KUNGL TEKNISKA HÖGSKOLAN

HØGSKOLEN I GJØVIK

NISlab
Norwegian Information Security Laboratory

A process for Security Metrics Program (SMP)

Geir Simonsen

Institutionen för
Data- och Systemvetenskap

Examensarbete
Nr 2004-x-164
2004

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

Masteroppgave

Kandidatens navn:	Geir Simonsen
Oppgavens tittel:	En prosess for Sikkerhets Metrikk Program (SMP)
Utfyllende tekst:	
Linje:	02MAIS
Studieretning:	Master Program
Fagområde:	Informasjonssikkerhet
Tidsrom:	1.1.2004 – 28.6.2004
E-post:	geir.simonsen@hig.no

Abstract

(This Master of Science Thesis is written in Norwegian. This chapter is the only chapter in English.)

Title: A process for Security Metrics Program (SMP)

Service providers often have a lot of networks interconnected in complex architectures. This architecture is in continuous change, it may be a lot of reasons for this. It may, for example, be because of technical changes or because customers are to be connected or disconnected from the architecture. The changes are often preformed with a time pressure. This does not give opportunities to evaluate the security in the networks affected by the changes. This may often results in an extra, and may be unnecessary, security mechanism put in between networks, or changes are made, which are not optimal regarding security.

To perform changes in a complex architecture, connecting, disconnecting or changing the configuration of a network without influencing the trustworthiness of the architecture, we have developed a process which can be used to say something about the trustworthiness of the networks. By using the process it is possible to indicate the trustworthiness of the networks (segments) in a complex architecture. It may also be used to say something about networks trustworthiness before we interconnect to an existing architecture.

When we started the work with this process, we soon realised that the process can be used to perform all kind of measurements. To have something concrete to verify our work with the process, we used trustworthiness of a network/system as a basis.

A process which shall be used to measure the trustworthiness has to be simple and cost-effective to use. Simultaneously it has to give the right picture of networks trustworthiness. The process we have developed can be used for any kind of measurement, as long as the metrics are defined using the defined template.

It exists several ways to evaluate a system. Most of them can say something about networks trustworthiness. This is methods/tools which are used through the development of a product or system and methods/tools used to do real-time measurements of systems. We have the opinion that those systems are very time consuming, and will therefore not be cost-effective to use. At the same time we also see that a process like this has to have the ability to easily be adjusted towards a business security policy, and the ability to be tailored to the regulations we use for measurements.

Our most important steak-holder in this work is ErgoIntegration, which is one of Norway's biggest service providers. ErgoIntegration has a complex architecture which always is in change. Therefore it is important that the security level not is reduced when changes are made in the architecture. To take care of this we have developed a process which shall be cost-effective to use.

We have developed a process which will be useful for those who want to measure and estimate a network's trustworthiness. The process is developed around three sub-processes. The first sub-process a business has to go through is to find out which policy they want to

measure their networks towards. This can be done using an existing policy or reference model. It can also be done by using surveys and/or interviews with persons who are responsible for the security and those who work with the security in the business. We have the opinion that, for surveys and interviews, people representing all parts of the business should attend, including participants from technical as and non-technical departments.

The process we have developed contain three sub processes. The policy which is defined in the first sub-process shall be broken down into security metrics, which is the second sub-process in the process. This way we get defined points to measure and use in the inspection. The metrics are defined after a given template. The results from the inspection can be presented as a single value, which can be used to compare the results from other inspections.

When a metric is defined, it can be implemented in a toolkit, for carrying out the inspection. We have developed a prototype of the toolkit as a relational-database which can be used for any kind of measurements with metrics defined within the given template.

Forord

Denne master oppgaven er skrevet i forbindelse med mitt Master i Informasjonssikkerhet studie ved Høgskolen i Gjøvik. Oppgaven er gjennomført i løpet av vårsemesteret 2004. Oppdragsgiver i dette arbeidet har vært min arbeidsgiver ErgoIntegration (EI). Arbeidet har vært gjort for å gi EI noe som de kan benytte som en prosess i den daglige driften av sine egne, kunders og leverandørers komplekse sammensetning av datanettverk.

Jeg må benytte anledningen til å rette en stor takk til min kone, Rita Elin, og barna, som har latt meg gjennomføre studiet. Og ikke minst godtatt at jeg har vært så mye borte de siste to årene.
Min arbeidsgiver ErgoIntegration må også takkes. Som ikke bare har gitt meg muligheten til å jobbe med dette spennende temaet dette semesteret, men som også har gitt meg muligheten til å gjennomføre Master studiet ved Høgskolen i Gjøvik de siste 2 årene.

Takk til Louise Yngström for veldig nyttige tilbakemelding og synspunkter på vår studietur til KTH og etter presentasjonene på Gjøvik. En takk til opponent Frank-Arne Stamland for bra tilbakemeldinger. Må også rette en takk til min veileder Einar Snekkenes for nyttige og konstruktive tilbakemeldinger på arbeidet.

Jeg vil til slutt rette en stor takk til alle de som har deltatt med sine bidrag i undersøkelsen som ble gjennomført i forbindelse med dette arbeidet.

Det eneste vi vet med sikkerhet er at alt er usikkert.

Francois de Voltaire
1694-1778

Sammendrag

Tjenesteleverandører har ofte mange nettverk koblet sammen i komplekse arkitekturer. Denne arkitekturen er i stadig endring, det kan være grunnet endringer som må gjøres pga tekniske løsninger, eller for at noen kunder skal kobles inn i arkitekturen eller ut av arkitekturen. Arbeidet med disse endringene gjøres ofte under et tidspress, dette gir ikke store muligheter til å gjøre evalueringer rundt sikkerheten i nettverkene som er berørt. Dette medfører at man ofte kan legge på unødvendige sikkerhetsbarrierer mellom nettverk, eller at man kobler inn eller gjør endringer i arkitekturen som ikke er optimal med hensyn til sikkerhet.

For å kunne gjøre endringer i en arkitektur ved å koble inn, koble ut eller omkonfigurere nettverk, uten at dette skader den totale tillitsverdigheten til arkitekturen, har vi definert en prosess som kan benyttes for å si noe om tillitsverdigheten til nettverkene. Ved å benytte denne prosessen, vil man kunne angi de enkelte nettverk (segmenter) i en kompleks arkitektur sin tillitsverdighet. Man vil også kunne benytte prosessen for å angi et nettverks tillitsverdighet før man kobler det inn i en eksisterende arkitektur.

Når vi startet arbeidet med utviklingen av en slik prosess, så vi raskt at dette var en prosess som i utgangspunktet kan benyttes til alle typer målinger ved hjelp av metrikker. Men for at vi skulle ha noe konkret å sjekke prosessen opp mot, har vi benyttet oss av tillitsverdigheten til et nettverk/system som grunnlag for utviklingen av prosessen.

En prosess som skal benyttes til en slik måling av tillitsverdighet må være enkel og kostnadseffektiv å benytte. Samtidig som den skal gi det riktige bildet av et nettverks tillitsverdighet. Prosessen som vi har utviklet kan benyttes til andre målinger, så lenge metrikkene er laget etter gitt mal.

Det eksisterer flere måter å evaluere systemer på. De fleste vil kunne si noe om et nettverk sin tillitsverdighet. Dette er både metoder/verktøy som benyttes i utviklingsfasen av et produkt eller system, og metoder/verktøy som benyttes til å gjøre sanntidsmålinger av systemene. Vi mener at slike systemer er veldig tidkrevende, og vil derfor ikke være kostnadseffektive å benytte. Samtidig ser vi et behov for at en slik prosess enkelt skal kunne tilpasses en virksomhet sine policyer, og kunne skreddersys etter hvilke regler man ønsker å anslå tillitsverdigheten.

Vår viktigste interessent i dette arbeidet er ErgoIntegration, som er en av Norges største tjenestetilbyder. ErgoIntegration har en kompleks infrastruktur som til en hver tid er i forandring, og det er derfor viktig at sikkerheten ikke blir redusert ved at det gjøres endringer i arkitekturen. For å ivareta dette har vi utviklet denne prosessen som skal være kosteffektivt å bruke.

Vi har utviklet en prosess som vil kunne være en nyttig hjelp til de som ønsker å gjøre målinger og anslå et system sin tillitsverdighet. Prosessen er basert på tre del-prosesser. Den første del-prosessen en virksomhet må gjennom er å finne ut hvilke policy de ønsker å måle sine nettverk opp mot. Dette kan gjøres ved at man benytter eksisterende policy eller referansemodeller. Det kan også gjøres ved hjelp av undersøkelser og samtaler med personer som har ansvaret for sikkerheten og de som jobber med sikkerheten i en virksomhet. Vi ser det i så fall som avgjørende at det er deltagere fra flere deler av en organisasjon som er med på arbeidet. Dette bør være deltagere fra både teknisk og ikke tekniske avdelinger.

Prosessen vi har utviklet inneholder tre del-prosesser. Den policy man kommer frem til i Del-Prosess 1, skal brytes ned i metrikker, som er den andre del-prosessen, slik at man får konkrete målepunkter å måle på. Disse metrikkene defineres etter en gitt mal. Resultatene fra undersøkelsene som gjennomføres i Del-Prosess 3 kan enkelt angis med en verdi som er enkel å gjenbruke for sammenligning av resultater fra forskjellige undersøkelser.

Når metrikkene er definert, vil disse kunne implementeres inn i et toolkit, som benyttes får å gjøre selve målingen av nettverket. Prototyp av toolkitet har vi utviklet som en relasjonsdatabase, og vil kunne benyttes for målinger av hvilke som helst metrikker, så lenge de er definert etter den gitte malen.

Innhold

Abstract i
Forord iii
Sammendrag iv
Innhold vi
Tabelliste vii
Figurliste viii
1 Innledning 1
1.1 Problembeskrivelse 1
1.2 Forskningsspørsmål 2
1.3 Metode 2
1.4 Eget bidrag 3
1.5 Interessenter 4
1.6 Omfang og avgrensninger 4
2 Teori og bakgrunn (kjent kunnskap) 5
3 En prosess for Sikkerhets Metrikk Program (SMP) 10
3.1 Del-Prosess 1 - Undersøkelse / Kartlegging 12
3.1.1 Gjennomkjøring av Prosess 1 – Undersøkelsen / intervjuer 14
3.2 Del-Prosess 2 – Sikkerhetsmetrikker 19
3.2.1 Definisjon av metrikker 19
3.2.2 Mål 20
3.2.3 Gjennomføring av Prosess 2 - Sikkerhetsmetrikker 23
3.3 Del-Prosess 3 – Gjennomføring av måling med toolkit 23
3.3.1 Definerte metrikker basert på undersøkelse 27
3.3.2 Prototyp på Toolkit 32
4 Konklusjon 45
5 Videre arbeid 47
6 Referanseliste 49
Vedlegg A - Presentasjon holdt for deltagerne av undersøkelsen 51
Vedlegg B - E-post til deltagere av undersøkelse 56
Vedlegg C - Svarskjema til undersøkelsen 57
Vedlegg D - Elementer fra resultatene 59
Vedlegg E - Mulige metrikker på elementene 61
Vedlegg F – Besvarelser av undersøkelsen 62
Vedlegg G - Regneark for simulering av undersøkelse 70
Vedlegg H - Prototyp av toolkit 70
Vedlegg I – Metrikker for Personopplysningsloven som policy 71
Stikkordsliste 83

Tabelliste

Tabell 1 - Elementer fra undersøkelse i Del-Prosess 1 18
Tabell 2 - Definisjon av metrikker 19
Tabell 3 - Elementer som input til Prosess 2 28
Tabell 4 - Metrikk - Brannmurer 28
Tabell 5 - Metrikk - Tilgangskontroll på systemprogramvare 29
Tabell 6 - Metrikk - Sikkerhetsledelse 29
Tabell 7 - Metrikk – Kabling 30
Tabell 8 - Metrikk - Avlytting over kablede strekk 30
Tabell 9 - Metrikk - Mottak for eksterne VPN forbindelser 31

Figurliste

Figur 1 - Fordeling av områder med hensyn til tid og kostnad 6
Figur 2 - Struktur for sikkerhets metrikk program 7
Figur 3 - SMP implementerings prosess 8
Figur 4 – Sammenhenger i prosessen 10
Figur 5 - Sammenheng mellom element, metrikk og underspørsmål 12
Figur 6 – Del-Prosess 1 - Intervjuer / Undersøkelse 14
Figur 7 – Del-Prosess 2 - Sikkerhetsmetrikker 22
Figur 8 - Simulering med metrikkformel 25
Figur 9 - Simulering av resultater for metrikker 25
Figur 10 - Simuleringsresultater for undersøkelser 26
Figur 11 – Del-Prosess 3 - Gjennomføring av måling med toolkit 27
Figur 12 - Sammenhenger i databasen til prototyp av toolkit 33
Figur 13 - Toolkit - Velkomstbilde 34
Figur 14 – Toolkit - Meny i prototyp 35
Figur 15 - Toolkit - Ny Policy 35
Figur 16 - Toolkit - Metrikker til policy 36
Figur 17 - Toolkit - Legg til metrikk 36
Figur 18 - Toolkit - Metrikk detaljer 37
Figur 19 - Toolkit - Subspørsmål til metrikker 37
Figur 20 - Toolkit - Legg til subspørsmål 38
Figur 21 - Toolkit - Rapport policy med metrikker 39
Figur 22 - Toolkit - Policy med metrikker og underspørsmål 40
Figur 23 – Toolkit - Registrering av virksomhet 41
Figur 24 – Toolkt - Systemer for virksomhet 41
Figur 25 - Toolkit - Detaljert system informasjon 42
Figur 26 - Toolkit – Undersøkelseskriterier 42
Figur 27 - Toolkit - Besvarelse av undersøkelse 43
Figur 28 - Toolkit - Undersøkelsesverdi 44

1 Innledning

Tjenestetilbydere har ofte ansvaret for mange og kompliserte nettverk og systemer. Det kan være nett til både kunder, leverandører (3djeparter) og egne nettverk som er koblet sammen i komplekse arkitekturer (stokastiske nett). Flere av nettene vil ha forskjellige sikkerhetsnivå, og vil derfor måtte beskyttes fra hverandre, og kobles sammen på riktig måte (nivå). En utfordring i kompliserte arkitekturer til større tjenestetilbydere er at de stadig er i endring. Nye nett skal kobles inn, endringer skal gjøres i konfigurasjoner med mer. Og det er alltid snakk om tidsfrister og krav til realisering når slikt skal gjennomføres. Sammenkobling av nettverk kan føre til økt sårbarhet. Forskjeller i sikkerhetsnivåene til disse nettverkene gjør at de ikke bare kan kobles sammen uten videre.

1.1 Problembeskrivelse

I dette kapittelet vil vi beskrive utfordringene vi ser, og som gjør vårt arbeid interessant. En utfordring for tjenestetilbydere i dag, er at det ikke finnes metoder for raskt å kunne finne et nettverks sikkerhetsmessige tillit. Dette er nødvendig for blant annet å kunne si noe om hvor et nytt nett skal kunne kobles sammen med eksisterende arkitektur uten å medføre en reduksjon i tillitsnivået til eksisterende eller nye nettverk.

Sikkerhets policy hos virksomheter inneholder oftest krav til virksomheten om hvordan sikkerheten i infrastrukturen skal være, samt hvordan sikkerheten ved tilkoblinger av 3djeparter skal ivaretas. Problemet med dette er å finne ut hvordan man gjør dette i praksis og hvordan man bryter ned kravene gitt i en policy til målepunkter, metrikker, som kan benyttes for å finne tilliten til et eksisterende eller nye nettverk/system som skal kobles inn i en eksisterende arkitektur.

I dette arbeidet har vi sett på om det er mulig å finne en prosess for effektivt og lite ressurskrevende å anslå et nettverks, nytt eller eksisterende, tillitsverdighet. Vi ønsker da å se på det som i et nettverk går på sikkerhetsmessig tillit. Bishop [Bish] definerer ”sikkerhetsmessig tillit” (oversatt til norsk fra ”security assurance” i [Ivers]) som: ”tilliten til at en enhet tilfredsstiller sine sikkerhets krav”. Vi benytter oss derfor av denne definisjonen i det videre arbeidet.

Vi mener at et av problemene man står ovenfor, er at dagens evalueringssystemer er for kostbare og omfattende. De gir ikke en direkte sammenheng med en virksomhets sikkerhetspolicy og de gir ikke muligheten for enkel justering i henhold til en sikkerhetspolicys endringer. Vi ser et behov for å finne en prosess for raskt og kostnadseffektivt å kunne måle om et nettverk er tillitsverdig, samtidig med at det som måles er i henhold til gitt policy. For å kunne ha nytte av det over tid må også et toolkit for måling, hvor en samling av data lagres for å sammenligne måleresultater, utvikles.

Prosessen skal være et daglig verktøy som kan benyttes til for eksempel å angi i hvilken grad et nettverk er tillitsverdig, og dermed kunne si noe om hvor i en eksisterende arkitektur det kan kobles inn, ut eller endres, og være et underlag til avgjørelse på hvorvidt det er behov for ekstra sikkerhetsmekanismer, eller om noen kan fjernes.

1.2 Forskningsspørsmål

For å besvare de utfordringer vi har sett i problembeskrivelsen har vi definert noen spørsmål som vi ønsker besvart i vårt arbeid.

Er det mulig å definere en prosess for måling av sikkerhet ved hjelp av metrikker?

Vi ønsker å finne ut om det er mulig å definere en prosess, som kan være et daglig hjelpemiddel for en virksomhet som ønsker å ha en kontroll på informasjonssikkerheten. En slik prosess må være enkel å bruke, samtidig med at den er kostnadseffektiv. Prosessen skal også ta for seg etableringen av sikkerhetsmetrikker. Arbeidet vårt har konsentrert seg rundt målingen av tillitsverdigheten til et nettverk/system, men samtidig har vi sett på muligheten for å bruke prosessen til alle typer målinger ved hjelp av metrikker.

Kan vi finne en måte å presentere resultatene av en måling på en enkel måte?

Det er ønskelig at en måling kan presenteres på en så enkel måte at det lett lar seg gjøre å sammenligne målinger over tid og mellom systemer.

Er det mulig å benytte en undersøkelse som for eksempel intervjuer for å komme frem til de kriterier man skal måle etter?

Det er ikke alltid at man ønsker å gjøre sine målinger basert på kriterier gitt i for eksempel et lovverk eller eksisterende sikkerhetspolicy. Det kan hende det ligger helt andre kriterier til grunn når man ønsker å gjøre en undersøkelse av et system. Vi ser det derfor som en mulighet å benytte undersøkelser basert på intervjuer eller lignende for å finne den policy man ønsker å undersøke et system opp mot.

Er det mulig å utvikle et toolkit som kan benyttes til å gjennomføre målingene?

Et toolkit som hadde tatt for seg selve målingen hadde gjort prosessen mer brukervennlig og nyttig over tid. En forutsetning for et slik verktøy, må være at det skal være enkelt å bruke og kunne benyttes over tid som en benchmark til sammenligning av resultater.

1.3 Metode

For å få besvart de forskningsspørsmålene vi har definert og komme frem til det målet vi har med oppgaven, har vi benyttet både litteraturstudie, undersøkelse og utvikling som fremgangsmåter. Vårt arbeid kan defineres som en kombinert metode (oversatt fra eng Mixed Method) [cres].
Vi har i oppgaven sett på teorier og definert en prosess, en måte å gjennomføre en del av prosessen og et verktøy for gjennomføring av resten av prosessen. Vi har understøttet og verifisert våre teorier og definisjoner ved at vi har etterprøvd disse med hjelp av forsøk.

Er det mulig å definere en prosess for måling av sikkerhet ved hjelp av metrikker?

Litteraturstudie er benyttet i vesentlig grad for å utvikle og få på plass selve prosessen og metrikkdefinisjonene. Vi har her fokusert på arbeid som har vært gjort i forbindelse sikkerhetsmetrikker og sikkerhets metrikk program.

For å verifisere prosessen har vi benyttet en undersøkelse hvor vi har intervjuet både personer som har god kjennskap til de informasjonssikkerhet og personer som i tillegg jobber med daglig forvaltning av informasjonssikkerhet.

Kan vi finne en måte å presentere resultatene av en måling på en enkel måte?

Også for å besvare dette spørsmålet, har vi benyttet oss av litteraturstudier, og kommet frem til de resultater som presenteres i denne rapporten.

Er det mulig å benytte en undersøkelse som for eksempel intervjuer for å komme frem til de kriterier man skal måle etter?

For å besvare dette spørsmålet, har vi basert oss på en undersøkelse ved bruk av intervjuer. Vi ønsket å benytte oss av en kvalitativ metode for innsamling av våre data. Denne metoden legger blant annet til grunn gjensidig tillit til og en god forståelse mellom oss og respondentene [holm]. Vår måte å gjennomføre undersøkelsen på er basert på intervjuer. Spørsmålene i undersøkelsen er også veldig runde, og det finnes ikke noe eksakt svar på de spørsmål som stilles.

Er det mulig å utvikle et toolkit som kan benyttes til å gjennomføre målingene?

Som en del-prosess har vi utviklet en prototyp av et toolkit som skal benyttes til gjennomføring av selve målingene, som vi i vårt arbeid kaller undersøkelser.

1.4 Eget bidrag

Basert på de forskningsspørsmål vi har definert ønsker vi med dette arbeidet å tilføre ny kunnskap, relatert til våre forskningsspørsmål, som angitt i dette kapittelet.

Er det mulig å definere en prosess for måling av sikkerhet ved hjelp av metrikker?

Vi ønsker å definere en enkel og kostnadseffektiv prosess for måling av informasjonssikkerhet. I dette arbeidet er prosessen fokusert rundt måling av tillitsverdigheten til et system/nettverk.

Kan vi finne en måte å presentere resultatene av en måling på en enkel måte?

For at målinger skal kunne benyttes over tid og kunne gi muligheten for å sammenligne målinger, ønsker vi å presentere en enkel måte å få et enkelt sammenlignbart mål.

Er det mulig å benytte en undersøkelse som for eksempel intervjuer for å komme frem til de kriterier man skal måle etter?

Vi ønsker å utføre en undersøkelse for å se om dette kan være med på å etablere en policy (kravsett) som man skal gjøre målingene opp mot.

Er det mulig å utvikle et toolkit som kan benyttes til å gjennomføre målingene?

Vi ønsker å utvikle et enkelt og gjenbrukbart verktøy (toolkit), for å la vårt arbeid kunne være et daglig verktøy, og for å lagre resultater av målinger, samt gjenbruke metrikker.

1.5 Interessenter

ErgoIntegration (EI) [ergo] er en tjenestetilbyder med systemer koblet sammen i nettverk i en kompleks arkitektur. EI håndterer blant annet både kunders, leverandørers (3djeparter) og egne nettverk og systemer.
EI har en definert sikkerhetspolicy som blant annet sier at EI skal "… *ha tilstrekkelig kompetanse til å kunne behandle sikkerhetsspørsmål på en profesjonell og effektiv måte. Det skal etableres oppfølgings- og kontrollopplegg for å påse at ErgoIntegration har riktig nivå på informasjonssikkerheten slik at sikkerhetsarbeidet blir ivaretatt på en god måte.*"
Dette kravet i policy sier at man må ha på plass et kontrollopplegg. I dette arbeidet har vi arbeidet med å definere et kontrollopplegg for EI og eventuelt andre tjenesteleverandører som har tilsvarende utfordringer. Vi tar i dette arbeidet kun for oss en liten del av et slikt kontrollopplegg, og ser på hvordan man kan kontrollere om et nettverk er tillitsverdig.

1.6 Omfang og avgrensninger

For å få besvart forskningsspørsmålene på tilfredsstillende måte, har vi gjort noen avgrensinger i vårt arbeid. Disse er beskrevet i dette kapittelet.

Omfang
I arbeidet har vi jobbet frem en prosess som skal kunne være et daglig hjelpemiddel ved måling av informasjonssikkerhet. Vi har konsentrert oss om en interessent i dette arbeidet, EI, men slik vi ser det er dette også en prosess som vil kunne benyttes av mange flere.

Arbeidet vårt har konsentrert seg om måling av tillitsverdigheten til et system eller nettverk. Dette er gjort for at vi skal ha et konkret tilfelle å jobbe med. Slik at vi kan teste ut det arbeidet vi har utført i forbindelse med definisjonen av prosessen.

Utviklingen av en prototyp av toolkitet har vi konsentrert om å få på plass en databasemodell, som det kan lages et skall for brukervennlighet rundt. En del av skallet har vi utviklet, men dette mest for å verifisere databasemodellen.

Avgrensninger
Prosessen vi har definert tar for seg det vi ser for oss som nødvendig for at den skal kunne være et daglig hjelpemiddel i arbeidet med måling av informasjonssikkerheten. Men det er ikke mulig å dekke en hel slik prosess i den tiden vi har hatt til rådighet. Vi har derfor begrenset denne prosessen til å omfatte de konkrete aktiviteter som må gjennomføres for at man skal kunne benytte dette som et daglig verktøy.

Vi har også begrenset en del av arbeidet utført for å verifisere prosessen til å omfatte måling av tillitsverdigheten til et nettverk/system. Og arbeidet med etablering av metrikker er derfor konsentrert rundt dette.

Utviklingen av prototypen til toolkitet har vi avgrenset til å omfatte etableringen av en databasemodell, og enkelte skjema for innlegging av data. Tester med å avlese metrikkverdier og undersøkelsesverdier er også utført, men disse må videreutvikles. Videre arbeid med toolkitet er beskrevet i eget kapittel (Kapittel 5 Videre arbeid).

2 Teori og bakgrunn (kjent kunnskap)

Det er utført en del arbeid tidligere når det gjelder måling av sikkerhet og sikkerhetsmetrikker. Temaet er også ganske vidt, vi har her gitt en liten oversikt over litteratur og tidligere arbeid, som vi har studert i forbindelse med vårt arbeid.

Når man snakker om måling av sikkerhet kan det være alt i fra evaluering av produkter ifm utvikling til penetrasjonstesting. Det er vel ingen uenighet om at alle aspekter av dette kan si noe om et system er tillitsverdig. Om vi kikker litt på de forskjellige metoder som eksisterer for dette i dag så finner vi mye innenfor alle områder.

Relatert til våre forskningsspørsmål, har vi funnet en del litteratur som vi har studert og kommentert.

Er det mulig å definere en prosess for måling av sikkerhet ved hjelp av metrikker?

[payn] mener at det vil bli brukt mer og mer ressurser på måling av sikkerhet, og at det vil tvinge seg frem på lik linje med de krav man har til å måle effekten av andre ledd i en organisasjon. Og om man også legger til grunn, som [payn] påpeker, at en aktivitet ikke kan administreres om den ikke kan måles, så må det tvinge seg frem løsninger som gjør det mulig å måle sikkerhet også.
[payn] peker på 7 steg for å etablere et metrikkprogram. De 7 stegene tar for seg hele prosessen ved etablering av et slikt program.

1. Definer metrikkprogrammets formål.
2. Bestem hvilke metrikker som skal defineres
3. Utvikle en strategi for å definere metrikkene
4. Etabler benchmarks og mål
5. Bestem hvordan metrikkene skal rapporteres
6. Lag en handlingsplan og gjennomfør den, og
7. Etabler et vurderings- og forbedrings- program

Vi har i vårt arbeid sett på alle disse stegene, og vi ser at dette er viktige og nødvendige deler av et metrikkprogram. I vår prosess har vi implementert alle disse stegene inn i tre del-prosesser.

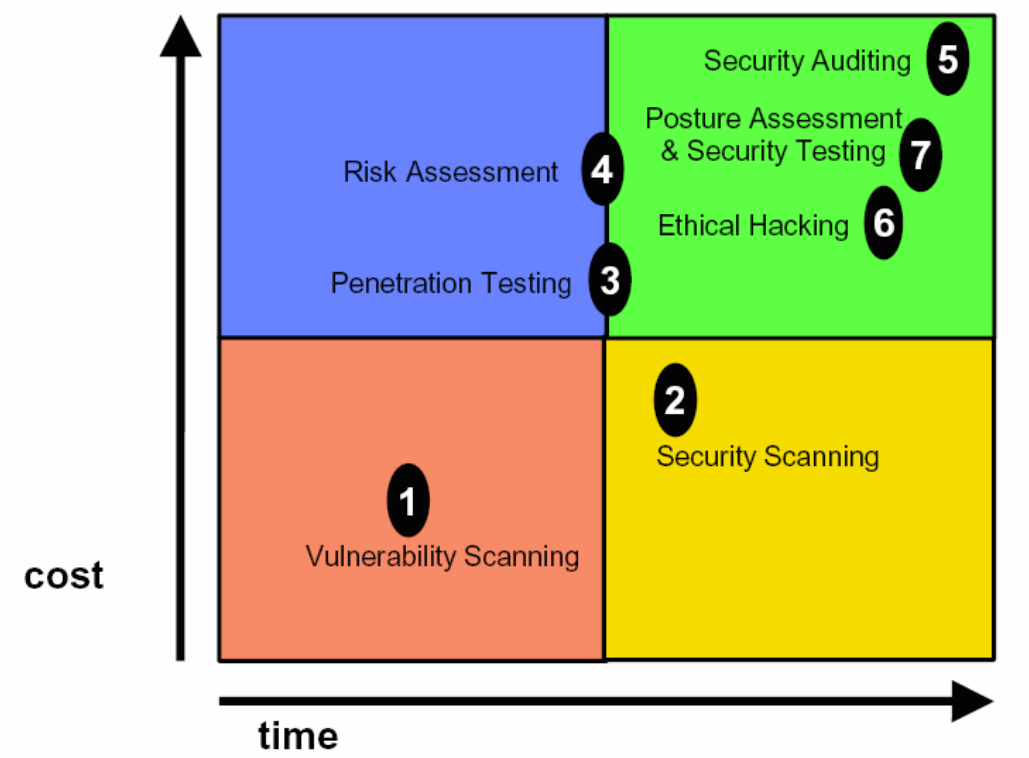
Evalueringer av systemer før og under utvikling har eksistert lenge og i mange varianter. Common Criteria (CC) er en slik metode som kan benyttes til å hjelpe leverandørene å sette tillit til sine produkter. CC sier mye om utviklingen av produktet, og at denne er gjort etter gitte kriterier, og sier ikke noe direkte om tillitsnivået til produktet når det er kommet i sitt operative miljø.

[frost] gir en kort introduksjon i hvordan man skal definere og benytte metrikker på et senior ledelses nivå. Det beskrives en metode for å bruke metrikker som anbefaler at man har en tilnærming til utfordringene med å gjøre målinger ved at man deler metrikker inn i to kategorier. De som observeres utenfra virksomheten (eksterne), og de som fokuserer på interne prosesser og evner. Disse kalles henholdsvis Primære og Avanserte metrikker. Han definerer en 3 stegs metode. Først skal men finne de hovedemner (Performance Topics) man ønsker å undersøke. For hvert hovedemne finnes det så flere kritiske suksess faktorer (critical success factors). Disse har igjen mange ytelses indikatorer (performance indicators).

Et system som er mer knyttet til det operative er OSSTMM [OSST]. OSSTMM er en åpen standard som definerer en metode for å gjennomføre sikkerhetstesting. Dette baserer seg på penetrasjonstesting og utnyttelse av kjente sårbarheter. Men den tar også med seg andre metoder og verktøy for å gjennomføre testene, som social engieneering, intervjuer og nettverks analyser (protokoll analyser). Skal man gjennomføre alt som står i OSSTMM vil dette ta lang tid, da metoden er omfattende og dekker mange områder.

1. Sårbarhets undersøkelser (Vulnerability Scanning)
2. Sikkerhets undersøkelser (Security Scanning)
3. Penetrasjonstester (Penetraton Testing)
4. Risiko vurdering (Risk Assessment)
5. Sikkerhets audit (Security Auditing)
6. Etisk Hacking (Ethical Hacking)
7. Holdnings undersøkelser og Sikkerhets testing (Posture Assessment and Security Testting)

Figur 1 - Fordeling av områder med hensyn til tid og kostnad - viser hvordan disse forskjellige områdene fordeler seg mht tid og kostnad.



Figur 1 - Fordeling av områder med hensyn til tid og kostnad

Man kan av figuren se at de mer on-line systemene er mer kostbare både med hensyn til tid og rene kostnader. Vi mener at det skal være mulig å finne en prosess som gjør at man ikke i så stor grad har behov for å gjøre de kostbare metodene (både med hensyn til tid og penger), men kan benytte en prosess som gir den målingen man har behov for i hvert enkelt tilfelle.

I [yeeb] konkluderes det med at det ikke er nok med at man måler kun enkelte elementer av en virksomhet, eks. nettverk, men at en videre måling som dekker flere områder er nødvendig for å kunne si noe om sikkerheten. Vi ser også dette som nødvendig, og ønsker derfor at vår prosess for benchmarking også skal kunne benyttes til alle områder som man ønsker å måle.

Vi tar i dette arbeidet for oss nettverk, og bruker dette som et element av den totale sikkerheten for å få utført de praktiske delene av arbeidet (undersøkelsen, metrikkdefinisjoner og utvikling av prototypen).

Det er gjort et stort arbeid med hvordan man skal implementere et Sikkerhets Metrikk Program (SMP) i [NIST]. Dette er en rapport som skal være en guide for å utvikle, velge og implementere et Sikkerhets Metrikk Program (SMP). Rapporten er delt i fem seksjoner, en innledende seksjon, en seksjon som beskriver roller og ansvar ved innføring av SMP. Seksjon tre går i dybden på bakgrunnen til sikkerhetsmetrikker og definisjoner for sikkerhetsmetrikker, fordeler med implementering, forskjellige typer sikkerhetsmetrikker, og faktorer som direkte påvirker suksessen til SMP. Seksjon fire tar for seg utviklingen av sikkerhetsmetrikker, og seksjon fem beskriver hvordan man implementerer et SMP. I tillegg til disse fem seksjonene er det også et vedlegg som lister en rekke eksempler på sikkerhetsmetrikker.

Vi har konsentrert oss om seksjon tre, fire og fem i dette arbeidet. Vi har også benyttet oss av appendikset og implementert noen av metrikkene i vår prototyp av toolkitet. Vi ser selvsagt at de andre seksjonene som dokumentet omhandler er avgjørende for en vellykket implementering av et komplett SMP. Men at vi i vårt arbeid har sett på den mer praktiske gjennomføringen (prosessen) rundt å benytte et slikt program. Og ikke minst konsentrert oss om å få prosessen enkel og ikke så omfattende.

[NIST] definerer fire komponenter som er avhengige av hverandre. Figur 2 - Struktur for sikkerhets metrikk program viser disse komponentene. Alle komponentene er viktige for at innføringen av et SMP skal være vellykket.

Figur 2 - Struktur for sikkerhets metrikk program

Støtte fra ledelsen (Strong Upper-Level Management Support) er vel den viktigste komponenten. Dette gjelder også for det praktiske arbeidet med informasjonssikkerhet. Uten støtte fra ledelsen vil ikke et SMP kunne gjennomføres.

Praktisk Sikkerhets policy og prosedyrer (Practical Security Policies & Procedures) er neste komponent som må være på plass i følge [NIST]. Denne komponenten er nødvendig for at

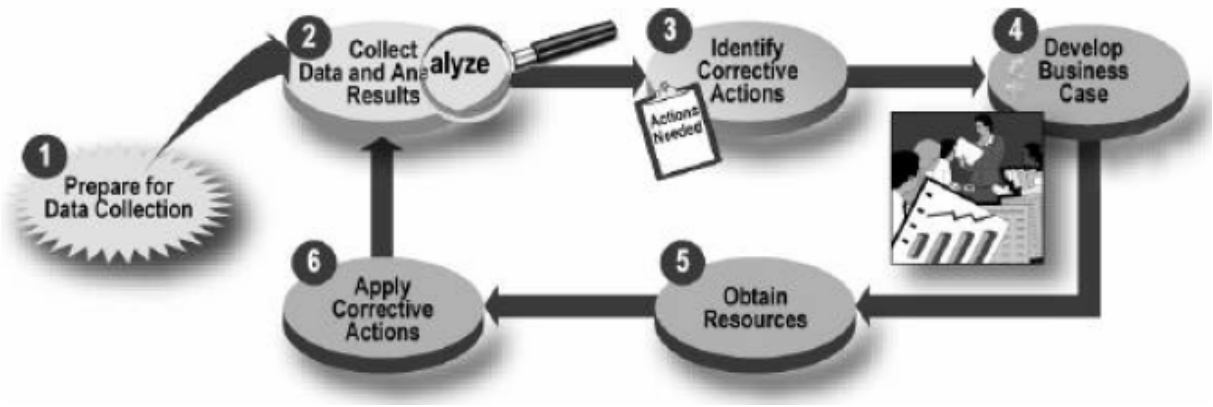
man skal kunne finne de metrikker man ønsker å benytte. I vårt arbeid, ønsker vi at dette skal kunne være, ikke bare virksomhetens eksisterende interne policies og prosessedyrer, men også lover og regler virksomheten er underlagt eller en policy som man ønsker å definere for å gjøre konkrete målinger av et system (eksempelvis et nettverk). I [wold] har det parallelt med vårt arbeid blitt utført en masteroppgave som ser på det med sikkerhetspolicyer og hvordan metrikker kan benyttes for å undersøke godheten av disse.

Kan vi finne en måte å presentere resultatene av en måling på en enkel måte?

Den tredje komponenten som må være med er selve definisjonen av gode sikkerhetsmetrikker. Det må være enkelt å få frem data til en metrikk, og det må være gjennomførbart å måle de. I tillegg nevner [NIST] at en sikkerhetsmetrikk må være gjentagende, gi relevante data over tid, være nyttige til å spore endringer og styre ressurser. Vi lar også dette ligge til grunn når vi lager metrikker til vår prosess.

Fjerde og siste element i pyramiden er evaluering av resultatene av metrikkdataene (Result-Oriented Metrics Analysis). Dataene må her benyttes for å justere metrikker, finne forbedringer i eksisterende sikkerhetsmekanismer og for å planlegge nye sikkerhetsmekanismer for å møte fremtidige sikkerhetskrav.

[NIST] tar i seksjon fire frem et forslag til hvordan et SMP skal implementeres. Figur 3 - SMP implementerings prosess, viser implementeringsprosessen. Vi har i vårt arbeid jobbet med del 1 og 2 av denne prosessen, med hovedvekt på å definere hvordan vi skal finne ut hva vi skal måle opp mot (policy) og hvordan vi skal måle (toolkit).



Figur 3 - SMP implementerings prosess

Er det mulig å utvikle et toolkit som kan benyttes til å gjennomføre målingene?

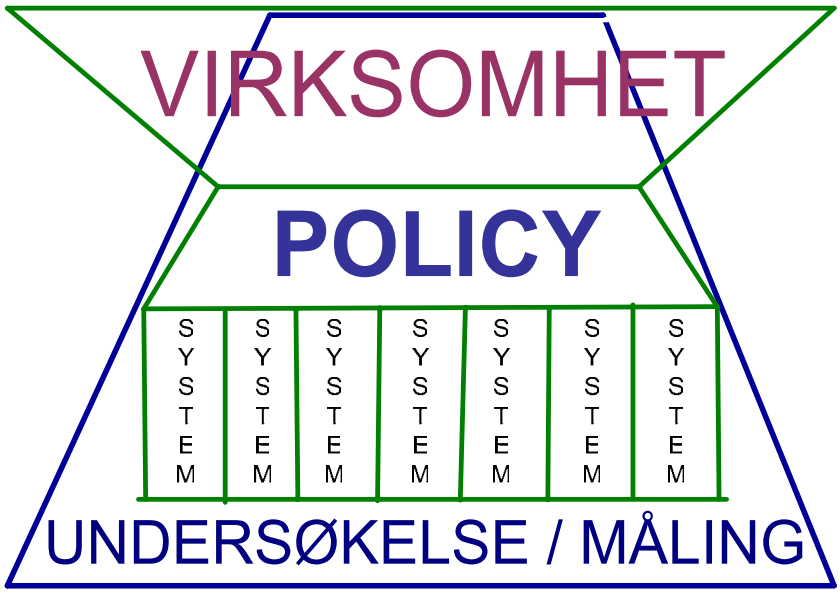
[isap] og [risk] er to av mange verktøy som er utviklet for å gjennomføre risiko og sårbarhetsvurderinger. [isap] er et komplett verktøy som benyttes til risikohåndtering. [risk] benyttes til risikovurderinger. Begge disse verktøyene er etter vår menig for omfattende, og gir en for lang vei til resultatet. [risk] gir til viss grad en karakter på en vurdering, men denne er veldig knyttet opp mot det økonomiske bildet. Det vil si hva får man igjen for å implementere mottiltak som blir anbefalt basert på manglende krav som kommer frem under en vurdering. Verktøyene baserer seg i stor grad på at det skal utføres intervjuer med mange personer i en virksomhet før man kommer frem til resultatene. Vi ønsker å utvikle en prototyp

på et toolkit som ikke skal være så omfattende, men samtidig gi en riktig måling av ønskede metrikker.

3 En prosess for Sikkerhets Metrikk Program (SMP)

I dette kapittelet presenterer vi vårt arbeid og de resultater vi er kommet frem til. Vi ønsket i vårt arbeid å konsentrere oss om å få på plass de delene av et SMP som går på planlegging av hva det skal etableres metrikker på, og hvordan man utfører målingene med metrikkene. Vi ser for oss at dette skal kunne gjøres ved hjelp av en prosess som inneholder 3 del-prosesser. Vi mente disse var nødvendige med bakgrunn i de erfaringer vi har og med bakgrunn i litteraturen referert til i kapittel 2. For å kunne konkretisere dette mer og kunne få utført noen tester for å verifisere måten vi ser for oss at en slik prosess skal være, definerte vi de tre del-prosesser man må utføre for å kunne gjennomføre målingene. Vi gjorde de konkrete verifiseringene av del-prosessene rundt det å anslå om et nettverk er tillitsverdig.

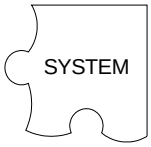
Bakgrunnen for at vi ønsker å komme opp med denne prosessen er, som tidligere beskrevet, at det er behov for en enkel og kostnadseffektiv metode å anslå om et nettverk er tillitsverdig. Dette, som vi tidligere også har beskrevet, for at foreksempel en tjenestetilbyder skal kunne ha en bedre kontroll med de forskjellige nettverkene som er med på å bygge opp en kompleks infrastruktur. Vi setter derfor krav til prosessen, om at det skal kunne benyttes for en (eller flere) virksomheter, og at metrikker skal kunne defineres fritt. Det vil si at det ikke skal være begrensninger i hva man legger til grunn for sine målinger. Prosessen vår er derfor lagt opp slik at den er egnet til å gjøre gjentatte målinger. Dette for at man skal kunne sammenligne resultatene med tidligere målinger, og målinger mot andre systemer. I Figur 4 – Sammenhenger i prosessen, ser vi hvordan dette er bygget opp. En policy er i prosessen det regelsettet man ønsker å kjøre undersøkelsen rundt. Dvs. at policy definerer hvilke krav man skal måle et system opp mot. En policy kan for eksempel være eksisterende selvpålagte krav, krav gitt gjennom lovverket eller krav gitt av kunder eller lignende.



Figur 4 – Sammenhenger i prosessen

Prosessen baserer seg på å kunne gjøre undersøkelser som dekker deler av virksomheten. Det er ikke noe mål at prosessen skal dekke hele virksomheten på en gang. Samtidig vil en policy definert i prosessen kunne dekke alle virksomhetens relevante systemer, som har behov for målinger. Prosessen skal kunne gjøre målinger mot flere systemer med samme policy som bakgrunn.

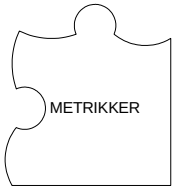
Prosessen baserer seg på at en virksomhet skal kunne gjøre målinger mot sine systemer. Men samtidig er det ingen begrensinger i dette, slik at det er mulig, og også et tenkt tilfelle, at man skal kunne gjøre undersøkelser mot andre nettverk. Prosessen legger opp til at det vil være virksomheten som vil være høyeste nivå. Dette vil si at man må legge inn en virksomhet som eier av de systemer som skal måles. Vi ser for oss at dette er hensiktsmessig slik at prosessen kan benyttes på tvers av virksomheter. En virksomhet i denne sammenhengen kan godt være forskjellige avdelinger under samme juridiske virksomhet, eller forskjellige juridiske virksomheter i et større konsern.



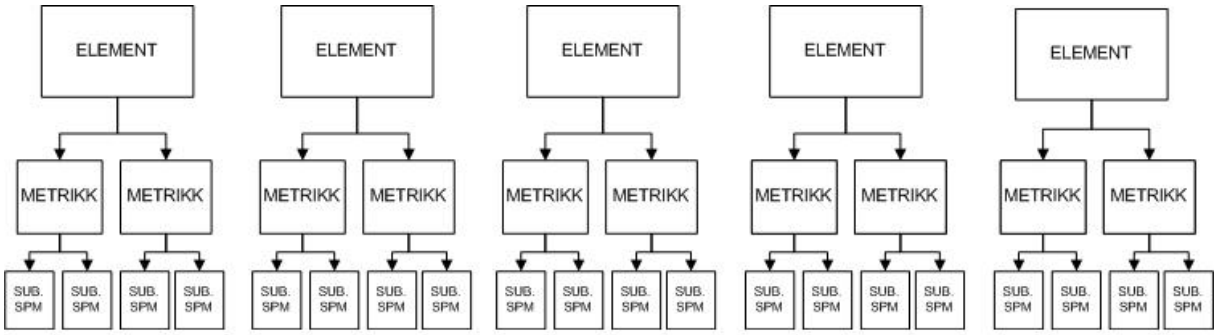
Systemer er i dette arbeidet det samme som nettverk, eller deler av et nettverk, som man ønsker å finne ut om er tillitsverdig, eller rettere sagt i hvilken grad de er tillitsverdig. Men vi ser også at et system kan være hva som helst innen en organisasjon som man ønsker å kjøre målinger mot.

For at man skal kunne gjøre noen målinger mot systemer må det også legges til grunn hvilke kriterier man skal måle opp mot. Det vil si at man må ha en policy som definerer hva man skal måle. En policy kan være eksisterende lovverk eller bedriftens eksisterende sikkerhetspolicy eller retningslinjer. For en større tjenesteleverandør kan en slik policy også være krav som kommer fra en kunde eller samarbeidspartner. I forbindelse med å gi en 3djepart tilgang til en virksomhets systemer, kan eksempelvis en policy være de retningslinjer virksomheten har for slike tilganger og 3djeparter. I prosessen er det ingen begrensninger i hva som kan være en policy, og hva som legges til grunn for denne.

For å få på plass policyen trekker man frem noen overordnede elementer som er viktige å overholde og som man ønsker å undersøke om man har kontroll på. I vår gjennomkjøring av prosessen benyttet vi en undersøkelse for å komme frem til de elementer som man anså som viktige for å si noe om et nettverk er tillitsverdig. Dette er det [frost] definerte som hovedemner (Performance topics). Disse elementene blir så brutt ned i metrikker, som benyttes som grunnlag for policyen.



Når [frost] nå for sine hovedemner definerer neste steg som kritiske suksess faktorer, kaller vi dette metrikker, og lar de ble definert ved at de elementer som man kommer opp med i policyen som viktige brytes ned i metrikker. Metrikkene blir målepunkter, som er konkrete målbare punkter i det systemet som skal måles. Figur 5 - Sammenheng mellom element, metrikk og underspørsmål viser sammenhengen mellom elementer og metrikker. Samtidig viser den at en metrikk er bygget opp med ett eller flere underspørsmål, som er de konkrete spørsmål som besvares og er det som [NIST] definerer som bevis for implementering og [frost] kaller ytelsesindikatorer.



Figur 5 - Sammenheng mellom element, metrikk og underspørsmål

Med disse fire delene på plass vil man kunne kjøre målinger og ha muligheten for å gjøre benchmark for systemene.

Fremgangsmåten for å komme gjennom prosessen har vi lagt inn i tre del-prosesser. Disse del-prosessene utgjør til sammen det arbeidet som må gjøres for å etablere et grunnlag for målinger. Vi definerer også den ene prosessen som gjentagende, for å kunne utføre målinger over tid, og ha en prosess for benchmark, som samler resultater over tid.

Den første del-prosessen – Del-Prosess 1 Undersøkelse/Kartlegging – skal utføres for å konkretisere hva man ønsker at metrikkene skal måle, en policy etableres. Dette tilsvarer steg 1 i [NIST], ref Figur 3 - SMP implementerings prosess. Andre del-prosess – Del-Prosess 2 Sikkerhetsmetrikker – skal ta tak i de elementer man finner i Del-Prosess 1, og definere sikkerhetsmetrikker ut av disse. Den tredje prosessen er selve målingen ved hjelp av metrikker definert i Del-Prosess 2. Disse to prosessene er tilsvarende steg 2 i [NIST], ref Figur 3 - SMP implementerings prosess. De to første del-prosessene er prosesser som i hovedsak kun trengs gjennomført første gangen man skal benytte prosessen i en virksomhet. Del-Prosess 3 vil være den som til daglig benyttes for å anslå tillitsverdigheten til eksisterende eller nye nettverk.

3.1 Del-Prosess 1 - Undersøkelse / Kartlegging

Denne del-prosessen skal utføres første gang man etablerer prosessen i en virksomhet, om man foretar større endringer i policyer eller man blir underlagt nye eller andre sikkerhets krav, fra enten myndigheter eller kunder.

Del-Prosessen har som formål å definere en policy med tilhørende elementer som man anser som viktig når man skal anslå den sikkerhetsmessige tilliten til et nettverk. Dette skal basere seg på sikkerhetspolicy, lover og regler man er underlagt, krav fra kunder og de daglige rutinene som benyttes i virksomheten.

Formålet med del-prosessen er å komme ut med en liste over elementer som man ønsker å bryte ned i sikkerhetsmetrikker. Elementer defineres som deler av et nettverk som kan brytes ned i metrikker. Disse blir så de konkrete målepunkter.

Prosessen er vist i Figur 6 – Del-Prosess 1 - Intervjuer / Undersøkelse, og inneholder følgende aktiviteter:

1. Start del-prosess 1
   Ingen input data er nødvendige til denne prosessen. Initieres ved at man skal ta i bruk prosessen i en ny virksomhet, er pålagt andre krav eller underlagt andre lover, som gjør at man må definere en ny policy. Prosessen kan også initieres ved at man ønsker å kjøre benchmark mot systemer med en ny policy.

   Avhengig om man ønsker å benytte en eksisterende policy eller ikke, går man videre i del-prosessen. En eksisterende policy kan eksempelvis være Personopplysningsloven, bedriftens interne policies og retningslinjer eller andre premissgivende input.

2. Prosjekt / Undersøkelse (intervjuer)
   Om det ikke eksisterer noen policy man ønsker å benytte, kan man definere en ny policy som man ønsker å måle sitt system opp mot. Denne delen av del-prosessen kan utføres på flere måter. Det kan i enkelte sammenhenger være riktig å utføre denne aktiviteten som et prosjekt i en virksomhet. Eller man kan la aktiviteten baserer seg på at det skal utføres intervjuer med personer i en virksomhet. Prosjektet eller intervjuene bør gjøres med/av personer som kjenner til virksomhetens sikkerhetsarbeid, personer som jobber med informasjonssikkerhet til daglig, personer som jobber med fysisk sikring, personer som er eksperter på informasjonssikkerhet og de som kjenner sikkerhetspolicy og retningslinjer.

   For å kunne kategorisere både metrikker og underspørsmål, ønsker vi å definere noen kategorier som vi kan dele metrikker og underspørsmål inn i. De kategoriene vi her har kommet frem til her, er definert med bakgrunn i undersøkelsen vi gjennomførte i Del-Prosess 1. De er definert for å dekke alle de elementer som kom frem fraundersøkelsen. Se kapittel 3.1.1 Gjennomkjøring av Prosess 1 – Undersøkelsen / intervjuer.

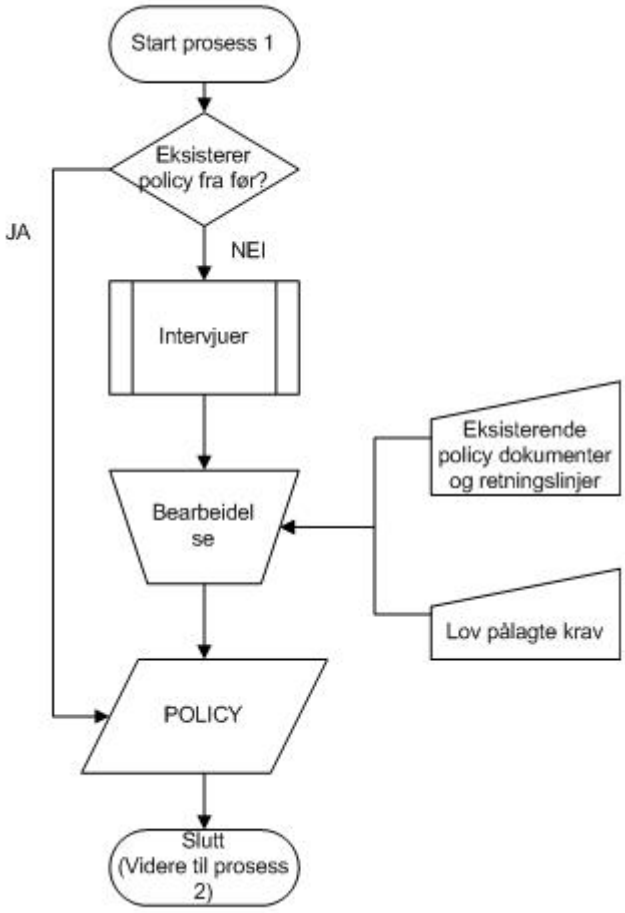
   Kategorier:
   a. Sikkerhets administrasjon
      Dette er alt med sikkerhetspolicy, drift og vedlikehold, ledelse osv.
   b. Programvare og maskinvare sikkerhet
      Her legges det som har med programvare og/eller maskinvare.
   c. Nettverksfunksjoner
      Nettverksfunksjoner er tjenester, svitsjer, routere osv
   d. Aksess kontroll
      Her legges det som har med autentisering, brannmurer osv
   e. Fysisk sikkerhet
   f. Avviks planlegging/håndtering
      Her legges alt som har med rutiner og mekanismer for avvikshåndtering og planlegging.

   Disse seks kategoriene endres om man ønsker at prosessen skal måle andre typer systemer (dette kan være måling innen helt andre fagområder; økonomi, personal, ledelse med mer).

3. Resultatene fra arbeidet i del 2 bearbeides. Resultatene sammenstilles om ønskelig med eksisterende policydokumenter, retningslinjer og lovpålagte krav. Og eventuelle andre forhold man må ta til etterretning når man skal gjennomføre en måling.

4. Ut fra dette sitter man igjen med en POLICY som man ønsker å måle systemet opp mot.

5. De elementene som policyen inneholder blir tatt med til Prosess 2



Figur 6 – Del-Prosess 1 - Intervjuer / Undersøkelse

For å sjekke ut om våre tanker rundt Del-Prosess 1 var riktige, gjennomførte vi en undersøkelse rettet mot tillitsverdigheten til et nettverk. Undersøkelsen ble utført med personer fra EI.

3.1.1 Gjennomkjøring av Prosess 1 – Undersøkelsen / intervjuer

Formålet med undersøkelsen var å kartlegge hva som ble sett på som de viktigste elementene når man skal anslå om et nettverk er tillitsverdig. Vi gjennomførte undersøkelsen blant ti personer som i større eller mindre grad jobber med utfordringer i forbindelse med endringer i infrastruktur til daglig, og har en bakgrunn innen informasjonssikkerhet og nettverk. Alle som deltok i undersøkelsen er ansatte i EI.

Deltagerne var fordelt mellom de som har ansvaret for vedlikehold og utvikling av sikkerhetspolicyer, og de som til daglig jobber med sikkerhetsarkitekturen til EI. Noen deltagere var også fra EI sitt fagmiljø på sikkerhet, som til daglig jobber med rådgivning intern og eksternt med sikkerhetsrelaterte spørsmål.

Undersøkelsen ble bygget opp rundt to case med tilhørende spørsmål som skulle besvares.

Bakgrunnen for at vi la opp undersøkelsen rundt to case, var at vi ønsket at deltagerne skulle tenke mest mulig på utfordringer de møter i virkeligheten når de besvarte undersøkelsen. Casene var bygget opp rundt situasjoner som er høyst aktuelle for en stor tjenestetilbyder. Begge casene tok utgangspunkt i at det skulle gjøres endringer i EIs infrastruktur. I den første casen hadde EI kjøpt opp en mindre bedrift, som skulle innlemmes i EIs infrastruktur. Og i det andre skulle EI outsource sin interne server drift til en ekstern tjenestetilbyder. Spørsmålene i begge case gikk så på hvilke elementer deltagerne så på som de viktigste når de skulle si noe om tillitsnivået til et nettverk.

Det var en stor variasjon i svarene, og dette skyldes nok deltagernes forskjellige bakgrunn, som varierte fra teknisk til administrativt innen informasjonssikkerhet.

3.1.1.1 Case

3.1.1.1.1 Case 1 – Oppkjøp av en BigBucks AS

Case:
EI har kjøpt et lite IT-selskap – BigBucks AS. Infrastrukturen til de to selskapene skal kobles sammen. Men først ønsker EI å anslå hvilken tillit de kan ha til BBs nettverk.

Spørsmålene som skulle besvares i dette caset var:
Q1a.: Skriv ned de elementer[1] i BBs nettverk som du mener er viktig å vurdere når man skal si noe om tilliten til BBs nettverk.
Q1b.: For hvert av elementene beskrevet i Q1a, prøv å beskrive de underelementer[2] som er viktige for hvert element.
Q2.: Skriv ned andre sikkerhetselementer EI bør vurdere når de
- Q2a.: kjøper BB
- Q2b.: kobler BBs infrastruktur sammen med EIs interne infrastruktur.

3.1.1.1.2 Case 2 - Outsourcing av driftstjenester

Case:
EI har skrevet en avtale med med TheBestSupplier AS (TBS). TBS skal drifte og vedlikeholde EIs interne servere. For å gjøre dette trenger TBS tilgang til EIs servere fra deres ”round-the-clock” driftssenter.

[1] Eksempel på element kan være brannmur, kabler, servere …
[2] Eksempler på underelementer for en brannmur kan være OS, HW, brannmur SW, NICs …

Infrastrukturen til de to selskapene skal kobles sammen. Men først ønsker EI å anslå hvilken tillit de kan ha til TBS nettverk.

Spørsmålene som skulle besvares i dette caset var:
Q1a: Skriv ned de elementer[3] i TBSs nettverk som du mener er viktig å vurdere når man skal si noe om tilliten til TBSs nettverk.
Q1b.: For hvert av elementene beskrevet i Q1a, prøv å beskrive de underelementer[4] som er viktige for hvert element.
Q2.: Skriv ned andre sikkerhets elementer EI bør vurdere når de

Q2a.: outsourcer til TBS

Q2b.: kobler BBs infrastruktur sammen med EIs interne infrastruktur.

3.1.1.2 Gjennomføring

Undersøkelsen ble planlagt gjennomført med ca 20 personer, og skulle gjennomføres ved at det ble utført intervjuer av deltagerne. Deltagerne var ansatte i ErgoIntegration. Det viste seg mest praktisk å plukke deltagere fra ErgoIntegration for å gjennomføre dette uten alt for store forsinkelser.

Intervjuer ble avholdt med 5 personer, hvor det var satt av ca en time til hver. Vi holdt en presentasjon (Vedlegg A - Presentasjon holdt for deltagerne av undersøkelsen) for deltageren for å gi dem en introduksjon til temaet. Det ble lagt vekt på at det ikke skulle gis for mye informasjon før de besvarte casene. Dette for at de ikke skulle bli påvirket av våre meninger og tanker rundt sikkerhetsmetrikker. Det viste seg i midleritid at den tilmålte timen gikk med til presentasjon av tema og diskusjoner rundt dette. Tid til besvarelse av Case ble det derfor ikke i den tilmålte tiden. Av praktiske årsaker så var det ikke mulig å gjennomføre nye runder med disse personene, og det viste seg også vanskelig å få satt av to timer, som vi anså som nødvendige, med de andre deltagerne. Vi måtte derfor legge om måten undersøkelsen ble gjennomført på. Videre besvarelser av undersøkelsen ble derfor basert på at utsendelse av en e-post med beskrivelse av problemstillingen (Vedlegg B - E-post til deltagere av undersøkelse), en kopi av forrapporten til denne master oppgaven [simg] og skjema som de kunne benytte for å besvare spørsmålene i casene (Vedlegg C - Svarskjema til undersøkelsen).

3.1.1.3 Erfaringer

Undersøkelsen gav oss en del erfaringer. Det viktigste vi så var at vi kunne fått mer utfyllende og konkrete svar om vi hadde kunnet gjennomføre intervjuene med mer tid tilgjengelig. Diskusjonene som oppstod i intervjuene gav også verdifull informasjon som man mistet ved utsendelse av spørreskjemaene.

Det hadde nok også vært nyttig og fått gjennomført noen forsøk på intervjurunder på forhånd, og dermed kunne anslått tiden og omfanget av dette. Dette hadde muligens gjort det lettere å få satt av nødvendig tid hos deltagerne til å gjennomføre intervjuer.

[3] Eksempel på element kan være brannmur, kabler, servere …
[4] Eksempler på underelementer for en brannmur kan være OS, HW, brannmur SW, NICs …

Spørsmålenes form tillot deltagerne å svare veldig rundt. Dette hadde blitt litt styrt under en intervjuseanse. Men når de skulle fylle ut dette selv så var det fritt frem for deltagerne å skrive det de ønsket. Det vi fikk inn ble derfor også veldig arbeidskrevende å sammenstille. Spørsmålsformuleringen kunne nok, når besvarelsesforman var slik den var, vært mye mer konkret, og eventuelt hatt en flervalgsform.

3.1.1.4 Resultater

I behandlingen av dataene som kom inn, så vi det ikke nødvendig å sammenstille dette med eksisterende policydokumenter eller retningslinjer. Det samme gjelder lovpålagte krav eller andre faktorer som hadde vært naturlig i en ”skarp” bruk av prosessen. Vi ser på denne oppgaven som en bearbeidelse, og vil ikke ha påvirkning på prosessen i sin helhet, men mer på resultatet av prosessen, hvilken policy man kommer opp med.

Besvarelsene av casene varierte som sagt en god del. Det som også viste seg var at besvarelsene på Case 1 og 2 var like. Man anså altså at det var de samme elementer som var gjeldende for begge case.

Ved å studere alle bidrag så kom vi opp med følgende konklusjon på besvarelsene til spørsmålene i de to casene:
De elementer som ble trukket frem i besvarelsene av spørsmålene varierte en del, men noen elementer ble tatt frem av store deler av deltagerne. En oversikt over de viktigste elementer som ble trukket frem i dette spørsmålet finner vi i Tabell 1 - Elementer fra undersøkelse i Del-Prosess 1. Noen elementer ble trukket frem av nesten hele gruppen, det var blant annet en stor enighet om at hvorvidt en aksesskontroll og perimeter sikring var på plass hadde mye å si på om et nettverk er tillitsverdig. Det skal også være samsvar mellom fysiske og elektroniske grenser, dvs. at det settes perimetersikring på de rette stedene. Av konkrete elementer som trekkes frem for å ivareta denne inndelingen, så trekkes det fram i hovedsak brannmurer, routere og VLAN konfigurasjoner. Men også VPN-enheter, modemer, HUBer med mer bør vurderes.

Et annet element som trekkes frem som viktig er om det er på plass et godt innarbeidet nettverksovervåkings- og kontroll- system. Herunder skal også implementeringsrutiner, driftsrutiner og endringshåndtering være på plass.
Viktig er det også at den fysiske infrastruktur som for eksempel kabling og trådløse soner er sikret tilfredsstillende.

Tilgangen fra maskiner koblet i nettverket er et annet viktig element å vurdere. Det vil være viktig å finne ut om alle enheter i nettverket har direkte kontakt med omverdenen eller om all kommunikasjon går via eksempelvis proxy-server eller terminalservere for klienter. Er det enheter i nettverket som har andre tilganger enn gjennom nettverket, eksempelvis med egne modemer eller lignende. Er det muligheter for å ta med maskiner ut av nettet, og koble til i andre nettverk. Hvordan er i så fall kommunikasjonen sikret? Viktig er det også å kartlegge om det er 3djeparts tilganger direkte til elementer i nettverket, og om det finnes, og i så fall hvilke, løsninger eksisterer for fjerndrift.

Intrusion Detection System IDS er et element som vurderes som viktig for å kunne oppdage potensielle angripere. Det legges vekt på at en IDS skal fange opp både interne og eksterne aktiviteter. Videre legger besvarelsene vekt på at det må være på plass et vedlikeholdsopplegg på systemene i nettverket. Det gjelder både programvare og maskinvare oppdateringer. Herunder også sikkerhetsoppdateringer (sikkerhetslapping).

Beskyttelse av WAN - forbindelser ved hjelp av eksempelvis VPN anses også som elementer som må vurderes i denne sammenhengen. Antivirus programvare på klienter og i e-post system anses også som et element som har med den sikkerhetsmessige tilliten til et nettverk å gjøre. Men dette kom ikke høyest opp på prioriteringslisten blant de som deltok i undersøkelsen. Dette henger også sammen med beskyttelse av klienter mot inntregning (lokal brannmur). Og da spesielt om maskiner benyttes utenfor nettverket på arbeidsplassen, eks. direkte på Internet. Begge disse elementene ligger under kategorien endepunktssikkerhet.

Akkrediteringer, sertifiseringer og eksterne revisjoner trekker deltagerne også frem som viktige elementer når man snakker om tillitsnivået i et nettverk.

Tillitsnivået til et nettverk vil også gjenspeile seg i den fysiske sikkerheten i virksomheten. Hvorvidt virksomheten er samlokalisert med andre og om det eksisterer rutiner for besøkende og adgang til lokaler og datahaller med mer.

Autentisering og autorisasjons løsninger bør være på plass, og knyttet opp mot policy.

Besvarelsene gav oss en liste med 33 elementer som deltagerne har trukket frem som viktige med hensyn til å si noe om et nettverk er tillitsverdig eller ikke. Vi tar her med de 11 punktene der 20 % eller mer hadde pekt på dette punktet, for å bruke disse som input til del-prosess 2. Hele listen med elementer ligger i Vedlegg D - Elementer fra resultatene.

Tabell 1 - Elementer fra undersøkelse i Del-Prosess 1

#	Tekst	% pekt på dette elementet
1	Perimetersikring og tilgangskontroll	70 %
2	Nettverks- og system- management verktøy	70 %
3	Fysisk sikkerhetsinfrasturktur (kabling/trådløse soner)	40 %
4	Eksterne tilganger	30 %
5	Intrusion Detection System (IDS)	30 %
6	Programvare og maskinvare oppdateringer (lapping),	30 %
7	Beskyttelse av WAN forbindelser	20 %
8	Antivirus på klienter, server og e-postssystemer	20 %
9	Endepunktssikkerhet (lokal brannmur)	20 %
10	Akkrediteringer, sertifiseringer og eksterne revisjoner	20 %
11	Fysisk sikkerhet (adgangskontroll med mer)	20 %

De fem viktigste elementene blir tatt med til Del-Prosess 2 for å brytes ned i sikkerhetsmetrikker.

3.2 Del-Prosess 2 – Sikkerhetsmetrikker

Del-Prosess 2 skal ta tak i de elementer som kom frem som et resultat fra Del-Prosess 1, og bryte disse ned i sikkerhetsmetrikker. Når man har benyttet prosessen en del, og lagt inn en del metrikker i toolkitet vil det være store muligheter for at man kan gjenbruke de metrikkene som ligger der. Det vil også være mulig at man finner en tilsvarende policy i toolkitet, og det vil derfor ikke være stort behov for å lage nye metrikker.

3.2.1 Definisjon av metrikker

Oppbyggingen av metrikker har vi basert på måten sikkerhetsmetrikker defineres i [NIST] og [simg2]. Vi benytter ikke de definisjonene helt likt, har fjernet noen felter som vi ikke har behov for her, og lagt til noen felter vi mener er viktige å ha med. Metrikkene som skal benyttes i prosessen defineres derfor opp etter følgende mal:

Tabell 2 - Definisjon av metrikker

Metrikk ID	*Unikt nummer som identifiserer hver metrikk.* *Dette nummeret vil bli tildelt av toolkitet.*
Navn	*Navn på metrikken (kort navn)*
Kategori	*Hver metrikk defineres inn i en av de følgende kategoriene, dette er de samme kategorier som er definert i Del-prosess 1.* *A – Sikkerhets administrasjon* *B – Programvare og Maskinvare Sikkerhet* *C – Nettverks funksjoner* *D – Aksess kontroll* *E – Fysisk Sikkerhet* *F – Avviks planlegging/håndtering* *Kategoriene er her beregnet på måling i forbindelse med informasjonssikerhet. Og vil endres om det er helt andre målinger man ønsker å utføre.*
Beskrivelse	*Beskrivelse av metrikken (kan ofte være krav fra lovverk eller policy).*
Tiltak	*Hvilke tiltak kan settes inn for å øke sikkerhet i forhold til denne metrikken.*
Krav	*Konkret referanse til hvor kravet er beskrevet. Er det ikke en konkret henvisning benyttes N/A.*
Metrikk	*Underspørsmål som skal gi en oversikt over grad av implementasjon.* *En metrikk kan bestå av ett eller flere underspørsmål, som til sammen skal si noe om hvorvidt tiltak er ivaretatt for å motstå truslene denne metrikken identifiserer.* *Hvert enkelt underspørsmål vektlegges mht sin viktighet i metrikken (se Formel).*

Formel	*Beskrivelse av beregningene som gjøres av svarene for å få en verdi på resultatet av metrikken.* *For at en metrikk skal få en verdi som kan benyttes til å gjøre kalkulasjoner i forbindelse med en undersøkelse, har vi definert opp en formel som skal kunne gi hver metrikk et tall som resultat. Hvert enkelt underspørsmål vektes i metrikken, og vil dermed ha forskjellig betydning for resultatet av metrikken i en undersøkelse.* *Vi har definert følgende vektnivåer for underspørsmålene til en metrikk:* ***0** – Ingen betydning* *Dette vil si at dette underspørsmålet ikke har noen betydning i denne metrikken. Konkret vil dette si at graden av implementasjon i forhold til dette underspørsmålet, ikke har noen betydning på sikkerheten.* ***1** – Liten betydning* *Om et underspørsmål har liten vekt i en metrikk, benyttes denne vekten. Dette vil si at det har liten konsekvens for sikkerheten om dette underspørsmålet er ivaretatt.* ***2** – Noen betydning* *Denne vekten benyttes om det har noen betydning om underspørsmålet er ivaretatt.* ***3** – Stor betydning* *Dette underspørsmålet har stor betydning, og det er viktig at mottiltakene som skal beskytte mot truslene dette underspørsmålet identifiserer er på plass.* ***4** – Avgjørende betydning* *Dette underspørsmålet er viktig, og representerer noe som man i metrikken anser som avgjørende for sikkerheten.* *Alle metrikker er bygget opp slik at lavest verdi alltid er dårligst. Og høyest skår er best.*
Hensikt	*Hva er målet ved å bruke denne metrikken?*
Kostnad	*Hva koster det å gjennomføre målingene i denne metrikken, måles i timer (t).*
Gyldighet	*Vurdering av metrikkens gyldighet, måler vi det som er gitt i kravene? (Tatt med for å kvalitetssikre metrikken).*
Pålitelighet	*Vurderingen av metrikkens pålitelighet. Er den motstandsdyktig mot tilfeldige feil? (Tatt med for å kvalitetssikre metrikken).*

3.2.2 Mål

For at prosessen skal kunne være enkel å benytte, og fleksibel, samtidig som det skal kunne gjøres målinger over tid. Er det viktig at resultatene som kommer ut av en måling er riktig, og kan sammenlignes med tidligere og nye målinger. Slik vi bygger opp prosessen, vil det være mulig å sammenligne systemer som er målt opp mot samme policy. En policy vil bestå av et sett med metrikker, disse metrikkene vil ikke endre seg innenfor en policy. Man kan derfor sammenligne måleresultater mellom

forskjellige systemer målt mot samme policy og målinger av samme system til forskjellige tider.

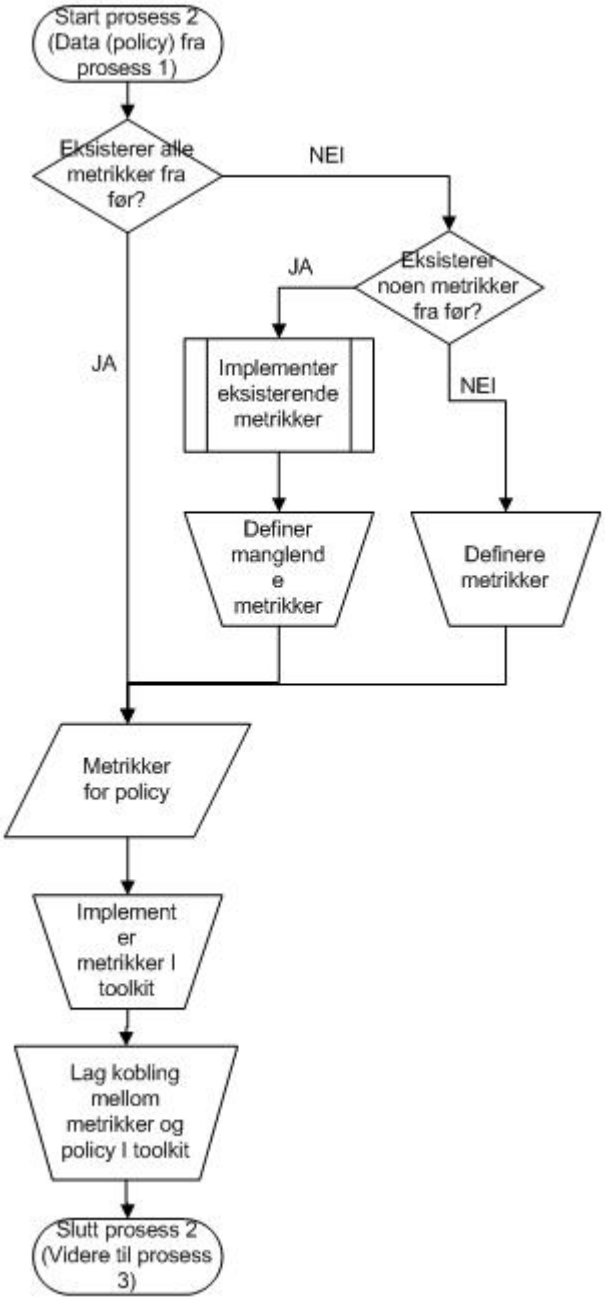
Et viktig kriterium i vårt arbeid var at målingene skulle være enkle å sammenligne. Vi har derfor valgt å lage et system basert på vekting av metrikkene i en undersøkelse. Dette gir oss muligheten til å fremstille resultatene av en undersøkelse med en enkelt tallverdi.

Når en metrikk skal knyttes inn i en policy vil den vektes i forhold til sin viktighet/relevans for den gitte policy. Vi har definert følgende vektgrader for metrikker inn i en policy:

- 0 – Ingen betydning
  Dette vil si at metrikken ikke har noen betydning i denne policyen. Konkret vil dette si at implementering av denne metrikken, eller mottiltak i forhold til hva denne metrikken skal måle, ikke har noen betydning på sikkerheten.
- 1 – Liten betydning
  Om en metrikk har liten vekt i en policy, benyttes denne vekten. Dette vil si at om det ikke har store konsekvenser for sikkerheten om denne metrikken er ivaretatt.
- 2 – Noen betydning
  Denne vekten benyttes om det har noen betydning om metrikken er ivaretatt.
- 3 – Stor betydning
  Denne metrikken har stor betydning, og det er viktig at mottiltakene som skal beskytte mot truslene denne metrikken identifiserer er på plass.
- 4 – Avgjørende betydning
  Denne metrikken er viktig, og representerer noe som man i policyen anser som avgjørende for sikkerheten.

De aktiviteter som er nødvendige for å komme gjennom del-prosess 2 er vist i Figur 7 – Del-Prosess 2 - Sikkerhetsmetrikker, og viser følgende aktiviteter:

1. Start prosess
   Data fra Del-Prosess 1 blir tatt inn som input.
2. Eksisterer metrikkene?
   En gjennomgang av eksisterende policies (og da gjerne direkte i toolkit) vil gi et svar på om det eksisterer en policy fra før som kan brukes, om deler av en policy kan benyttes, om enkelte metrikker fra noen policies kan benyttes. Eller om det må defineres helt nye metrikker for den ønskede policy.



Figur 7 – Del-Prosess 2 - Sikkerhetsmetrikker

3. Definisjon av metrikker

4. Implementer metrikker i toolkit
   Etter at det er plukket ut hvilke eksisterende metrikker som kan benyttes, og eventuelt nye er definert, kan disse legges inn i toolkitet.

5. Lag kobling mellom metrikker og policy i toolkit
   Den definerte policy må knyttes opp mot de metrikker som skal være en del av policyen.

3.2.2.1 Måleresultater for en metrikk

En metrikk er, som tidligere beskrevet, bygget opp rundt ett eller flere underspørsmål. Avhengig av resultatene på underspørsmålene i en metrikk, vil man etter en gitt utregning (se 3.3 Del-Prosess 3 – Gjennomføring av måling med toolkit) få en verdi for resultatet av hver metrikk.

3.2.3 Gjennomføring av Prosess 2 - Sikkerhetsmetrikker

Undersøkelsen ga oss en liste med de elementer som for EI ble vurderte ved endringer i en kompleks arkitektur. Vi velger ut de 5 elementene som ble rangert høyest og bryter disse ned i metrikker.

Metrikkene er definert i 3.3.1 Definerte metrikker basert på undersøkelse.

3.3 Del-Prosess 3 – Gjennomføring av måling med toolkit

Den tredje prosessen er selve målingen. Her defineres policy med tilhørende metrikker inn i toolkitet (dette kan, og vil oftest, være gjort i Del-Prosess 2) og målingene utføres.

Når undersøkelsen skal gjennomføres, benytter man toolkitet og besvarer de underspørsmål som er definert inn i hver metrikk. Vi har definert opp fem svaralternativer for hvert underspørsmål. Med følgende 5 svaralternativer mener vi at vi har dekket opp de nødvendige graderingene av svar:

- 0 – Ikke på plass
  Dette vil si at man ikke har tatt høyde for den trusselen dette underspørsmålet representerer. Eller man har ikke implementert de mottiltak som er nødvendig for å ivareta dette spørsmålet.
- 1 – Noe på plass
  Har man i noen grad tatt høyde for dette spørsmålet svarer man med dette svaret. Dvs. at man ikke har de viktigste mottiltak på plass, men noen av mindre betydning kan være ivaretatt.
- 2 – Det meste er på plass
  Når det gjelder dette spørsmålet er det meste på plass, men det kan fortsatt mangle noen viktige aspekter.
- 3 – De viktige aspekter er på plass,
  men det kan mangle noen av mindre betydning.
- 4 – Alt implementert
  Dette vil sa at dette spørsmålet er ivaretatt på alle områder.

For hver enkelt metrikk, kan vi nå regne ut en verdi:

$$mv = \frac{(s_1 * vu_1) + (s_2 * vu_2) + \ldots\ldots + (s_u * v\,u_u)}{(s_{1_{max}} * vu_1) + (s_{2_{max}} * vu_2) + \ldots + (s_{u_{max}} * vu_u)}$$

, der

mv = metrikkverdi
s = svaret gitt på et underspørsmål
vu = vekten til underspørsmålet i metrikken (0, 1, 2, 3 eller 4)
u = antall underspørsmål
max = maksimal svar verdi for et underspørsmål, her 4.

Dette vil gi oss en verdi for hver metrikk som ligger mellom 0 og 1.

For å få en verdi for hele undersøkelsen setter vi opp formelen:

$$ur = \frac{(mv_1 * vm_1) + (mv_2 * vm_2) + \ldots + (mv_m * vm_m)}{vm_1 + vm_2 + \ldots + vm_m}$$

, der

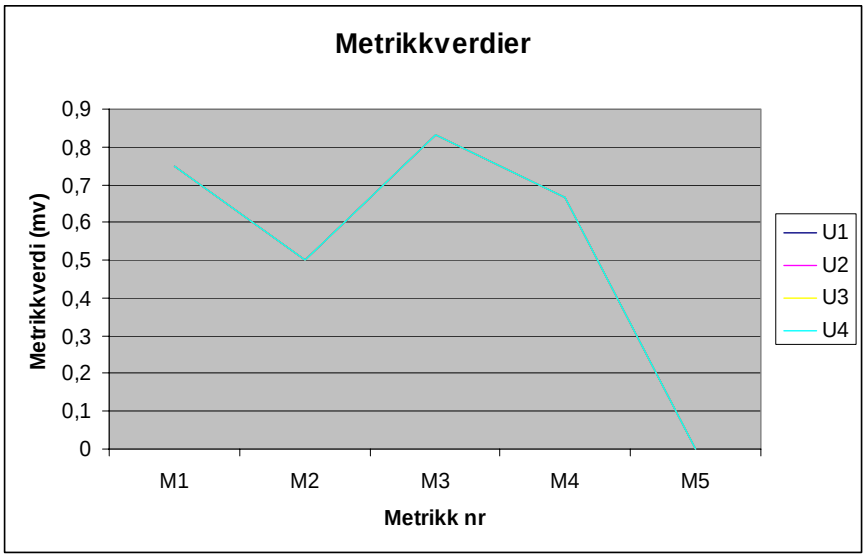
ur = undersøkelse verdi
mv = metrikkverdi
vm = vekten metrikken har i policyen (0, 1, 2, 3 eller 4)
m = antall metrikker i policy

Denne formelen vil gi oss en verdi på hver enkelt undersøkelse som ligger mellom 0 og 1.

Arbeidet gav oss ikke tid til å gjøre skarpe målinger av et system. Og vi valgte derfor å simulere noen målinger for å undersøke om prosessen og formlene så riktige ut. Vi la derfor disse formlene inn i et regneark, og gjorde noen simuleringer for å se hva resultatene ble. Fire undersøkelser ble lagt inn i regnearket, hver undersøkelse inneholdt fem metrikker som igjen hadde fire underspørsmål (Regnearket finnes i Vedlegg G - Regneark for simulering av undersøkelse).

Ved å legge inn i regnearket, at alle metrikker hadde fire underspørsmål, og disse ble vektet likt i alle 5 metrikker, simulerte vi resultatene som vist i Figur 8 - Simulering med metrikkformel. Her er besvarelsene gjort slik at metrikkene 1 og 3 er besvart ved at underspørsmålene med høyest betydning er gitt høyest verdi. Og metrikkene 2 og fire er besvart ved at underspørsmålene med lavest betydning har fått høyest score.

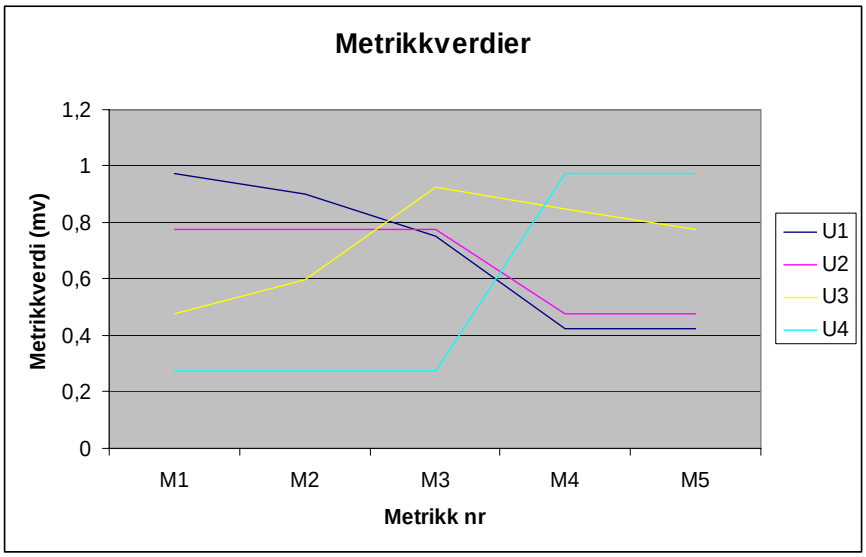
Som forventet, så får vi best score på de metrikker som er besvart med høyest verdi for underspørsmål med høyest vekt. Siden alle fire undersøkelser er besvart likt, er resultatene for undersøkelsene her sammenfallende.



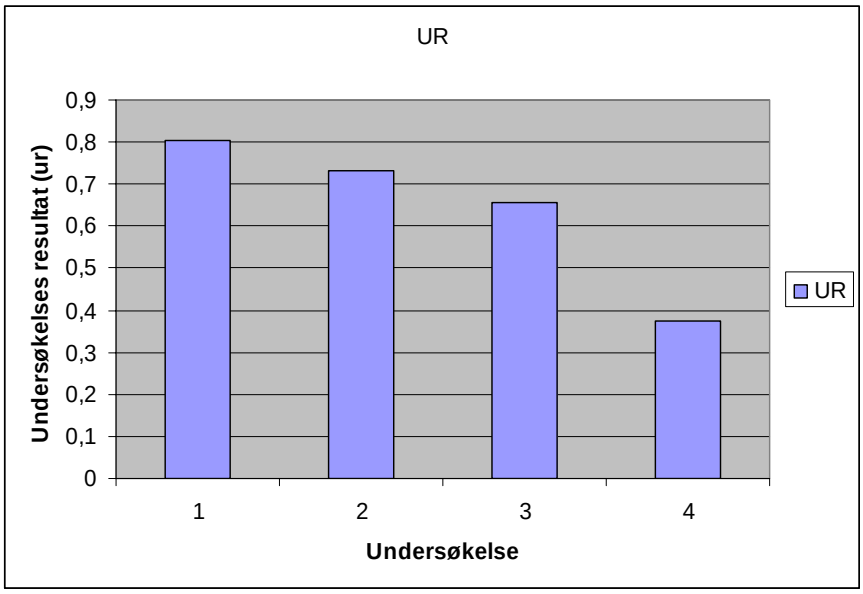
Figur 8 - Simulering med metrikkformel

Vi gjorde en simulering til, der lot vi metrikkene i undersøkelse 1 og 3 ha samme vekting, det samme hadde undersøkelse 2 og 4. Alle metrikker hadde et underspørsmål i hver vekt kategori. Dvs. ett spørsmål med vekt 1, ett spørsmål med vekt 2 osv.

Besvarelsene i undersøkelsen var fordelt slik at i Undersøkelse 1 og 2, besvarte vi de spørsmål med høyest vekt (størst betydning) i de metrikker med høyest vekt med det høyeste svaralternativet (4). I undersøkelse 3 og 4 gav vi de metrikker med lavest vekt (minst betydning) de høyeste svarene. Resultatene i Figur 10 - Simuleringsresultater for undersøkelser viser som forventet at det er undersøkelse 1 og 2 som gir best resultat. Hvor de mest betydningsfulle metrikker fikk best score.



Figur 9 - Simulering av resultater for metrikker

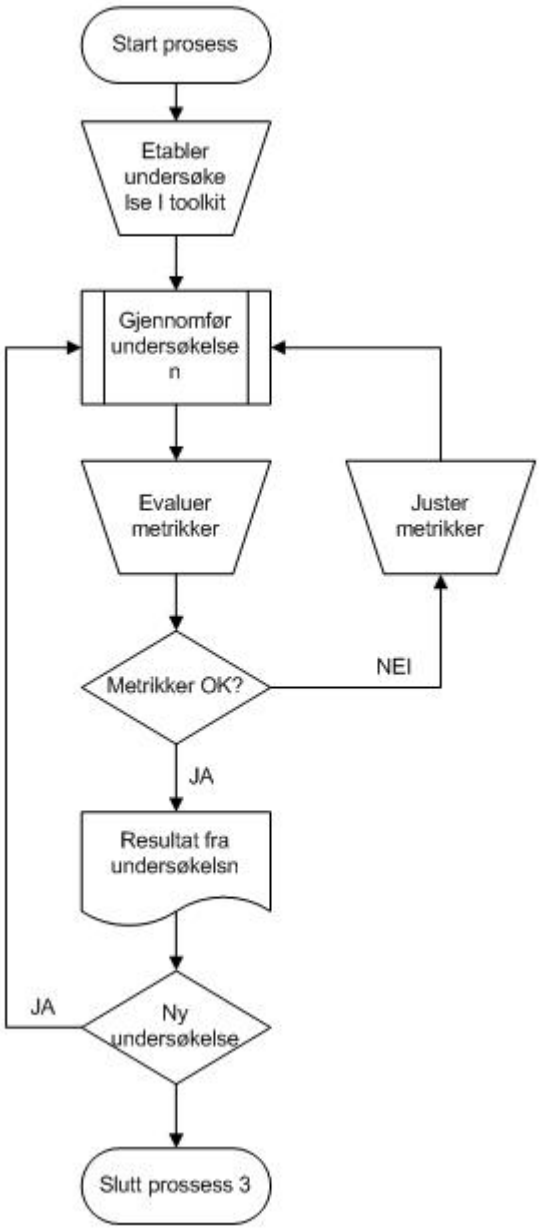


Figur 10 - Simuleringsresultater for undersøkelser

Det vi ikke har implementert i denne versjonen av toolkitet og i måten vi regner resultater på er at vi nok i enkelte policies som defineres vil finne elementer og metrikker som er helt avgjørende. Og hvor det derfor med en vekting på maks 4 ikke vil gi nok utslag i resultatet om metrikken ikke er ivaretatt fullt ut. Dvs. at vi nok bør legge inn i prosessen at det bør kunne defineres metrikker som har en avgjørende betydning, som altså vil være en ”show stopper” for policyen som det måles opp mot.

Selve prosessen for å utføre undersøkelsen består av følgende aktiviteter:

- Start del-prosess 3
- Etablere undersøkelse i toolkit.
  Den undersøkelsen knyttes så opp mot et system og en policy.
- Kjøre gjennom undersøkelsen
  Her går man gjennom undersøkelsen, og besvarer metrikkene.
- Evaluerer metrikker
  Når man kjører gjennom en undersøkelse, må metrikkene og knytningene mot policy evalueres. Dette er spesielt viktig når man kjører gjennom en undersøkelse med en ny policy, og hvor det er definert nye metrikker.
  Ser man at noen av metrikkene har mangler, eller ikke passer inn i policy, må disse justeres.
- Resultater fra undersøkelsen
  Når man har kjørt gjennom undersøkelsen, vil man kunne hente ut resultatet fra toolkitet med en gang.



Figur 11 – Del-Prosess 3 - Gjennomføring av måling med toolkit

3.3.1 Definerte metrikker basert på undersøkelse

I dette underkapittelet har vi definert opp eksempler på metrikker. Metrikkene er bare noen få eksempler på metrikker, og ikke en komplett liste. Metrikkene har vi definert selv, med bakgrunn i undersøkelsen utført. En liste over forslag til målepunkter for et element ble listet opp av deltagerne. Denne listen er gjengitt i sin helhet i Vedlegg E - Mulige metrikker på elementene. Vi har også hentet innspill til metrikker fra [NIST] og [simg2].
I Vedlegg I – Metrikker for Personopplysningsloven som policy har vi også lagt ved de metrikker som vil danne grunnlaget for Personopplysningsloven som policy. Dette arbeidet ble utført i [simg2].

Tabell 3 - Elementer som input til Prosess 2

#	Tekst
1	Perimetersikring og tilgangskontroll
2	Nettverks- og system- management verktøy
3	Fysisk sikkerhetsinfrasturktur (kabling/trådløse soner)
4	Eksterne tilganger
5	Intursion Detection System (IDS)

3.3.1.1 Perimetersikring og tilgangskontroll

Tabell 4 - Metrikk - Brannmurer

Metrikk ID	*<tildeles av toolkit>*
Navn	*Brannmurer*
Kategori	*D – Aksess kontroll*
Beskrivelse	*Er alle brannmurer i systemet sikret og fungerer som de skal?*
Tiltak	*Det må etableres rutiner og prosedyrer for å ivareta nødvendige sikkerhet for brannmurer.*
Krav	*Undersøkelse i EI januar 2004*
Metrikk	1. *Er brannmurens OS patchet i henhold til anbefalt versjon?* *Vekt = 3* 2. *Er det definerte endringsrutiner for brannmurene? Som følges og som inkluderer sikkerhetsvurderinger ved alle endringer i regelsett.* *Vekt = 4* 3. *Er brannmuren i stand til å skille og evaluere kommunikasjonen på det protokollnivå som beskyttes i brannmuren?* *F.eks er det mye som kan gå over port 80. Det holder ikke å verifisere at dette er gyldig http-trafikk med riktige sesjonsnummer, pakketellere, flag etc.* *Vekt = 4* 4. *Blir logger reglemessig undersøkt i brannmuren?* *Vekt = 3*
Formel	$\frac{(s_1 * 3) + (s_2 * 4) + (s_3 * 4) + (s_4 * 3)}{(4*3) + (4*4) + (4*4) + (4*3)}$
Hensikt	*Tilse at alle brannmurer er sikkerhetsmessig funksjonelle.*
Kostnad	*(15 minutter pr brannmur) *(antall brannmurer) / 60 timer*
Gyldighet	*Her er det en konkret undersøkelse av alle brannmurer, som er det vi ønsker å måle. Metrikken kan derfor sees på som pålitelig.*
Pålitelighet	*Her vil alle brannmurer sjekkes opp mot at alle skal ha oppfylt kravene i metrikken. Dette er konkrete krav og metrikken vil være pålitelig.*

Tabell 5 - Metrikk - Tilgangskontroll på systemprogramvare

Metrikk ID	*<tildeles av toolkit>*
Navn	*Tilgangskontroll på systemprogramvare*
Kategori	*D – Aksess kontroll*
Beskrivelse	*Er det etablert et tilgangskontrollsystem for tilgang til systemprogramvare, som NOS (Nettverks Operativ Systemer), personal systemer osv…*
Tiltak	*Det må etableres tigangskontrollsystem for tilgang til systemprogramvare.*
Krav	*Undersøkelse i EI januar 2004*
Metrikk	1. *Er det etablert tilgangskontrollsystem for systemprogramvare på rutere?* *Vekt= 3* 2. *Er det etablert tilgangskontroll på systemprogramvare på brannmurer?* *Vekt= 4* 3. *Er det etablert tilgangskontroll på systemprogramvare på servere (nettverks operativsystemer)?* *Vekt= 4* 4. *Er det etablert tilgangskontroll på systemprogramvare for forretnings applikasjoner?* *Vekt=3* 5. *Er det etablert tilgangskontroll på systemprogramvare for personalsystem (inkl lønn)?* *Vekt= 4*
Formel	$\frac{(s_1 * 3) + (s_2 * 4) + (s_3 * 4) + (s_4 * 3) + (s_5 * 4)}{(4*3) + (4*4) + (4*4) + (4*3) + (4*4)}$
Hensikt	*Finne eventuelle svakheter i tilgangskontroll på systemprogramvare.*
Kostnad	*(2 minutter pr system) *(antall systemer) / 60 timer*
Gyldighet	*Her er det en konkret undersøkelse av systemer og deres tilgangskontroll løsning, som er det vi ønsker å måle. Metrikken kan derfor sees på som gyldig.*
Pålitelighet	*Metrikken kan sees på som pålitelig da alle systemer undersøkes i forhold til om de har et tilgangskontroll system.*

3.3.1.2 Nettverks- og system- management verktøy

Tabell 6 - Metrikk - Sikkerhetsledelse

Metrikk ID	*<tildeles av toolkit>*
Navn	*Sikkerhetsledelse*
Kategori	*A – Sikkerhets administrasjon*
Beskrivelse	*Det skal være en sikkerhetsleder i virksomheten.*
Tiltak	*Etablere ansvarsforhold og utnevne en sikkerhetsansvarlig.*
Krav	*Undersøkelse i EI januar 2004*

Metrikk	1. *Er det utnevnt en sikkerhetsansvarlig i virksomheten?* *Vekt = 3* 2. *Blir sikkerhetsansvarligs oppgaver kontrollert?* *Vekt = 4*
Formel	$\frac{(s_1 * 3) + (s_2 * 4)}{(4*3) + (4*4)}$
Hensikt	*Ansvaret for informasjonssikkerhet må være klart definert. Og en sikkerhetsansvarlig må derfor være utnevnt. Og bevisst sine oppgaver. Samtidig med at arbeidet som utføres blir kontrollert.*
Kostnad	*5 / 60 time*
Gyldighet	*Gyldigheten er høy, da dette er basert på organisatoriske kjente, for de som vil utføre slike målinger, forhold.*
Pålitelighet	*Metrikken er avhengig av at noen kjenner til de forhold som eksisterer i virksomheten. Siden dette blir en subjektiv vurdering, vil påliteligheten vær middels.*

3.3.1.3 Fysisk sikkerhetsinfrastruktur (kablinger/trådløse soner)

Tabell 7 - Metrikk – Kabling

Metrikk ID	*<tildeles av toolkit>*
Navn	*Kabling*
Kategori	*E – Fysisk Sikkerhet*
Beskrivelse	*Er kabling i henhold til de standarder som er for slike systemer?*
Tiltak	*Etablere kabling som tilsvarer de krav definert for systemet.*
Krav	*Undersøkelse i EI januar 2004*
Metrikk	1. *Er alle systemer korrekt kablet?* *Vekt = 4* *(Besvares ut fra om ingen (0 %) kabler er korrekt kablet (0) til alle systemer er korrekt kablet (4)(100 %))*
Formel	$\frac{(s_1 * 4)}{(4*4)}$
Hensikt	*Verifiser at kablingen er i henhold til krav for det undersøkte systemet.*
Kostnad	*(Antall systemer undersøkt) * (10 min pr. system (inkl transport)) / 60 (time)*
Gyldighet	*Dette vil være en eksakt undersøkelse av gitte systemer. Gitt at kabel kvalitet lett kan verifiseres, er denne metrikkens gyldighet god.*
Pålitelighet	*Høy pålitelighet siden antall systemer er kontrollert mot antall systemer med korrekt kabling.*

Tabell 8 - Metrikk - Avlytting over kablede strekk

Metrikk ID	*<tildeles av toolkit>*
Navn	*Avlytting over kablede strekk*
Kategori	*E – Fysisk Sikkerhet*
Beskrivelse	*Er det kontrollert tilgang til kablinger som frakter sensitiv informasjon i klartekst (ukryptert) for systemet.*

Tiltak	*Kabler som overfører sensitiv informasjon i klartekst (ukryptert) må sikres mot fysisk tilgang.*
Krav	*Undersøkelse i EI januar 2004*
Metrikk	1. *Er alle kabler internt i virksomheten (innefor samme bygg) sikret mot fysisk tilgang?* *Vekt = 3* 2. *Er alle aksesspunkter mellom kablinger (internt/eksternt) sikret mot fysisk tilgang?* *Vekt = 4* 3. *Er alle kabler eksternt sikret mot fysisk tilgang?* *Vekt = 4*
Formel	$\frac{(s_1 * 3) + (s_2 * 4) + (s_3 * 4)}{(4*3) + (4*4) + (4*4)}$
Hensikt	*Ivareta all kabling og hindre at uvedkommende kan avlytte kabelstrekk som inneholder sensitiv informasjon.*
Kostnad	*(Antall kabelstrekk undersøkt) * (15 min pr. strekk (inkl transport)) / 60 (time)*
Gyldighet	*Alle kabelstrekk undersøkes og kravet er klart. Metrikken har derfor høy gyldighet.*
Pålitelighet	*Alle kabelstrekk sjekkes manuelt for ikke sikrede strekk, påliteligheten er høy.*

3.3.1.4 Eksterne tilganger

Tabell 9 - Metrikk - Mottak for eksterne VPN forbindelser

Metrikk ID	*<tildeles av toolkitet>*
Navn	*Mottak for eksterne VPN forbindelser*
Kategori	*C – Nettverks funksjoner*
Beskrivelse	*Et mottak for eksterne VPN forbindelser vil være en åpning inn i virksomhetens nettverk. Disse må derfor plasseres på en godt vurdert sted og sikres.*
Tiltak	*Eksternt mottak for VPN forbindelser må plasseres på et egnet sted, og det bør sikres med nødvendige sikkerhetsmekanismer.*
Krav	*Undersøkelse EI januar 2004.*
Metrikk	1. *Er mottak for eksterne VPN forbindelser plasser på et eget brannmurben?* *Vekt = 3* 2. *Filtreres inngående VPN trafikk i et aksessfilter (router, brannmur el.)?* *Vekt = 2* 3. *Filtreres trafikken fra sentralt VPN mottak videre inn i virksomhetens nettverk gjennom en brannmur?* *Vekt = 4*
Formel	$\frac{(s_1 * 3) + (s_2 * 4) + (s_3 * 4)}{(4*3) + (4*4) + (4*4)}$
Hensikt	*Sørge for at alle eksterne VPN tilkoblinger kommer inn gjennom et sentralt kontrollert og sikret punkt.*
Kostnad	*((antall VPN mottak som kontrolleres) * (20 min pr. stk)) / 60*
Gyldighet	*Her kontrolleres hvert enkelt VPN mottak, og konkrete kontroller blir utført. Gyldigheten til metrikken må ansees som høy.*

Pålitelighet	*Her vil konkrete punkter kontrollers rundt VPN mottaket. Konkrete sjekker gjøres i og rundt systemet, og man vil ha en pålitelig måling/metrikk.*

3.3.1.5 Intrusion Detection System (IDS)

Her har vi ikke definert egne metrikker. I [tven] utføres parallelt med vårt arbeid en masteroppgave hvor man ser på benchmarking av IDS-verktøy. Resultatet av dette arbeidet vil være med på å gi underlag for etablering av metrikker rundt IDS. Det er også i blant andre [Puke], [Song] og [Atha] diskutert hvordan man skal måle godheten av IDS systemer.

3.3.2 Prototyp på Toolkit

For å kunne gjennomføre målingene og gjennomføre sammenligninger av forskjellige målinger, har vi laget en prototyp på et verktøy.

Hensikten med verktøyet er å kunne gjennomføre målinger på et system, for å se om systemet er tillitsverdig og kunne gi en verdi på tillitsnivået til systemet som undersøkes.

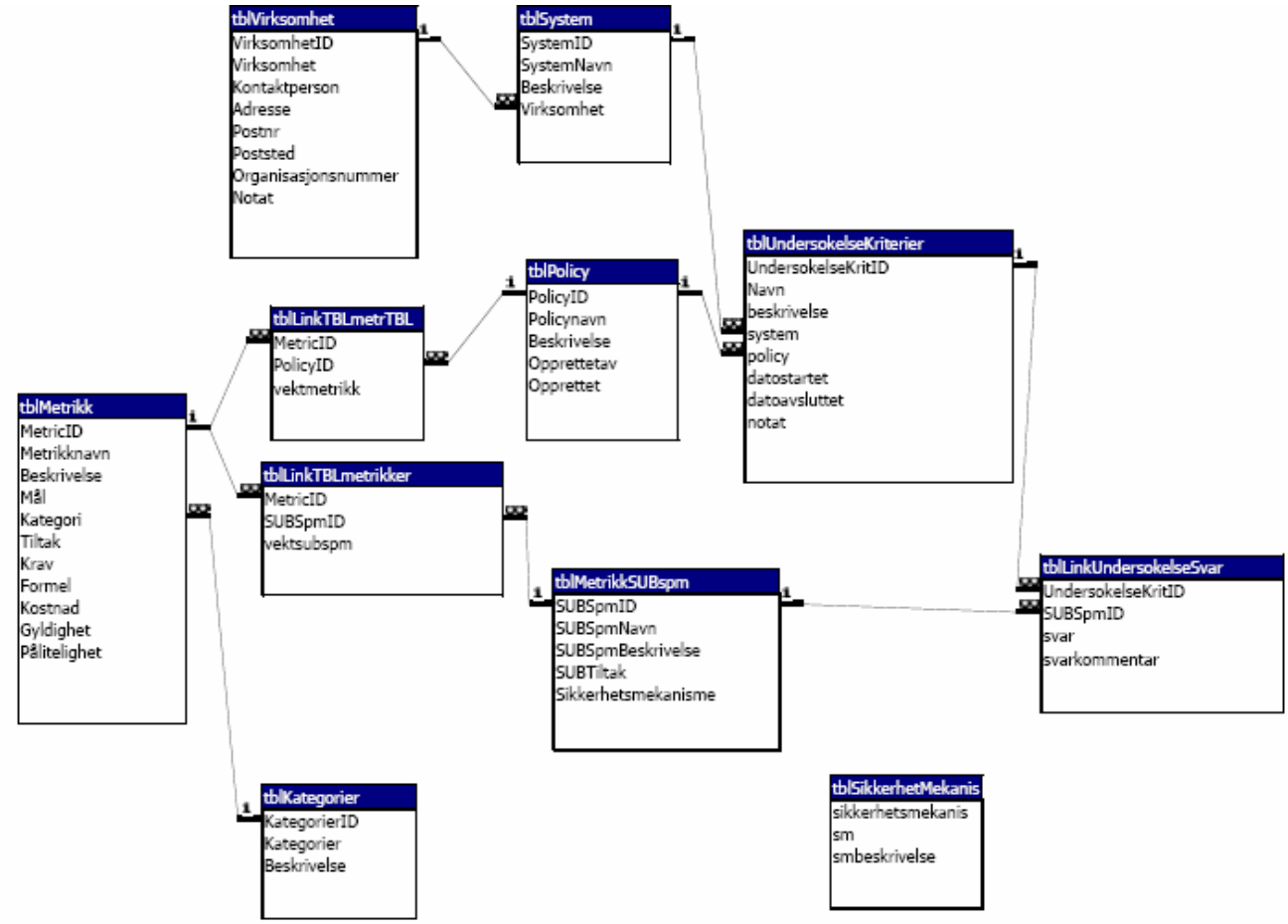
Det er lagt vekt på at dette verktøyet skal kunne benyttes av EI i den daglige forvaltningen av sine, sine kunders og leverandørers nettverk og systemer.

Verktøyet er en database hvor et viktig element er å lagre resultater fra tidligere undersøkelser for å kunne sammenligne og dermed spore endringer over tid.

3.3.2.1 Utvikling

Verktøyet er utviklet ved hjelp av Microsoft Access 2003 [acce] og Microsoft Visual Basic 6.3 [vba6].
Vi laget en datamodell for prototypen basert på innholdet i prosessene. I Figur 12 - Sammenhenger i databasen til prototyp av toolkit (som vi har valgt å kalle EItwa (ErgoIntegration Trust Worthiness Assessment), men som vi etterkant ser blir et begrensende navn. Men vi lar dette stå som navnet på prototypen ☺) ser vi en oversikt over de sammenhenger mellom tabeller som er i prototypen av toolkitet. Denne oversikten representerer hele prosessen.

Som tidligere beskrevet, så blir Virksomheten (tblVirksomhet) det øverste nivået i databasen. (Vi beskriver ikke her de forskjellige feltene i databasen.) Det legges så opp til at en virksomhet kan ha mange systemer, som lagres i en egen tabell (tblSystem).



Figur 12 - Sammenhenger i databasen til prototyp av toolkit

Følgende tabeller er definert i EItwa:

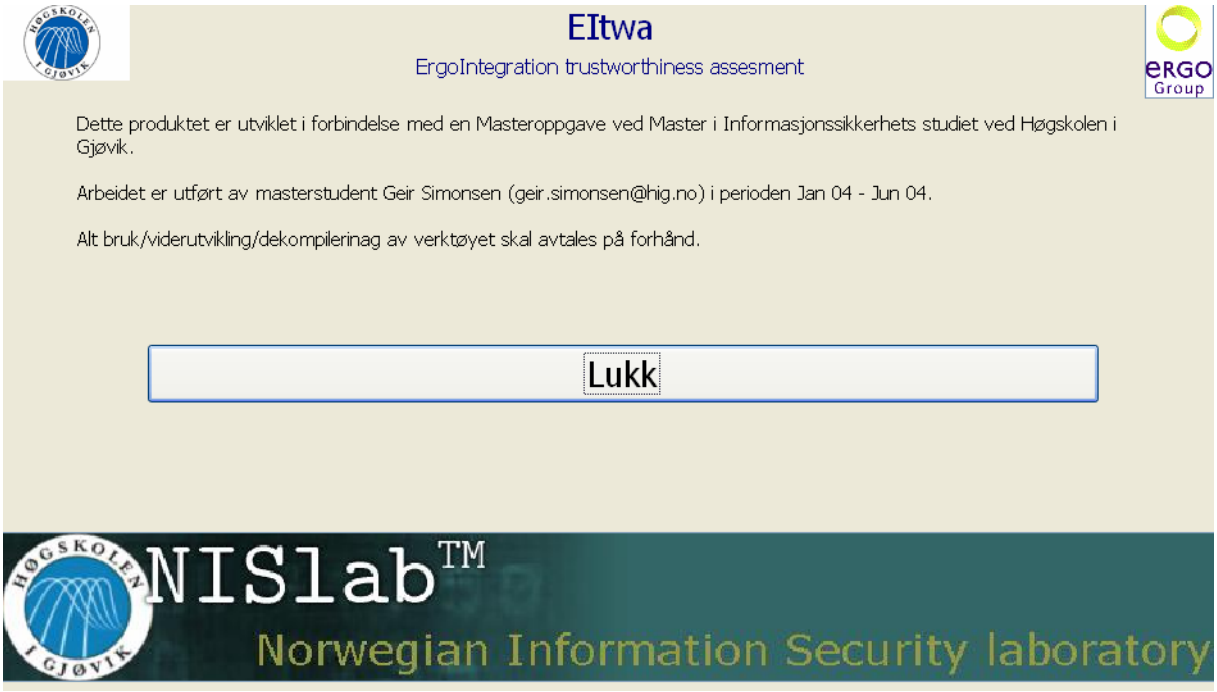
- tblVirksomhet
  Inneholder all informasjon om virksomhetene som eier systemene som skal måles. Dette kan være den virksomhet som har en definert policy, som kan benyttes mot systemer i forskjellige virksomheter.
- tbl System
  Her defineres de systemer som skal måles, og knyttes opp mot en virksomhet.
- tblPolicy
  Her defineres policyene, disse kan være tilgjengelige for alle som bruker toolkitet, og kan benyttes i alle undersøkelser.
- tblMetrikk
  Her defineres metrikkene som beskrevet i Del-Prosess 2.
- tblMetrikkSUBspm
  Denne tabellen er knyttet mot metrikkene. Her defineres inn underspørsmål til en metrikk.
- tblKategori
  Alle metrikker knyttes opp mot en kategori, disse er beskrevet i Del-Prosess 2.
- tblUndersokelseKriterier
  I denne tabellen defineres en undersøkelse opp, og knyttes mot en policy og det systemet som skal undersøkes.

- tblUndersokelseSvar
  Her registreres svarene på alle underspørsmål i en undersøkelse, som ligger i en metrikk tilhørende en policy
- tblSikkerhetsmekanisme
  Hvert enkelt underspørsmål knyttes til de kjente sikkerhetsmekanismer (Konfidensialitet, Integritet og Tilgjengelighet). Kombinasjonene av disse er definert i denne tabellen (K, I, T, KI, KT, IT og KIT).
- tblLinkTBLmetrTBLpolicy
  I denne tabellen knytter man de definerte metrikker opp mot de gitte policy de skal benyttes i.
- tblLinkTBLmetrikker
  Vi har laget denne tabellen, for å kunne gjenbruke underspørsmål i flere metrikker. Og dette gjøres i denne tabellen.

3.3.2.2 Prototyp toolkit – bruk (en slags brukerveiledning)

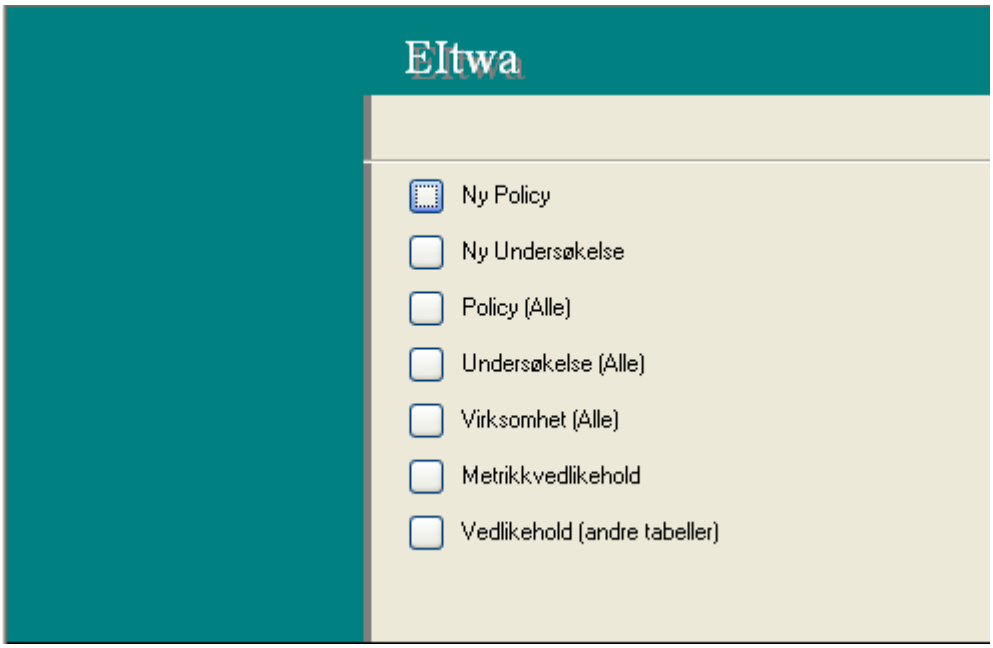
Det grafiske grensesnittet i toolkitet er ikke utviklet med en optimal MMI (Menneske Maskin Grensesnitt), vi har fokusert på å få ferdig de deler vi trenger for å legge inn verdier til å teste prototypen. I prototypen ligger det også synlig mange felter for kontroll i utviklingen, disse virker forvirrende, og vil ikke være nødvendige å ha synlige når produktet blir mer enn en prototyp.

Ved oppstart av prototypen, vil man få opp et velkomstbilde Figur 13 - Toolkit - Velkomstbilde.



Figur 13 - Toolkit - Velkomstbilde

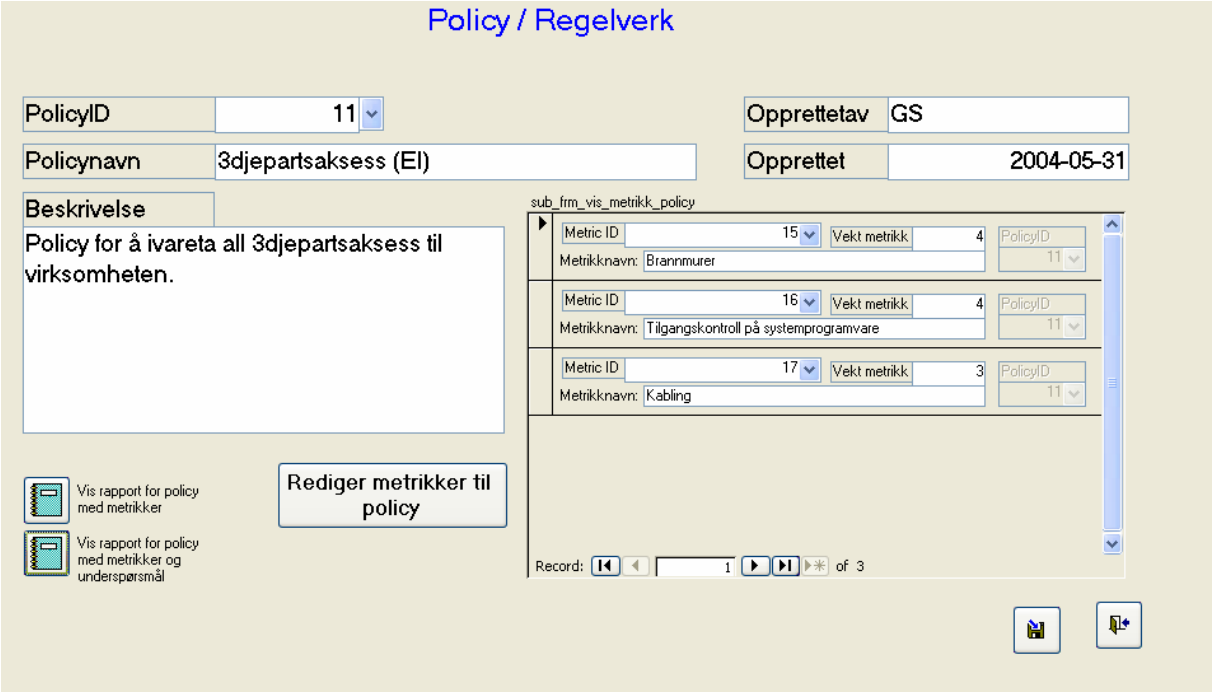
Når velkomstbildet lukkes, vil den implementerte enkle menyen, med de mest brukte funksjonene komme opp Figur 14 – Toolkit - Meny i prototyp.



Figur 14 – Toolkit - Meny i prototyp

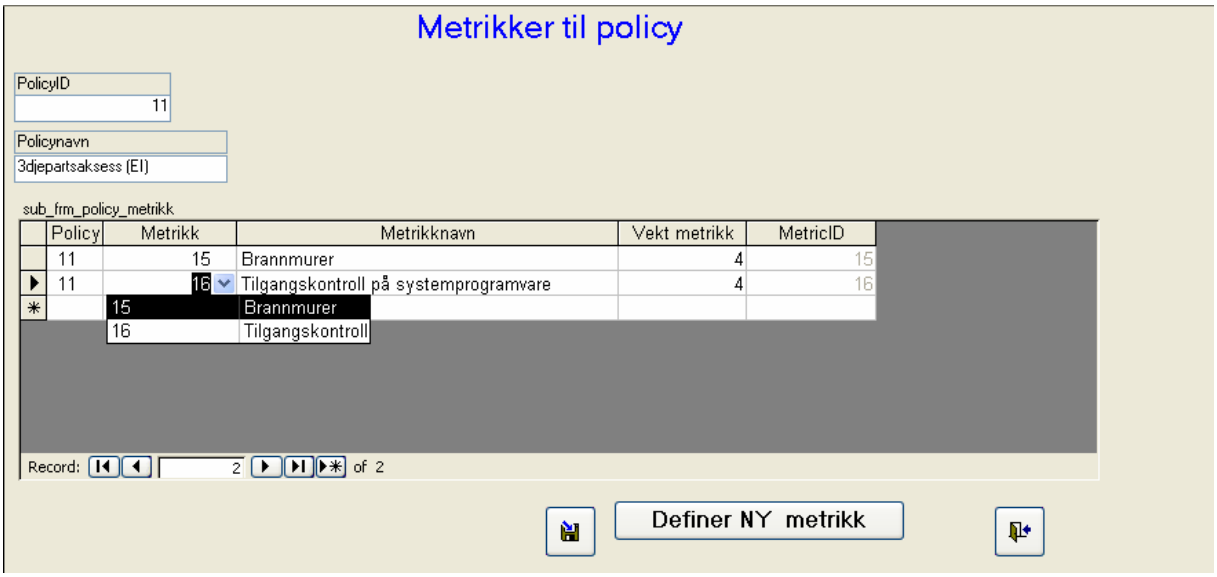
3.3.2.2.1 Definisjon av policy, metrikker og underspørsmål

For å etablere en ny policy, velger man Ny Policy i Hovedmenyen.



Figur 15 - Toolkit - Ny Policy

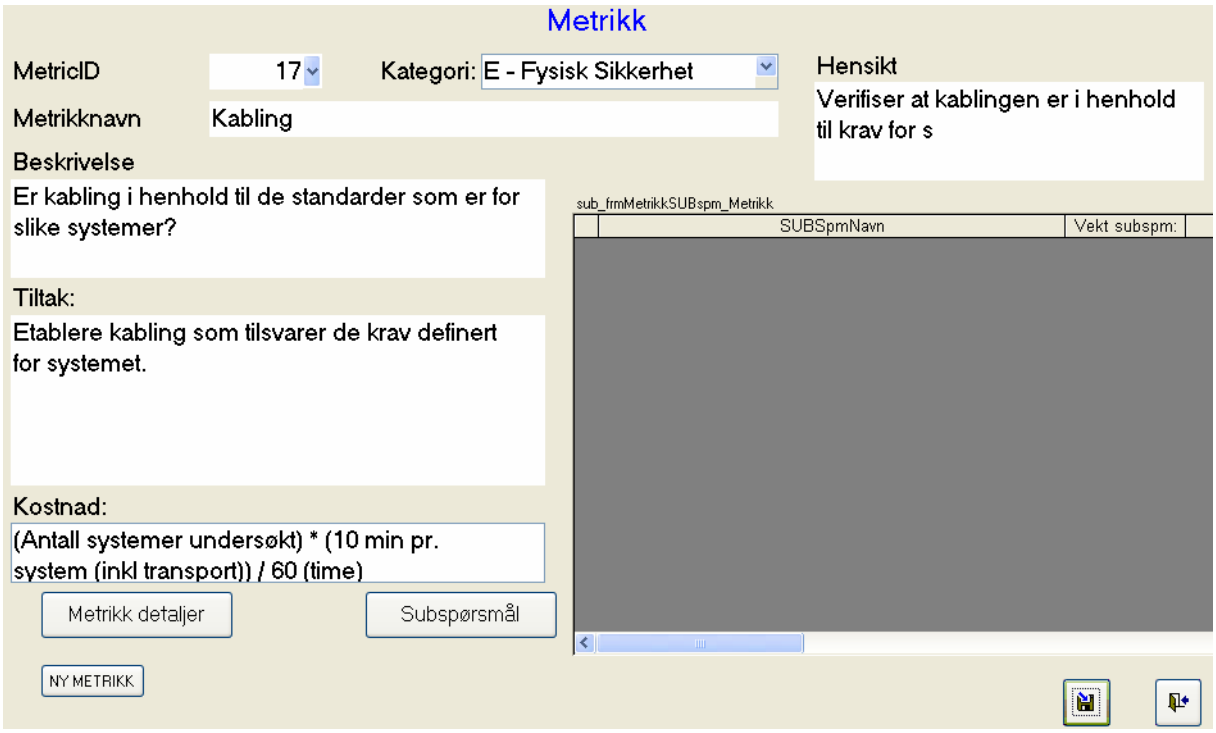
Her registreres inn alle opplysninger om den policy man skal etablere.
For å legge til eller opprette metrikker for denne policyen klikk på knappen ”Rediger metrikker til policy”.



Figur 16 - Toolkit - Metrikker til policy

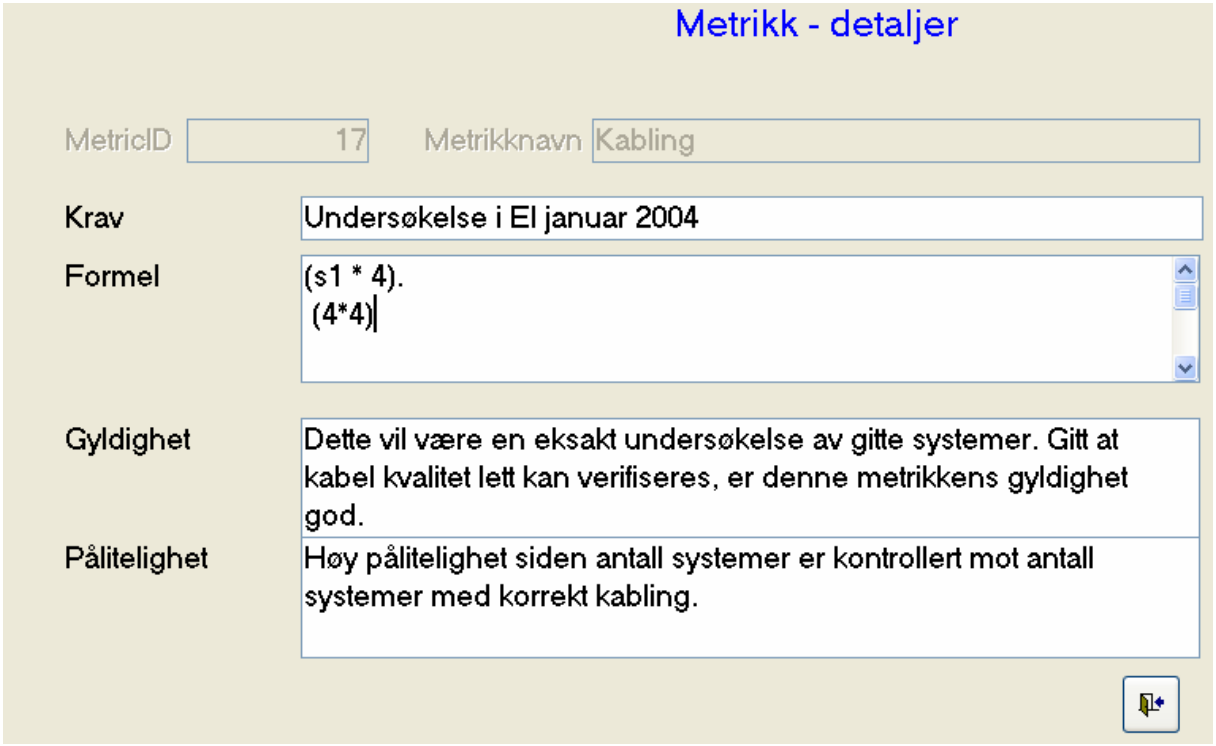
Velg så de metrikker som ønskes knyttet mot policyen. Dette gjøres ved å klikke i feltet ”Metrikk” og velg fra nedtrekksmenyen. Skriv så inn vekten denne metrikken skal ha i policyen. Dette skrives inn i ”Vekt metrikk” feltet.

Om den ønskede metrikken ikke finnes i nedtrekksmenyen, kan en ny metrikk legges til ved å klikken ”Definer NY metrikk”.



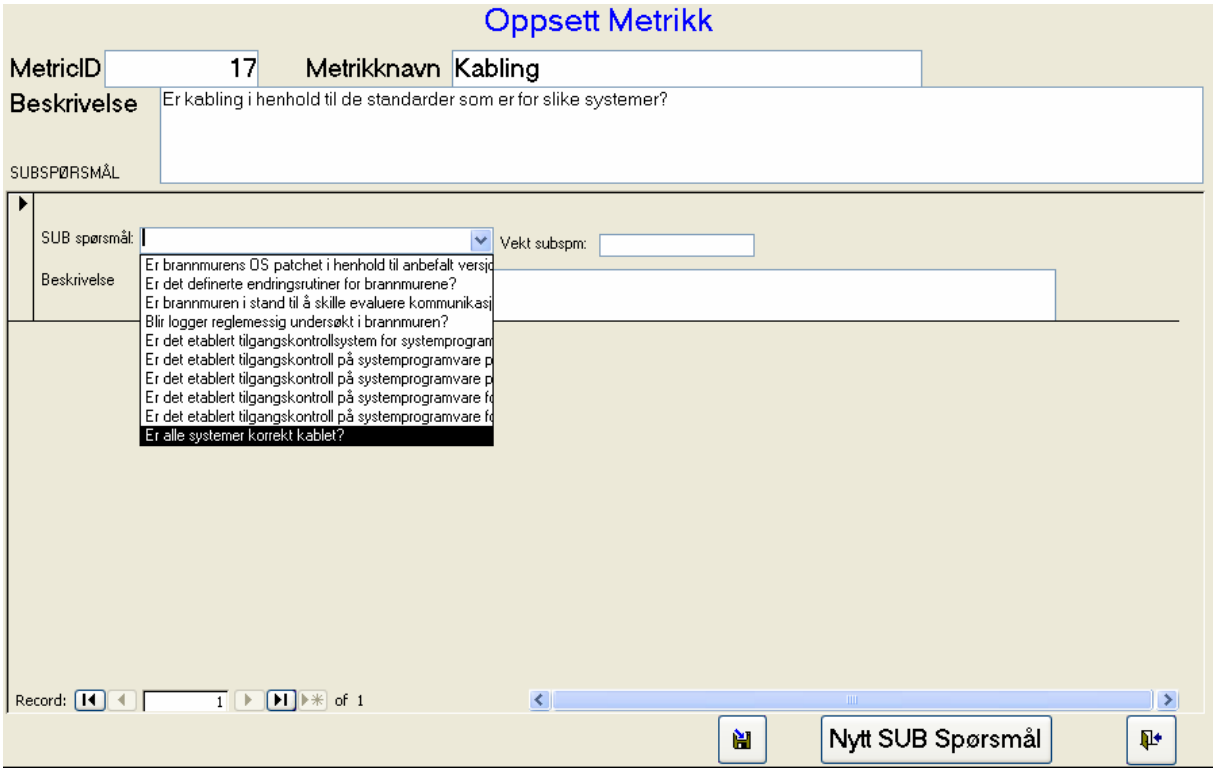
Figur 17 - Toolkit - Legg til metrikk

Alle opplysninger for metrikken legges inn i dette vinduet. Mer detaljer kan også legges til ved å klikke på knappen ”Metrikk detaljer”.



Figur 18 - Toolkit - Metrikk detaljer

Når alle detaljer er lagt inn, kan vinduet lukkes. Og man er tilbake på Figur 17 - Toolkit - Legg til metrikk, her kan man nå legge inn de subspørsmål som man ønsker å knytte til denne metrikken. Dette gjøres ved å klikke på knappen ”Subspørsmål”.



Figur 19 - Toolkit - Subspørsmål til metrikker

Her legges subspørsmålene inn ved at man velger fra nedtrekksmenyen i feltet ”SUB spørsmål”. Om ønsket subspørsmål ikke er definert, kan dette legges til ved å klikke på ”Nytt SUB Spørsmål”.

Figur 20 - Toolkit - Legg til subspørsmål

Når et subspørsmål er laget, og vinduet er lukket, er man tilbake i Figur 19 - Toolkit - Subspørsmål til metrikker. Her finner man nå det nye subspørsmålet i nedtrekkmenyen, og det kan velges for denne metrikken. Og vekten til dette subspørsmålet for denne metrikken legges inn i feltet ”Vekt subspørsmål”.

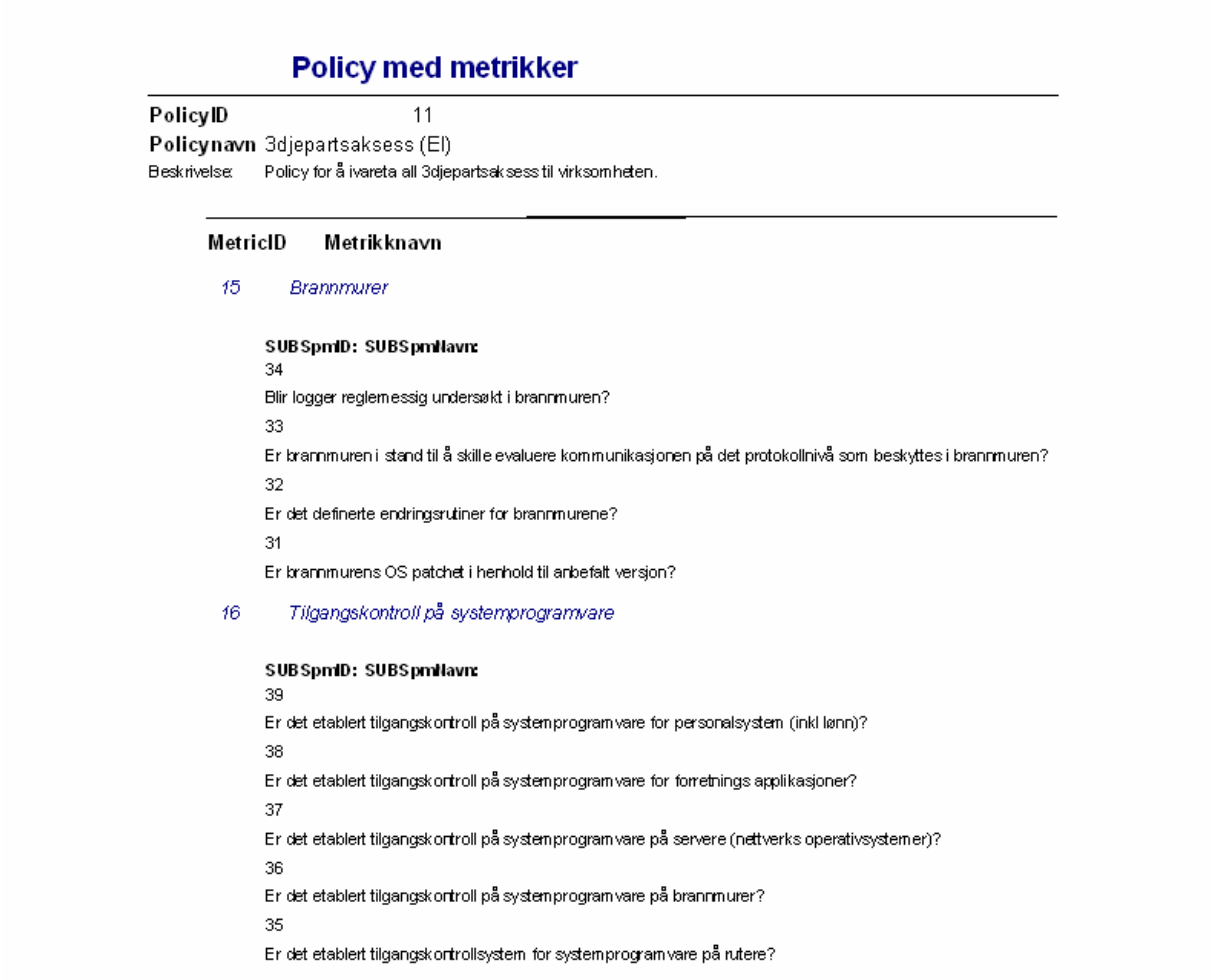
Man fortsetter gjennom disse stegene til man er ferdig med å definere opp en policy.
Er det ønskelig, kan en rapport vises som viser policyen med tilhørende metrikker. Denne vises i Figur 21 - Toolkit - Rapport policy med metrikker. En rapport som også har med underspørsmål til metrikkene, Figur 22 - Toolkit - Policy med metrikker og underspørsmål, kan vises.

Policy med tilhørende metrikker

PolicyID	Policynavn	Opprettet av	Opprettet	MetricID	Vekt metrikk	Metrikknavn
11						
	3djepartsaksess (EI)	GS	2004-05-31			
				15	4	Brannmurer
				16	4	Tilgangskontroll på systemprogram
				17	3	Kabling

31. mai 2004 Page 1 of 1

Figur 21 - Toolkit - Rapport policy med metrikker

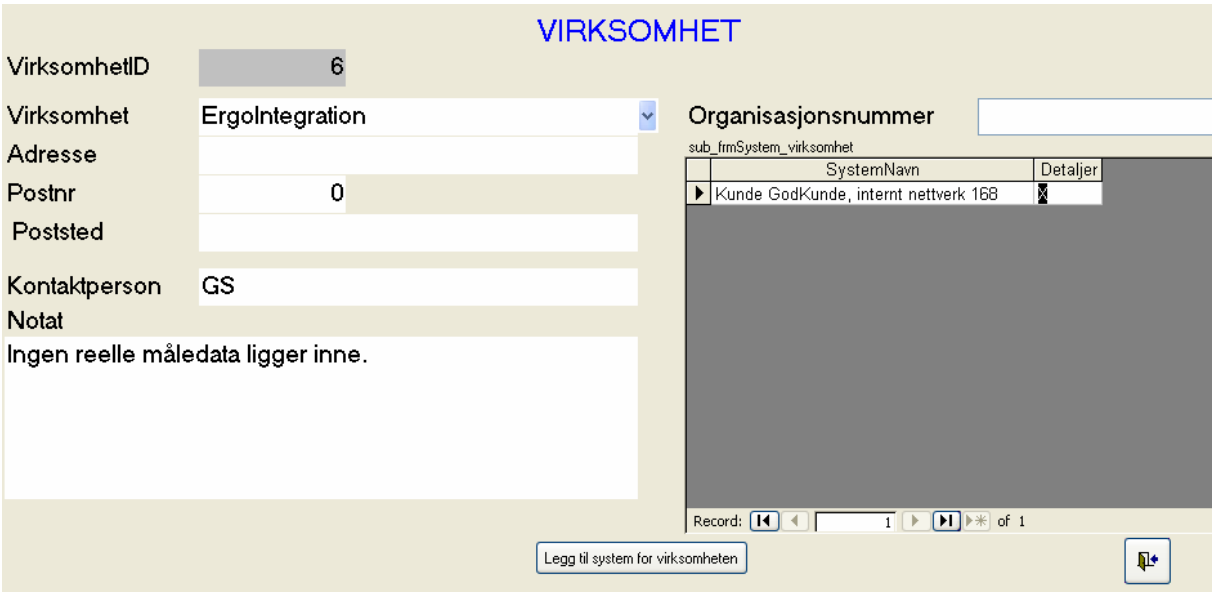


Figur 22 - Toolkit - Policy med metrikker og underspørsmål

Nå er en policy ferdig definert, og man kan kjøre undersøkelser mot systemer, med den gitte policy.

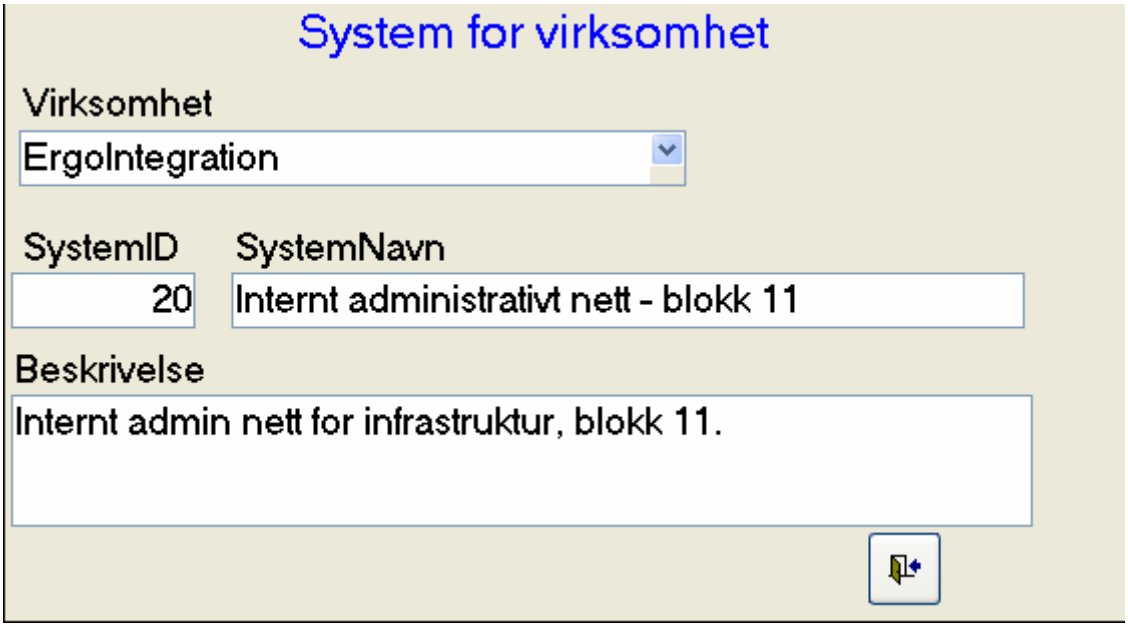
3.3.2.2.2 Undersøkelse

Alle systemer som defineres inn i toolkitet må knyttes opp mot en virksomhet. Og denne må derfor defineres inn. Se Figur 23 – Toolkit - Registrering av virksomhet. Her legges virksomhetens navn inn, sammen med kontaktperson og notater. I dette vinduet finner man også en liste over de systemer som er definert for denne virksomheten. Er virksomhet og system definert fra før, kan man gå direkte til registrering av den nye undersøkelsen Figur 26 - Toolkit – Undersøkelseskriterier.



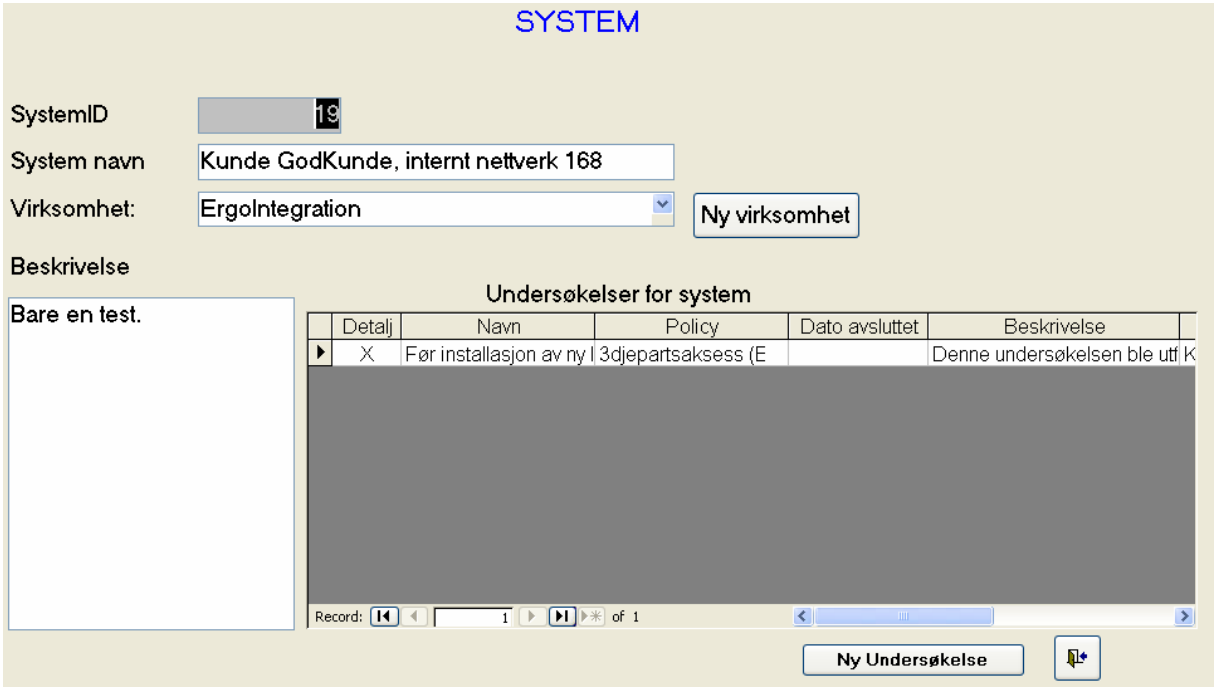
Figur 23 – Toolkit - Registrering av virksomhet

Finnes ikke det systemet som det skal kjøres undersøkelse mot, kan dette legges inn ved å klikke på knappen ”Systemer”.



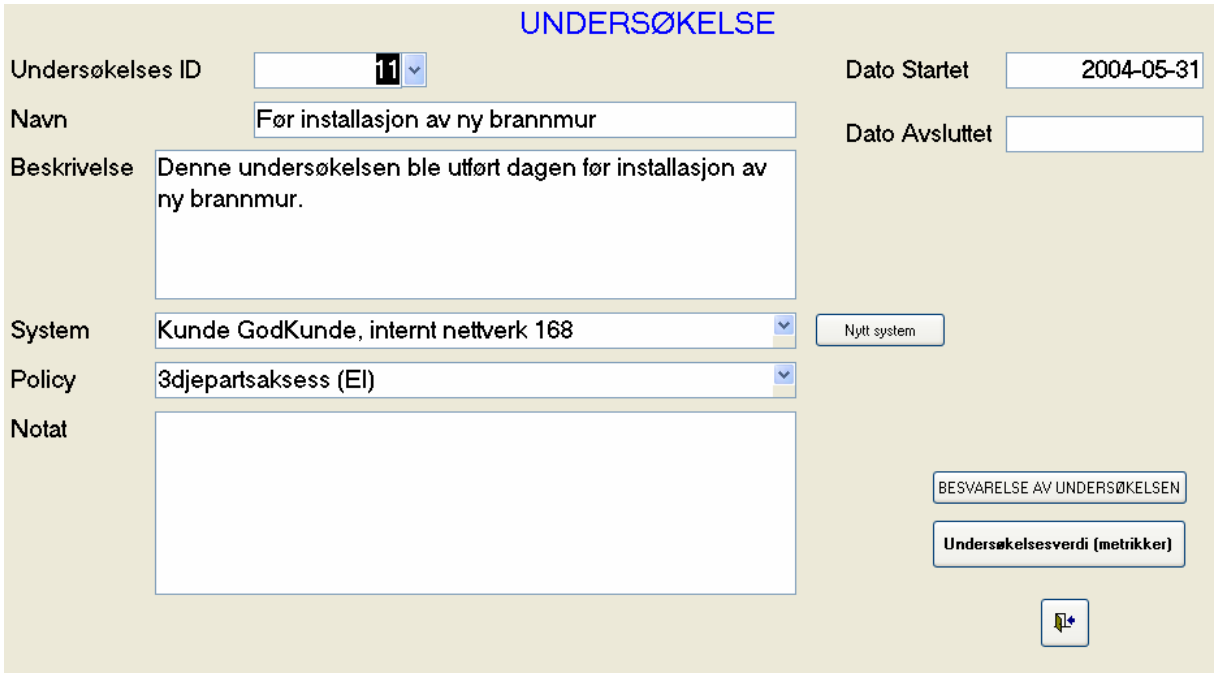
Figur 24 – Toolkt - Systemer for virksomhet

I Figur 23 – Toolkit - Registrering av virksomhet kan man klikke på detaljer bak hvert system, for å få opp en mer detaljert informasjon om systemet, og se hvilke undersøkelser som er kjørt mot dette systemet.



Figur 25 - Toolkit - Detaljert system informasjon

Ønsker man å se mer detaljert på kriteriene bak en av undersøkelsene, kan man her klikke på ”Detalj”.

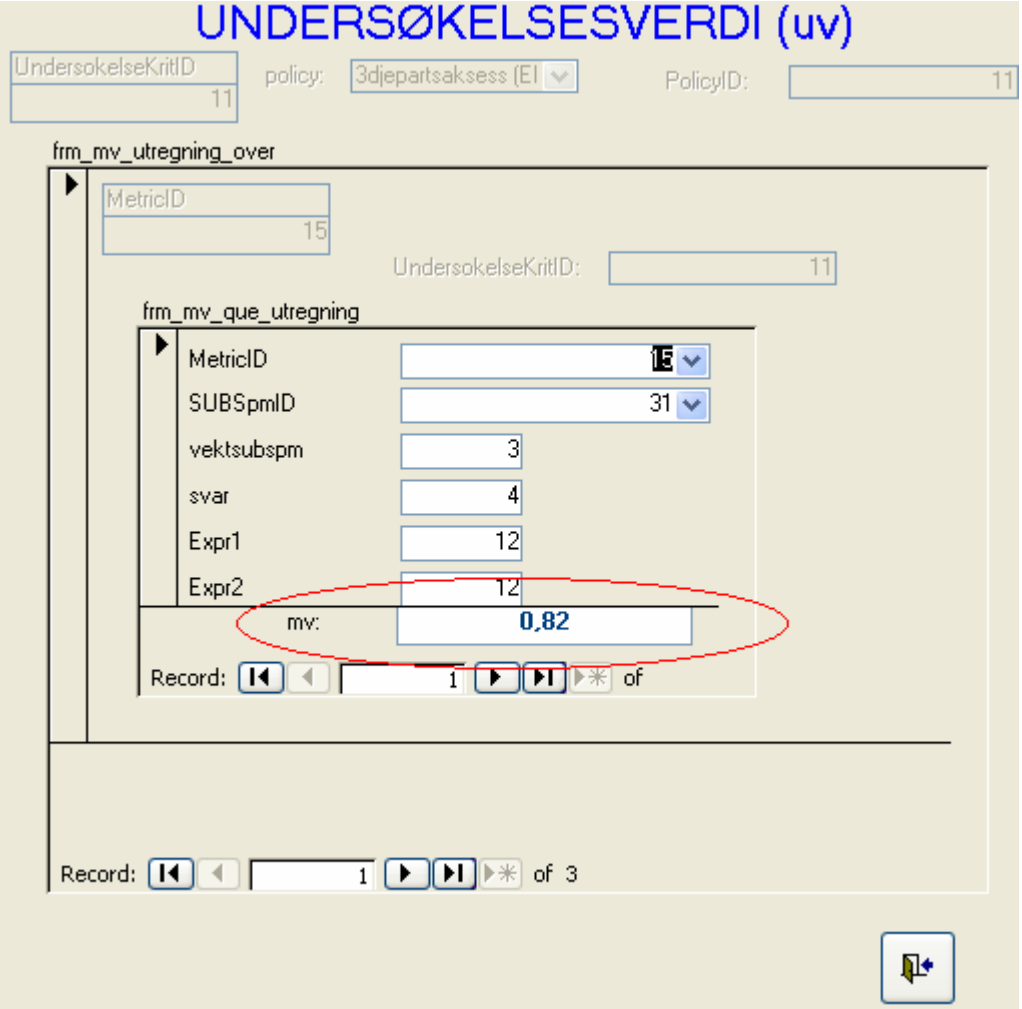


Figur 26 - Toolkit – Undersøkelseskriterier

Ved å klikke på knappen ”BESVARELSE AV UNDERSØKELSEN” kan man gå inn å besvare metrikkenes underspørsmål (Se Figur 27 - Toolkit - Besvarelse av undersøkelse).

Figur 27 - Toolkit - Besvarelse av undersøkelse

Ved å klikke på knappen ”Undersøkelsesverdi (Metrikker)” i Figur 26 - Toolkit – Undersøkelseskriterier vil man se hvilket resultat de forskjellige metrikkene fikk i undersøkelsen.



Figur 28 - Toolkit - Undersøkelsesverdi

Vi har i dette arbeidet ikke kommet så langt at vi har fått implementert uv utregningen. Dette er kommentert i Kapittel - 5 Videre arbeid. Men det vil komme i samme vindu som viser mv (metrikkverdien).

4 Konklusjon

Vi har med dette arbeidet sett at det har vært utført mye arbeid innenfor området med sikkerhetsmetrikker. Og en del innenfor området Sikkerhets Metrikk Program (SMP). Det som imidlertid viser seg, sett fra vårt ståsted, er at når det gjelder å ta dette i bruk som et daglig verktøy er det et stykke igjen. De løsningene som eksisterer er omfattende, og krever mye ressurser for å gjennomføres.

Vårt arbeid har tatt frem en prosess som inneholder de mest nødvendige stegene for å ta et SMP i bruk. Denne prosessen er utviklet med et mål om at den skal være kostnadseffektiv og gi et mest mulig riktig bilde av sikkerheten. Prosessen bygges opp rundt tre del-prosesser. Den første Del-Prosessen har som formål at det skal komme ut en liste med de elementer man ønsker å definere policyen basert på. Disse elementene sammen, blir den policy som inneholder kravene man ønsker å måle systemet opp mot. Policyen man skal komme ut med fra Del-Prosess 1 trenger ikke være noe man definerer selv, men kan være krav gitt lover, forskrifter, interne sikkerhetspolicies eller andre krav eller retningslinjer. I vår gjennomkjøring for å teste Del-Prosess 1 benyttet vi en undersøkelse basert på intervjuer og utsendelse av spørreskjema for å finne ut hvilke elementer man skal legge vekt på når man skal se på tillitsverdigheten til et nettverk.

Del-Prosess 2 vil være å ta tak i den policy med tilhørende elementer som ble definert i Del-Prosess 1, og bryte dette ned i bestemte målepunkter, metrikker. Disse metrikkene defineres etter den standard vi har kommet frem til. Det vil i mange tilfeller både for Del-Prosess 1 og Del-Prosess 2 være mulig å gjenbruke tidligere definerte policyer og metrikker. For å holde orden på disse, og ikke minst for å kunne utføre målingene, så har vi utviklet en prototyp på et toolkit, som er med på å redusere tiden man må bruke på et SMP. Samtidig vil toolkitet når det er ferdig kunne holde orden på alle de målinger man gjør mot et system. Og på den måten være et benchmark verktøy for sammenligning av målinger mot samme system, og sammenligning av målinger mot forskjellige systemer, med samme policy lagt til grunn.

Del-Prosess 3 er selve gjennomføringen av målingene ved hjelp av toolkitet. Denne prosessen vil være den som man til daglig benytter. Her vil man benytte toolkitet, og kjøre nye undersøkelser for systemer, og få en oversikt på om status har endret seg.

Prosessen som vi har definert her er enklere en de forsøk på slike veiledninger og lignende vi har sett for SMP. Del-Prosess 1 og Del-Prosess 2 er de som krever mest tid og arbeid. Disse del-prosessene blir kjørt en gang pr. policy man ønsker å etablere. Måten man velger seg en policy på vil variere, noen har gitte krav å forholde seg til, som lovverk og annet. Man kan her også ønske å etablere en egen policy, det kan for eksempel være egen policy for tilgang for 3djeparter. Måten man definerer slike policies på er ikke låst fast i denne prosessen. Vi anbefaler at dette enten gjøres som et prosjekt i en virksomhet. Hvor deltagerne er fra forskjellige fagfelt i virksomheten. Eller at det gjøres som vi har gjort i dette arbeidet, at det utføres en intervjurunde med personer som har sterk kunnskap innen for det området man ønsker å etablere en policy. Samtidig er det viktig at dette blir en gruppe bestående av personer fra alle ledd i virksomheten, slik at ikke resultatene blir styrt av en del av et fagmiljø. Det er også viktig at man planlegger en slik undersøkelse godt, og setter av nok tid. Vår erfaring ble at det ble knapp tid for å gjennomføre undersøkelsene, og at dette gav merarbeid i bearbeidelsen av resultatene.

Definisjon av metrikker i Del-Prosess 2 krever også en del arbeid. Malen vi har gitt for metrikker må følges. Det krever uansett en del arbeid og trening for å definere de rette metrikkene. For å få på plass gode metrikker, har vi i Del-Prosess 3 lagt inn en sløyfe hvor vi kan justere metrikker som ikke er helt optimale. Toolkitet hjelper til med å redusere arbeidet på Del-Prosess 1 og Del-Prosess 2 ved at man etter å ha etablert en policy og metrikker i toolkitet selvsagt kan benytte disse også ved senere målinger mot andre systemer, eller samme systemer med andre policies.

5 Videre arbeid

Selv om dette arbeidet har gitt oss mange fine resultater og en definisjon på hvordan prosessen skal være, er det mye arbeid som gjenstår og som må fullføres før dette blir en ferdig prosess til bruk for EI og andre.

Prosessen

I selve prosessen som vi har definert, er det en del gjenstående arbeid på dokumentasjonssiden. For at prosessen skal kunne benyttes av andre, må det som et minimum etableres følgende dokumentasjon

- Referanseverdi
  Det er også muligheter for å la denne prosessen kunne måles mot en referanseverdi. Med dette mener vi at det bør utvikles en mulighet for å angi hva man ser på som ”godtatt” score på en undersøkelse. Og at de målinger man gjør blir sammenlignet med denne referanseverdien. Ut i fra dette vil man da se om systemet som undersøkes er dårligere eller bedre enn den gitte referanseverdien.
- Prosessbeskrivelse
  som beskriver alle deler av prosessen i detalj. Slik at man kjenner til hva som må utføres på hvert enkelt steg i prosessen. Dette vil bli som en brukerveiledning for prosessen.
- Brukerveiledning
  Det må etableres en enkel brukerveiledning, som kan ta brukeren gjennom alle del-prosesser.

I tillegg må det gjøres noe arbeid med selve prosessen

- Metrikker som har stor betydning
  Slik prosessen er bygget opp i dag, ligger det ikke inne noen mulighet for å gradere en metrikk over 4. Men vi ser det som en fordel å kunne ha et alternativ der en metrikk kunne settes som vesentlig mye viktigere en andre. Dvs. at denne metrikken MÅ være på en score over for eksempel 0.95 for at undersøkelsen skal få en score over 0. (Disse verdiene er kun et eksempel, og ikke vurdert og etterprøvd).
- Underspørsmål med stor betydning
  Slik Del-Prosess 2 er bygget opp i dag, ligger det ikke inne noen mulighet for å gradere underspørsmål over 4. Men vi ser det som en fordel å kunne ha et alternativ der et underspørsmål kunne settes vesentlig mye viktigere en andre. Dvs. at dette underspørsmålet MÅ ha en score på 4 for at metrikken skal få en score over 0. (Verdien 0 er kun et eksempel, og ikke vurdert og etterprøvd).
- Autometrikker
  Prosessen har også muligheter for at Del-Prosess 3 kan benytte seg av autometrikker. Med autometrikker mener vi innsamling av for eksempel logger fra brannmurer, IDS, servere osv. Implementering av dette ville gitt muligheten for metrikker som var mer i retning av sanntidsmålinger. Dette kan også gjøres rett i toolkitet ved at man tar inn data fra eksisterende logganalyse verktøy, som for eksempel eIQnetworks FirewallAnalyzerEnterprise [eiqn].

Toolkitet

Vår utvikling av toolkitet har blitt konsentrert om å finne den riktige databasemodellen slik at dette fungerer sammen med prosessen. Og slik at gjenbruk at underspørsmål og metrikker kan gjøres i stor grad. Vi ser for oss at følgende videreutvikling av toolkitet er nødvendig

- MMI
  Det må utvikles en bedre MMI. Slik vi har laget det i dag, har vi kun konsentrert oss om å få se at databasemodellen fungerer. Det krever noe mer for at dette skal være et toolkit som er intuitivt for brukerne.
- Tidsmålinger
  Alle metrikker som legges inn i toolkitet vil inneholde en verdi som sier noe om hvor tidkrevende denne artikkelen er å gjennomføre.
  Det er i metrikkene lagt opp til at dette skal kunne måles basert på antall systemer som må undersøkes. Dvs. at en formel i en metrikk kan være:
  Tid = (antall systemer som skal sjekkes) * (2 min pr. system)
  Toolkitet må derfor inneholde informasjon om antall systemer, og benytte formelen for estimat av tid.
- Status
  Toolkitet må utvikles med en mer grafisk fremstilling av hvor langt man er kommet i en undersøkelse. Dvs. at det må være en % angivelse underveis i undersøkelsen, som forteller om hvor mange prosent av spørsmålene som er besvart.
- Sammenligning av resultater
  Toolkitet inneholder pr. i dag ikke en grafisk fremstilling av resultatene for en undersøkelse, med mulighet for å sammenligne disse med tidligere undersøkelser for samme system. Det samme gjelder sammenligning av undersøkelser gjort på forskjellige systemer, men med samme policy.
  Dette er viktig å få på plass, slik at man kan få opp de daglige nødvendige rapporter.
- WEB
  Toolkitet er i dag utviklet i Microsoft Access, dette er et verktøy som ikke skalerer bra (dette er kun vår personlige mening) og toolkitet bør derfor konverteres over på en SQL database. Samtidig bør grensesnittet mot brukeren byttes ut med et WEB-basert grensesnitt.
- Policy etableringer / Intervjuer
  En mulighet for verktøyet er også at det legges opp slik at det inneholder en mulighet for å gjøre intervjuer av personer gjennom dette grensesnitte, og dermed samle inn data som kan benyttes i Del-Prosess 1 for etablering av Policy, og i Del-Prosess 2 for etablering av metrikker.
  Også en modul som foreslår en policy basert på innsamlede resultater, kan defineres. Herunder også å foreslår metrikker basert på innsamlede resultater.

6 Referanseliste

[acce] Micrisift WEB side for Access, http://www.microsoft.com/norge/office/access/prodinfo/overview.mspx, Juni 2004 32

[Atha] Athanasiades N., Abler R., Levine J., Owen H., Riley G., Intrusion Detection Testing and Benchmarking Methodologies, First IEEE International Information Assurance Workshop, 2003 32

[Bish] Bishop M., Computer Security, 2002, ISBN 0-201-44099-7..... 1

[cres] Creswell, John C., Research Design, Qualitative, Quantitative, and Mixed Methods Approaches, Second Edition, July 2002..... 2

[eiqn] eiQNetworks, Firewall Analysis, webside, http://www.eiqnetworks.com/products/firewallanalyzer.shtml 47

[ergo] ErgoIntegration AS, websider http://www.ergointegration.no/ 4

[frost] Bob Frost. Measuring Performance - Using new metrics to deploy strategy and improve performance. Measurement International, 2000 ..... 5, 11

[holm] Holm, O., Risikohåndtering av informasjonssystemer i dynamiske omgivelser, Master oppgave, HiG, 2004 3

[isap] ISAP Risk Management, toolkit for risk managment, webside: http://www.ais.no/ , Juni 2004..... 8

[Ivers] Kenneth R. Iversen (KITH) og Jon Ølnes (Norsk Regnesentral), Håndbok for informasjonssikkerhet i informasjonsnett, p. Forprosjektrapport, 1998, Norges forskningsråd, NIN-programmet, http://helmersol.nr.no/doc/forprosjekt/sluttrapport.html.. 1

[Lewi] Lewis, Roger J., Reliability and Validity: Meaning and Measurement, Department of Emergency Medicine, Harbor-UCLA Medical Center, UCLA School of Medicine, 1999 Annual Meeting of the Society for Academic Emergency Medicinec (SAEM) in Boston, Massachusetts, http://www.ambpeds.org/ReliabilityandValidity.pdf..... 71

[NIST] National Institute of Standards and Technology, NIST Special Publication 800-55, Technology Administration, U.S Department of Commerce, Computer Security Devision, http://www.nist.gov/..... passim

[OSST] Herzog, P., OSSTMM 2.1, Open-Source Security testing Methodology Manual, Institute for security and open methodologies, August 2003, http://www.isecom.org/osstmm/ 6

[payn] Payne, Shirley C., SANS Information Security Reading Room, A Guide to Security Metrics, 2001, http://www.sans.org/rr/papers/index.php?id=55..... 5

[Puke] Puketza N. J., Zhang K., Chung M., Mukherjee B., Olsson R. A., A Methology for testing Intrusion Detection Systems, IEEE Transactions and Software Engineering, 2001 32

[risk] Verktøy for risikovurdering, Risk Check, leveres av Solid Consulting AS, ref. Brønnøysundsregistrene http://www3.brreg.no/oppslag/enhet/detalj.jsp?orgnr=886215932 , Juni 2004 8

[simg] Simonsen G., Master i Informasjonssikkerhet, Prosjektplan, Sikkerhetsmetrikker for sikkerhet i infrastruktur og ved tilgang for tredjeparter, 2003. 16

[simg2] Simonsen G., Mathisen J., Metrics for Privacy, Report in the course “Security Metrics” at Gjøvik University College, 2003 http://www.nislab.no,..... 19, 27

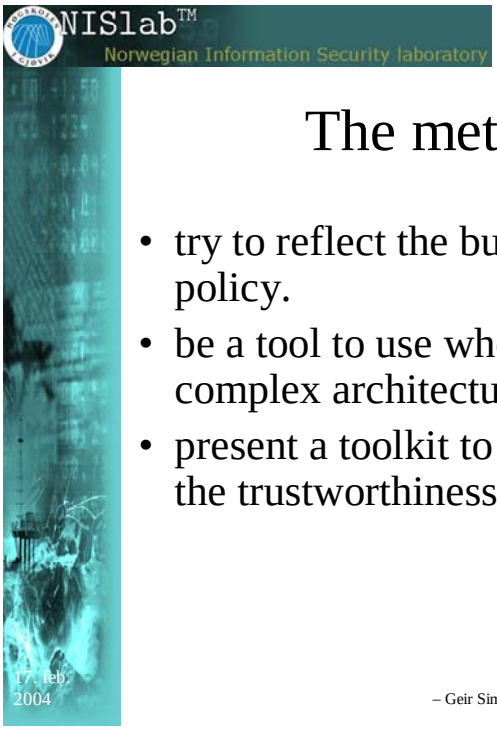
[Song] Song D., Shaffer G., Undy M., Nidsbench - A network intrusion detection system test suite, Anzen Computing RAID99, 1999 32

[tven] Tvenge Morten, Using benchmarking to improve IDS configurations, NISlab, Høgskolen i Gjøvik, 2004, http://www.nislab.no/ 32

[vba6] Micrisoft WEB side for Visual Basic, http://msdn.microsoft.com/vbasic/productinfo/, Juni 2004 32
[wold] Wold G., Key Factors in making Information Security Policies Effective, Masteroppgave ved Høgskolen i Gjøvik, 2004 8
[yeeb] Yee, Bennet s., Security Metrology and the Monty Hall Problem, University of California, 2001, http://www.bennetyee.org/ucsd-pages/pub/metrology.pdf 6

Vedlegg A - Presentasjon holdt for deltagerne av undersøkelsen

Denne presentasjonen ble holdt for de deltagerne av undersøkelsen som var gjennom en intervjubasert besvarelsesform.



NISlab™ Norwegian Information Security laboratory

Case 1

ErgoI have bought a small IT-company - BigBucks AS.

The infrastructure of the two companies are about to be interconnected. But first EI want to assess the trustworthiness of BigBucks network.

Q1a: Write down the elements* of BBs network you think is important to consider when assessing the trustworthiness of BBs network.

Q1b: For each element, try do describe which sub elements are important for that element.

Q2.: Write down other security elements EI should consider when

Q2a.: buying BB

Q2b.: interconnecting BBs network to EIs internal infrastructure

*Example of element can be firewall, cables, servers ….

NISlab™ Norwegian Information Security laboratory

Case 2

ErgoI have written a agreement with TheBestSupplier AS (TBS). TBS shall manage and do maintenance on EIs internal servers. To do this TBS needs to access the servers from their round-the-clock operational center.

The infrastructure of the two companies are about to be interconnected. But first EI want to assess the trustworthiness of TBS network.

Q1a: Write down the elements* of TBSs network you think is important to consider when assessing the trustworthiness of TBSs network.

Q1b: For each element, try do describe which sub elements are important for that element.

Q2.: Write down other security elements EI should consider when

Q2a.: buying services from TBS

Q2b.: interconnecting TBSs network to EIs internal infrastructure

If answers are the same as for Case 1, just indicate that on the form.

*Example of element can be firewall, cables, servers ….

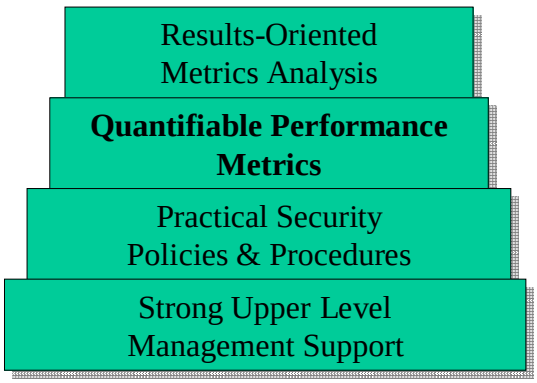
NISlab™ Norwegian Information Security laboratory

Security metrics

- NIST (National Institute of Standards and Technology)
  - Security Metrics Guide for Information Technology Systems
    - Important factors defining metrics for benchmarking
      - Metrics must yield quantifiable information (percentage, averages, and numbers)
      - Data supporting metrics needs to be readily obtainable
      - Only repeatable processes should be considered for measurement
      - Metrics must be useful for tracking performance and directing resources

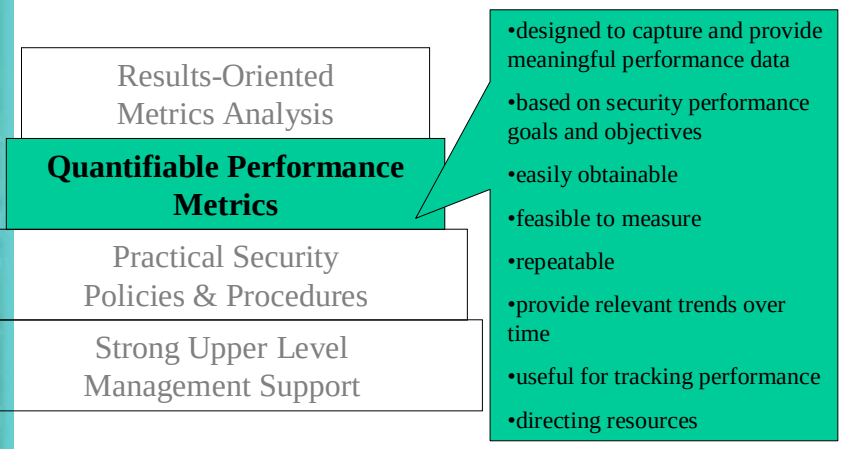
NISlab™ Norwegian Information Security laboratory

Security metrics program (1)



NISlab™ Norwegian Information Security laboratory

Security metrics program (2)



NISlab™ Norwegian Information Security laboratory

ErgoIntegration Security Policy (1)

- EIs security policy says (3.7): "*ErgoIntegration skal ha tilstrekkelig kompetanse til å kunne behandle sikkerhetsspørsmål på en profesjonell og effektiv måte. Det skal etableres oppfølgings- og kontrollopplegg for å påse at ErgoIntegration har riktig nivå på informasjonssikkerheten slik at sikkerhetsarbeidet blir ivaretatt på en god måte.*"

ErgoIntegration Security Policy (2)

- EIs security policy says (3.3): *"Det skal hele tiden tilstrebes en infrastruktur i informasjons- og kommunikasjonstekniske systemer som gjør det mulig å begrense, eventuelt isolere tilgangen til informasjon som er kritisk for virksomheten.* ***Alt IT-utstyr skal kvalitetsgodkjennes før installasjon i ErgoIntegration****. Om nødvendig skal sikkerhetsanbefalinger innhentes. Informasjonssikkerheten i ErgoIntegration kan påvirkes av tredjeparts adgang til bygninger og rom hvor IT-utstyr er plassert. Det samme gjelder* ***tredjeparts elektroniske tilgang til systemer og operativsystem via eksterne forbindelser eller direkte tilgang lokalt****. For å minske risikoen for brudd på informasjonssikkerheten og sikre overensstemmelse med ErgoIntegrations policy og retningslinjer, reguleres disse forholdene av kontrakter som beskriver vilkårene for informasjonssikkerhet og krav til taushetserklæring"*

Vedlegg B - E-post til deltagere av undersøkelse

From: Geir Simonsen
Sent:
To:
Subject: Undersøkelse - Masteroppgave

Hei,

i forbindelse med min Masteroppgave som skal skrives dette semesteret,
så er jeg avhengig av innspill fra eksperter inne datakommunikasjon og sikkerhet.
Jeg håper derfor du har muligheten til å sette av litt tid til å besvare det vedlagte skjema (Det tar deg ikke lang tid).

Det jeg ønsker tilbakemeldinger på er hva du legger vekt på (eller mener er viktig) om man skal kunne si noe om den sikkerhetsmessige godheten (tilliten/"trustworthiness") til et nettverk.

I vedlegget ligger det to Case til slutt i dokumentet.

Skjemaet i begynnelsen benyttes for å besvare spørsmålene i casene.
Spørsmål 1 i hver case går på nettverkssikkerhet.
Spørsmål 2 går på andre sikkerhetsrelaterte elementer (faktorer) (eks. policy, personell mm).
Håper du kan ta deg tid til å besvare begge spørsmålene.

Fyll ut skjemaet og returner det elektronisk til meg.

På forhånd takk!
Skulle du av en eller annen grunn ikke ha anledning, lyst eller noe annet til å gjøre dette,
si gjerne i fra om det også.

Her dere spørsmål, eller ønsker å diskutere casene så ta kontakt!

Med vennlig hilsen,

Geir Simonsen

Vedlegg C - Svarskjema til undersøkelsen

Security metrics
for security in infrastructure and 3rd party access

Survey

Name: _____
(will not be used by others than the author)

Cases are listed at the end of the document.

(Feel free to answer in Norwegian)

Question	Answer
CASE 1	
Q1	
Q1.a	
Q1.b	
Q2	
Q2.a	
Q2.b	
CASE 2	
Q1	
Q1.a	
Q1.b	
Q2	

Q2.a	
Q2.b	

Case 1

ErgoI have bought a small IT-company - BigBucks AS.
The infrastructure of the two companies are about to be interconnected. But first EI want to assess the trustworthiness of BigBucks network.
Q1a: Write down the elements* of BBs network you think is important to consider when assessing the trustworthiness of BBs network.
Q1b: For each element, try do describe which sub elements** are important for that element.
Q2.: Write down other security elements EI should consider when
Q2a.: buying BB
Q2b.: interconnecting BBs network to EIs internal infrastructure

*Example of element can be firewall, cables, servers ….
**Sub elements of firewall can be, OS, hardware, fw software, NICs….

Case 2

ErgoI have written an agreement with TheBestSupplier AS. TBS shall manage and do maintenance on EIs internal servers. To do this TBS needs to access the servers from their round-the-clock operational center.
The infrastructure of the two companies are about to be interconnected. But first EI want to assess the trustworthiness of TBS network.
Q1a: Write down the elements* of TBSs network you think is important to consider when assessing the trustworthiness of TBSs network.
Q1b: For each element, try do describe which sub elements** are important for that element.
Q2.: Write down other security elements EI should consider when
Q2a.: buying TBS
Q2b.: interconnecting TBSs network to EIs internal infrastructure

If answers are the same as for Case 1, just indicate that on the form.

*Example of element can be firewall, cables, servers ….
**Sub elements of firewall can be, OS, hardware, fw software, NICs….

Vedlegg D - Elementer fra resultatene

1

Har BB definerte perimeter hvor elektroniske grenser samsvarer med fysiske? Prevention on the perimeter by firewalls, router filters, switch-configuration (VLANs etc.), and out-of-band admin of elements exposed to external networks. - logisk infrastruktur (sikkerhetsarkitektur), modem, hussentraler, rutere, svitsjer, HUB'er, brannmurer, viruskontroll, VPN-bokser, - Routers, Switches and/or hubs, Firewalls - Cables, Modems, FW, vpn-enheter, soneinndeling, ACR i rutere, Har BB oppdatert brannmur for opprettholdelse av elektroniske perimeter i henhold til sikkerhetspolitikk? Har firmaet egen policy for tilgangskontroll og hvordan er tilgangskontrollen eventuelt organisert. Reguleres tilgangskontrollen ved hjelp av aksessfiltere i ruter eller benyttes dedikerte brannvegger. Videre bør det gjøres en gjennomgang av polycier for filtrering på brannmurer, rutere og annet nettverksutstyr.

2

Check that BB has a well founded network/system management system in place (i.e. efficient use of e.g. OpenView or UniCenter). - implementeringsrutiner, driftsrutiner, endringshåndtering, logging, - - Management routines - NETWORK MANAGEMENT, TRAFFIC MANAGEMENT, NETWORK, Documented change-management and procedures., hvilke verktøy som brukes til administrasjon, Videre må driftsrutiner dokumenteres, For all configurable elements, check (or at least the obviously critical ones) that the configurations are sound and that there is a prudent configuration management system in place.

3 fysisk infrastruktur (kabling/trådløst), Physical security of network infrastructure. Fysisk sikkerhet av utstyret bør også dokumenteres - er f.eks. trådløse nett tilgjengelige fra utsiden?

4 Har hver enkelt maskin i nettverket direkte kontakt med ressurser i eksterne nettverk, eller går all trafikk via utstyr som separerer datastrømmen innad og utad – f.eks terminalserver? Vurder kommunikasjonsmessige svakheter/trusler. Har de for eksempel egen internettaksess, hjemmekontor løsninger, 3-part aksesser osv. - fjernaksess for brukere, løsninger for fjerndrift, 3djeparts forbindelser,

5 Detection of unauthorized activity by use of IDS (both host and net-based) that checks both the outside perimeter and critical portions of the internal systems. - IDS, Endelig fins verktøy for å oppdage angrep - virusskannere, IDS

6 Level of maintenance (sw/hw upgrades), Finnes det et opplegg for Patch management. hvordan håndteres f.eks sikkerhetspatching

7 Hvordan BB har beskyttet sine eksterne dataforbindelser. - WAN-løsninger

8 Har BB oppdatert anti-virus på alle klienter og i e-post-system?

9 Er hver enkelt maskin lokalt beskyttet mot elektronisk inntrengning (lokal FW) dersom maskinen benyttes i nettverk utenfor bedriften – f.eks direkte tilkoblet Internet?, Level of end-point security on client workstations.

10 Er BB sitt nettverk akkreditert i henhold til et graderingsnivå i f.eks Sikkerhetsloven? Gjennomgå rutiner, sertifiseringer og eventuelle eksterne revisjoner de har gjennomført.

11 Vurder fysisk sikkerhet på selskapet. Er de for eksempel. Samlokalisert med andre? Har de rutiner for besøkende, adgang til lokaler, datahaller m.m. NB! Dette må vurderes fordi fysisk sikkerhet også har med nettsikkerhet å gjøre. - Fysisk sikkerhet (adgangskontroll, datarom ol), PC'er, stormaskiner, servere, applikasjoner (web, mail osv),

12 Autentiserings- og autorisasjonsløsninger, Policy for autentisering og autorisasjon må legges fram.

13 Dokumentasjon, Architecture and design must be properly documented.

14 Det bør også foretas en vurdering av de nettverkskomponentene som finnes i nettet. Leveres disse fra anerkjente leverandører., Begge firmaer bør avgi en egenerklæring om hva slags nettverksutstyr de bruker

15 Hvordan BB autentiserer eksternt plasserte brukere

16 Har BB en aktiv sårbarhetsovervåkning?

17 Kan brukere i BB sitt nettverk installere programvare på sin egen maskin?

18 -driftansvar/avtaler, -hva er outsourcet, aksesser inn i nettet til Bbfra leverandører m.m

19 Har ansatt og innleide underskrevet taushetserklæringer og nødvendig klarering/autoriseringer for å komme inn i EI sitt nett.

20 Check if they have implemented the prevention, detection and response “regime”. Response must be in place for unwanted events (both errors and malicious activity) based on information from general network management tools and IDS.

21 Check that there are no unauthorized paths from outside of BB into any internal systems.

22 If any sensitive information is transmitted over public networks, check that strong a enough confidentiality measures are in place.

23 If BB has different internal sensitivity levels, check that these are segmented by prudent measures (VLAN, firewall, router filters, etc.).

24 Check that user rights are administrated well (i.e. that policies and tools are in place.). Further there should be some form of centralized user management, so that users rights might be easily revoked.

25 protokoller

26 redundans

27 Servers

28 Printers

29 A common goal regarding security philosophy.

30 Security features and solutions must include countermeasures against every documented risk (and perhaps a few more).

31 Første skitt vil være å skaffe tilveie informasjon om hvilken risikoprofil bedriften har lagt til grunn for sin aktivitet., Det første testen er at firmaet har foretatt en kartlegging og at denne er dokumentert.

32 Har hvert enkelt eller en samling av systemer en systemeier med dedikert ansvar for funksjonalitet og sikkerhet

33 Hvor mange av kompentene er sertifisert iht. anerkjente sikkerhetsstandarder.

Vedlegg E - Mulige metrikker på elementene

Brannmur	operativsystem, a. OS with patches
Brannmur	Type FW (stateful inspection o.l),b. FW software
VPN Enheter	kryptoalforitme
Servers	OS with patches
Brannmur	Finnes det endringsrutiner som følges og som inkluderer sikkerhetsvurderinger ved alle endringer i regelsett (kan egentlig også gjelde generelt også for andre komponenter)?
Brannmur	Vurderer brannmurene trafikken på det protokollnivå som benyttes i kommunikasjonen gjennom brannmuren? F.eks er det mye rart som kan gå over port 80. Det holder ikke lengre å verifisere at dette er gyldig http-trafikk med riktige sesjonsnummer, pakketellere, flag etc. Man bør ofte også analysere hva som foregår på høyere lag – en kjempeutfordring…
Brannmur	FW regelsett
Brannmur	Interface cards
Brannmur	Passwords for remote management
Brannmur	Logging
Brannmur	Hardware
Installasjon av programvare på egen maskin	Er dette styrt gjennom administrative pålegg
Installasjon av programvare på egen maskin	Er dette styrt gjennom sentral konfigurasjon slik at bruker ikke kan bryte med bestemmelsen?
Installasjon av programvare på egen maskin	Undersøkes det (periodisk eller ved stikkprøver) at det ikke finnes ikke-autorisert programvare på hver enkelt maskin?
Printers	OS with patches
Printers	Available services (often open for telnet)
Printers	Passwords (often set to default or blank)
Routers	OS with patches
Routers	Available services
Routers	Passwords (often set to default)
Routers	Access lists
Routers	Interface cards
Switches and/or hubs	OS with patches
Switches and/or hubs	Available services
Switches and/or hubs	Passwords (often set to default)
Switches and/or hubs	Access lists
Switches and/or hubs	Interface cards
IDS	OS with patches
IDS	FW software
IDS	Interface cards
IDS	Passwords for remote management
IDS	Logging
Cables	Hardware (Fibre, twisted pair, coax etc.)
Cables	Physical security
Modems	Configuration (call-back etc.)
Modems	Unregistered “private” modems in the network
Management routines	Closing and removal of unused accounts
Management routines	Backup and recovery
Management routines	Monitoring
Management routines	Reporting of incidents
Servers	Applications
Servers	Hardware;USB ports (memory stick), IR port, Bluetooth, Floppy drive, CD-drive
Servers	Herding

Vedlegg F – Besvarelser av undersøkelsen

Navn/ Spørsmål	P1	P2	P3	P4	P5
Case 1					
Q1					
Q1a	Kommentar: Graden av sammenkobling kan være styrende for hvilke elementer man bør være opptatt av. Eks. kan det ”bare” være sammenkobling for å nå hverandres interne webserver, eller det kan være ”full integrasjon” av hverandres nettverk slik at man har den samme funksjonalitet i begge nett… Hvordan BB har beskyttet sine eksterne dataforbindelser Hvordan BB autentiserer eksternt plasserte brukere Har BB definerte perimeter hvor elektroniske grenser samsvarer med fysiske? Har BB oppdatert anti-virus på alle klienter og i e-post-system? Har BB oppdatert brannmur for opprettholdelse av elektroniske perimeter i henhold til sikkerhetspolitikk? Har BB en aktiv sårbarhetsovervåkning? Kan brukere i BB sitt nettverk installere programvare på sin egen maskin? Er hver enkelt maskin lokalt beskyttet mot elektronisk inntrengning (lokal FW) dersom maskinen benyttes i nettverk utenfor bedriften – f.eks direkte tilkoblet Internet? Har hver enkelt maskin i nettverket direkte kontakt med ressurser i eksterne nettverk, eller går all trafikk via utstyr som separerer datastrømmen innad og utad – f.eks terminalserver? Er BB sitt nettverk akkreditert i henhold til et graderingsnivå i f.eks Sikkerhetsloven?	**Vurdere behovet til BB selskapet og hva de forventer å få tilgang til av tjenester/funksjoner i EI sitt nett.** **Gjennomgå rutiner, sertifiseringer og eventuelle eksterne revisjoner de har gjennomført.** **Vurder fysisk sikkerhet på selskapet. Er de for eksempel. Samlokalisert med andre? Har de rutiner for besøkende, adgang til lokaler, datahaller m.m** NB! Dette må vurderes fordi fysisk sikkerhet også har med nettsikkerhet å gjøre. **Vurder kommunikasjonsmessige svakheter/trusler. Har de for eksempel egen internettaksess, hjemmekontor løsninger, 3-part aksesser osv** -driftansvar/avtaler -hva er outsourcet -aksesser inn i nettet til BB fra leverandører m.m. Har ansatt og innleide underskrevet taushetserklæringer og nødvendig klarering/autoriseringer for å komme inn i EI sitt nett.	Check if they have implemented the prevention, detection and response “regime”. Prevention on the perimeter by firewalls, router filters, switch-configuration (VLANs etc.), and out-of-band admin of elements exposed to external networks. Check that there are no unauthorized paths from outside of BB into any internal systems. If any sensitive information is transmitted over public networks, check that strong a enough confidentiality measures are in place. If BB has different internal sensitivity levels, check that these are segmented by prudent measures (VLAN, firewall, router filters, etc.). Check that user rights are administrated well (i.e. that policies and tools are in place.) Further there should be some form of centralized user management, so that users rights might be easily revoked. Detection of unauthorized activity by use of IDS (both host and net-based) that checks both the outside perimeter and critical portions of the internal systems. Check that BB has a well founded network/system management system in place (i.e. efficient use of e.g. OpenView or UniCenter). Response must be in place for unwanted events (both errors and malicious activity) based on information from general network management tools and IDS. In general if a network/system looks shoddy (e.g. no structured cabling, bad or missing documentation, etc.), then the subjective gut reaction that this can’t be good probably is correct… “Abstract”: Look for elements that functions as countermeasures on confidentiality, integrity and availability, and that support an efficient security process based on prevention, detection and response.	Fysisk sikkerhet (adgangskontroll, datarom ol), PC’er, stormaskiner, servere, applikasjoner (web, mail osv), fysisk infrastruktur (kabling/trådløst), logisk infrastruktur (sikkerhetsarkitektur), modem, hussentraler, rutere, svitsjer, HUB’er, brannmurer, viruskontroll, VPN-bokser, Autentiserings- og autorisasjonsløsninger, protokoller, fjernaksess for brukere, løsninger for fjerndrift, 3djeparts forbindelser, redundans, implementeringsrutiner, driftsrutiner, endringshåndtering, logging, WAN-løsninger, dokumentasjon.	FW, vpn-enheter, soneinndeling, ACR i rutere, kontroll over internkabling, IDS
Q1b	**Vedrørende brannmur:** Finnes det endringsrutiner som følges og som inkluderer	Har prøvd å beskrive det i Q1.a	For all configurable elements, check (or at least the obviously critical ones) that	**For alle fysiske komponenter: HW og OS.**	FW operativsystem, type

	sikkerhetsvurderinger ved alle endringer i regelsett (kan egentlig også gjelde generelt også for andre komponenter)? Vurderer brannmurene trafikken på det protokollnivå som benyttes i kommunikasjonen gjennom brannmuren? F.eks er det mye rart som kan gå over port 80. Det holder ikke lengre å verifisere at dette er gyldig http-trafikk med riktige sesjonsnummer, pakketellere, flag etc. Man bør ofte også analysere hva som foregår på høyere lag – en kjempeutfordring… Vedrørende installasjon av programvare på egen maskin Er dette styrt gjennom administrative pålegg Er dette styrt gjennom sentral konfigurasjon slik at bruker ikke kan bryte med bestemmelsen? Undersøkes det (periodisk eller ved stikkprøver) at det ikke finnes ikke-autorisert programvare på hver enkelt maskin?		the configurations are sound and that there is a prudent configuration management system in place.	Brukervennlighet (muligheten for bevisst eller ubevisst å gjøre feil), programmeringsspråk, malverk for dokumentasjon, rutiner for dokumentasjon, rutiner for fjerndrift og endringer.	FW (stateful inspection o.l) FW regelsett, kryptoalgoritme i VPN-enheter.

Q2					
Q2a	Er BB sertifisert i henhold til ISO 17799 eller lignende?	**Vurder eierforhold (+/-50%) og juridisk ansvar** Kontrollere policyer og rutiner og etterlevelse av rutinene (intervju med personer i BB) Be om å få resultatene fra eventuelle risikoregistere og sertifiseringer. Taushetserklæringer og autorisering	Aside from financial due diligence, I think that the most important elements would be a check to see whether or not BB has the necessary policies, guidelines, procedures, etc., and that these aren't to dissimilar to ErgoI's.	Policy, forskrifter og retningslinjer, nødvendig kompetanse, status for gjennomføring og plan for opplæring og informasjon, oversikt over eventuelt tidligere sikkerhetsbrudd og implementering av tiltak.	Sikkerhetspolicy for BB
Q2b	Har BB en sikkerhetspolicy som følges? Er sikkerhetsansvar klart plassert i BB Er sikkerhetsansvarlig i BB plassert høyere i organisasjonen enn de personene som avgjør implementeringer og endringer i BB sitt nettverk (altså: har sikkerhetsansvarlig reell myndighet)? Har BB en sentralt styrt IT-infrastruktur (sentral beslutningsmyndighet for alle investeringer og endringer) eller er det opp til den "lokale høvding" å gjøre som han vil med IT-løsningene? Har BB en riktig og oppdatert oversikt over sin egen IT-løsning, sin egen IT-organisasjon og sin egen sikkerhetsorganisasjon – har man et noenlunde felles helhetsbilde? Har BB etablerte og kjente		See Q2.a.	Policy, forskrifter og retningslinjer må harmoniseres og samkjøres. Kultur-, holdnings-, opplærings- og informasjonsarbeid må samkjøres. Det må finnes en klar og uttalt sikkerhetsstrategi fra ledelsen for selskapet. Tilfredsstille rammeverk for sikkerhet (BS7799) og kvalitet (ISO 900X). Gjennomføre vurdering av verdi og gradering på informasjon, og definere kriterier for akseptabel risiko. Klargjøring av ansvar og myndighet, og definisjon av roller knyttet til	Sikkerhetspolicy for BB, tilgangskontroll til data rom og koblingsrom, oppfølging av FW logg, IDS logg og krypto logg, Endrings rutiner i BBs nett, sikkerhetsrutiner rundt VPN enhetene (management og nøkkelhåndtering o.l)

	rutiner for å melde inn svakheter (og hendelser) samt å vurdere / forbedre disse?			sikkerhetsarbeidet.	

Case 2					
Q1					
Q1a	Samme som i case 1	**Det må inngås en juridisk bindende avtale med leverandøren. Avtalen må inneholde ansvar, forpliktelser, eskaleringsrutiner, målekriterier (SLA krav)** Gjennomgå rutiner, sertifiseringer og eventuelle eksterne revisjoner de har gjennomført. De ansatte må underskrive taushetserklæring ovenfor. Alternativet ved fysisk service på HW er at leverandøren møter opp i våre lokaler. Det må gjennomføres revisjon av løsningen etter at den er etablert.	See Case 1 Q1.a.	Samme som case 1.	FW, vpn-enheter, soneinndeling, kontroll over internkabling, overvåkingsservere
Q1b	Samme som i case 1	Se over	See Case 1 Q1.b.	Samme som case 1.	kryptoalgoritme i VPN-enheter, operativsystem i overvåkingsservere, FW operativsystem og FW regelsett.

Q2					
Q2a	Samme som i case 1		See Case 1 Q2.a., and ensure that there exists a contract that gives ErgoI the necessary legal “tools” to “force” TBS to behave… ☺	Samme som case 1.	Sikkerhetspolicy, personellklarering, rutiner
Q2b	Vurder konsekvensene av sikkerhetsbrudd hos TBS i forhold til EI sine løsninger og tjenester. På bakgrunn av dette må man vurdere om de servere som skal driftes av TBS bør skilles ut i et eget segment i nettverket slik at TBS ikke får adgang til unødvendig mange ressurser. Avtal med TBS hvilke protokoller og adresser som skal benyttes for fjerndriften og begrens kommunikasjonen til det som er avtalt. Vurder behov for IDS-overvåkning av den trafikk som går mellom EI og TBS og for den trafikk som går mellom de fjerndriftede		See Case 1 Q2.a.	Samme som case 1.	Sikkerhetspolicy, personellklarering, rutiner, tilgang inn i Eis nett slik at TBS ikke får mer tilgang enn nødvendig.

	serverne og resten av infrastrukturen. Sensorene bør gi alarm ved oppdagelse av kjente signaturer samt hvis det gjøres forsøk på kommunikasjon utover de protokoller og adresser som avtales for fjerndriften. Etabler integritetskontroll på de fjerndriftede serverne (TripWire etc) slik at man oppdager når det gjøres endringer, installeres ny programvare etc. på serverene. Sikre kommunikasjonen mellom EI og TBS med kryptering. Etabler koblinger mellom EI og TBS sine rutiner for endringshåndtering, varslig ved hendelser etc.				

Navn/ Spørsmål	P6	P7	P8	P9	P10
Case 1					
Q1					
Q1a	Servers Printers Routers Switches and/or hubs Firewalls IDS Cables Modems Management routines	NETWORK MANAGEMENT TRAFFIC MANAGEMENT NETWORK OPERATIONS LOCAL SECURITY MANAGEMENT VOICE NETWORKS	Architecture and design must be properly documented. A common goal regarding security philosophy. Security features and solutions must include countermeasures against every documented risk (and perhaps a few more). Documented change-management and procedures. Level of maintenance (sw/hw upgrades). Physical security of network infrastructure. Level of end-point security on client workstations.	**Første skitt vil være å skaffe tilveie informasjon om hvilken risikoprofil bedriften har lagt til grunn for sin aktivitet. Dersom dette ikke finnes vil det uansett være en fornuftig start å innhente informasjon om dette. Dette vil gi et bilde av hvilken arkitektur og utstyrspark man kan forvente å finne i bedriften.** Det vil kunne være en lang rekke av komponenter som avgjør tilliten. Det første testen er at firmaet har foretatt en kartlegging og at denne er dokumentert. Dersom dette ikke er gjort vil dette i seg selv være lite tillitsvekkende. Kartlegging må da gjøres av BB nettverk (infrastruktur). Hvilke systemer finnes og hvilke systemer er det som kommuniserer ut til evt. 3djeparter. Finnes det hjemmekontorløsninger. PKI systemer, faste/leide linjer. Har firmaet egen policy for tilgangskontroll og hvordan er	De to scenariene leder i praksis til svært like vurderinger. I begge tilfeller kan man stille følgende spørsmål: 1. Hva betyr "interconnection".? Det kan tenkes mange grader av nettverksaksess mellom firmaene fra "fulle aksess uten noen slag kontroll" over "noen tjenester - f.eks. mail, serveradminverktøy tilgjengelig" til "ingen aksess". Husk også at i dag er nesten alle på internettet, slik at man med få unntak allerede er "interconne

				tilgangskontrollen eventuelt organisert. Reguleres tilgangskontrollen ved hjelp av aksessfiltere i ruter eller benyttes dedikerte brannvegger. Har hvert enkelt eller en samling av systemer en systemeier med dedikert ansvar for funksjonalitet og sikkerhet. Det bør også foretas en vurdering av de nettverkskomponente ne som finnes i nettet. Leveres disse fra anerkjente leverandører. Er de oppdatert/ patchet til siste nivå. Finnes det et opplegg for Patch management.	cted". Ofte er firmaer, f.eks. ErgoI representert ved eksterne web-tjenester. De følgende spørsmålen e bør graderes ut fra hvor mye interkonnek tivitet som er ønskelig. 2. Nettverksut styr: Begge firmaer bør avgi en egenerklæri ng om hva slags nettverksuts tyr de bruker, og hvilke verktøy som brukes til administrasj on. Videre bør det gjøres en gjennomga ng av polycier for filtrering på brannmurer , rutere og annet nettverksuts tyr. 3. Tilsvarende for servere og klienter: Hva slags utstyr og verktøy fins og hvilke applikasjon er anvendes. Policy for autentiserin g og autorisasjon må legges fram. Videre må driftsrutiner dokumenter es, hvordan håndteres f.eks sikkerhetsp atching. Endelig fins verktøy for å oppdage

					angrep - virusskanner, IDS? 4. Fysisk sikkerhet av utstyret bør også dokumenteres - er f.eks. trådløse nett tilgjengelige fra utsiden? 5. Sikkerheten av selve forbindelsen mellom EI og de to firmaene må også sjekkes - er det mulig å lytte? Blir kryptering implementert? 6. For at alt dette skal fungere må det være en viss enighet om standarder som skal brukes, f.eks på krypto-utstyr. Polycier må kanskje også standardiseres. 7. Dersom man føler at dette ikke er vidtgående nok bør man gjennomføre en risiko- og sårbarhetsanalyse av de to firmaene. En slik analyse kan også ha mange nivåer, fra en rein papirtest til en fullpenetrasjonstest også fra det interne nettet til

					firmaene. Hva skiller så de to scenariene ? Jeg føler at scenario en er mest krevende i og med at BB formodentlig skal ha nokså vidtgående aksess til vårt bedriftstest. Derimot vil TBS bare ha adgang til de tjenestene de skal drifte. Men vi må stole helt på dem i denne sammenhengen dersom de som oftest er tilfelle trenger privilegert aksess til tjenesteserverne i det aktuelle tilfellet.
Q1b	Servers OS with patches Applications Hardware USB ports (memory stick) IR port Bluetooth Floppy drive CD-drive Printers OS with patches Available services (often open for telnet) Passwords (often set to default or blank) Routers OS with patches Available services Passwords (often set to default) Access lists Interface cards Switches and/or hubs Same as for routers Firewalls OS with patches FW software Interface cards Passwords for remote management Logging IDS Same as for firewalls Cables Hardware (Fibre, twisted pair,	Roles and responsibilities Network design Network resilience Network documentation Service providers Configuring network devices Firewalls External access Wireless access Network monitoring Change management Incident management Physical security Back-up Service continuity Remote maintenance Local security co-ordination Security awareness Security classification Risk analysis Security audit/review Voice network documentation Resilience of voice networks Special voice network controls	Network topology including brand of devices. Awareness of security policies and acceptable user behaviour. Security devices and configuration. Level of managed security. Awareness of frequency and duration of change window. How to enforce the routines and policies. Antivirus definitions, Microsoft critical updates, Physical access control to the network infrastructure and user terminals. Antivirus, application control.	Hvert element som blir kartlagt må dokumenteres. Det vil være naturlig å starte i endepunktet eksempelvis server. Det må vurderes om OS er patchet til siste sikkerhetsnivå. Er serveren herdet på en tilfredstillende måte. Hvor mange av kompentene er sertifisert iht. anerkjente sikkerhetsstandarder. Videre må det foretas en vurdering av komponentene i tjenestekjeden. Det må foretas en vurdering av hvor gode disse er mhp. Konfidensialitet, integritet, Tilgjengelighet, administrasjon. Hvilken type brannmur finnes. Vurdering av HW plattform, OS og applikasjon må foretas. Gjennomgang av policy for servere og	

	coax etc.) Physical security Modems Configuration (call-back etc.) Unregistered “private” modems in the network Management routines Closing and removal of unused accounts Backup and recovery Monitoring Reporting of incidents			brannmurer bør foretas for å verifisere hvor åpent miljøet er konfigurert. Ved utveksling av informasjon mot andre må det undersøkes om det benyttes kjente krypteringsmekanismer, eksempelvis SSH, SSL, IPSEC baserte systemer. Hvis ja må det foretas en gjennomgang nøkkelutvekslingsmekanismer (key management). Ved bruk av PKI systemer må det foretas en vurdering av hvilken tillit vi kan ha til sertifikatutsteder (CA).	

Q2					
Q2a	Policies, routines, physical security +++	the business risks associated with the access are assessed responsibility for authorising access is assigned to sufficiently senior personnel agreed security controls are implemented testing is performed agreed contracts are in place. ensure that controls are commensurate with business risks protect the interests of the enterprise in relation to ownership of information and systems information about the risks associated with the access guidelines on how to secure connections make all users accountable for their actions authenticate users in line with the type of access granted		**Det bør undersøkes om firmaet har en sikkerhetspolicy og i hvilken grad teori og praksis stemmer overens.** Det vil være en rekke andre faktorer som også berører sikkerhet og som vil elementer i det totale bildet mhp på hvilken tillit vi kan ha til firmaet og deres systemer. Dette vil være fysiske sikringstiltak, personell og administrative tiltak.	
Q2b	Other networks connected to BB			Se svar I Q1.	

Case 2					
Q1					
Q1a	In addition to the elements mentioned in Case 1 it is important to ensure proper separation of all TBS customer’s networks.	Brukere Servere Nettverk Arbeidsstasjoner Aksess			
Q1b	Physical and logical separation as well as administrative routines to prevent data passing from one customer’s network to another.	Samme regler for brukere i samme Infrastruktur Konsolidere servere, samme sikkerhetsnivå, samme versjoner og patche rutine Bytte leverandørpassord og andre ” service” konto Passord på alle			

		komponenter i Infrastrukturen (servere, nettverkskomponenter, arbeidsstasjoner, mv.) Samme politikk og klassifiserings nivå for informasjon Kontroll og likt sikkerhetsnivå på alle tilkoblingsmuligheter WLAN, GSM, ISDN, ADSL osv			

Q2					
Q2a	Same as for Case 1	Organisasjon Fysisk Risiko			
Q2b	None	Ansvar, prosessr Samme nivå Samme syn på risiko og samme toleranse nivå			

Vedlegg G - Regneark for simulering av undersøkelse

Filen Formelanalyse.xls finnes i vedlagt fil ”VEDLEGG - En prosess for Sikkerhets Metrikk Program.ZIP”.

Vedlegg H - Prototyp av toolkit

Siste versjon av vår prototyp av toolkitet finnes i vedlagt fil ”VEDLEGG - En prosess for Sikkerhets Metrikk Program.ZIP”. Toolkitet er utviklet som en del av denne oppgaven, som også er et oppdrag fra vår hovedinteressent. All undersøkelse, videreutvikling eller annen bruk av toolkitet må avklares med forfatterne av dette dokumentet.
Toolkitet består av filene EItwa.mdb og EItwaDB.mdb.

For å kunne benytte toolkitet, må tabellene i EItwaDB.mdb knyttes opp mot EItwa.mdb.

Kjente feil i vedlagt versjon

- Besvarelse
  Det er en koblingsfeil mellom underforms og tabeller i databasen. Dette gjør at en boks med spørsmål om UndersøkelsesID kommer opp. Denne skrives inn manuelt (den sees i vinduet bak øverst til venstre). Denne boksen vil også komme opp ved besvarelser på underspørsmålene, og må her også skrives inn manuelt for hvert spørsmål.
- uv
  Undersøkelsesverdien kommer ikke opp i resultatvinduet av en undersøkelse. Dette skyldes at vi ikke har hatt tid til å implementere dette.

Vedlegg I – Metrikker for Personopplysningsloven som policy

Her har vi listet de metrikker som er definert i [simg2], den rapporten er skrevet på engelsk, og er gjenngitt på original språket her. Definisjonen på metrikker avviker litt. I definisjonene brukt i [simg2] mangler feltene tiltak og kategori. Dette er enkle felt og legge til, disse metrikkene kan derfor enkelt importeres inn i verktøyet, og benyttes for en policy for den norske personopplysningsloven. Vi har lagt metrikkene inn i vår mal, men ikke fylt ut feltene som manglet.

Metrikk ID	PM1
Navn	Precaution against unauthorized access
Kategori	
Beskrivelse	Steps shall be made against unauthorized access to personal data. Unauthorized access to other information regarding information security must also be prevented.
Tiltak	
Krav	Regulation Section 2-11
Metrikk	Percentage of systems where unauthorized access is prevented.
Formel	PM1 = (number of systems ok / total number of systems)*100
Hensikt	Prevent unauthorized access to personal data.
Kostnad	CPM1 = (time to check one system * number of systems + travelling time) * price pr. hour.
Gyldighet	The claim is subjective and can be difficult to measure. The questions have to be as objective as possible.
Pålitelighet	To make this metric reliable, we use the alternative form method. Different forms and control routines must be developed, and randomly selected for every new control (measure).

Metrikk ID	PM2
Navn	Statutory authority
Kategori	
Beskrivelse	Personal data (cf. section 2, no. 1) may only be processed if the data subject has consented thereto, or there is statutory authority for such processing, or the processing is necessary as specified in the act. (See also PM3)
Tiltak	
Krav	Section 8
Metrikk	Percentage of systems that is using subject approval as basis for the processing, or has statutory authority, or the processing is necessary.
Formel	PM2 = (number of systems ok / total number of systems)*100
Hensikt	To check if system owner has a statutory authority or a necessary reason in place to process the personal data.
Kostnad	CPM2 = (time to check one system * number of systems) * price pr. hour.
Gyldighet	A system must be checked and evaluated by a person and will therefore be a subjective evaluation. Hence the validity may not be high.

Pålitelighet	If the processing is based on statutory authority or necessity, this must be pointed out in the notification, which is needed before beginning processing personal data, to the Data Inspectorate. If all systems are identified it should be easy to find the related notification, and check for statutory authority or necessity.

Metrikk ID	PM3
Navn	Subject approval
Kategori	
Beskrivelse	To process personal data the data subject has to consent thereto. (See also PM2)
Tiltak	
Krav	Section 9
Metrikk	Percentage of data subject approvals in place.
Formel	PM3 = (number of data subject approvals / number of data subjects for whom personal data is collected) * 100
Hensikt	To check if the system owner has data subject approval to process the personal data.
Kostnad	CPM3 = hours to check subject approvals * price pr. hour.
Gyldighet	This metric will check registration vs. approval and will be an exact count. Errors in the databases can affect the validity.
Pålitelighet	An exact check between registered approvals and data subjects, which it is collected data about, will make this metric reliable.

Metrikk ID	PM4
Navn	Erasing data
Kategori	
Beskrivelse	The system owner is responsible for erasing, if imposed, incorrect personal data and erasing personal data that is no longer needed for the purpose of the processing.
Tiltak	
Krav	Section 27 and Section 28
Metrikk	Percentage of claims implemented in routines. Claims identified: 1. Do one or more routines include erasing of incorrect personal data? 2. Do one or more routines include erasing data not longer needed?
Formel	PM4 = (number of claims implemented / total number of claims) * 100
Hensikt	Check if it is defined a routine for correcting incorrect personal data, including erasing if imposed. Check if it is defined a routine for erasing data not needed.
Kostnad	CPM4 = (number of routines checked * hours pr. routine) * price pr. hour.
Gyldighet	The routines are checked and the claims are clear. The validity will therefore be high.

Pålitelighet	This metric needs someone to go through the documentation of a system. The routines inspected must be known in the organization, and the employees who are processing personal data must comply with them. To check if the routines are followed and known an interview or survey can be accomplished, but this must be measured in another metric.

Metrikk ID	PM5
Navn	Rectification of deficient data
Kategori	
Beskrivelse	The system owner is responsible for correcting deficient data and to prevent unauthorized change of personal data.
Tiltak	
Krav	Sections 27, 11e and regulation section 2-13
Metrikk	Number of claims implemented in routines. Claims identified: • Do one or more routines include checking the correctness of the data? • Are there made any precautions against unauthorized alternation of the personal data processed? • Are there made any precautions against unauthorized alternation of other information with significance for the information security? • Are there made precautions against destructive software?
Formel	PM5 = (number of claims implemented / total number of claims) * 100
Hensikt	Check if it is defined a routine for correcting incorrect personal data, if there are made any precautions against unauthorized alternation of personal data processed and information with significance for the information security, and if there are made precautions against destructive software.
Kostnad	CPM5 = (number of routines checked * time pr. routine) * price pr. hour
Gyldighet	The claims are clear and the validity will therefore be high.
Pålitelighet	The routines inspected must be known in the organization, and the employees who are processing personal data must comply with them. To check if the routines are followed and known an interview or survey can be accomplished, but it is most likely that this should be measured in another metric.

Metrikk ID	PM6
Navn	Alternative routines
Kategori	
Beskrivelse	Alternative routines must be defined to take care of personal data processing in cases where normal use is impossible.
Tiltak	
Krav	Regulation Section 2-12

Metrikk	Percentage of systems having an alternative routine in place.
Formel	PM6 = (number of systems with an alternative routine in place / number of systems) * 100
Hensikt	Check if there is a routine in place, defining alternative processing of personal data.
Kostnad	CPM6 = (number of routines checked * hours pr. routine) * price pr. hour
Gyldighet	The number of systems is checked vs. number of routines for alternative processing, and this should give be valid metric.
Pålitelighet	This metric is reliable since number of systems is checked vs. number of routines for alternative processing, which is what we want to measure.

Metrikk ID	PM7
Navn	Backup
Kategori	
Beskrivelse	Personal data and other information needed to restore normal use must be backed up.
Tiltak	
Krav	Regulation Section 2-12
Metrikk	Percentage of systems processing personal data having a backup routine in place.
Formel	PM7 = (number of systems with a backup routine / total number of systems processing personal data) * 100
Hensikt	Check if a backup routine is in place, to ensure that information needed to restore normal processing is backed up.
Kostnad	CPM7 = number of routines to check * time pr. system * price pr. hour
Gyldighet	The routines are checked and the claim is clear. The validity will therefore be high.
Pålitelighet	This metric is reliable since number of systems is checked vs. number of systems with a routine for backup, which is what we want to measure.

Metrikk ID	PM8
Navn	Aberration handling
Kategori	
Beskrivelse	All processing of personal data that is in conflict with defined routines shall be treated as an aberration.
Tiltak	
Krav	Regulation Section 2-6
Metrikk	Percentage of systems with an aberrational handling routine in place.
Formel	PM8 = (number of systems with a routine for aberrational handling defined / number of systems) * 100
Hensikt	To check if a routine taking care of aberration handling is in place.

Kostnad	CPM8 = number of routines to check * hours pr. routine * price pr. hour
Gyldighet	The routines are checked and the claim is clear. The validity will therefore be high.
Pålitelighet	This metric is reliable since number of systems is checked vs. number of routines for aberrational handling, which is what we want to measure.

Metrikk ID	PM9
Navn	Certain identification
Kategori	
Beskrivelse	Personal identity numbers and other clear means of identification may only be used in the processing when there is an objective need for certain identification and the method is necessary to achieve such identification.
Tiltak	
Krav	Section 12
Metrikk	Is personal identity numbers (pin) and other clear means of identification used only if an objective need is in place? Percentage of systems using pin that have an objective need for certain identification.
Formel	PM9 = (number of systems needing pin / number of systems using pin) * 100
Hensikt	Check if it is an unnecessary use of personal identity numbers.
Kostnad	CPM9 = number of systems to check * time pr. system * price pr. hour
Gyldighet	Counting the systems that need pin can easily be done. It may be harder to count number of systems that doesn't need it but still use it.
Pålitelighet	Reliability is high since we are counting directly the systems that shouldn't use pin but still use it.

Metrikk ID	PM10
Navn	Obligation to provide information
Kategori	
Beskrivelse	The system owner is obligated to provide information to the data subject the information is collected from.
Tiltak	
Krav	Sections 18-22, 31

Metrikk	Is a routine in place, which handles information obligation? And does the routine consider all claims? Claims 1. Name and address to the system owner? 2. Purpose of processing? 3. Will the information be distributed, if so to whom? 4. Is it voluntary to provide the information? 5. Any other circumstances that will enable the data subject to exercise his rights pursuant to this Act in the best possible way, such as information on the right to demand access to data.
Formel	PM10 = (number of claims implemented / number of claims) * 100
Hensikt	To check whether a routine taking care of the obligation to provide information is in place or not, and to check if the routine has implemented all claims.
Kostnad	CPM10 = number of routines to check * time to check a routine * price pr. hour
Gyldighet	The validity will be high as we check the routines directly, and the claims are clear.
Pålitelighet	This metric needs someone to go through the documentation of a system. The routines inspected must be known in the organization, and the employees who are processing personal data must comply with them. To check if the routines are followed and known an interview or survey can be accomplished. But this must be measured in another metric.

Metrikk ID	PM11
Navn	Right of access
Kategori	
Beskrivelse	Any person who so requests shall be informed of the kind of processing of personal data a controller is performing.
Tiltak	
Krav	Section 18
Metrikk	Check if routine is in place, taking care of giving out information to the data subject.
Formel	PM11 = (routine in place OR routine not in place) *100
Hensikt	Check if a routine is in place, taking care of the routine giving the data-subjects information about which information is collected about them.
Kostnad	CPM11 = time used to check for routine * price pr. hour
Gyldighet	This metric checks if it is a routine in place. The validity will be high since it will give the same result on every check.
Pålitelighet	We want to check if a routine is in place. And that is what the metric is measuring. The reliability is therefore high.

Metrikk ID	PM12
Navn	Purpose

Kategori	
Beskrivelse	The controller shall ensure that personal data that are processed are used only for explicitly stated purposes that are objectively justified by the activities of the controller.
Tiltak	
Krav	Section 11b
Metrikk	Percentage of systems that only uses data for explicitly defined objective.
Formel	PM12 = (number of systems to check using data only to defined objective / number of systems) * 100
Hensikt	Check number of systems having a purpose defined, and if data processed only are used for that explicit purpose
Kostnad	CPM12 = number of systems to check * time pr. system * price pr. hour
Gyldighet	The validity is high since this is a concrete check of every system.
Pålitelighet	This metric is reliable since it is a check on every system vs. the defined purpose.

Metrikk ID	PM13
Navn	License
Kategori	
Beskrivelse	A license from the Data Inspectorate is required for the processing of sensitive personal data.
Tiltak	
Krav	Section 33
Metrikk	Percentage of systems handling sensitive personal data with license in place.
Formel	PM13 = (number of systems with license in place / number of systems processing sensitive personal data) * 100
Hensikt	To check if all systems processing sensitive personal data have a license in place.
Kostnad	CPM13 = number of systems to check * time pr. systems * price pr. hour
Gyldighet	The validity may not be high since the definition of sensitive personal data isn't clear.
Pålitelighet	High, concrete checking of every system vs. written license.

Metrikk ID	PM14
Navn	Physical security
Kategori	
Beskrivelse	It shall be taken action against unauthorized access to equipment used to process personal data. Other systems with signification for the information security shall also be protected.
Tiltak	
Krav	Regulation Section 2-10
Metrikk	Percentage of systems where unauthorized access is prevented.

Formel	PM14 = (number of systems physically secured / number of systems) * 100
Hensikt	To check that every system processing personal data, and every system with significance to the information security is physically secured.
Kostnad	CPM14 = number of systems to check * time pr. system * price pr. hour
Gyldighet	It is very subjective to decide if the physical security of a system is good enough. Therefore this metric has a low validity.
Pålitelighet	The check is a direct check of every system and is therefore reliable.

Metrikk ID	PM15
Navn	Documentation
Kategori	
Beskrivelse	The systems processing personal data and the security measures must be documented. Routines for use of the systems processing personal data must be in place.
Tiltak	
Krav	Section 13 and regulation section 2-16
Metrikk	Percentage of claims implemented. Check if following claims are implemented in routines: 1. Routines for use (documented) 2. Saved in min 5 years 3. Registering of authorized use shall be saved in at least 3 months 4. Unauthorized use shall be saved in at least 3 months 5. All other security events shall be saved in at least 3 months 6. The documentation shall be available for the Data Inspectorate 7. The documentation shall be available for all employees who have need
Formel	PM15 = (number of claims implemented / number of claims) * 100
Hensikt	To check if documentation and routines to handle the documentation are in place.
Kostnad	CPM15 = time to check routines * price pr. hour
Gyldighet	Can check if routine exists but not if all are followed. Some of the routines can be checked directly.
Pålitelighet	This metric needs someone to go through the documentation of a system. The routines inspected must be known in the organization, and the employees who are processing personal data must comply with them.

Metrikk ID	PM16
Navn	Organization
Kategori	

Beskrivelse	Organizational and system-technical implementations shall be in place, to define responsibility.
Tiltak	
Krav	Regulation Section 2-7
Metrikk	Percentage of claims implemented. Clear and documented responsibility relations shall be defined for use of the information system (IS). Claims: 1. Documented responsibility relations 2. Routine preventing documentation from being altered without authorization (ref 1) 3. The IS is configured to take care of the information security (responsibilities) 4. The configuration of the IS is documented 5. Routine preventing documentation not being altered without authorization (ref 4) 6. The use of the IS is according to established routines.
Formel	PM16 = (number of claims implemented / number of claims) * 100
Hensikt	To check if the organizational claims in the act is implemented.
Kostnad	CPM16 = number of systems to check * time to check a system * price pr. hour
Gyldighet	The claims are easily checked and the metric has a high validity
Pålitelighet	The claims are directly counted, and the metric has a high reliability

Metrikk ID	PM17
Navn	Security management
Kategori	
Beskrivelse	The claims in the act are the responsibility of general manager of the business.
Tiltak	
Krav	Regulation Section 2-3
Metrikk	Percentage of claims implemented. Claims 1. The purpose of the processing shall be described in the security goals 2. The overriding guidelines regarding use of the information system shall be described in the security goals 3. Choices and priorities regarding information security shall be written in a security policy
Formel	PM17 = (number of claims implemented / number of claims) * 100
Hensikt	To check if the claims regarding security management is implemented.
Kostnad	CPM17 = number of documents to check * time pr. document * price pr. hour

Gyldighet	Validity is high, since the metric is based on checking the routines and talking to the general manager.
Pålitelighet	The metric is reliable since it is a direct check of the claims.

Metrikk ID	PM18
Navn	Risk evaluation
Kategori	
Beskrivelse	The business shall define acceptable risk regarding processing of personal data.
Tiltak	
Krav	Regulation Section 2-4
Metrikk	Percentage of claims implemented. Claims: 1. Is there an account over all kinds of personal data processed? 2. Has the business defined criteria for acceptable risk connected with processing of personal data? 3. Has a risk evaluation been run to find the possibility and consequences of a security breach? 4. Are the results from risk evaluation documented? 5. Is there defined in any routine that a new risk evaluation must be done when a change regarding information security is done?
Formel	PM18 = (number of claims implemented / number of claims) * 100
Hensikt	To check if the business performs risk evaluations with belonging activities
Kostnad	CPM18 = time to check a claim * number of claims to check * price pr. hour
Gyldighet	The claims are easily checked, and the metric has a high validity
Pålitelighet	The claims are directly counted, and the metric has a high reliability

Metrikk ID	PM19
Navn	Security revision
Kategori	
Beskrivelse	Regular revision of the use of the systems processing personal data shall be made and the revisions shall be documented.
Tiltak	
Krav	Section 13 and regulation 2-5

Metrikk	Percentage of claims implemented. Claims: 1. Is there a routine in place ensuring a security revision to be run frequently? 2. The security revision must include check of organization 3. The security revision must include check of security measures 4. The security revision must include check of use of communication partners 5. The security revision must include check of suppliers 6. Does the revision handle aberrational handling? 7. Are the results from the revision documented?
Formel	PM19 = (number of claims implemented / number of claims) * 100
Hensikt	To check if security revisions are run and handled according to the act.
Kostnad	CPM19 = number of claims to check * time pr. claim * price pr. hour
Gyldighet	The claims are easily checked and the metric has a high validity
Pålitelighet	The claims are directly counted, and the metric has a high reliability

Metrikk ID	PM20
Navn	Outsourcing
Kategori	
Beskrivelse	Personal data may not be turned over to another person for storage or manipulation without an agreement.
Tiltak	
Krav	Section 15
Metrikk	If outsourcing is used, is a written agreement in place? Percentage of systems outsourced having a written agreement in place.
Formel	PM20 = (number of outsourced systems having a written agreement in placed / number of outsourced systems) * 100
Hensikt	To check if there are written agreements regulating personal data processing if outsourcing is used.
Kostnad	CPM20 = time to check outsourcing agreements * price pr. hour
Gyldighet	Validity is high since the metric is based on agreement revision and talking to the general manager.
Pålitelighet	The metric is reliable since it is a direct check of the claims.

Metrikk ID	PM21
Navn	Internal control
Kategori	
Beskrivelse	The controller shall establish and maintain planned and systematic measures that are necessary to fulfil the requirements laid down in or pursuant to this Act, including measures to ensure the quality of personal data.
Tiltak	

Krav	Section 14
Metrikk	Percentage of claims in place. Claims: 1. Is a system taking care of the claims regarding internal control in place? 2. Is the documentation/system available to the right persons / instances?
Formel	PM21 = (number of claims implemented / number of claims) * 100
Hensikt	To check if a routine taking care of internal control is in place.
Kostnad	CPM21 = time to check claims * price pr. hour
Gyldighet	The claims are easily checked and the metric has a high validity.
Pålitelighet	The claims are directly counted, and the metric has a high reliability.

Metrikk ID	PM22
Navn	Duty of confidentiality
Kategori	
Beskrivelse	Every employee who is processing or is in contact with the personal data processed (e.g. in administration of the computer system) must sign a duty of confidentiality.
Tiltak	
Krav	Regulation Section 2-9
Metrikk	Percentage of employees who have signed a duty of confidentiality.
Formel	PM22 = (number of employees who is processing data and have signed a duty of confidentiality / number of employees who is processing personal data) * 100
Hensikt	To check if all employees who is processing or in contact with the personal data processed have signed a duty of confidentiality.
Kostnad	CPM22 = time used to check the duties of confidentiality * price pr. hour
Gyldighet	High validity, because all duty of confidence are written and signed, and thus easy to count correctly.
Pålitelighet	This metric needs someone to go through the documentation of the system. If the list of employees who is processing data is accurate and up to date this metric will be quite reliable.

Stikkordsliste

3djepart.....1, 4, 11, 17, 45
arkitektur iv
EI*Se Ergo Integration*
ErgoIntegration.....iv, 4
IDS .....*Se Intrusion Detection System*
Intrusion Detection System 18
kostnadseffektiv .....iv, 1, 2, 3, 10
metrikk ....iv, 2, 3, 4, 5, 7, 8, 10, 11, 12, 16, 19, 20, 22, 23, 24, 25, 26, 27, 45, 47
Metrikk.....33
POLICY 14
prosess .iv, 1, 2, 3, 4, 5, 6, 8, 10, 11, 12, 13, 17, 18, 21, 26, 45
Prosess 14, 18, 33, 46, 48
security assurance ... *Se sikkehtsmessig tillit*
Sikkerhets Metrikk Program..... 7
sikkerhetsmessig tillit 1
sikkerhetsnivå 1
sikkerhetspolicy 1, 2, 4, 11, 12, 13, 15
SMP .....*Se Sikkerhets Metrikk Program*
stokastiske nett..... 1
tillitsverdig.....*Se sikkerhetsmessig tillit*
Tjenesteleverandører..... iv
tjenestetilbydere..... 1