettverket, noe som bidrar til den høye påvirkningskraften. Sannsynligheten for at den inntreffer er kanskje liten, men dersom hendelsen inntreffer vil det få stor påvirkning på sannsynligheten for urettmessig tilgang som leder til betydelig tap inntreffer.

Som vist i figuren over antas kontrollene; tilgangsstyring, kontroll for ondsinnet programvare, kontroll av serviceleverandør og nettverkskontroller å ha lik påvirkning. Det er ikke funnet argumenter for at den ene kontrollen er vesentlig viktigere enn den andre. Men, ved detaljert gjennomgang med eksperter fra banken, så er det mulig at dette ville blitt justert noe. Som nevnt er kontrollene modellert på et overordnet nivå, så vektleggingen er gjort sett som en helhet av kontrollmiljøet.

Figuren under viser rangeringen av årsakene til kritiske systemfeil:

Ranering av input noder	Navn på input node	Sannsynlighet (p) for urettmessig tilgang	Endring i (P) for urettmessig tilgang gitt dårligste tilstand i input noden
1	DDoS for sabotasje/utpressing	60,00 %	17,00 %
2	Ikke produksjonslike testmiljø	53,66 %	10,66 %
3	Kompleks IT-infrastruktur	53,39 %	10,39 %
4	Manglende kontroll ved migrering til produksjon	52,61 %	9,61 %
5	Tilstand kontroll programutvikling	50,74 %	7,74 %
6	Gamle kjernesystem	49,87 %	6,87 %
7	Utkontraktering	48,11 %	5,11 %
8	Tilstand periodisk uavhengig kontroll av servicelever	47,80 %	4,80 %
9	Tilstand computer operations (drift)	47,80 %	4,80 %
10	Tilsand kontinuitet og katastrofeberedskap	47,44 %	4,44 %
11	Manglende kartlegging av kritiske komponenter	46,79 %	3,79 %
12	Manglende segmentering av reserveløsning fra prod	46,16 %	3,16 %
13	Manglende skille på utviklingsmiljø, test- og produks	46,16 %	3,16 %
14	Økt system sårbarhet	43,09 %	0,09 %
15	Endring med utilsikted feil	43,00 %	0,00 %
16	Mangelfull opplæring	42,82 %	-0,18 %
17	Hasteendring med utilsikted feil	42,82 %	-0,18 %
18	Konfigurasjonsendring med utilsikted feil	42,82 %	-0,18 %

Figur 30: Rangering av påvirkningsfaktorer, kritiske systemfeil.

Som vi ser er årsaken med mest påvirkning ikke uventet DDoS. Antallet tjenestenektangrep har vært økende og blir stadig mer sofistikert. Det kan også være vanskelig å oppdage. En annen årsak med stor påvirkning er hendelse hvor testmiljø ikke er lik produksjonsmiljø. Som beskrevet under kompleks IT-infrastruktur så er det en utfordring for bankene å ha oppdaterte testmiljø på alle systemer og for ulike aktører involvert. Dersom testmiljøene ikke er like produksjon vil eventuelle endringer eller oppgraderinger kunne inneholde feil eller uønskede effekter som ikke blir oppdaget i test, pga. endringen oppfører seg annerledes pga. miljøet er annerledes. Tilstanden for kontrollen ved migrering til produksjon er av avgjørende betydning, pga. det er den endelige sjekken, nøkkel kontrollen at alt er gått riktig for seg i endringshåndteringsporsessen og endringer følgelig trygt kan foretas i produksjonsmiljøet.

Figuren under viser rangeringen av årsaker for ødeleggelse av kritisk utstyr:

Ranering av input noder	Navn på input node	Sannsynlighet (p) for urettmessig tilgang	Endring i (P) for urettmessig tilgang gitt dårligste tilstand i input noden
1	Tilstand kontinuitet og beredskap	82,00 %	73,00 %
2	Physical security	41,00 %	32,00 %
3	Manglende tilbakekallelse av tilangstillatelse	24,00 %	15,00 %
4	Naturkatastrofe	12,00 %	3,00 %
5	Brann	9,00 %	0,00 %
6	Strømbrudd	9,00 %	0,00 %
7	Vannlekasje	9,00 %	0,00 %

Figur 31: Rangering av påvirkningsfaktorer, ødeleggelse av kritisk utstyr.

Som vi ser av figuren over er tilstanden på kontinuitets løsninger og beredskap avgjørende for risikoeksponeringen i forhold til ødeleggelse av kritisk utstyr. Fysisk sikkerhet er også betydningsfull, men ikke på langt nær like avgjørende for om kritiske ødeleggelser. Det er ikke bankenes utstyr som er avgjørende i tapsbeløp, men bankens evne til videre drift og sikring av data.

6.7.4 Basel II krav til modeller på AMA-nivå

Krav som stilles til modeller på AMA-nivå (tidligere omtalt i kap.2.1.1):

- Tapsprediksjon over en ettårs periode innenfor et konfidensintervall på 99,9%
- Reflektere endringer i risikoeksponeringen som følge av daglig risikostyrings arbeid
- Basert på de 4 informasjonskildene (eksterne-, interne data, forretningsmiljø og interne kontroll faktorer, scenario analyse)
- Tilfredsstiller «use test»

Metoden som valgt å benytte i denne oppgaven, bayesianske nettverk, dekker første punktet ved at en angir prosentsatsen for konfidensintervall selv i modellen.

Som vist i case scenarioene og sensitivitetsanalysen gjenspeiler modellen endringer i de ulike påvirkende faktorene. For eksempel en forbedring i brukerbevissthet omkring informasjonssikkerhet og/eller forbedring i kontroller gir en nedgang i risikoeksponeringen. Sensitivitetsanalysen viser også hvilke faktorer som har størst påvirkning.

Modellen kombinerer på en god måte de 4 informasjonskildene. Bankens interne tapshistorikk og eksterne data kan legges inn med statistiske sannsynligheter i input nodene. Modellen reflekterer bedrift spesifikke faktorer. Dette gjøres i tilstanden på kontrollmiljøet (kontroll variablene) i tillegg til i organisasjonsmiljø faktorene; brukerbevissthet omkring informasjonssikkerhet, ansattes bruk av sosiale medier, ansattes bruk av private mobile enheter, om brukere klikker på suspekte lenker etc.

«Use test» innebærer at modellen skal benyttes i bakens daglige risikostyringsaktiviteter og gi støtte i beslutningsprosessene. Forfatteren av denne oppgaven vil hevde at modellen i BN er et kraftfullt verktøy som dekke flere bruksområder. I første omgang er det et godt verktøy for risikoidentifikasjon og analyse. Den visuelle fremstillingen gjør det svært nyttig i kommunikasjon og diskusjon mellom ulike eksperter. Det gir en helhetlig oversikt på risikobildet samtidig som en kan jobbet detaljert ved å gå dypere i årsakssammenhengene. Identifikasjons- og analyse arbeidet i modellen vil gi betydelig læring tilbake i organisasjonen og øke bevisstheten omkring risiko. Den helhetlige oversikten og rangeringen av årsaksdrivere gir beslutningsstøtte i forhold til prioritering av tiltak og effekt av tiltak. I tillegg gir modellen kvantitativ måling av risikoeksponeringen.

Risikotallene vil vekke tillitt på bakgrunn av at årsakssammenhengene er analysert og visualisert. Måling og risikostyring er med andre ord integrert i et verktøy.

7. KONKLUSJON

På samme måte som annen operasjonell risiko, så er det også for IT-risiko behov for et godt verktøy for styring og kvantifisering. Operasjonell risiko er et relativt nytt fagfelt for bankene og IKT-teknologi er i stadig utvikling. Det bør tilstrebes å ha verktøy som kan håndtere de nye behovene i en risikostyringskontekst. En av målsetningene for oppgaven var å utarbeide en kvantitativ modell for analyse og måling av IKT-risiko på AMA-nivå, herunder beregning av økonomisk tap. I denne oppgaven har vi vist hvordan bayesianske nettverk er velegnet til formålet.

Nettverket som vist i denne oppgaven gir en god oversikt over risikobildet, avhengigheter mellom årsakene og hendelser og hvilke faktorer som påvirker mest. I motsetning til en opplisting av årsaker i en risikomatrise, så mener forfatteren av denne oppgaven at bayesianske nettverk gir en mye bedre forståelse av årsakssammenhengene. Ved å jobbe med nettverket og følge nodene fra årsak til hendelse og til konsekvens så øker forståelsen og total oversikten. Det at flere eksperter kan gi input til «sine» fagfelt i samme oversikt gir et helhetlig risikoperspektiv. Det bayesianske nettverket er et levende verktøy i den forstand at læring og økt forståelse oppdateres i nettverket, nye årsaker og bedre forståelse av sammenhenger kan enkelt oppdateres og utgjør følgelig et kontinuerlig forbedret grunnlag for beslutningsstøtte.

BN kobler sammen årsaksbildet og tapsprediksjonen. Beregning av økonomisk tap skjer i samme verkøyet som analysen av årsakssammenhenger. Dette bygger troverdighet omkring risikotallene. Modellen er en kunnskapsmodell og sannsynligheter og risikotall må kommuniseres på en måte som bygger tillitt. BN i denne oppgaven bygger på en subjektiv forståelse av risikobegrepet. Subjektiv sannsynlighet inkluderer all tilgjengelig kunnskap.

Et viktig moment i håndteringen av IKT-risiko er bevisstheten om at informasjonssikkerhet ikke bare handler om teknologiske løsninger, men vel så mye om oppfølging av retningslinjer og fordeling av ansvar. Det innebærer en helhetlig tilnærming med valg av sikkerhetsteknologi i tillegg til ansvarliggjøring av den enkelte, bevisstgjøring og opplæring i trygg bruk. Dette vil være med å forme en god risikokultur.

I forkant av modelleringen i BN, var det nødvendig med en risikoidentifikasjonsprosess. Å kartlegge kritiske IKT-hendelser for banknæringen var en målsetning for oppgaven.

Risikoidentifikasjonsprosessen ble utført sammen med en ekspertgruppe fra en lokal bank. I forkant av møtet ble også faglitteratur konsultert samt rapportering av aktuelle hendelser fra finanstilsynet. De mest kritiske IKT-hendelsene ble definert til; urettmessig tilgang, kritiske systemfeil og ødeleggelse av kritisk utstyr. Det viste seg i denne prosessen av selve avklaringen rundt hva som er reelle tapshendelser, årsaker, influerende faktorer og konsekvenser var svært oppklarende og gjorde det lettere å starte analysen av årsakssammenhengene. I faglitteraturen er det ofte ikke satt i en sammenheng eller bare definert som risikoområder.

For å kunne være i stand til å modellere IKT-risiko for bankene samt årsakssammenhenger så var det nødvendig å kartlegge bankenes rammebetingelser og IKT-styring og informasjonssikkerhet. Dette var også en av målsetningene for oppgaven. Rammebetingelsene generelt for oprisk er Basel II regelverket. IKT-forskriften er bankene pliktet å følge. I tillegg finnes det flere anerkjente standarder for informasjonssikkerhet og IT-styring. Fordelen med BN er at reguleringen samt kontroller for informasjonssikkerhet og god IT-styring kan tas hensyn til i nettverket. Arbeidsprosesser som IT-avdelingen følger i dag kan gjenspeiles i verktøyet. For eksempel dersom banken følger ITIL som er et rammeverk for kvalitetssikring av leveranse, drift og support innen IT. Dersom man bruker samme terminologi i nettverket som allerede er kjent og brukes av de ansatte, så vil dette bidra til at BN brukes i daglig risikostyringsarbeid fordi det føles kjent. Et annet moment er at det ved den grafiske fremstillingen vil kunne benyttes i opplæringsøyemed og visualisere viktigheten av at rutiner og kontroller følges. Det vil gi en økt forståelse for at overholdelse av rutinene er viktig.

8. FORSLAG TIL VIDERE ARBEID

Med denne oppgaven ønsker forfatteren å bidra til at forståelsen av totalbilde for hvordan IT påvirker banken bedres. Mye av arbeidet er basert på tilgjengelig litteratur, egne erfaringer, intervju med bankansatte samt tapshendelse database fra flere banker. Tidsbegrensninger har gjort at modellen ikke er validert sammen med banken. Videre arbeid vil være å utføre ytterligere kalibrering av modellen med banken. Dette innebærer sensitivitetsanalyse sammen med eksperter på området, med deres fagkunnskap og kjennskap til bankens særegenheter. Modellen vil nok måtte justeres for å ta høyde for bankens forretningsmiljø- og interne kontrollfaktorer på en mer detaljert måte. Dette vil være nødvendig for at banken skal kunne bruke det bayesianske nettverket videre i sitt arbeid. Videre arbeid vil også omfatte ytterligere undersøkelser av bankenes IT infrastruktur, kritiske komponenter og ansvarsforhold mellom banken selv og serviceleverandører. Betydningen av eventuelle svakheter i kontroller hos de ulike aktørene involvert, hvordan det påvirker de ulike applikasjonene, og hvilke forretningsprosesser det igjen rammer.

Det vil også være nyttig å koble opp modellen sammen med de andre nettverkene som er utarbeidet i forbindelse med Oprisk prosjektet (forkningsprosjektet ved UIS, tidligere omtalt i denne oppgaven). Spesielt for området organisasjonskultur vil være nyttig å se sammenheng og evt. avhengigheter i forhold til IKT risiko.

Litteraturliste

ABC Nyheter. (2012, 07 06). *ABC Nyheter*. Hentet fra Pengene går alltid via et muldyr: http://www.abcnyheter.no/penger/oekonomi/2012/07/06/pengene-gar-alltid-et-muldyr

Aftenposten. (2012, 10 12). *Aftenposten*. Hentet fra "Sandy" avslører strømtrøbbel: http://www.aftenposten.no/nyheter/uriks/Sandy-avslorer-stromtrobbel-7031920.html#.UbMyCXY4XVI

Andersen, L. B., & Häger , D. (2012). *Modelling for the Analysis of Operational Risk - The Advanced Measurement Approach Reconsidered.* Stavanger: University of Stavanger.

Andersen, L. B., & Häger, D. (2009). *Contributions to Bayesian Network Model Design for Operational Risk in the Financial Industry.* Stavanger: University og Stavanger.

Andersen, L. B., & Häger, D. (2011). *Objectivity and the Measurement of Operational Risk, Reconsidered.* Stavanger.

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research* , ss. 1-11.

Bank Info Security. (2013, 03 01). *Bank Info Security.* Hentet fra Security Agenda: Re-Assessing Risk - Evolving Threats Require a New Approach to Risk Management: http://www.bankinfosecurity.com/handbooks/security-agenda-re-assessing-risk-evolving-threats-require-new-h-41

Bankenes Standardiserings Kontor (BSK). (2013, 06 06). *BSK*. Hentet fra BSK: http://bsk.no/hovedmeny/om-bsk/om-oss.aspx

Basel Committee on Banking Supervision . (2011). *Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches.* Basel: BIS.

Basel Committee on Banking Supervision. (2009). *History of the Basel Committee and its Membership.* Basel: BIS.

Basel Committee on Banking Supervision. (2006). *International Convergence of Capital Measurement and Capital Standards.* Basel: BIS.

Bodur, Z. (2012). Operational risk and operational risk related banking scandals/large incidents. *Maliye Finans Yazilari* , 61-82.

Chernobai, A., Jorion, P., & Yu, F. (2011). The Determinants of Operational Risk in U.S. Financial institutions. *Journal of financial and quantitative analysis* , 1683-1725.

Dagens IT. (2013, 04 16). *Dagens IT*. Hentet fra DNB rammet igjen: Inen vet hvorfor nettangrepene øker kraftig: http://www.dagensit.no/article2596863.ece

Dagens Næringsliv. (2013, 05 21). Indisk it under lupen . *Dagens Næringsliv* . Oslo: DN.

Dagens Næringsliv. (2013, 01 09). Rekrutterer mellommenn via datingtjenester. *DN* , ss. 4-5.

Datatilsynet. (2012). *Regjeringen.no.* Hentet 01 22, 2013 fra Datatilsynet: http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf

DIFI Direktoratet for forvaltning og IKT. (2012). *Styringssystem for informasjonssikkerhet. Erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27002.* Oslo: DIFI Direktoratet for forvaltning og IKT.

E24 Digital. (2013, 04 11). Danske banker utsatt for nettangrep av Anonymous.

Ellison, R. J., & Woody, C. (2010). Supply-Chain Risk Management: incorporating Security into Software Development. *Proceedings of the 43rd Hawaii International Conference on System Sciences - 2010* (ss. 1-10). Hawaii: IEEE Computer Society.

Finansdepartementet. (2006). *Finansdepartementet. Nytt kapitaldekningsregelverk*. Hentet January 16, 2013 fra Regjeringen.no: http://www.regjeringen.no/nb/dep/fin/dok/regpubl/otprp/20052006/otprp-nr-66-2005-2006-/8.html?id=132961

Finansdepartementet. (2013, 03 22). *Regjeringen.no.* Hentet fra Nye lovregler om kapitalkrav for banker: http://www.regjeringen.no/nb/dep/fin/pressesenter/pressemeldinger/2013/nye-lovregler-om-kapitalkrav-for-banker.html?id=720596

Finanstilsynet. (2012). *Risiko- og sårbarhetsanalyse (ROS) 2011. Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT).* Finanstilsynet.

Finanstilsynet. (2013). *Risiko og Sårbarhetsanalyse (ROS) 2012. Finansforetakenes bruk av informasjons- og kommunikasjons teknologi (ikt).* Finanstilsynet.

Finanstilsynet. (2008). *Risikobasert tilsyn: Modul for vurdering av Operasjonell risiko.* Finanstilsynet.

Finanstilsynet. (2011). *Rundskriv: Økte krav til bankene i lyse av driftsproblemene i påsken 2011.* Oslo: Finanstilsynet.

Frank, S. J. (2005). Source out, risk in. Offshoring software development can put intellectual property at risk. *IEEE Spectrum* (ss. 60-62). IEEE.

Ginzberg, M. J., & Moulton, R. T. (1990). *Information Technology Risk Management.* IEEE.

Ginzberg, M. J., & Moulton, R. T. (1990). *Information Technology Risk Management.* IEEE.

Goldstein, J., Chernobai, A., & Bernaroch, M. (2011). An Event Study Analysis of the Economic Impact of IT Operational Risk and its Subcategories. *Journal of the Association for Information Systems* , 601-631.

Guo, Q., Zhan, Z., Wang, T., & Zhao, X. (2012). Risk Assessment and Optimal Proactive Measure Selection for IT Service Continuity Management. *IEEE Conference Publications* (ss. 1386-1391). IEEE.

Hardware.no. (2012, juli 6). Hentet fra Trojanere stjal 700 000 kroner fra nettbankkunder: http://www.abcnyheter.no/penger/oekonomi/2012/07/06/pengene-gar-alltid-et-muldyr

Hinz, D. J. (2005). High Severity Information Technology Risks in Finance. *Proceeding of the 38th Hawaii International Conference Sciences - 2005* (ss. 1-6). IEEE.

Häger, D. (2011, 02 22). MOS140 Introduksjon til bayesianske nettverk. *Forelesningsnotat* . Stavanger: UIS.

Häger, D., & Andersen, L. B. (2009). A knowledge based approach to loss severity assesment in finance using Bayesian networks and loss determinants. I D. Häger, *Stochastic Modelling for the Analysis of Operational Risk in Financial Institutions.* Stavanger: University of Stavanger.

Häger, D., & Andersen, L. B. (2010, June 19). A knowledge based approach to loss severity assessment in financial institutions using Bayesian networks and loss determinants. *European Journak of Operational Research* , ss. 1635-1644.

Häger, D., Andersen, L. B., Aven, T., & Bø, F. (2007). The Basel II Capital Accord and operational risk management; Status and the way forward. *The International Business & Management Conference, Hawaii.* University of Stavanger.

IKT nytt.no. (2013, 05 12). *Internetts største bankran – bytte ble 260 millioner kroner*. Hentet fra iktnytt.no: http://iktnytt.no/internetts-storste-bankran-er-gjennomfort-bytte-ble-260-millioner-kroner/

Information Systems Audit and Control Association (ISACA). (2009). *Grunnleggende retningslinjer for god IT-skikk.* ISACA Norway chapter.

InformationWeekSecurity. (2013, 04 04). *Information Week Security*. Hentet fra Banks hit downtime milestone i DDOS attacks: http://www.informationweek.com/security/attacks/banks-hit-downtime-milestone-in-ddos-att/240152267

ITGI. (2008). *Aligning cobiT 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit.* Hentet 01 22, 2013 fra ISACA: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf

Jensen, F. V. (2001). *Bayesian Networks and Decision Graphs.* Springer-Verlag.

Korb, K. B., & Nicholson, A. E. (2004). *Bayesian Artificial Intelligence, Second Edition.* Chapman & Hall / CRC Computer Science & Data Analysis.

KPMG. (2011). *KPMG analysis of global patterns of fraud: Who s the typical fraudster?* KPMG international .

Kredittilsynet. (2007). *Modul for vurdering av Operasjonell risiko.* Kredittilsynet.

Matloff, N. (2005, July/August). Offshoring: What Can Go Wrong? *IT Pro* , ss. 39-45.

Natvig, B. (1997). En introduksjon til bayesiansk statistikk og beslutningsteori. *En introduksjon til bayesiansk statistikk og beslutningsteori. Notat til ST115 2. utgave* . Oslo: Matematisk institutt, Universitetet i Oslo.

Neapolitan, R. E. (2003). *Learning Bayesian Networks.* Chicago: Prentice Hall Series in Artificial Intelligence.

Neil, M., Häger, D., & Andersen, L. B. (2009). Modeling operational risk in financial institutions using hybrid dynamic Bayesian networks. *The Journal of Operational Risk* , ss. 3-33.

Norges Bank. (2003). Modernisering og utkontraktering av Norges Banks oppgjørsystem. *Penger og Kreditt 4/03* , ss. 206-211.

Norges Bank. (2012). *Årsrapport om betalingssystem 2011.* Oslo: Norges Bank.

NorSIS Norsk senter for informasjonssikring. (2013, 03 18). *NorSIS*. Hentet fra NorSIS Leksikon: http://www.norsis.no/leksikon/

NS-ISO/IEC. (2005). *NS_ISO/IEC 27002:2005 Informasjonsteknologi Sikkerhetsteknikk Administrasjon av informasjonssikkerhet.* Standard Norge.

OGC. (2010). *ITIL.* Hentet 01 22, 2013 fra ITIL offical site: http://www.itil-officialsite.com/

Operational Risk & Regulation. (2012). *Top 10 operational risks for 2013.* Risk.net.

Oprisk.no. (2013). *Oprisk.no*. Hentet 01 25, 2013 fra Oprisk.no: http://www.oprisk.no/index.php?sideID=328&ledd1=316

Pearl, J., & Russell, S. (2001). *Bayesian Networks.* Los Angeles: University og California, Computer Science Department.

Reuters. (2012, 12 09). *The New York Times*. Hentet fra Aramco Says Cyberattack Was Aimed at Production: http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html

Sanford, A. D., & Moosa, I. A. (2012, April). A Bayesian network structure for operational risk modelling in structured finance operations. *Journal of the Operational Research Society* , ss. 431-444.

Spremic, M. (2012). Corporate IT Risk Management Model: a holistic view at managing information system security risks. *Proceedings of the ITI 2012 34th Int. Conf. on Information Technology Interfaces* (ss. 299-304). Cavtat: IEEE.

Standard Norge. (2009). *God IT Styring og Kontroll i norske foretak - Prosjekt NorSox.* Lysaker: Standard Norge.

Transparency International. (2013, april 15). *Corruption perceptions index 2012*. Hentet fra Corruption perceptions index 2012: http://www.transparency.org/cpi2012/results

Warren, K. V. (2010). *Security Controls in Service Management.* SANS Institute.

Webber, M. A. (2013, 02). The invisible threat. *Operational Risk & Regulation* , ss. 19-22.

Zadeh, J., & De Volder, D. (2007). Software Development and Related Security Issues. (ss. 746-748). IEEE.

Öbrand , L., Augustsson, N.-P., Holmström, J., & Mathiassen, L. (2012). The Emergence of Information Infrastructure Risk Management in IT. *45th Hawaii International Conference on System Sciences 2012* (ss. 4904-4913). IEEE Computer Society.

VEDLEGG 1: Ordliste

Kilde (NorSIS Norsk senter for informasjonssikring, 2013).

Advanced Persisten Threat (APT)

På norsk Avansert vedvarende trussel. I vanlige angrep vil en angriper ta kontroll over systemet for å oppnå et mål. Deretter forlate systemet. Avanserte Vedvarende Trusler omhandler trusler hvor en uatorisert person får tilgang, og deretter gjør alt man kan for å bli vedvarende på systemet og ikke bli oppdaget. En APT benytter ofte bakdører og rootkits for å skjule sin aktivitet, samtidig som man sørger for kontinuerlig tilgang til systemet.

Botnet

En bot (av robot) eller zombie er en kompromittert datamaskin som kan kontrolleres eksternt. Et bot-program på en bot åpner en kanal (port) mot omverdenen der den mottar instruksjoner. Instruksjoner kan være å sende ut virus og e-postreklame (spam), eller delta i tjenestenektangrep. Et botnet er en samling av boter som blir kontrollert av én person eller datamaskin. Til enhver tid er flere millioner datamaskiner over hele verden med i aktive botnet uten at eierne er klar over det. Botnet og bot-programvare blir leid ut eller omsatt blant spammere og utpressere. Mindre botnet lages også for å unngå å bli oppdaget, og for å kunne gjennomføre målrettede angrep.

Cracking

Å bryte seg inn i datamaskiner og nettverk uten tillatelse.
Også brukt om å modifisere programvare for å fjerne kopibeskyttelse.

DDoS

Distributed-denial-of-service. I et distribuert tjenestenektingsangrep kan en angriper bruke din maskin for å angripe en annen maskin. Ved å utnytte sikkerhetshull eller sårbarheter kan en angriper ta kontroll over datamaskinen din, og sende store mengder data til et nettsted, eller til å spamme bestemte e-postadresser. Angrepet sies å være distribuert fordi angriperen bruker flere maskiner for å utføre angrepet. Ved hjelp av et distribuert tjenestenektangrep kan en angriper totalt lamme en bedrifts IT-systemer. Hvis bedriften er helt avhengig av de berørte systemene kan dette gi store konsekvenser

Hacker	Den mest kjente definisjonen av en «hacker» er en person som bryter seg inn i datamaskiner og nettverk uten tillatelse. Uttrykket «hacker» ble tidligere brukt om dyktige programutviklere.
Malware	Fellesbegrep for programvare som er laget for å infisere eller skade datamaskiner eller nettverk. Malware kommer av de engelske ordene Malicious Software og er en fellesbetegnelse på ondsinnet programvare. Eksempler på malware er datavirus, ormer, trojanere, spyware, adware, backdoors, rootkit og keyloggere.
Man-in-the-middle attack	Et angrep hvor angriperen kan lese, redigere og modifisere beskjeder mellom to kommuniserende parter uten at noen av partene er klar over at det foregår. Angriperen må få muligheten til å observere og avskjære beskjeder mellom to ofre. Angriperen kan endre innholdet i kundens transaksjon til banken.
Man-in-the-browser	Man in the browser is a security attack where the perpetrator installs a Trojan horse on a victim's computer that's capable of modifying that user's Web transactions as they occur in real time. According to security expert Philipp Guhring, the technology to launch a man in the browser attack is both high-tech and high priced. Use of the tactic has been limited to financial fraud in most cases, due to the resources required. Both Firefox and Internet Explorer on Windows have been successfully targeted.
“Mulldyr”	Rekrutterte personer som får betalt for å stille egen bankkonto til disposisjon for de kriminelle. Det betyr å ta i mot penger på kontoen sin, ta ut pengene, og sende dem til utlandet for eksempel med pengeoverføring. Slike personer kalles «muldyr».
Offshoring	Offshoring kalles det når IT-tjenester leveres fra leverandører i andre land. Dette er ofte en del av Cloud Computing-konseptet.
Phishing	Phishing er angrepsmetode der angriperen prøver å lurer til seg opplysninger som kan brukes i vinnings øyemed. Eksempler er henvendelser på e-post der mottakeren bes oppsøke en webside (f.eks. en nettbank) hvor de må legge inn sine passord. Internettsiden ser ut til å være troverdig, men i realiteten en falsk side for at angriperne skal få tilgang til dine opplysninger. Det har også vært eksempler hvor andre kanaler som telefon og chattekanaler er brukt.

Vishing	Vishing er en type phishing-angrep som involverer Voice over IP-teknologi (bredbåndstelefoni) for å stjele sensitiv informasjon om offeret. Til forskjell fra phishing ber ikke vishing-post deg om å gå inn på aktive lenker, men om å ringe et telefonnummer.
Virus	Ondsinnet programvare som kopierer seg selv inn i filer eller datamaskinens oppstartsektorer. Virus kan kun spres dersom noen kjører en infisert fil. Det vil si at infiserte filer må overføres til mottakers maskin via diskett, CD, USB-pinne, eller via nedlasting av filer, for eksempel vedlegg i epost.
Skimming	Skimming er et begrep som brukes om uautorisert kopiering av betalingskort. Skimming foregår vanligvis i minibanker ved at svindlerne fester en liten kortleser som kopierer kortinformasjonen over kortleseren i minibanken. Denne type innretninger kan være meget sofistikerte og kan være veldig vanskelig å oppdage. Det er også vanlig at svindlerne monterer et kamera over tastaturet i minibanken for å filme inntastingen av PIN-koden. Kortinformasjonen som blir kopiert på denne måten blir vanligvis brukt til å produsere falske kort, som igjen brukes til minibankuttak eller varekjøp. Dette har blitt en veldig vanlig måte å kopiere kort på. Svindlerne kan i løpet av noen få timer kopiere hundrevis av kort og svindle bankene for millionbeløp.
Spyware/spionprogramvare	Programvare med skadelig kode som har til hensikt å uthente informasjon fra datamaskinen. Dette kan være alt fra personinformasjon til søkevaner. Spionprogramvare kan føre til at datamaskinen arbeider tregere enn normalt. Spionprogramvare kan også berøre ditt personvern, avhengig av hva slags informasjon som blir fanget opp, hvem som mottar denne informasjonen og hvordan den brukes.
SQL injection	SQL Injection er en angrepsteknikk der man utnytter svakheter i webapplikasjoner ved å ”tvinge inn” SQL-koder på databaseserveren for å få tilgang til informasjon man verken er autorisert til å se, endre eller slette.