UNIVERSITETET I BERGEN

Det samfunnsvitenskapelige fakultet

Sikkerhet i virksomhetsarkitektur

- *Norske virksomheters modenhet innen sikkerhet og virksomhetsarkitektur.*

Masteroppgave

Av:

Thomas Gudmestad

tgu024@student.uib.no

FORORD

Det har vært en lang vei for å komme i mål med dette arbeidet, og timevis med frustrasjon. Derfor er det spesielt fornøyd med å kunne levere denne oppgaven nå. Det å begi seg ut på en kvantitativ analyse viste seg mer utfordrende enn forespeilt.

Jeg vil gjerne takke veilederen min Andreas Lothe Opdahl for engasjement, og gode idéer. Det var aldri vanskelig å slå av en prat og alltid positive tilbakemeldinger.

Jeg vil også takke kameratene på lesesalen, Kristin for korrekturlesing og alle som har tatt seg tid til å svare på spørreundersøkelsen.

Thomas Gudmestad

30.11.2011

INNHOLDSFORTEGNELSE

FIGURLISTE

1 - INNLEDNING

Dette studiet er fokusert rundt sammenkoblingen av informasjonssikkerhet og virksomhetsarkitektur i norske virksomheter, og deres modenhet rundt temaet. Det teoretiske hovedfokuset er på rammeverket Sherwood Applied Business Security Architecture(heretter SABSA). Det presenteres relevant teori innen virksomhetsarkitektur, som Zachman Enterprise Framework og The Open Group Architectural Framework.

For å måle norske virksomheters modenhet innenfor dette området har jeg gjennomført en kvantitativ spørreundersøkelse. Forskningsarbeidet er basert på to av lagene i SABSA matrisen, det konseptuelle- og logiske nivåene. SABSA matrisen er grunnsteinen i SABSA rammeverket, og slekter sterkt på det kjente rammeverket for virksomhetsarkitektur; Zachman Enterprise Framework.

1.1 HOVEDRESULTATER

Det viste seg at valgt analysemetode ikke fungerte så veldig bra på datasettet jeg hadde innhentet, og resultatene ble dermed ikke som forventet. I faktoranalysen viste det seg at de uthentede faktorene ikke samsvarte med underliggende teoretisk rammeverk. Det eneste som kan sies er at konseptuell- og logisk arkitektur fordelte seg mellom faktorene med bare få tilfeller av spørsmål fra begge nivåene i en faktor. Klyngeanalysen viste heller ikke resultater av betydning. Det ble derfor vanskelig å trekke konklusjoner ut fra innhentede data.

Den deskriptive statistikken viser at respondentene har svart veldig likt på spørsmålene, og kan vise til problemer med formuleringen min av spørsmålene. Demografisk tilhører respondentene mine hovedsakelig personer som betegner seg selv som ledere og mellomledere. Hele 60 % havner under disse to kategoriene. 48,5 % av respondentene jobber innen IT bransjen. Denne likheten mellom respondentene kan være en av grunnene til at svarene er så like.

1.2 STUDIETS RELEVANS

Virksomhetsarkitektur begynner å bli viktigere og viktigere for norske virksomheter. I et land der prisen på arbeidskraft er såpass høy som i Norge, er virksomhetene nødt til å finne måter å optimalisere måten man jobber på.

Å innføre sikkerhetsaspektet til virksomhetsarkitektur er et ungt tema, men fortsatt veldig viktig. Det nytter ikke å ha en gjennomført virksomhetsarkitektur, om man ikke har tenkt på sikringen av elementene i arkitekturen. Informasjonssikkerhet i seg selv er et utarbeidet fagfelt, men ikke sett i sammenheng med resten av virksomhetens løsninger.

1.3 PROBLEMBESKRIVELSE/DAGENS SITUASJON

En av hovedanbefalingene i Mørketallsundersøkelsen 2010: «Verdivurdering. Mer fokus på prosesser og rutiner i virksomheten for å ivareta og beskytte egne verdier».

Jeg har ikke lyktes i å finne andre lignende undersøkelser rundt temaet informasjonssikkerhet og virksomhetsarkitektur, hverken i Norge eller verden forøvrig.

Dog har jeg brukt deler av Global Information Security Survey 2010 (Kessel 2010) og Mørketallsundersøkelsen 2010. Mørketallsundersøkelsen 2010 baserer seg på informasjon innhentet fra norske virksomheter, har blitt gjennomført syv ganger før, og gjør seg dermed spesielt egnet. Den er utført av Næringslivets Sikkerhetsråd (NSR) i samarbeid med: Norsk Senter for Informasjonssikring (NorSIS), Kripos, Nasjonal sikkerhetsmyndighet, SINTEF, SECODE, Telenor, Det Norske Veritas og Forsvarets Forsknings institutt. NSR definerer mørketall som: «…er differansen mellom den anmeldte kriminalitet som fremkommer i politiets statistikk og den kriminalitet som virksomhetene og privatpersoner faktisk blir utsatt for.» (NSR 2010)

Disse undersøkelsene holder et lavere abstraksjonsnivå og fokuserer mer på operasjonell informasjonssikring og trender innen næringslivet.

Både Global Information Security Survey og Mørketallsundersøkelsen fokuserer på hvilke trusler som beveger seg ute i dag, sammen med generelle beste praksis råd. De fokuserer ikke så mye på hvordan virksomhetens sikkerhetsstrategi er utformet og ser dermed ikke informasjonssikkerhet som et helhetlig tiltak. Begge undersøkelsene ønsker å vise et bilde av dagens trusler og dekke de nyeste teknologiene. I Global Information Security Survey 2011, av Ernst og Young, er undertittelen «Borderless Security» og den baserer seg hovedsakelig på innføringen av skytjenester. (Young 2010)

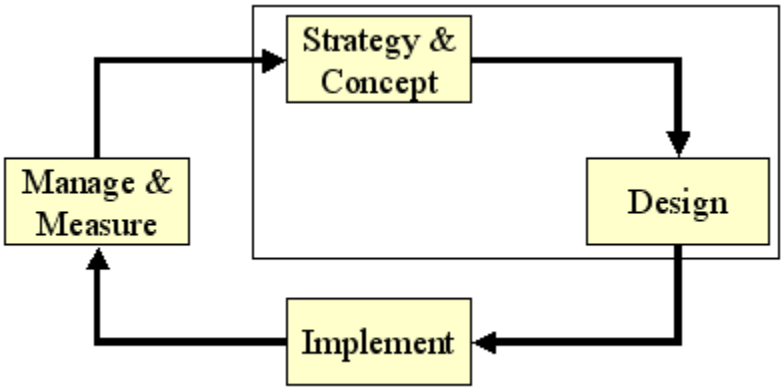
1.4 FORSKNINGSSPØRSMÅL

Jeg syntes både informasjonssikkerhet og virksomhetsarkitektur er veldig interessant. Da jeg skulle sette i gang med forprosjektet til denne oppgaven undersøkte jeg om det fantes noe teori som koblet disse to fagområdene sammen. Jeg fant fort ut at det var et relativt nytt fagområde, som var lite spesifisert hos de største aktørene innen virksomhetsarkitektur. Dette gjorde meg bare mer interessert, og syntes det hørtes spennende ut å se hvordan norske virksomheter samkjørte disse to områdene. Dette førte til forskningsspørsmålet:

«Implementerer norske virksomheter informasjonssikkerhet i sin virksomhetsarkitektur?»

Som underspørsmål til dette ønsket jeg å se på hvor stort fokuset deres var, hvordan det ble gjort og hvor langt det hadde kommet i arbeidet. Det ble også innhentet informasjon om sektor, størrelse og felt. For å kunne se på forskjeller innen modenhet.

1.5 MÅL OG BEGRENSNINGER



Figur 1 - SABSA Lifecycle

Dette arbeidet har som mål å se på modenheten i norske virksomheters implementering av informasjonssikkerhet i sin virksomhetsarkitektur. Jeg har valgt å fokusere på den konseptuelle- og den logiske arkitekturen i SABSA rammeverket. Dette valget ble tatt fordi jeg syntes det hørtes mer interessant ut å se på sikkerhet fra et strategisk ståsted, og ikke fokusere så mye på de fysiske løsningene. Det ville kanskje også vært vanskeligere å få personer til å delta i spørreundersøkelsen om man hadde spurt for detaljert rundt hver enkelt virksomhets informasjonssikkerhetsløsninger, som kunne ført til at de anså det som en risiko at sensitiv informasjon kunne komme på avveie. Arbeidet fokuserer på informasjonssikkerhet som en helhet gir også innsyn i hvorvidt avgjørelsene som tas er basert i en analytisk vurdering av virksomhetens krav.

Det faller ikke under denne oppgavens omfang å se på fysisk sikring av f.eks bygg. En vil heller ikke gå inn i detaljer om hvilke sikkerhetsløsninger de forskjellige virksomhetene bruker, eller outsourcing av IT-tjenester.

1.6 OPPGAVENS STRUKTUR

Det første kapittelet tar for seg oppgavens premisser, etterfulgt av de teoretiske kapitlene to, tre og fire. Kapittel to er omhandler informasjonssikkerhet generelt, tre fokuserer på virksomhetsarkitektur og fire tar for seg sammenkoblingen mellom de to forrige kapitlene. Kapittel fem beskriver valgt metode for oppgaven, sammen med en beskrivelse av de statistiske metodene som er brukt og kapittel seks viser resultatene. Det siste kapittelet, kapitel syv er konklusjonen.

2 - INFORMASJONSSIKKERHET

"Threats to security – like the weather – are hard to predict" (PWC 2012)

Informasjonssikkerhet, og sikkerhet generelt, blir ofte sett på som en ekstra byrde en virksomhet er nødt til å investere penger og tid i. Det legges begrensninger på tilgang til bygg og datasystemer over en lav sko, noe som fører til at folk flest har en negativ innstilling til konseptet sikkerhet. (John Sherwood 2005)

Sikkerhet blir som oftest sett på som en mekanisme som gjør arbeidet mindre effektivt. Et ekstra passord man må huske for å få tilgang til det systemet man trenger for å utføre en viss oppgave. En ekstra sjekk som må gjøres av datasystemet, eller programmet, som fører til at det hele går som sirup. Et adgangskort med en tallkode man har glemt, eller at sjefen ikke har husket å godkjenne eller utvide tilgangen tilhørende adgangskortet. Men sikkerhet er mye mer enn bare tilgangskontroll og en endeløs rekke med passord å huske. Informasjonssikkerhet baserer seg i bunn og grunn på tre hovedprinsipper; konfidensialitet, integritet og tilgjengelighet. Disse opprettholdes ved å beskytte informasjonen mot tilgang, bruk, avsløring, modifisering eller ødeleggelse fra uvedkommende. (Bishop 2004)

Sikkerhet og hva som kan betegnes som sikkert er et spørsmål som er vanskelig å svare på, og avhenger veldig av konteksten det blir stilt i. Det som kan være sikkert for en bedrift, eller bare for et tilfelle i en bedrift, kan bli sett på som veldig usikkert for en

annen. Det hele baserer seg på risiko. Hva er risikoen for at informasjonsaktiva blir kompromittert? Og hvilke følger bærer det med seg om utenforstående får tilgang til den?

Denne risikoevalueringen avhenger av hvilken virksomhet den blir gjort i. Aspekter som segment og strategi er viktige pekepinner for retningen en ønsker å ta. Det er viktig å ta hensyn til hva som skal sikres. I de fleste virksomheter i dag finnes det informasjonsaktiva i flere former og fasonger, noen er viktigere enn andre og må dermed sikres bedre. Det er viktig for en bedrift som driver med banktjenester at transaksjon- eller kontoinformasjon ikke kommer på avveie. Hvis noe slikt skulle skje vil det føre med seg negativ omtale av bedriften, og kan kanskje til og med forårsake at privatpersoner og andre virksomheter ikke vil benytte seg av tjenestene deres.

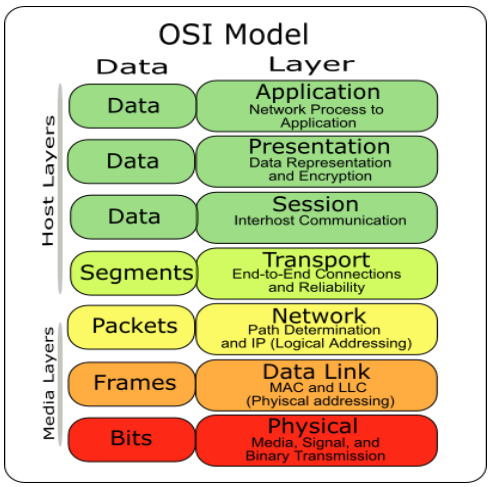
Enhver form for informasjonsaktiva har avhengigheter. Disse avhengighetene er alt fra datasystemene som bruker den, personene som bruker den og hva informasjonsaktivaen brukes til. Disse avhengighetene, og påvirkningsgraden informasjonsaktivaen har på dem er viktig å evaluere nøye, sammen med trusselen for at noen skal være interesserte i å få tak i denne informasjonen. Trusselbildet vil alltid være vanskelig å avgjøre, men er definitivt noe en må passe spesielt godt på. Trusselen er ofte en sammenheng av hvor enkelt det er å få tak i informasjonen, sårbarhet, sammen med underliggende måter informasjonen kan brukes til, eller kan tenkes å brukes til. Kredittkortinformasjon er et godt eksempel på informasjon de fleste kan forestille seg at uvedkommende kan ha interesse av å få tak i. Evalueringen av risiko er altså en sammenheng av disse tingene; informasjonens verdi (eller antatte verdi), avhengigheter og påvirkningsgrad, trussel og sårbarhet. Disse er nært knyttede faktorer, som sammen bestemmer risiko. Selvfølgelig vil forskjellige virksomheter ha forskjellig fokus. Noen virksomheter ønsker kanskje bare å følge de lover og regler som tilrettelegges av statlige institusjoner, andre ønsker en risikosenkende effekt av informasjonssikkerhetsstrategien deres. (M. Eric Johnson 2007)

Det er derfor utrolig viktig å vite sin plass i økosystemet. Plassen kan være internt i virksomheten, som en enhet eller virksomheten som en helhet. Denne bevisstgjørelsen er essensiell for at en fornuftig sikkerhetsstrategi kan virkeliggjøres. Det som ofte er

situasjonen i større bedrifter i dag er massevis av uavhengige prosjekter og løsninger, initiert og oppfulgt av forskjellige interessenter i bedriften, for å løse et problem som har oppstått der og da. Dette fører til at bedriften kanskje har fem, eller ti, løsninger som beskytter mot samme trussel. De er kanskje uavhengige av hverandre, laget spesifikt for det problemet i den avdelingen. Sikkerhetsløsningen er kanskje til og med laget som en modifikasjon på en tidligere løsning for samme sårbarhet, men ny informasjon fører til at nye sikringssteg må tas. Denne lappeteppeteknikken er ofte en følge av at virksomheten har gamle *legacy* systemer i bunn, som de er avhengige av, og dermed ikke har oppdatert til dagens standarder. De virker jo slik de står i dag, og en ser kanskje ikke en kost/nytte effekt av det. En annen grunn til at en oppdatering av løsningen i bunn, kanskje med teknologibytte og det som er, ikke har blitt gjort er at de ansatte ikke har kompetanse på de nye teknologiene. De har kanskje deltatt i utviklingen av løsningen, og føler dermed et sterkt eierskap, som får de til å unngå å anbefale endringer i løsningen. (John Sherwood 2005)

2.1 OSI MODELLEN

Historisk har man ofte referert til OSI modellen(Open System Interconnection Model) for å vise til sårbarheter i datasystemer. OSI Modellen er et abstrakt rammeverk for datakommunikasjon, og blir hovedsakelig sett på som en modell for nettverksarkitektur.



Figur 2 - OSI modellen

Modellen ble laget som et initiativ fra ISO (International Organization for Standarisation) og ble først introdusert i 1978. Dette arbeidet var en følge av at det fantes lite standardisering for hvordan datalagene kommuniserte sammen, så de forskjellige virksomhetene innen feltet hadde sine egne måter å gjøre det på. Det fantes ingen unison måte dette skulle fungere på. (Microsoft 2011) Den ble først introdusert med fem struktureringslag, dette ble senere utvidet til å romme syv. Utvidelsen til syv lag var nødvendig for å holde følge med de

teknologiske nyvinningene på nettverkssiden. Kanskje mest på grunn av introduseringen av ARPANET, det som vi i dag kjenner som internett. (Wikipedia 2011)

OSI modellen brukes ofte som basis i informasjonssikkerhetsarbeid. Hovedsakelig for å forstå de forskjellige sammenhengene i informasjonsflyten mellom lagene. Dette gir en mulighet til å sikre de lagene hvor sikring trengs. Eksempelvis har vi ofte sikkerhetsfunksjoner koblet til det fjerde laget i OSI modellen; transportlageret. Hvor informasjonen som sendes med HTTP over internett ofte krypteres ved hjelp av krypteringsfunksjoner som Secure Socket Layer(SSL)/Transport Layer Security(TLS).

2.1.1 EKSTRA LAG I OSI MODELLEN

Utover de syv kjente lagene i OSI modellen belyses det nå at det finnes tre ekstra lag en ikke har tatt høyde for. Nemlig *politikk, religion og økonomi*. Disse tre ekstralagene berører både småprosjekter og hele virksomheter og det er alle tre en følge av menneskelig påvirkning. Det politiske laget, som (Scheidell 2008) beskriver som det åttende laget av OSI modellen, er hovedsakelig konsentrert rundt personlige preferanser hos de som sitter med siste ordet. Det kan være mange faktorer som spiller inn, sjefen har kanskje en kamerat som jobber hos en potensiell leverandør, og den beste løsningen blir ikke nødvendigvis valgt. Dette gjelder alt fra fysiske brannmurer til programvare og valg av rammeverk. Det niende laget, religion, er basert på tilhørigheten og merkevare/kvalitetsfølelsen noen leverandører har opparbeidet seg. Om man har gjennomført Microsoft som teknologisk religion, kan det være vanskelig å velge produkter fra en annen leverandør. Dette har rot i at de fleste virksomheter ser på det å skifte teknologi som tidkrevende og vanskelig. Økonomi, som er det tiende laget kan være et mangehodet monster. Kanskje finnes det rett og slett ikke nok midler til å implementere de sikkerhetsløsningene en skulle ønsket, eller så blir sikkerhet rett og slett ikke prioritert. (Scheidell 2008)

2.1.2 INFORMASJONSSIKKERHET ER MER ENN OSI MODELLEN

«CIO's must manage IT risk as business risk.» (Gartner 2007)

En helhetlig strategi for informasjonssikkerhet er viktig for å oppnå det målet man ønsker og for å oppnå en slik helhetlig strategi kreves nøye evaluering av den informasjonsaktivaen virksomheten har og segmentet den befinner seg i. Dette er det første initiativet som beskrives i SABSA metoden, og er nærmere forklart i kapittel 3.

3 - VIRKSOMHETSARKITEKTUR

Virksomhetsarkitektur (Eng: Enterprise Architecture) er et bredt begrep, som blir forklart på mange forskjellige måter;

"An enterprise architecture tries to describe and control an organisation's structure,

processes, applications, systems and techniques in an integrated way." (Lankhorst 2009)

"A way to describe business structures and processes that connects business structures." (University)

"The ANSI/IEEE Standard 1471-2000 specification of architecture (of software-intensive systems) may be stated as: "the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution." (Hilliar 2000)

Virksomhetsarkitektur er en abstrakt måte å se på en organisasjon. Det vil si at den ikke tar for seg alle de forskjellige delene i detalj, men heller fokuserer på å gi en helhetlig oversikt over hvilke egenskaper organisasjonen har.

For å få dette til, er det essensielt at profesjonelle fra både forretningssiden og IT-ansvarlige samarbeider. Begrepet virksomhetsarkitektur ble introdusert i 1987 da J.A. Zachman publiserte artikkelen "A Framework for Information Systems Architecture" i IBM Systems Journal. Zachman avdekket her to hovedproblemer i en større virksomhet.

Den økende kompleksiteten til datasystemer og dårlig samkjøring mellom forretningssiden og IT-siden i virksomheten.

"The cost involved and the success of the business depending increasingly on its information systems require a disciplined approach to the management of those systems" (Zachman 1987)

(John Sherwood 2005) forklarer virksomhetsarkitektur ved å sammenligne det med det tradisjonelle synet på arkitektur, bygningsarkitektur.

Når man skal bygge et hus, kreves det at bygningsarkitekten har kunnskap om alle aspektene ved det å bygge huset. Det skal følge gitte lover og regler, være konstruert på riktig måte og med passende materiale. Andre viktige ting å tenke på er hvilken funksjon bygget skal ha, bygningsarbeidernes kompetanse og det landskapet bygningen befinner seg i. Disse er alle elementer som må tas til etterretning når man skal bygge et hus. Det å sammenligne virksomhetsarkitektur med husbygging blir kanskje ikke helt riktig, det anbefales heller å se på det som en hel by. Først da begynner man å forstå kompleksiteten av virksomhetsarkitektur, og gjør det mulig å identifisere de forskjellige komponentene som finnes.

Idéen bak virksomhetsarkitektur er at man skal skape en korrekt og helhetlig modell av organisasjonen. Modellen skal inkludere alle deler av organisasjonen, slik at den best mulig kan støtter forretnings- og IT-initiativer. En velutviklet virksomhetsarkitektur ønsker å optimalisere alle prosessene i en virksomhet. Dette gjøres ved å eliminere redundans og eventuelle motsigelser dem i mellom. Men det støtter ikke bare virksomheten på prosessnivå. En gjennomtenkt virksomhetsarkitektur hjelper også virksomheten til å dele informasjonsaktiva og komponenter de allerede har i løsningene sine på en enklere måte. Hvis virksomheten følger gitte standarder for klassifisering og håndtering av data er det mye enklere for nye løsninger å ta i bruk eksisterende informasjonsaktiva. En følge av dette er redusering av dobbeltlagring, og de feil som kan forekomme av uryddig versjonshåndtering. Samtidig som det kan føre til hurtigere utvikling av nye løsninger. Virksomhetsarkitekturen hjelper med er å håndtere

uforutsette hull i dagens informasjonsaktiva. Ved å identifisere hvor det finnes avhengigheter og tilfeller som ikke er dekket. (John Sherwood 2005)

Virksomhetsarkitektur prøver å skape et speilbilde av virksomheten slik den er i dag, *as-is*, og slik man ønsker å utvikle den mot fremtiden, *to-be*. Disse er to viktige måleparametere for virksomheten og kartlegger hvordan virksomheten skal utvikle seg, hjelper til å gjøre valg og strømlinjeformer virksomhetens visjon. (Pontus Johnson 2004)

Analyseselskapet Gartner kommet opp med seks anbefalte steg, eller «faser», for å utvikle en velfungerende virksomhetsarkitektur. Det første steget virksomheten må tenke på er å utvikle en helhetlig strategi, som både inkluderer IT- og forretningssiden, og planlegging. Dette består hovedsakelig i å skape enighet innad i virksomheten for hvilke mål og oppgaver de mener er de viktigste og gjennom dette kartlegge en beskrivelse av den fremtidige virksomhetsarkitekturen. *To-be* konseptet. Deretter anbefaler de å virksomheten i å utføre en analyse av virksomhetens modenhet i dag gjennom å samle all informasjonsaktiva virksomheten har. Typisk informasjonsaktiva det siktes til her er prosessmodeller, styrende dokumentasjon, beste praksis dokumenter, databeskrivende dokumenter og beskrivelse av løsninger. Dette blir også referert til som *As-is konseptet*. Nå er det tid for å analysere kompetanser som befinner seg i virksomheten. Kompetanse i denne sammenhengen inkluderer både budsjett for de forskjellige initiativene i virksomheten og de ansatte, sammen med andre krav som kan finnes. Man skal se på hvordan disse i sammenheng brukes strategisk i virksomheten i dag, og om det finnes noen måte å effektivisere de på. Det fjerde punktet i Gartner listen bygger på å sikre godkjenning av virksomhetsarkitektur som en strategisk sammenkobling og effektivisering av virksomheten hos besluttelsestagere. Dette gjøres gjennom å utarbeide en tentativ plan for virksomhetsarkitekturen, basert på den tidligere innhentede informasjonen. Planen krever så videre behandling og det anbefales å involvere IT og forretningssiden av virksomheten til å sammen utvikle krav og estimater. De to siste stegene er implementering og drift og videreutvikling. Implementeringen baserer seg på å avdekke hull i planene man laget tidligere, og prioriteringen av hvordan man skal tette de. Man ser på investeringsplaner gjennom case jobbing og gjennom dette prøver å få de godkjent av intressenter og sjefer. Det

siste steget er videreutvikling av virksomhetsarkitekturen, og handler om å gjennomføre de planlagte strategiene og med dette oppnå en høyere detaljeringsgrad. Detaljeringsgraden skal øke, helt til man oppnår ønsket fremtidstilstand, *to-be*,som ble utformet i det første steget.(Buchanan 2010)

3.1 INNDELING I VIRKSOMHETSARKITEKTUR

De forskjellige rammeverkene innen virksomhetsarkitektur har ofte forskjellige inndelinger for virksomhetens arkitektur. Felles for de fleste er at de benytter seg av tre nivåer; (Group 2010)

- Forretningsarkitektur
- Informasjonsarkitektur
- Teknologiarkitektur

Nivået for sikkerhetsarkitektur har nylig blitt introdusert.

3.1.1 FORRETNINGSARKITEKTUR

Forretningsarkitekturen modellerer organisasjonens forretningsprosesser, roller, ansvar og struktur. Den skal reflektere hvordan virksomhetens prosesser passer sammen med hvordan organisasjonen fungerer.

3.1.2 INFORMASJONSARKITEKTUR

Inneholder informasjonsaktiva og integrasjon- og applikasjonsmodeller brukt for å styre organisasjonen. Disse er abstrakte modeller som er analysert på et konseptuelt, logisk og fysisk nivå.

Informasjonsaktiva kan være elektronisk, papir eller lagret på andre former. De kan være alt fra kundelister til forskningsdata. Informasjonsaktivaene er integrert i

informasjonssystemet gjennom programvare- eller maskinvareløsninger. Applikasjonsmodeller representerer teknologiske applikasjoner brukt for å gjennomføre oppgaver eller forretningsprosesser.

3.1.3 TEKNOLOGISK ARKITEKTUR

Den teknologiske arkitekturen representerer organisasjonens IT infrastruktur. Infrastrukturen består av både programvare- og maskinvarekonfigurasjonene organisasjonen har. Disse er basert på den abstrakte modellen fra forretningsarkitekturen og sikkerhetskravene som ble avdekket av informasjonsarkitekturen. Teknologiarkitekturen består av komponentene; data teknologi, integrasjonsteknologi, applikasjonsteknologi, samhandling, plattformer og nettverk.

Informasjonssikkerhet implementeres på dette nivået gjennom rigid konfigurering av systemene, oppdateringshåndtering, oppgraderinger, krypteringsteknologier. Man finner også metoder innenfor industristandarder og god praksis.

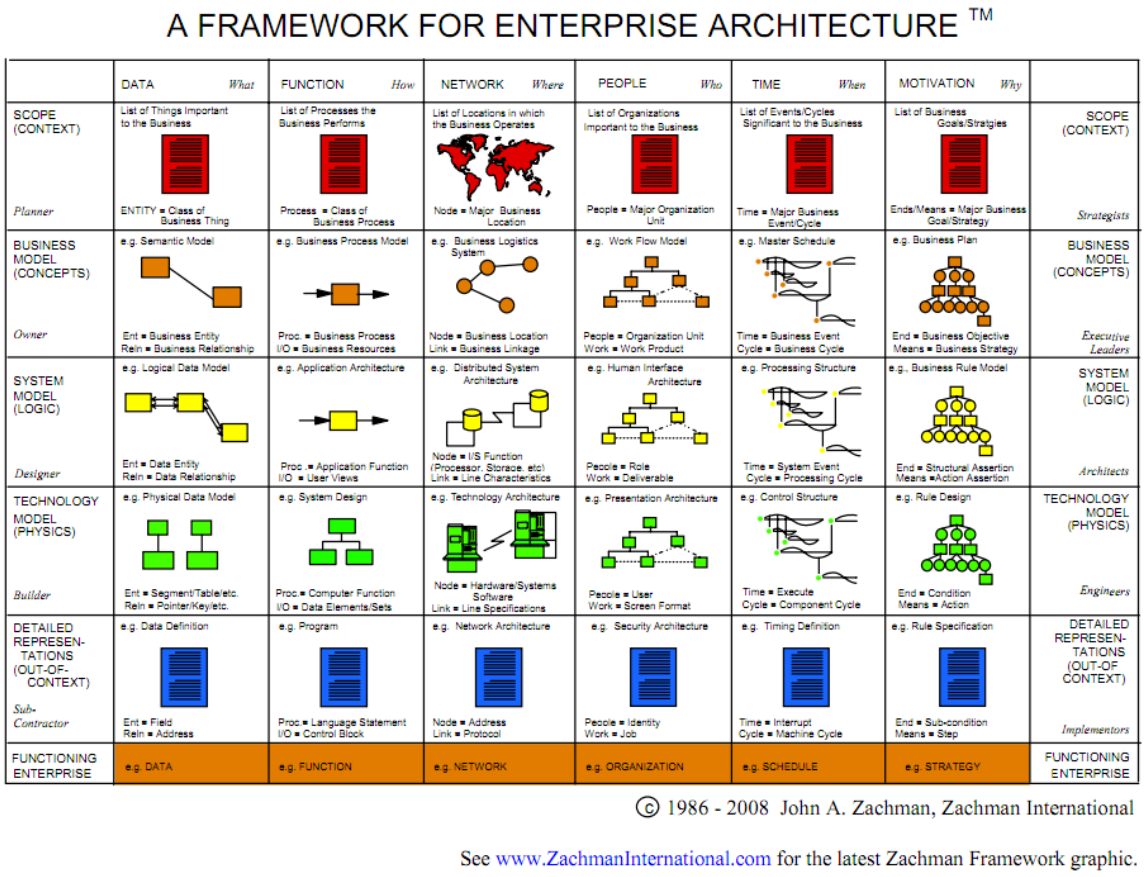
Hvert arkitekturnivå fokuserer på et perspektiv av organisasjonen, dette kan føre til redundans og hull, men sammen ser de til at forretning og IT støtter opp mot hverandre(Sessions 2007)

3.2 RAMMEVERK FOR VIRKSOMHETSARKITEKTUR

Det kan spekuleres i at alle virksomheter egentlig har en form for virksomhetsarkitektur. Har de ikke fulgt et fast rammeverk, blir det fort et sammensurium av gamle og nye løsninger. Det er derfor viktig å bruke de riktige verktøyene for å utvikle og optimalisere virksomhetsarkitekturen.

3.2.1 ZACHMAN ENTERPRISE FRAMEWORK

Zachman rammeverket var det første rammeverket innen virksomhetsarkitektur, og har overlevd i over 20 år. De ble tidlig en de facto standard for virksomheter som skulle utvikle en virksomhetsarkitektur. Mye av grunnen til det kan være måten Zachman designet rammeverket sitt. Det bygget på gamle måter å forklare arkitektur, og var derfor lettere å forstå og ta i bruk.



Figur 3 - ZIFA 2008

I ettertid har John Zachman forklart rammeverket sitt en logisk struktur for å klassifisere og organisere den deskriptive representasjonen av en virksomhet på en måte som gir verdi til ledelsen i virksomheten og videreutviklingen av virksomhetens systemer. (Zachman)

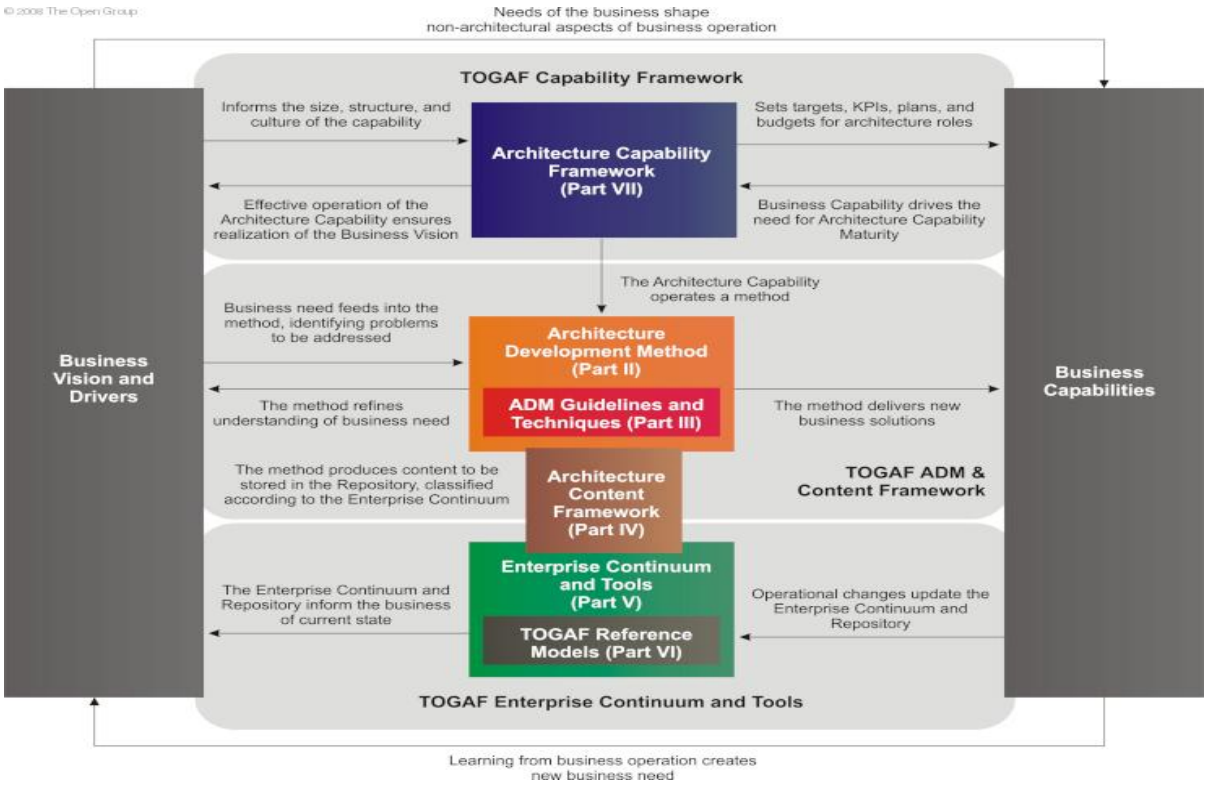
Selve rammeverket tilbyr en strukturert og formell måte å definere en virksomhet på. Essensen i rammeverket er en matrise på seks ganger seks celler. Inndelt i kategori langs den vertikale linjen og semantiske spørsmål på den horisontale linjen.

Ser man på rammeverket fra et BPM (Business Process Management) ståsted. Kan man se på det som en stegvis tilnærming til det å lage en arbeidsprosess fra start til slutt, med tilhørende inndeling i arbeidsflytdiagrammer etter behov. (Pedro Sousa 2007)

Zachman rammeverket har opplevd flere revisjoner i løpet av sin levetid, og kan i flere tilfeller referere til et av flere rammeverk J.A Zachman har utarbeidet. I 1997 og i 2008 kom det store oppdateringer. Det er versjonen fra 2008 som vises ovenfor.

3.2.2 THE OPEN GROUP ARCHITECTURE FRAMEWORK

Technical Architecture Framework for Information Management (TFAIM) hadde vært et av de første forsøkene på å implementere en virksomhetsarkitektur og var sterkt påvirket av Zachman rammeverket. Arbeidet ble avsluttet da den amerikanske kongressen fastslo at alle byråer hadde oppdaget negative konsekvenser av implementeringen. Prosjektet ansees som et at de største tapsprosjektene innen IT. (Sessions 2007) Etter at det amerikanske forsvarsdepartementet skrinla arbeidet sitt med TAFIM, tok den uavhengige organisasjonen The Open Group tok over arbeidet de hadde gjort og omdøpte det til The Open Group Architecture Framework.



Figur 4 - TOGAF 2008

TOGAF lister opp en rekke premisser for rammeverket sitt innen virksomhetsarkitektur:

- Forklare en metode for å definere informasjonssystemer med et sett av byggeklosser.
- Vise hvordan byggeklossene passer sammen
- Inneholde et sett av verktøy
- Inkludere en liste av anbefalte standarder
- Inkludere en liste av kompatible produkter som kan brukers til å implementere byggeklossene.

For å tilfredsstille disse premissene er rammeverket delt inn i 3 hovedkategorier

- Enterprise Architecture Domains
- Architecture Development Method
- Enterprise continuum
-

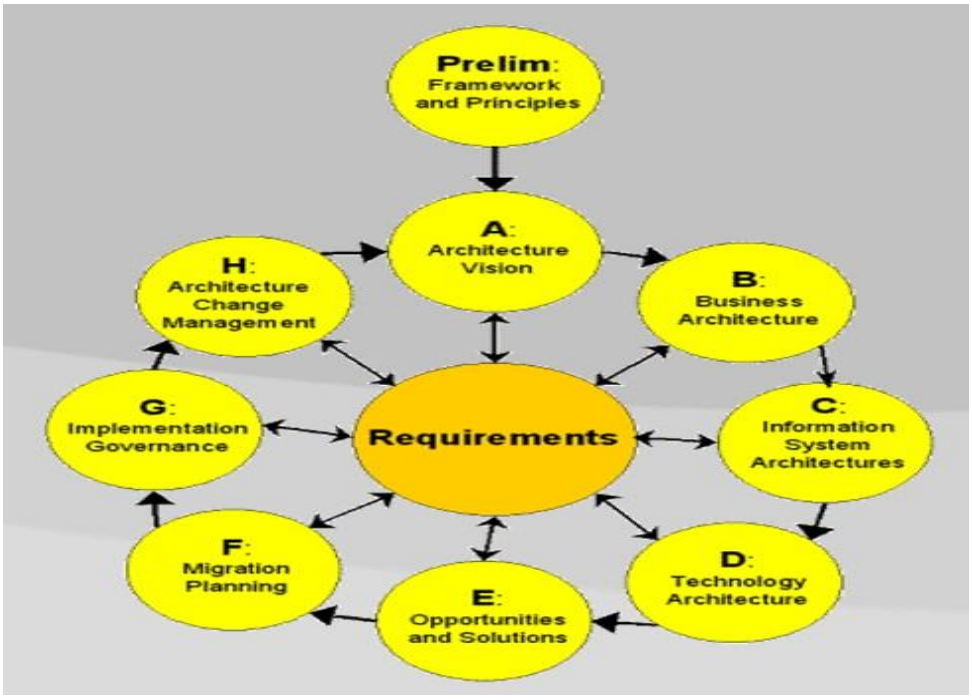
3.2.2.1 Enterprise Architecture Domains

Baserer seg på samme inndeling av informasjonsaktiva som BITS (Se kapittel 3.1) og består av 4 grunnpilarer;

- Forretningsarkitektur – Forklarer prosessene virksomheten bruker for å nå sine mål.
- Applikasjonsarkitektur – Forklarer hvordan applikasjoner er designet og hvordan de interagerer med hverandre.
- Data arkitektur – Forklarer virksomhetens informasjon er lagret og hvordan man får tilgang til den.
- Teknisk arkitektur – Forklarer virksomhetens maskinvare- og programvareinfrastruktur og hvordan disse samhandler.

3.2.2.2 Architecture Development Method

En beskrevet iterativ syklus som forklarer hvilke steg som skal tas for å utvikle en fullstendig virksomhetsarkitektur.



Figur 5 - TOGAF ADM 2008

3.2.2.3 Enterprise Continuum

– Kan sees på som et bibliotek for virksomheten, som gjenspeiler informasjonsaktiva virksomheten innehar og beste-praksis fra IT-industrien. Biblioteket, som inneholder alt fra prosessmodeller og styrende dokumentasjon til veikart for strategi. Virksomhetens informasjonsaktiva settes i sammenheng for gjenbruk eller videre modning av virksomhetsarkitekturen. Samtidig som å være et bibliotek kan det brukes for å referere til hvor en virksomhet befinner seg i utviklingen av virksomhetsarkitektur, og gjør det enklere for individer å ha et referansepunkt når man diskuterer. (Group 2010)

4 - HELHETLIG INFORMASJONSSIKKERHET

Det foregår et slags hamskifte i informasjonssikkerhetsverden. Det som før ble sett på som et pengesluk, uten håndfaste noen gevinstgivende funksjon for virksomheten, blir nå tatt mer og mer inn i varmen. Sikkerhet blir nå ansett som et viktig element å fokusere på og investere penger i om en vil drive en suksessfull forretning.

Sikkerhet var ikke et av hovedområdene da Zachman introduserte rammeverket sitt i 1987, men etterhvert som tiden har gått, har det vist seg at sikkerhet har fått et større fokus. Informasjonssikkerhet begynner å kreve sin plass i den strategiske tilnærmingen en virksomhet har til informasjonsteknologi, og blir sett på som en nødvendighet å ta med i den helhetlige forretningsstrategien.

Man leser til stadighet om brudd på informasjonssikkerheten til forskjellige bedrifter i tidsskrifter og aviser. Det går nesten ikke en uke uten en ny skandale. (NSR 2010) viser at de aller fleste tilfellene av informasjonssikkerhetshendelser ikke blir rapportert. Virksomheter har en tendens til å skamme seg litt etter at skaden faktisk har skjedd, og de vil dekke det opp. Dette er for så vidt forståelig. Mange virksomheter kan tape stort på dårlig sikring av data. Både i kunder, og i graden av tillit de har hos sine samarbeidspartnere.

4.1 BESTE PRAKSIS INNEN INFORMASJONSSIKKERHET

Informasjonssikkerhet blir virkeliggjort ved å implementere industristandarder og god/beste praksis. De best kjente retningslinjene for strategisk informasjonssikkerhet er:

- International Organization for Standarization/International Electrotechnical Comission 27001 (ISO/IEC 27001)
- Standard for GoodPractice (SoGP)
- Organization for Economic Cooperation and Development (OECD)

ISO/IEC 2701 var tidligere kjent som ISO 17099. Det er en samling retningslinjer for informasteknologi, sikkerhetsteknikker, informasjonssikkerhetshåndertingssystemer og andre krav. (Watkins)

SoGP tar for seg informasjonssikkerhet fra et forretningsperspektiv. Retningslinjene blir utarbeidet av medlemmer av Information Security Forum(ISF), et nettsamfunn for informasjonssikkerhet med medlemmer fra hele verden. Retningslinjene er basert på forskning, medlemmenes ekspertise og praktiske erfaringer. De blir oppdatert annethvert år. (Forun 2003)

OECD fokuserer på retningslinjer innen lovgivende og juridiske krav, og ønsker å bringe økonomisk stabilitet gjennom riktig styring, gjennomsiktighet, eksterne revisjoner og intern forretningskontroll. (OECD 2011)

ISO/IEC og SoGP blir ansett som hoved autoriteten for retningslinjer innen informasjonssikkerhet.

Det finnes også retningslinjer for informasjonssikkerhet fra den norske stat. (Regjeringen 2006)

4.2 SIKKERHETSARKITEKTUR

Figur 6 - Sikkerhetsarkitektur (EDB Ergogroup)

Ved å introdusere sikkerhetsnivået som en ekstra underkategori av virksomhetsarkitektur, BIT(S), kommer flere krav man ikke har tatt hensyn til tidligere frem. Disse er blant annet kartlegging av forretningen, lovgivende og juridiske krav, teknologisk kartlegging, god praksis anbefalinger, industritrender og innspill fra visjonærer.

4.3 SHERWOOD APPLIED BUSINESS ARCHITECTURE (SABSA)

Sherwood Applied Business Architecture(SABSA) er både en modell og en metode for å introdusere informasjonssikkerhet og Service Management til arkitekturverden. Rammeverket er et arbeid av SABSA gruppen, som har redefinert og optimalisert metoden siden 1995. SABSA sier selv at rammeverket har vært, og er, i bruk av flere høyt profilerte virksomheter rundt om i verden med stor suksess.

Den fokuserer på en virksomhetsdrevet tilnærming, med målene for virksomheten som retningslinjer. Den viktigste egenskapen til rammeverket er at alt må hentes fra en

analyse av virksomhetens informasjonssikkerhetskrav. Gjennom kravanalysen skal rammeverket tilby en mulighet for virksomheten til å utnytte sikkerhet som en faktor for å muliggjøre utnyttelsen av nye forretningsmuligheter. SABSA forsikrer om at metoden deres tilbyr alle de nødvendige aspektene en entreprise trenger, og at informasjonssikkerhetstjenester er laget, levert og støttet som en helhetlig del av både forretning- og IT-strukturen av virksomheten.

Det første SABSA rammeverket foretar seg er å analysere virksomheten, dette produserer sporbarhet gjennom strategi og konsept til design og implementering. SABSA livssyklusen tilser at virksomhetsmandatet opprettholdes gjennom administrering og måling. Det finnes verktøy som støtter dette i rammeverket.

SABSA er et generisk rammeverk, og kan være startpunktet til en hvilken som helst virksomhet. Men gjennom å foreta seg den initiale analysen, og valgene definert av strukturen, ender man opp med et sluttresultat som er skreddersydd til den gjeldende virksomheten. Det man sitter igjen med er en virksomhetssikkerhetsarkitektur som enkelt kan tilpasses en unik forretningsmodell. Dette er en sentral del av suksess for å implementere en helhetlig sikkerhetsarkitektur for virksomheten. (John Sherwood 2005)

4.3.1 SABSA MODELLEN

Modellen er bygget opp av seks lag. Det er en ovenfra-og-ned(top-down) tilnærming, hvor det øverste laget kalt den kontekstuelle arkitekturen gjennomfører en definering av sikkerhetskravene sett fra et forretningsperspektiv. Etter hvert som man beveger seg nedover blir rammeverket mindre abstrahert og flere detaljer tas hensyn til. Gjennom den konseptuelle arkitekturen, den logiske, den fysiske infrastruktur, komponentarkitekturen og på det laveste laget operasjonell sikkerhetsarkitektur.

The Business View	Contextual Security Architecture
The Architect's View	Conceptual Security Architecture
The Designer's View	Logical Security Architecture
The Builder's View	Physical Security Architecture
The Tradesman's View	Component Security Architecture
The Facilities Manager's View	Operational Security Architecture

Figur 7 - SABSA 2009

Disse seks lagene representerer alle de involverte i prosessen med å spesifisere, designe, lage og bruke alle systemene forretningen trenger for å utføre sine oppgaver. For å definere disse seks lagene bruker SABSA rammeverket spørsmålene hva, hvorfor, hvordan, hvem, hvor og når ved hvert lag. Det er disse seks spørreord, arvet fra Zachman rammeverket, som er kjernen i SABSA matrisen.

4.3.2 SABSA MATRISEN

SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Figur 8 - SABSA Matrix 2009

I matrisen ovenfor ser man at de forskjellige spørreordene viser til forskjellige aspekter innen hvert arkitekturnivå.

- *Hva – eiendeler* (What – Assets): Dette er den informasjonsaktiva virksomheten har, og detaljerer hvordan man skal jobbe med den for å klassifisere, organisere og sikre at alle risikoer og avhengigheter er ivaretatt.
- *Hvorfor – motivasjon* (Why – Motivation): En risikoanalyse og verdiestimering av informasjonsaktiva. For å fastsette hvilke motiverende faktorer som ligger til rette for å sikre en gitt del av informasjonsaktivaen.
- *Hvordan – prosess* (How – Process): Kartlegging og forberding av informasjonsflyt mellom virksomhetens bruk av informasjonsaktiva. En oversikt over hvordan systemene interagerer med hverandre gjennom å en arkitektonisk tilnærming, gjerne basert på et rammeverk.
- *Hvem – mennesker* (Who – People): En utredning av hvem som skal bruke systemet, og en evaluering av hvilke informasjonsaktiva som skal være tilgjengelig for hvem. Ofte brukergruppekontrollert tilgang. Kategorisering av brukere for å håndtere tilgangskontroll; Eier, saksbehandler og bruker er en generell til dette.
- *Hvor – lokasjon* (Where – Location): Oversikt over virksomhetens domener, og hvem som skal ha tilgang hvor. Klassifisering av informasjonsaktiva for å tilrettelegge varierende grader av sikkerhetstiltak på bakgrunn av hvor den er tilgjengelig. For eksempel er noe informasjonsaktiva tilgjengelig ved hjemmekontor, mens annen kanskje ikke.
- *Når – tid* (When – Time): En risikotilnærming for å se på når informasjonsaktivaen er tilgjengelig. Skal den alltid inneha de samme klassifiseringene? For eksempel er en finansiell månedsrapport er mye viktigere å sikre fra uvedkommende før den har blitt publisert offentlig.

4.3.3 KONTEKSTUELL ARKITEKTUR

SABSA modellen betegner den kontekstuelle arkitekturen som forretningens syn. Dette laget tar for seg hvilken kontekst virksomheten befinner seg.

Hva er forretningskravene, hvorfor sikkerheten er nødvendig, hvordan sikkerheten skal integreres, hvem må være involvert og hvem får sikkerheten følger for, hvor er sikkerheten nødvendig og når er sikkerheten påkrevd.

4.3.4 KONSEPTUELL ARKITEKTUR

Det konseptuelle nivået er det helhetlige konseptet som gjør at forretningskravene til virksomheten kan imøtekommes. Dette er arkitektens nivå, som definerer prinsipper og fundamentale konsepter for å rettlede i prosessen med å velge å organisere det logiske og de fysiske elementene i lagene med lavere abstraksjonsnivå.

Hva man vil beskytte, hvorfor beskyttelsen er viktig, hvordan man vil oppnå beskyttelse, hvem som er involvert i sikkerhetshåndtering, hvor du vil oppnå beskyttelse og når beskyttelsen er relevant.

4.3.5 LOGISK ARKITEKTUR

Det logiske nivået innebærer å identifisere og spesifisere de logiske arkitekturelementene. Nivået blir i SABSA definert som designerens syn, og krever at virksomheten blir systematisk modellert. Det viser store arkitektoniske sikkerhetselementer ved logiske sikkerhetstjenester og forklarer den logiske flyten av kontroll og forhold mellom tjenestene. Det logiske nivået skal vise den logiske representasjonen av den informasjonsaktiva virksomheten har.

4.3.6 FYSISK ARKITEKTUR

Fysisk arkitektur er hvor planene og prosessene definert tidligere blir laget enda mer konkrete. Slik som bygningsarbeiderne mottar spesifikasjonene fra bygningsarkitekten, og kan virkeliggjøre disse, lages nå de fysiske modellene som støtter opp om det tidligere arbeidet. På dette nivået velger man hvilke fysiske komponenter som skal sikre virksomhetens informasjonsaktiva. For eksempel brannmurer, hvilke servere som skal brukes for å sikre virksomheten og hvilken teknologi som skal brukes.

4.3.7 KOMPONENTARKITEKTUR

For å virkeliggjøre planene i den fysiske arkitekturen trenger man ofte en bred kompetanse fra et utall personer. Det er viktig å få på plass den rette kompetansen for å integrere løsningen på best mulig måte. I komponentarkitekturen samles all kunnskap som trengs, gjennom individer med kompetanse, og man bygger løsningen.

4.3.8 OPERASJONELL ARKITEKTUR

Det operasjonelle nivået omhandler det som skjer etter at man er ferdig med alle de andre nivåene, og løsningen har blitt implementert. Her legges det vekt på driften av virksomhetens systemer. Hvordan de utfører revisjoner, måler om de lever opp til kravene, og forbedrer systemet gradvis hele tiden. (John Sherwood 2005)

5 - METODE

I dette kapittelet beskrives det hva en forskningsmetode er. Hvorfor det er viktig å velge rett metode til forskningsarbeidet og en kort gjennomgang av de generelle trinnene i forskningsmetoden.

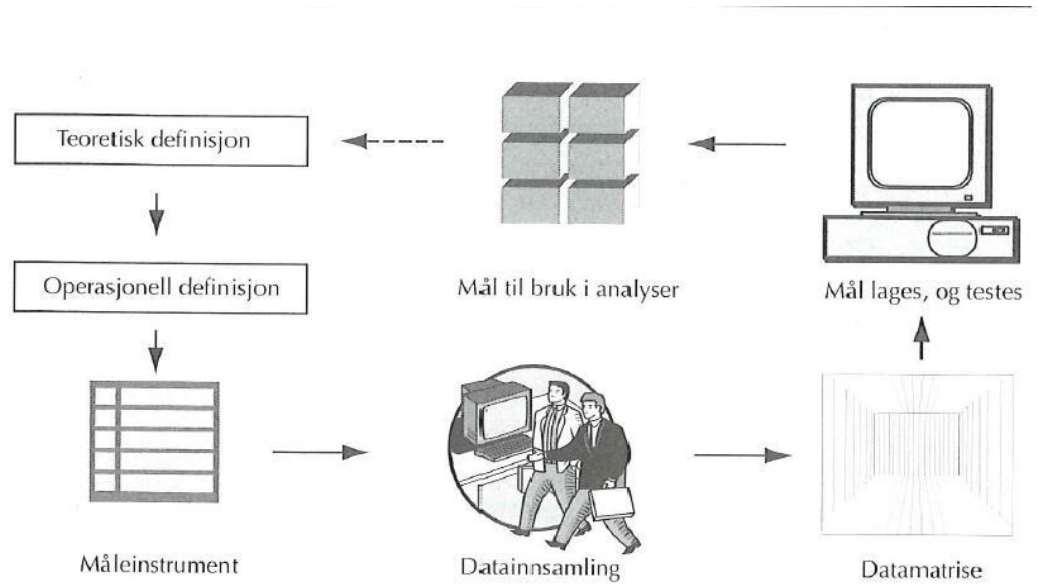
I ethvert forskningsarbeid er valget av *metode* viktig. Metoden dikterer hvordan arbeidet med å finne ny informasjon skal foregå og med retningslinjer for hvordan man skal gå frem. Det finnes utallige ulike metoder, og det er essensielt å velge en metode som belyser forskningsspørsmålet/problemstilling man ønsker å undersøke. Problemstillingen til arbeidet har derfor stor påvirkningskraft i valget av metode.

Det vil alltid finnes et prinsipielt forhold mellom data og observasjoner av virkeligheten. Den innhentede dataen innehar alltid en porsjon subjektivitet pålagt fra forskeren. (Ringdal 2007) Data innhentet i spørreundersøkelser er teoriladede, observasjonene er gjennomført innenfor et teoretisk rammeverk, og er derfor bare forståelige i den sammenhengen. Språket og begrepene som brukes påvirkes av den bakenforliggende teorien. Dette fører til at forskeren påvirker datainnhentingen, kanskje uten å være klar over det selv. Observasjoner som ikke blir påvirket av det teoretiske grunnlaget er derfor umulig. (Ringdal 2007)

Metoden i dette arbeidet er en kvantitativ forskningsmetode for å håndtere empiriske data. Forskningsspørsmålet; «Implementerer norske virksomheter informasjonssikkerhet i sin virksomhetsarkitektur?», krevde en tilnærming som fokuserte på å innhente en større mengde data fra mange kilder. Dette ble gjort for å skape et datagrunnlag som kunne brukes til å se på trender og modenhet i næringslivet rundt fagområdet.

For å hente inn data ble det brukt et spørreskjema, basert på SABSA matrisen. SABSA matrisen er nærmere forklart i kapittel 3.

5.1 MÅLEPROSESSEN



Figur 8.1 Måleprosessen

Figur 9 - Ringdal, K. 2007

Figuren ovenfor illustrerer stegene i måleprosessen. Det første man må gjøre er å lage en *teoretisk definisjon*, dette er en definisjon av den tilgjengelige teorien som er grunnlaget i arbeidet. Den teoretiske definisjonen blir så grunnlaget for en operasjonell utforming. Denne utformingen brukes for å måle de teoretiske begrepene, og kalles et måleinstrument. Det er i dette steget man transformerer teori til spørsmål i for eksempel et spørreskjema. Definisjonen måleinstrumentet kan henvise til et eller flere spørsmål. Måleinstrumentet brukes så til innsamling av data og registreres elektronisk i det som betegnes som en datamatrise i modellen. Med datamatrise menes som regel et regneark, eller statistisk programvare som SPSS eller STATA. Etter at alle de innhentede dataene har blitt registret oppretter man mål, disse kan være en indikator basert på et spørsmål i spørreskjemaet eller sammensatte mål som skalaer eller indekser. Å summere verdiene på hver enkelt variabel er den enkleste metoden å lage sammensatte mål. Når målene har blitt satt utfører man statistiske metoder på dem. (Ringdal 2007)

5.1.1 MÅLEINSTRUMENTET / SPØRRESKJEMA

De første spørsmålene i spørreskjemaet er demografisk informasjon, såkalte bakgrunnsvariabler. Disse er viktige å ha med for å få en oversikt over respondentenes demografi. Med demografi menes informasjon direkte knyttet til respondenten, og omhandler ikke spørreundersøkelsens tema. Disse variablene kan ha en forklarende kraft i senere utforsking av datasettet. (Ringdal 2007)

Den underliggende teorien ble operasjonalisert gjennom ved å fokusere på en del av SABSA rammeverket kalt SABSA matrisen. Denne matrisen har store likheter med Zachman rammeverket og det ble ansett at det ville være et sterkt teoretisk grunnlag å basere seg på. I likhet med Zachman rammeverket har SABSA matrisen 36 celler, spredt over 6 kategorier. For å holde spørreskjemaet på et håndterbart nivå er undersøkelsen avgrenset til to av lagene i SABSA matrisen. Konseptuell arkitektur og Logisk arkitektur. Se 3.2 for ytterligere beskrivelse av SABSA Matrisen.

SABSA MATRIX

	ASSETS (What)	MOTIVATION (Why)	PROCESS (How)	PEOPLE (Who)	LOCATION (Where)	TIME (When)
CONTEXTUAL ARCHITECURE	Business Decisions	Business Risk	Business Processes	Business Governance	Business Geography	Business Time Dependence
	Taxonomy of Business Assets, including Goals & Objectives	Opportunities & Threats Inventory	Inventory of Operational Processes	Organisational Structure & the Extended Enterprise	Inventory of Buildings, Sites, Territories, Jurisdictions, etc.	Time dependencies of business objectives
CONCEPTUAL ARCHITECTURE	Business Knowledge & Risk Strategy	Risk Management Objectives	Strategies for Process Assurance	Roles & Responsibilities	Domain Framework	Time Management Framework
	Business Attributes Profile	Enablement & Control Objectives; Policy Architecture	Process Mapping Framework; Architectural Strategies for ICT	Owners, Custodians and Users; Service Providers & Customers	Security Domain Concepts & Framework	Through-Life Risk Management Framework
LOGICAL ARCHITECTURE	Information Assets	Risk Management Policies	Process Maps & Services	Entity & Trust Framework	Domain Maps	Calendar & Timetable
	Inventory of Information Assets	Domain Policies	Information Flows; Functional Transformations; Service Oriented Architecture	Entity Schema; Trust Models; Privilege Profiles	Domain Definitions; Inter-domain associations & interactions	Start Times, Lifetimes & Deadlines
PHYSICAL ARCHITECTURE	Data Assets	Risk Management Practices	Process Mechanisms	Human Interface	ICT Infrastructure	Processing Schedule
	Data Dictionary & Data Inventory	Risk Management Rules & Procedures	Applications; Middleware; Systems; Security Mechanisms	User Interface to ICT Systems; Access Control Systems	Host Platforms, Layout & Networks	Timing & Sequencing of Processes and Sessions
COMPONENT ARCHITECTURE	ICT Components	Risk Management Tools & Standards	Process Tools & Standards	Personnel Man'ment Tools & Standards	Locator Tools & Standards	Step Timing & Sequencing Tools
	ICT Products, including Data Repositories and Processors	Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools	Tools and Protocols for Process Delivery	Identities; Job Descriptions; Roles; Functions; Actions & Access Control Lists	Nodes, Addresses and other Locators	Time Schedules; Clocks, Timers & Interrupts
SERVICE MANAGEMENT ARCHITECTURE	Service Delivery Management	Operational Risk Management	Process Delivery Management	Personnel Management	Management of Environment	Time & Performance Management
	Assurance of Operational Continuity & Excellence	Risk Assessment; Risk Monitoring & Reporting; Risk Treatment	Management & Support of Systems, Applications & Services	Account Provisioning; User Support Management	Management of Buildings, Sites, Platforms & Networks	Management of Calendar and Timetable

Figur 10 - SABSA Matrisen 2009

Innholdet til de forskjellige cellene i matrisen er teoretisk beskrevet i kapittel 4. Det er denne beskrivelsen som har blitt brukt til å lage spørsmål så nærliggende teorien som mulig. I måleinstrumentet er påstandene formet etter det underliggende rammeverket, slik at to og to spørsmål hører til samme celle i samme kategori. De to første spørsmålene hører for eksempel til cellen *hvorfor - eiendeler* i kategorien konseptuell arkitektur. Det er derfor naturlig å slå de sammenhengende spørsmålene sammen som en måleparameter.

Operasjonaliseringen resulterte i 25 spørsmål. Spørsmålene var utformet som påstander, der respondenten indikerer enighet. For å måle respondentens enighet i utsagnene ble det brukt en fem-punkts Likert skala der:

- en - uenig
- to - uenig
- tre - hverken enig eller uenig
- Fire - noe enig
- fem - enig.

Spørsmål laget med bakgrunn likertskalaen klassifisert som lukkede spørsmål. Respondentene har ikke muligheten til å velge hva de vil svare, men må ta stilling til hvorvidt de er enige i spørsmålet/påstanden.

5.1.2 SPØRRESKJEMA

Innledende spørsmål:

Hvilken stilling har du?

Hvor lenge har du vært ansatt i nåværende virksomhet?

Hvilken bransje befinner virksomheten seg i?

Er virksomheten offentlig eller privat?

Hvor mange ansatte har virksomheten?

IT-sikkerhet i virksomhetsarkitektur.

Gjennom hele undersøkelsen vil 1 representere svært uenig og 5 svært enig.

1. Vi har kartlagt våre forretningskritiske informasjonsaktiva, og hvordan disse hensiktsmessig kan sikres.

2. Vi har satt fokus på å koble sammen hva som skal sikres av informasjonsaktiva og overordnet forretningskrav til den digitale infrastrukturen.

3. Vi har arbeidet med å avklare hvilke informasjonssikkehetstiltak som understøtter forretningskravene som stilles til den digitale infrastrukturen.

4. Gjennom risikovurdering og revisjoner målet vi effektiviteten av informasjonssikkerhetstiltak.

5. Vi har strategisk arbeidet med å finne de beste løsningene for å sikre de forskjellige informasjonsaktiva.

6. Vi har brukt et rammeverk for å kartlegge forretningsprosessene våre.

7. Vi har strategier for hvordan vi sikrer datatrafikken vår.

8. Vi har strategisk forankret forvalting av hvem som har tilgang til den digitale infrastrukturen gjennom roller med definert ansvar.

9. Vi har en felles autoriseringsplatform for brukere i hele den digitale infrastrukturen.

10. Ved å involvere personell fra både IT og andre avdelinger sikrer vi at vi får et bredere syn på sikkerhet.

11. Vi kartlegger effektivitetstap før implementeringen av nye informasjonstiltak.

12. Vi har laget en oversiktsmodell over logiske og fysiske områder, som domener og plassering datamaskiner/servere.

13. Vi har strategisk sett på hva på hvilke relasjoner som må sikres mellom de forskjellige domenene i den digitale infrastrukturen vår.

14. Vi har strategisk utarbeidet en oversikt som viser hvor og i hvilken grad de forskjellige systemene våre monitoreres.

15. Vi har instrukser for de forskjellige sikkerhetsklassifiseringene av informasjonsaktiva.

16. Vi har egne mål og strategier(policies) for hvert område(domene).

17. Vi har dokumenterte mål og strategier(policies) overordnet for alle områder(domener) i den digitale infrastrukturen.

18. Vi har dokumenterte prosedyrer på hvordan informasjonssikkerhetstiltak fungerer og hvordan de overlapper med hverandre.

19. Det er flere av informasjonssikkerhetstiltakene som blir brukt over flere domener til flere tjenester.

20. Vi har utarbeidet et rammeverk over rettigheter og ansvar til de forskjellige brukergruppene i systemet.

21. Det er kartlagt i hvilken grad vi stoler på de forskjellige brukergruppene.

22. Vi har dokumenterte prosedyrer på hvordan de forskjellige klassene av informasjonsaktiva kan manipuleres av brukere.

23. Vi har egne prosedyrer for regelmessig og rutinemessig gjennomgang av informasjonssikkerhetsfunksjoner.

24. Vi har mål og strategier(policies) for hvordan den digitale infrastrukturen håndterer sesjoner og livstider. (F.eks registrering, sertifisering, innlogging, osv.).

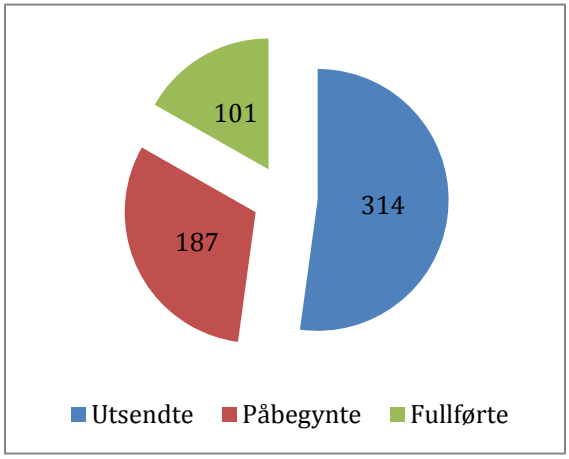
25. Jeg har god kjennskap til virksomhetens informasjonssikkerhetstiltak.

Kommentarer til undersøkelsen:

5.1.3 DATAINNSAMLING

For å hente inn en datamengde, som var stor nok til å brukes i en kvantitativ metode, ble først inngått et samarbeid med konferansen Javazone 2010 i Oslo. Arrangørene sa seg villig til å sende en link til undersøkelsen sammen med sammen med nyhetsbrevet deres som hadde rundt 10 00 mottakere. De ønsket å moderere undersøkelsen selv og laget undersøkelsen med tilgjengelig med verkøyet QuestBack. Dette resulterte i 10 svar fra individer som definerte seg selv som eksperter innen informasjonssikkerhet.

Spørreundersøkelsen ble deretter gjort tilgjengelig på internett gjennom verktøyet Laguna Survey. Den ble sendt til medlemmer av interessegrupper for virksomhetsarkitektur, informasjonshåndtering og informasjonssikkerhet i Dataforeningen. Ledere og ansvarlige for offentlige IT-samarbeid, IT-sjefer i kommuner og kommunale samarbeid, eksperter innen virksomhetsarkitektur, informasjonshåndtering, informasjonssikkerhet og IT-sjefer i private virksomheter.



Av 314 utsendte invitasjoner pr e-post, var det 187 påbegynte og 101 fullførte svar. De 10 overnevnte svarene ble lagt inn manuelt i verktøyet. Undesøkelsen ble avsluttet da 100 svar ble passert.

5.2 DATAANALYSE

Det innhentede datasettet har blitt påført flere statistiske tester ved hjelp av statistikkverktøyet Statistics Package for Social Sciences (SPSS), versjon 18.

Datasettets kvalitet må sikres, og må derfor testes for feil. Kvaliteten til datasettet testes gjennom reliabilitet- og validitetstester. Vi ser på den deskriptive statistikken til datasettet, for å få en rask oversikt over respondentenes svar, og gjennomfører så en faktoranalyse. Faktoranalysen identifiserer spørsmål som er nærliggende hverandre og samler dem i en andel *faktorer,* som kan forklare noe om datasettet og dets dimensjon. For å se på likheten mellom faktorene generert fra faktoranalysen, og det underliggende teoretiske rammeverket, lager jeg *indekser* av begge. Reliabilitetstesen Cronbach's alpha blir så påført indeksene, for å sikre deres kvalitet. Til slutt brukes utfallet av

faktoranalysen til å generere klyngeanalyser. Klyngeanalysene viser dataenes tilhørighet i klynger, og kan fortelle oss noe om hvordan svarene i spørreundersøkelsen er fordelt.

5.2.1 INDEKSER

Indekser lages for å samle nærliggende spørsmål i en variabel. I faktoranalysen identifiseres det sammenheng mellom spørsmålene, og de deles inn i faktorer. For å jobbe videre med disse faktorene opprettes de som indekser.

Det lages også indekser basert på det underliggende rammeverket. Indeksene blir generert på samme måte som spørsmålene. Der spørsmålene som hadde tilhørighet i samme celle i SABSA rammeverket ble slått sammen:

- Hva - *Eiendeler*
- Hvorfor - *Motivasjon*
- Hvordan - *Prosess*
- Hvem - *Mennesker*
- Hvor - *Lokasjon*
- Når - *Tid*

Dette reduserer tallet på 25 spørsmål til 12 indekser. Disse 12 indeksene inneholder de seks kategoriene nevnt ovenfor, inndelt i nivåene logisk- og konseptuell arkitektur.

I tillegg har det blitt laget indekser på nivåene, som er en samling av alle de seks indeksene for hvert nivå. Indeksene lages ved å regne ut medianverdien av spørsmålene og de slås sammen. Eksempelvis blir spørsmål en og to slått sammen til indeksen for konseptuell – eiendom.

5.2.2 RELIABILITET

Reliabilitetstester tar for seg hvor pålitelig måleprosessen er i henhold til tilfeldige feil. Datasettets reliabilitet kan måles ved *test-retest* metoden. Denne baserer seg på å utføre gjentatte målinger med samme måleinstrument over tid, eller på flere forskjellige utvalg av respondenter. Oppnår man samme resultat ansees måleprosessen å ha høy reliabilitet. En test-retester veldig tidkrevende, spesielt i en kvantitativ forskningsmetode, som krever et høyt antall respondenter, og faller dermed utenfor denne oppgavens omfang.

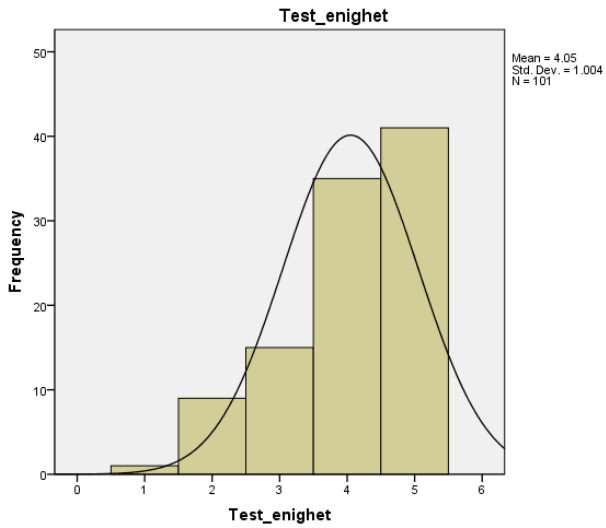
Det finnes også statistiske metoder for å regne ut reliabilitet ut i fra innhentet datasett. Det mest brukte testen er Cronbach's alpha. Cronbach`s alpha er et korrelasjonsmål, som viser hvor nært beslektede et sett av elementer er som en gruppe. Testen måler den interne konsistensen til elementene, og viser om de representerer en underliggende tendens i indeksene. (Wiik) Testen påvirkes av gjennomsnittlig korrelasjon mellom elementer og antall elementer. Et høyere antall elementer vil føre til en høyere Cronbach's Alpha verdi. Cronbach's Alpha testen gir vanligvis et resultat mellom 0 og 1, men det er mulig å oppnå negative tall som resultat i veldig store datasett. (Joseph A. Gliem 2003) Det er ønskelig å oppnå et tall over 0,7 og nærmest mulig 1. (Wiik), (Ringdal 2007)

5.2.3 VALIDITET

Validitetstester sikter på å sikre at måleprosessen måler det vi faktisk ønsker å måle. De måler datasettets gyldighet i henhold til systematiske feil og er knyttet til teoretisk sammenheng mellom begreper. Dette er i større grad en skjønnsmessig vurdering, men en forutsetning er å oppnå høy reliabilitet. (Ringdal 2007)

Spørreskjemaet er basert på SABSA rammeverket, som igjen har mange likhetstrekk med det anerkjente Zachman rammeverket. Dette gir et godt grunnlag for at de innhentede dataene skal ha høy validitet.

For å forhindre målefeil og for å sikre høy validitet har det også blitt utført pilottester av spørreskjemaet på 5 medlemmer av Dataforeningens informasjonssikkerhetsgruppe. Disse resulterte i revidering av ordbruk og eliminering av redundante spørsmål.

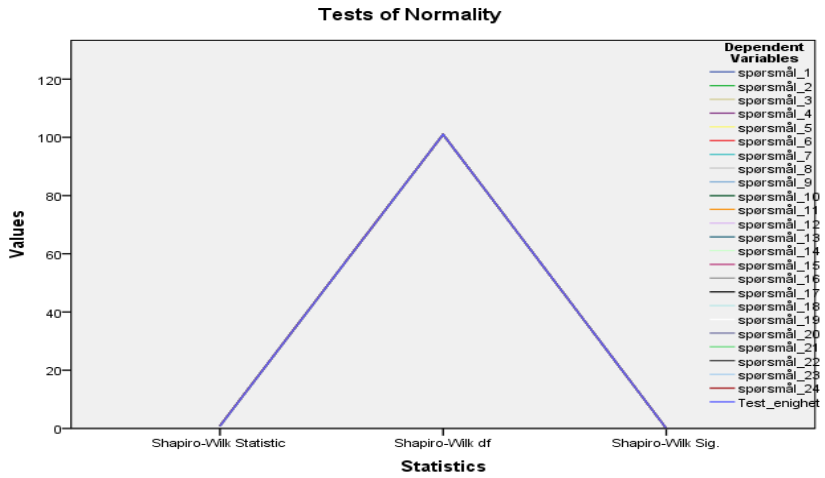


Det siste spørsmålet i spørreundersøkelsen *"Jeg har god kjennskap til virksomhetens informasjonssikkerhetstiltak"* er et testspørsmål som indikerer om respondenten anser seg selv som passende til å svare på spørreundersøkelsen. På dette spørsmålet er gjennomsnittet 4.05, noe som indikerer at respondentene anser seg selv som kunnskapsrike på dette feltet. Det høye gjennomsnittet gir oss en indikasjon på at validiteten til datasettet er høy.

Spørreundersøkelsens validitet ble sikret gjennom pilotundersøkelser med eksperter innen området. Spørsmålenes validitet sikres også av at de er nærliggende til rammeverkets definisjon av kategoriene. Disse har aktivt blitt brukt i utformingen av spørsmålene, og oversatt til termer brukt i arbeidslivet.

5.2.3 NORMALFORDELING

Det er viktig å måle om datasettets svar er normalfordelte. Om det ikke er normalfordelt kan det føre til at man må velge andre statistiske metoder enn de man hadde tenkt. Datasettets normalfordeling testes med Shapiro-Wilkes(SW) metoden, og kurtosis/skjevhet hentet fra den deskriptive statistikken i kapittel 6.



Vi ser ut i fra den genererte grafen ser normalfordelt ut. SW sammen med kurtosis/skjevhet test tilsier at datasettet er normalfordelt.

5.2.4 KORRELASJONSTEST

Korrelasjon betyr statistisk sammenheng mellom to variabler. Vi ser på hvor nærliggende spørsmålene er hverandre. For å måle korrelasjonen ble det gjennomført en korrelasjonstest med Bivariate med Pearson, som er den mest brukte testen. (University) Det kommer frem at signifikans på alle indekser er .000, statistisk signifikant på 99 % nivå. Se vedlegg for utregningen av korrelasjonstesten.

5.3 EKSPLORATIV FAKTORANALYSE

En eksplorativ analyse differensierer fra hypotesedrevet forskning ved å basere seg på at man ikke har noen forutsetninger datasettets egenskaper analysen. Der man i hypotesedrevet analyse har satt seg klare mål om hva man ønsker å undersøke på forhånd, og ønsker å bekrefte eller avkrefte dette, stiller faktoranalyse seg helt åpen til hva utfallet måtte bli. Videre analyse er drevet av de resultatene man oppnår. (Palmer)

En eksplorativ faktoranalyse ønsker å utforske datasettets underliggende sammenhenger.

Faktoranalysen bruker korrelasjonen mellom elementer til å lete etter grupperinger i datasettet. Den brukes for å identifisere klynger av intern-korrelerte variabler. Disse kalles faktorer. Det er en *multivariatstatistisk* teknikk for å undersøke korrelasjoner mellom variabler. Analysen tester teoretiske datastrukturer empirisk.

Det finnes to hovedårsaker til å bruke faktoranalyse; datareduserіng og teoridannelse.

Datareduserіng for å simplifisere datastrukturen. Hjelper med å eliminere eller identifisere elementer som kan forbedres; redundante variabler, uklare variabler og irrelevante variabler. Datareduseringen fokuserer på å teste datasettets dimensjoner, og gir en pekepinn på kvaliteten.

Faktoranalyse brukes til teoridannelse; å undersøke de underliggende korrelasjonene mellom mønstre delt av variablene for å teste teoretiske modeller. Teoridannelse fokuserer på å finne strukturer mellom variabler, for å klassifisere de sammen. Målet er å adressere et teoretisk spørsmål i motsetning til å kalkulere faktorscores. (Palmer)

5.3.1 FAKTORANALYSE

Det finnes flere måter å gjennomføre en faktoranalyse. De viktigste valgene er hvilken metode man velger for å determinere antall faktorer. Det kan være vanskelig å finne informasjon om de forskjellige metodenes styrker og svakheter, og eksperter er ofte

uenige på deres bruksområde. Dette har ført til litt forvirring rundt valget av metode for utvinning av faktorer, og er kanskje en grunn til at standardmetoden, Principal Component Analysis, ofte blir valgt. (Osborne 2005)

5.4 KLYNGEANALYSE

En klyngeanalyse benytter seg av flere statistisk metoder for å undersøke om det finnes klynger av informasjon i datasettet som har likhetstrekk eller oppfører seg likt. Klyngeanalyser brukes ofte innen markedsføring, da de er gode til å segmentere. Det finnes to hovedmåter å utføre en klyngeanalyse, hierarkisk og ikke-hierarkisk(fuzzy). Den mest populære er hierarkisk og baserer seg på å generere et tre som viser forhold mellom svar. Ikke hierarkiske metoder laget et definert punkt, som skal representere midten. Og klyngene genereres ut i fra distanse til dette sentrale punktet. Å finne dette punktet kan være vanskelig, og kan påvirkes av den som utfører analysen. Ikke-hierarkisk klyngeanalyse er dermed ikke så sikker, og kan lett vise feil.

6 - RESULTATER

Dette kapittelet vil omhandle de innhentede dataene fra spørreundersøkelsen. Først ser vi på bakgrunnsvariabler. Dette er demografisk ladet informasjon, som sier noe om respondentgruppen. Bakgrunnsvariablene blir vist gjennom deskriptiv statistikk.

Etter den beskrivende informasjonen rundt respondentenes demografi, vil vi ta en kikk på resulatetene av faktoranalysen. Faktoranalysens resultater brukes videre i klygeanalysen I klyngeanalysen vil vi se på hvordan indeksene i undersøkelsen fordeler seg i klynge, om det finnes sammenhenger og hvorvidt resultatene sammenfaller med det underliggende rammeverket for spørreundersøkelsen.

6.1 BAKGRUNNSVARIABLER

Deskriptiv statistikk gir et enkelt overblikk over respondentenes svar i spørreundersøkelsen.

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Stilling	101	1	4	2,26	1,110	,321	,240	-1,247	,476
Ansatt hvor lenge	101	,08	31,00	8,0454	6,80421	1,181	,240	1,018	,476
Sektor	101	1	2	1,42	,495	,347	,240	-1,918	,476
Antall ansatte i bedrift	101	1	5	3,44	1,539	-,448	,240	-1,257	,476
spørsmål_1	101	1	5	3,53	1,064	-,448	,240	-,364	,476
spørsmål_2	101	1	5	3,46	1,091	-,237	,240	-,616	,476
spørsmål_3	101	1	5	3,83	1,040	-,961	,240	,587	,476
spørsmål_4	101	1	5	3,19	1,111	-,025	,240	-,700	,476
spørsmål_5	101	1	5	3,50	1,026	-,467	,240	-,185	,476
spørsmål_6	101	1	5	3,24	1,305	-,123	,240	-1,073	,476
spørsmål_7	101	1	5	4,08	1,026	-1,180	,240	1,017	,476
spørsmål_8	101	1	5	4,05	1,126	-1,214	,240	,812	,476
spørsmål_9	101	1	5	3,89	1,272	-,892	,240	-,411	,476
spørsmål_10	101	1	5	3,80	1,086	-,597	,240	-,542	,476
spørsmål_11	101	1	5	2,64	1,119	,178	,240	-,708	,476
spørsmål_12	101	1	5	3,92	1,155	-,956	,240	,127	,476
spørsmål_13	101	1	5	3,73	1,094	-,848	,240	,154	,476
spørsmål_14	101	1	5	3,38	1,057	-,237	,240	-,553	,476
spørsmål_15	101	1	5	3,40	1,242	-,285	,240	-,898	,476

spørsmål_16	101	1	5	3,43	1,169	-,239	,240	-1,008	,476
spørsmål_17	101	1	5	3,39	1,183	-,314	,240	-,890	,476
spørsmål_18	101	1	5	3,25	1,178	-,384	,240	-,719	,476
spørsmål_19	101	1	5	3,57	1,178	-,575	,240	-,431	,476
spørsmål_20	101	1	5	3,56	1,178	-,475	,240	-,737	,476
spørsmål_21	101	1	5	2,89	1,207	,109	,240	-,751	,476
spørsmål_22	101	1	5	2,73	1,165	,308	,240	-,654	,476
spørsmål_23	101	1	5	3,41	1,226	-,525	,240	-,661	,476
spørsmål_24	101	1	5	3,21	1,267	-,281	,240	-1,011	,476
spørsmål_25	101	1	5	4,05	1,004	-,887	,240	,014	,476
Valid N (listwise)	101								

De borterste kolonnene, kurtosis og skjevhet viser hvordan respondentenes svar fordeler seg på den satte likertskalaen. For å kunne bruke statistiske metoder som krever normalfordeling er det anbefalt at disse ikke overstiger 1.96. Denne verdien betegnes som 1 % nivå av normalitet. (Sannes 2004) Ingen av spørsmålene i datasettet overstiger denne verdien, og vi kan dermed si at datasettet er normalfordelt.

Deskriptiv statistikk for teoribaserte indekser:

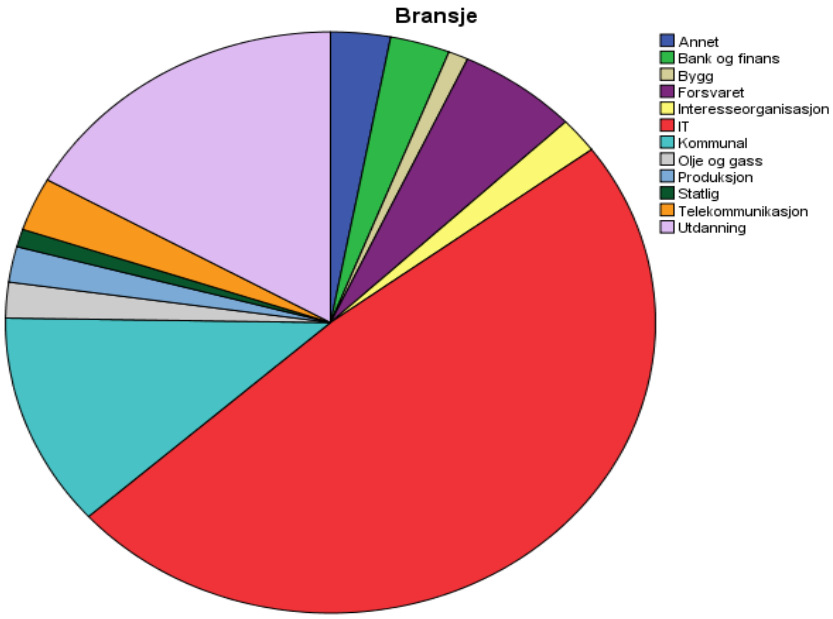
Descriptive Statistics

	N	Range	Minimum	Maximum	Sum	Mean	Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Konseptuell_What	101	4,00	1,00	5,00	353,00	3,4950	1,02346	1,047	-,279	,240	-,442	,476
Konseptuell_Why	101	4,00	1,00	5,00	354,50	3,5099	,92731	,860	-,528	,240	,277	,476
Konseptuell_How	101	4,00	1,00	5,00	340,50	3,3713	,96347	,928	-,310	,240	-,167	,476
Konseptuell_Who	101	4,00	1,00	5,00	404,67	4,0066	,91649	,840	-1,184	,240	1,469	,476
Konseptuell_Where	101	4,00	1,00	5,00	349,00	3,4554	,81066	,657	-,413	,240	-,252	,476
Konseptuell_When	101	4,00	1,00	5,00	359,00	3,5545	,91897	,845	-,568	,240	,121	,476
Logisk_What	101	4,00	1,00	5,00	344,50	3,4109	1,10543	1,222	-,206	,240	-,728	,476
Logisk_Why	101	4,00	1,00	5,00	335,00	3,3168	1,07871	1,164	-,232	,240	-,642	,476
Logisk_How	101	4,00	1,00	5,00	360,50	3,5693	1,00007	1,000	-,531	,240	-,267	,476
Logisk_Who	101	4,00	1,00	5,00	284,00	2,8119	1,08594	1,179	,265	,240	-,577	,476
Logisk_Where	101	4,00	1,00	5,00	344,00	3,4059	1,22620	1,504	-,525	,240	-,661	,476
Logisk_When	101	4,00	1,00	5,00	324,00	3,2079	1,26741	1,606	-,281	,240	-1,011	,476
Konseptuelt_nivå	101	3,86	1,14	5,00	362,50	3,5891	,77271	,597	-,581	,240	,500	,476
Logisk_nivå	101	4,00	1,00	5,00	331,60	3,2832	,90830	,825	-,382	,240	-,059	,476
Valid N (listwise)	101											

6.1.1 BRANSJE OG STILLING

For å innhente respondentens stilling og bransje ble det brukt et åpne spørsmål. Svarene ble deretter inndelt i kategorier basert på respondentens svar.

Kategoriseringen av bransje ble gjort ved å føre IT,IKT, Konsulentvirksomhet og programvareutvikling inn i paraplybegrepet IT. De andre kategoriene er forholdsvis uberørte, utenom 3 respondenter som ble lagt inn i kategorien annet.

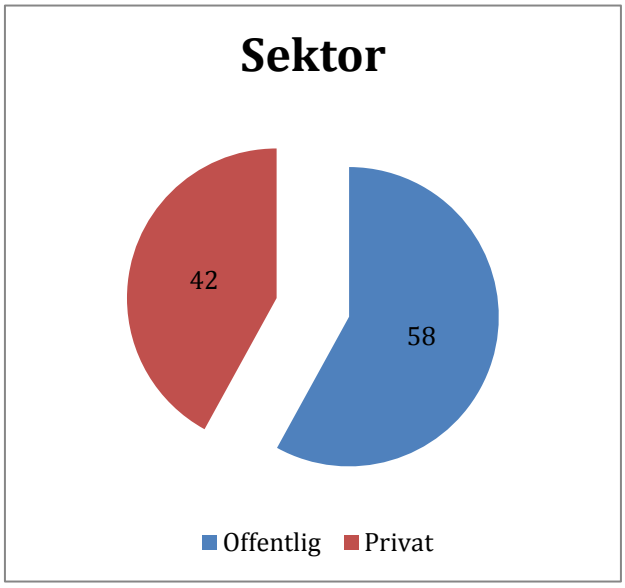


Vi ser at den største kategorien er IT, som utgjør 48,5% av respondentene. Etter fulgt av utdanning og kommunal, med henholdsvis 16,8% og 11,9%. Overblikket blir dessverre litt misvisende siden alle respondentene kunne ha svart IT, og innholdet i denne kategorien ikke er redegjort for. Utdanning inneholder for eksempel hovedsakelig IT-sjefer og ansatte ved Universiteters IT-avdeling.

Spørsmålet om stilling ble inndelt ved at kategorien leder inneholder IT-sjef, IT-leder og lignende betegnelser. Mellomleder er respondentene som har beskrevet seg selv som enhetsleder og prosjektleder. Konsulenter er fellesbetegnelsen for de fleste innen området, mens fagspesialist er de som har betegnet seg selv som sikkerhetseksperter eller sikkerhetsansvarlig.

Stilling	Antall	Prosent
Leder	33	32,7
Mellomleder	28	27,7
Konsulent	21	20,8
Fagspesialist	19	18,8
Total	101	100,0

6.1.2 SEKTOR

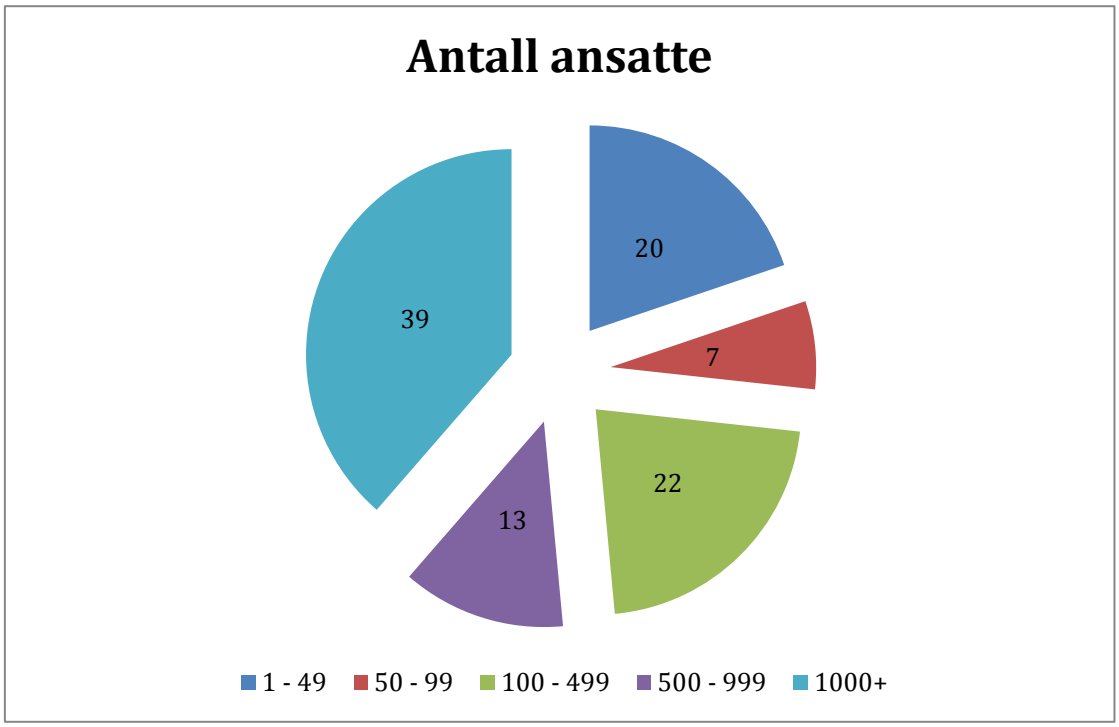


Av 101 besvarelser var 59 fra offentlige virksomheter og 42 fra private. Dette er tilsiktet fra min side da jeg opererte med en tilnærmet lik 50/50 deling ved valg av respondenter og utsendelse av spørreskjema.

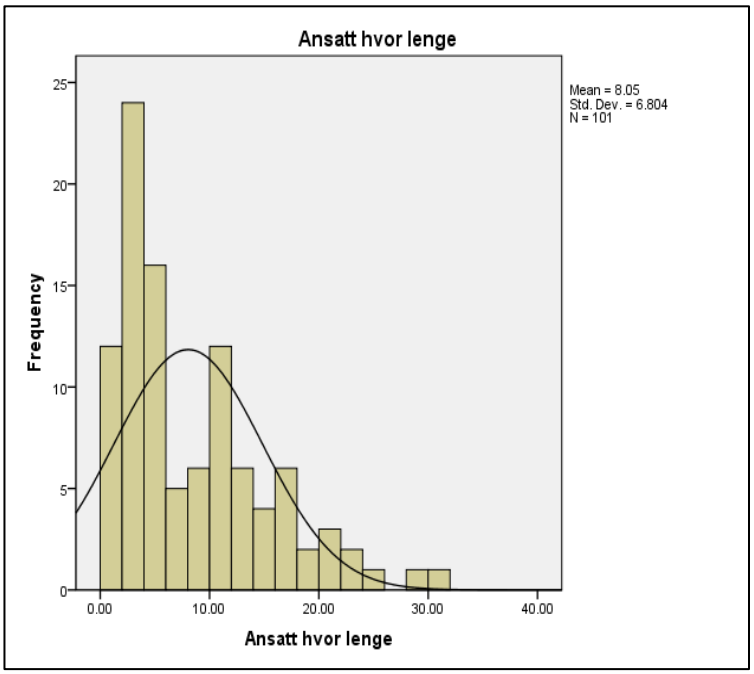
Sektor			
		Antall	Prosent
Valid	Offentlig	59	58,4
	Privat	42	41,6
	Total	101	100,0

6.1.3 ANTALL ANSATTE OG ANTALL ÅR ANSATT

Respondentene ble spurt hvor mange ansatte virksomheten de jobbet for hadde, og hvor lenge de hadde vært ansatt i gjeldende virksomhet.



Antall ansatte i virksomheten		
	Antall	Prosent
1 - 49	20	19,8
50 - 99	7	6,9
100 - 499	22	21,8
500 – 999	13	12,9
1 000+	39	38,6



Man ser at gjennomsnitt for ansettelsesperioden til respondentene litt over 8 år. De fleste jobber også i en stor virksomhet, med 1000 eller flere ansatte.

6.2 FAKTORANALYSE

For å teste om datasettet egner seg til faktoranalyse kan man bruke Kaiser-Meyer-Olkin(KMO) og Bartlett's test. I SPSS blir disse to testene kjørt samtidig og vises i samme resultat.

- KMO verdi: .919 med hele datasettet.
- KMO verdi: .947 med teoribaserte indekser.

Alle spørsmålene i spørreundersøkelsen oppnår en KMO verdi på .919, mens de teoribaserte indeksene får en enda høyrer score på .947. Dette er veldig høyt og viser at datasettet egner seg til faktoranalyse.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,919
Bartlett's Test of Sphericity	Approx. Chi-Square	1605,467
	df	276
	Sig.	,000

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,947
Bartlett's Test of Sphericity	Approx. Chi-Square	883,738
	df	66
	Sig.	,000

Bakgrunnsvariabler og spørsmål 25 er ikke tatt med i faktoranalysen, da de ikke har noen tilknytning til det teoretiske rammeverket.

METODE FOR FAKTORANALYSE

Den mest brukte metoden er *Principal Component Analysis* (PCA). PCA er standardmetoden for faktoranalyse i både SPSS og SAS, men det diskuteres om den kan kalles en ekte faktoranalyse i det hele tatt. Grunnen til at den ble så populær å bruke er hovedsakelig fordi det er en datareduksjonsmetode som krever lite datakraft, og derfor er lett tilgjengelig og enkel å bruke for alle. Dette er ikke et problem med dagens datamaskiner. (Osborne 2005)

Generelt sett er det anbefalt å bruke *Maximum Likelihood* om datasettet er normalfordelt og *Principal Factor Axis* om datasettet er veldig lite normalfordelt, men flere er uenige i dette og mener at andre metoder er bedre. Det er dog lite dokumentert at en utvinningsmetode er bedre enn en annen. (Osborne 2005)

Neste steg i analysen er å se på hvor mange faktorer metoden gir. Dette er en til dels subjektiv tilnærming, men det finnes måter man kan bruke for å hjelpe bestemme antall. Det to mest brukte hjelpemåtene er Kaiser-Guttmann kriteriet og albuemetoden. Disse mener A.B. Costello og J.W. Osborne er dårlige kriterier å bruke, og vil som oftest gjengi for mange faktorer. De anbefaler Velicer's MAP kriteriet og Parallell Analyse. Om

man ikke har de to overnevnte tilgjengelig anbefaler de albuemetoden, eller Scree-Test som det også kalles. (Osborne 2005)

Man må så velge rotasjonsmetode, hensikten med rotasjonsmetoden er å klarifisere de underliggende dataene. Dette er det steget som har minst å si for utfallet av analysen. Den mest brukte metoden er Varimax rotasjon, men også Direct Oblimin er ofte brukt. Den største forskjellen mellom de to er at Varimax rotasjonen, som er en ortogonal metode, produserer faktorer som ikke er korrelerte.

Direct Oblimin, en Oblique metode, produserer korrelerte faktorer. A.B. Costello og J.W. Osborne anbefaler å bruke en Oblique metode i samfunnsvitenskapelig forskning. Siden det ofte er er vanlig å forvente en viss korrelering mellom elementene. Man vil da miste viktig informasjon om man velger en ikke- korrelerende rotasjonsmetode. En Oblique metode vil da i teorien produsere et bedre resultat som også lar seg reprodusere lettere. (Osborne 2005)

6.2.1 ANTALL FAKTORER

I dette arbeidet, basert på en eksplorativ tilnærming, har det blitt brukt det blitt brukt tre metoder for å utvinne faktorer. Det var interessant å se på forskjeller mellom de tre metodene. Alle tre har brukt Direct Oblimin som rotasjonsmetode. Det har også blitt testet med Varimax rotasjon, men det resulterte i nesten identiske faktorer som med Direct Oblimin.

Principal Component Analysis (PCA)

Principal Component Analysis							
Faktor 1:	Eiendeler(1)	Eiendeler(2)	Motivasjon(3)	Motivasjon(4)	Motivasjon(5)	Prosess(7)	Mennesker(8)
	Mennesker(10)	Lokasjon(11)	Lokasjon(12)	Tid(13)	Eiendel(16)	Motivasjon(17)	Prosess(20)
Faktor 2:	Eiendeler(15)	Motivasjon(18)	Prosess(19)	Mennesker(21)	Mennesker(22)	Lokasjon(23)	Tid(24)
Faktor 3:	Prosess(6)	Tid(14)					
Faktor 4:	Mennesker(9)						

Principal Factor Axis (PFA)

Principal Axis Factoring							
	Prosess(6)	Lokasjon(11)	Tid(13)	Tid(14)	Eiendeler(15)	Eiendel(16)	Motivasjon(17)
Faktor 1:	Motivasjon(18)	Lokasjon(23)	Tid(24)				
Faktor 2:	Mennesker(21)	Mennesker(22)					
Faktor 3:	Prosess(7)	Mennesker(8)	Mennesker(9)	Mennesker(10)	Lokasjon(12)		
Faktor 4:	Eiendeler(1)	Eiendeler(2)	Motivasjon(3)	Motivasjon(4)	Motivasjon(5)		

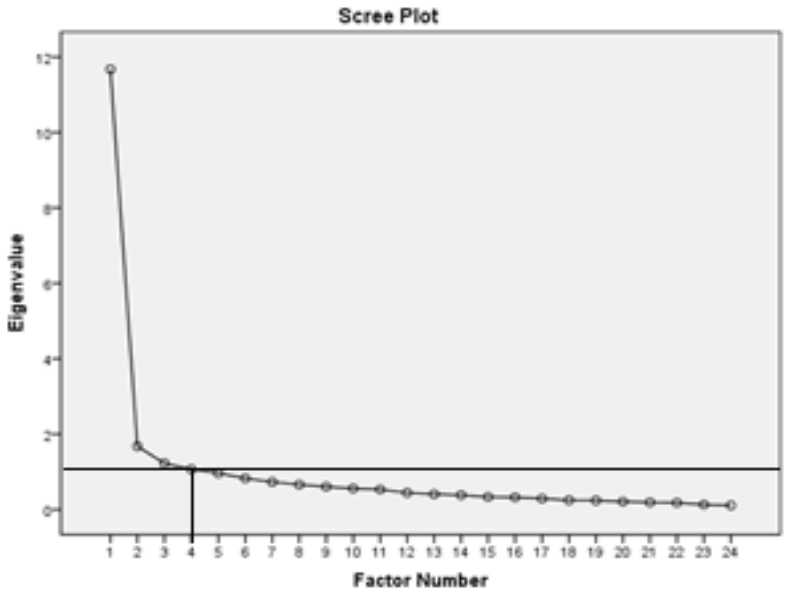
Maximum-Likelihood.

Maximum-Likelihood							
Faktor 1:	Eiendeler(1)	Eiendeler(2)	Motivasjon(3)	Motivasjon(4)	Motivasjon(5)	Tid(13)	
Faktor 2:	Mennesker(21)	Mennesker(22)					
Faktor 3:	Prosess(7)	Mennesker(8)	Mennesker(9)	Mennesker(10)	Lokasjon(12)	Prosess(20)	Prosess(6)
	Lokasjon(11)	Tid(14)	Eiendeler(15)	Eiendel(16)	Motivasjon(17)	Motivasjon(18)	
Faktor 4:	Prosess(19)	Lokasjon(23)	Tid(24)				

Konseptuell arkitektur
Logisk arkitektur

Som vi ser over resulterer alle metodene i 4 faktorer. De gir noe tilsvarende resultat for noen av faktorene, men det finnes fortsatt et stort avvik. Det er anbefalt å ha en faktorladning over 0,5. PCA, som egentlig ikke kan betegnes som en fullstendig faktoranalyse, gjør ikke forskjell på delt og unik varianse mellom faktorene og PAF regnes som å være best egnet til datasett som ikke er normalfordelt. I videre analyse brukes det derfor Maximum-Likelihood, som er den anbefalte metoden. (Osborne 2005) Det må noteres at jeg måtte utvide rotasjonummeret, fra det normale 25 til 35 for å få resultat.

Det brukes *Kaiser-Guttman* kriteriet, som velger bort elementer med eigenvalue over 1, og Albuemetoden for å sjekke antall faktorer funnet av Maximum-Likelihood. Verken Velcier's MAP kriteriet' eller Parallell Analyse er tilgjengelig i versjon 18 av SPSS, og har dermed ikke blitt testet.



Man bruker en *Scree Plot test*, også kalt albuemetoden, for å verifisere antall faktorer. I SPSS kan man velge å få ut et Scree Plot sammen med faktoranalysen. Grafen viser Eigenvalue mot antall faktorer og baserer seg på hvor stor del av variansen hver enkelt faktor står for. Desto lenger man kommer ut i faktornummer, desto mindre del står de for. Vi ser at grafen sakte men sikkert blir rettere.

Ut i fra dette Scree Plottet bruker man *Kaiser-Guttman,* som sier at faktorene skal ha en eigenvalue over 1. Det kan det av og til være vanskelig å skille hvor mange faktorer det finnes i datasettet ved å se på et Scree Plot, men det er ganske tydelig i dette tilfellet at 4 faktorer er korrekt.

6.2.2 RELIABILITET TIL FAKTORENE

For å sikre reliabiliteten til faktorene funnet i analysen ble de omgjort til indekser og testet med Cronbach`s alpha.

Cronbach's alpha på faktorindekser	
Faktor 1:	.909
Faktor 2:	.806
Faktor 3:	.814
Faktor 4:	.907

Vi ser at alle indeksene har en alfa verdi over .7, som er anbefalt.

6.2.3 INDEKSER BASERT PÅ TEORI

Cronbach`s alpha						
Nivå	Hvorfor - Eiendeler	Hva - Motivasjon	Hvordan- Prosess	Hvem - Mennesker	Hvor - Lokasjon	Når – Tid
Konseptuell	.892	.790	.755	.733	.652	.347
Logisk	.629	.682	.802	.613	.806	.761

Konseptuelt nivå	.913
Logisk nivå	.922

Cronbach`s alpha test har blitt kjørt på alle de genererte indeksene, og vi ser en gjennomsnittlig høy verdi. Dette betyr at indeksene har høy reliabilitet.

Vi så i det forrige kapittelet at det er anbefalt at sammensatte indekser har en Cronbach`s alpha verdi høyere enn .700.En verdi på over .7 blir betegnet som veldig god, .5 som god og .3 og lavere som dårlig.

I tabellen ser vi at åtte av tolv indekser tilfredsstiller dette målet, mens fire ikke gjør det. Det er bemerkelsesverdig at Konseptuell – Tid bare har en verdi på .347, denne er veldig lav. Dette er så lavt at den kanskje burde fjernes fra videre analyse.

6.2.4 FAKTORANALYSE MED TEORETISKE INDEKSER

Det ble også kjørt PCA, PFA og Maximum-Likelihood på indeksene generert ut i fra det teoretiske rammeverket. Alle testene resulterte i bare en faktor, selv om de hadde høy KMO verdi.

6.3 KLYNGEANALYSE

Fra faktoranalysen fikk vi rede på at datasettet inneholdt 4 faktorer, disse faktorene tas med i videre evaluering av datasettet og brukes i klyngeanalysen.

En klyngeanalyse sikter på samme måte som en faktoranalyse å se på underliggende faktorer for et datasett, og se om det kan finnes uforutsette sammenhenger. Klyngeanalysen ønsker å sette dataene sammen i grupper, som har fellestrekk. Typisk har medlemmene i en klynge liten distanse mellom hverandre, tilhører et område med høy tetthet, følger en viss satt intervall, eller følger en statistisk distribusjon. (Sambamoorthi)

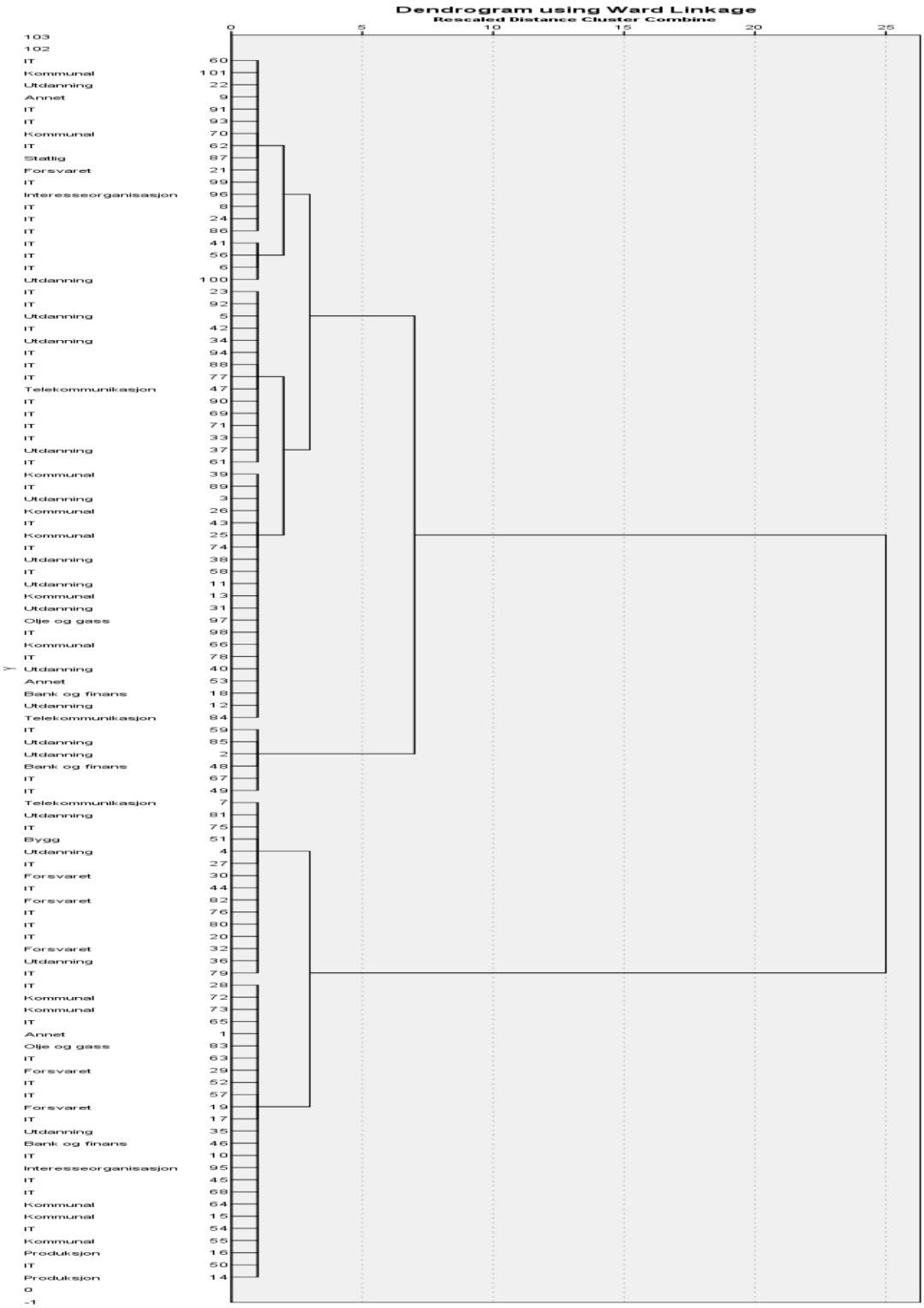
Et godt utgangspunkt for å hente ut antall klynger er resultatet fra faktoranalysen, men en kan også bruke hierarkisk klyngeanalyse.

6.3.1 HIERARKISK ANALYSE

Dette er en type klyngeanalyse som ofte gjennomføres først. Den viser datasettet og resulterer i et dendrogram. Dendrogrammet viser datasettet medlemskap i de forskjellige klyngene. Det er oppsummeringen av den agglomerative prosessen. I dendrogrammet vises de som vanlig klynger med lite medlemskap, disse er det anbefalt å fjerne i videre statistisk arbeid.

Ut i fra dendrogrammet under ser vi at det skapes ni klynger, men at fen av dem er små. Disse anbefales da å trekkes vekk i videre arbeid. De er såkalt svake klynger, som inneholder bare en liten del av datasettet. Når vi tar bort de svake klyngene ender vi opp med fire, altså like mange som faktoranalysen ga oss. Dedrogrammet ligger i vedlegg.

6.3.1.1KLYNGE BASERT PÅ BRANSJE



Vi ser at det danner seg åtte klynger, hvorav fire er veldig små. Dette samsvarer med faktoranalysen.

6.3.1.2 KLYNGE BASERT PÅ SEKTOR

Klyngeanalyse basert på sektor trekker seg mer og mer sammen og dataene samler seg rundt de to sektorene som er mulig å velge. Jeg vet ikke om dette kommer av at det spørsmålet bare har to svaralternativer, eller om de faktisk viser en signifikant tendens til at respondenter fra samme sektor svarer likt.

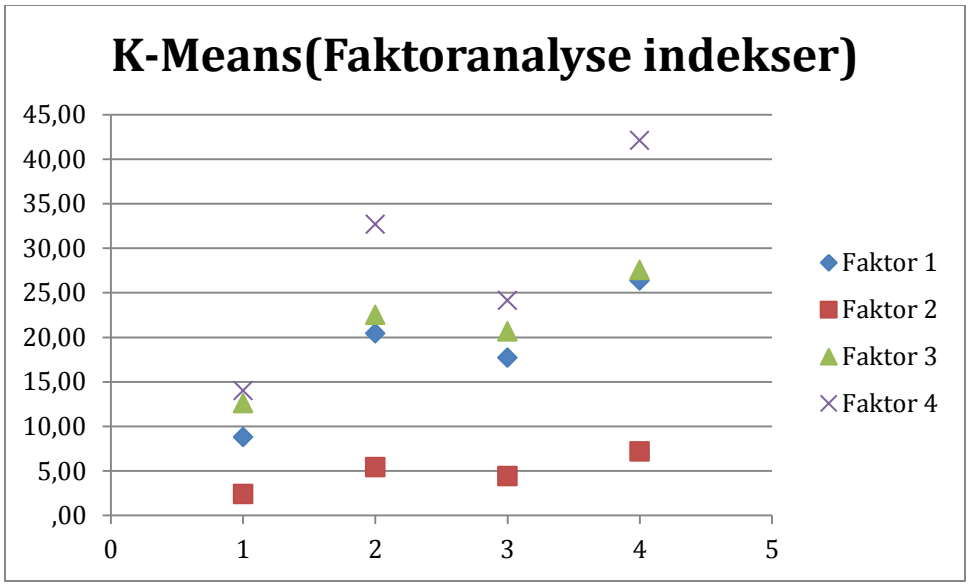
6.3.2 K-MEANS KLYNGEANALYSE

Etter flere gjenomkjøringer av K-Means analysen, ser det ut til at man ender opp med klynger som har lite innhold om man velger mer enn to. Two-Step analysen bekrefter dette.

K-Means med 4 klynger spesifisert, basert på indeksene fra faktoranalysen:

Final Cluster Centers

	Cluster			
	1	2	3	4
Faktor 1	8.80	20.44	17.72	26.37
Faktor 2	2.40	5.42	4.40	7.17
Faktor 3	12.60	22.53	20.64	27.54
Faktor 4	14.00	32.69	24.12	42.09

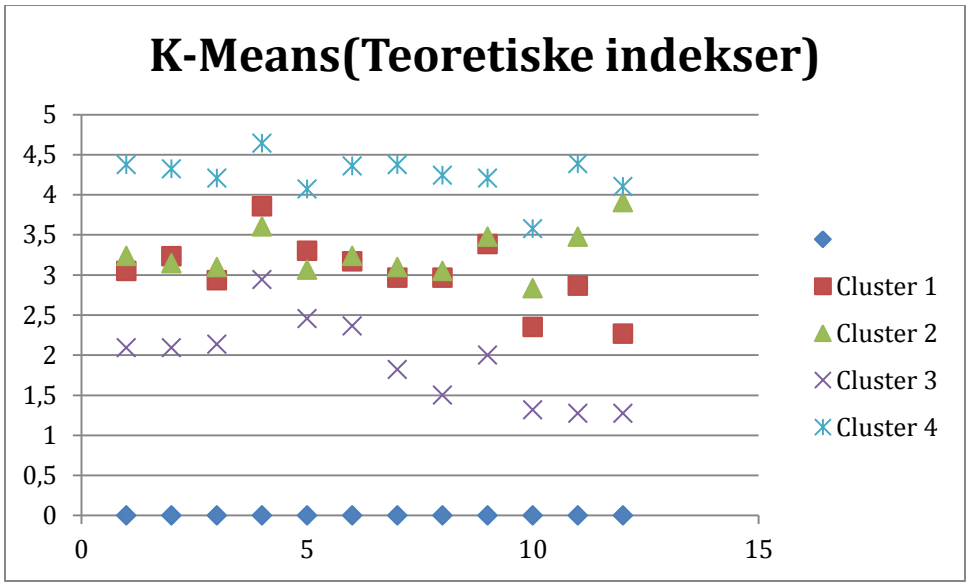


Vi ser at klynge to og tre er veldig like hverandre.

K-Means på teoretisk baserte indekser:

Final Cluster Centers

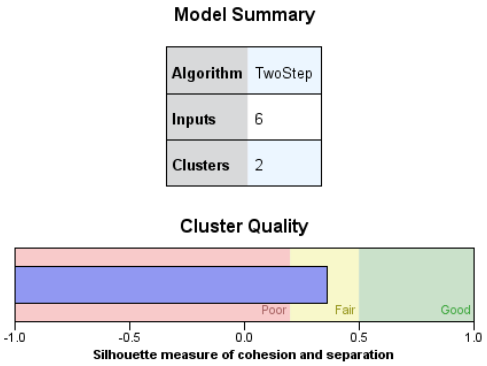
	Cluster			
	1	2	3	4
Eiendeler(K)	3.05	3.24	2.09	4.37
Motivasjon(K)	3.23	3.14	2.09	4.32
Prosess(K)	2.93	3.10	2.14	4.21
Mennesker(K)	3.86	3.60	2.94	4.64
Lokasjon(K)	3.30	3.06	2.45	4.07
Tid(K)	3.17	3.24	2.36	4.36
Eiendeler(L)	2.97	3.10	1.82	4.37
Motivasjon(L)	2.97	3.05	1.50	4.24
Prosess(L)	3.38	3.48	2.00	4.21
Mennesker(L)	2.35	2.83	1.32	3.58
Lokasjon(L)	2.87	3.48	1.27	4.38
Tid(L)	2.27	3.90	1.27	4.10



Vi ser at klynge en og to er veldig nærliggende hverandre. De to indeksene er ikke helt målbare, siden de ikke bruker samme måleparameter, men vi ser fortsatt at det finnes likheter mellom de to diagrammene.

6.3.3 TWO-STEP CLUSTER

Med indeksene fra faktoranalysen som kontinuerlige variabler og sektor og antall ansatte som kategoriske variabler ser vi at Two-Step metoden får to klynger.



Det samme resultatet oppnås egentlig samme hvilke premisser jeg setter for Two-Step analysen, så lenge bare 3 kategoriske variabler velgers for begge indekssettene. Velger en flere finner ikke metoden noen klynger.

7 - KONKLUSJON

Informasjonssikkerhet er et voksende område, og får stadig større plass i virksomheters strategi. Dagens økende utfordringer krever et helhetlig syn på sikkerhet. Ved å inkludere det som en del av virksomhetsarkitekturen. Jeg har i dette arbeidet prøvd å finne ut i hvilken grad norske virksomheter hadde begynt arbeidet med å innføre sikkerhetsprinsipper i sin virksomhetsarkitektur. Jeg hadde forventet en større spredning i svarene, og trodde at jeg kunne vise at kanskje større virksomheter trengte mere abstraksjon og styring. At de hadde en større trang for modellering av komplekse informasjonsflyter og sikkerhetsløsningene de har knyttet til seg.

Uheldigvis finner jeg ikke data som støtter dette i svarene fra spørreundersøkelsen. Den deskriptive statistikken viser at alle spørsmålene er normalfordelte, og faktoranalysen viser at de er alle svært nærliggende. Spesielt da jeg knyttet sammen spørsmålene til teorien de ble laget fra.

Dette kan være en følge av at SABSA rammeverkets nivåer har mange likheter, spesielt på konseptuelt og logisk nivå. Jeg hadde problemer med å lage spørsmål som skilte seg fra hverandre. Motivasjon – Konseptuell og Motivasjon – Logisk ble veldig like, i starten. Jeg prøvde da å skille de fra hverandre, med hjelp av pilottesting, men det kan virke som om det henger igjen.

Faktoranalysen fant dog fire faktorer, med Maximum-Likelihood på alle teoribaserte spørsmål. Disse plasserte i faktorene i henhold til nivåene i rammeverket, hvor bare et spørsmål av logisk og et av konseptuell lå med spørsmål fra det andre nivået. Dette kan tyde på at vi kan skimte litt av rammeverkets inndeling i resultatene.

For å differensiere svarene bedre kunne det kanskje vært interessant å tatt to nivåer som ikke etterfulgte hverandre.

Respondenter er hovedsakelig personer i ledelsesstillinger. Hele 60 % har svart at det innehar en leder-, eller mellomlederstilling i virksomheten de arbeider. Dette gir egentlig oppgaven et ovenfra-og-ned(top-down) syn på problemområdet. Dette var i utgangspunktet ønskelig. I gjennomsnitt har respondentene arbeidet i den samme

virksomheten i 8 år. Dette er et rimelig høyt tall, og viser at de sannsynligvis har vært med på flere initiativer rundt informasjonssikkerhet. Dette kan også ha hatt innvirkninger på hvorfor svarene ble så like. 48,5 % av respondentene sier at de jobber innenfor IT-bransjen. Dette er også noe som var ønskelig, man får da respondenter som har mye kompetanse på området og kunne mest sannsynlig gi gode svar. I ettertid kunne det vært spennende å sett om andre bransjer har samme syn.

Informasjonssikkerhet i seg selv er også et vanskelig tema å behandle, jeg tror at respondenter ikke nødvendigvis er helt ærlige når de svarer på spørsmålene.

7.1 TILBAKEMELDINGER FRA SPØRREUNDERSØKELSEN

Tilbakemeldingene fra kommentarfeltet i spørreundersøkelsen var veldig forskjellige. De fleste ønsket meg lykke til. Fire var veldig positive til undersøkelsen, mens flere var negative. De negative tilbakemeldingene gikk hovedsakelig ut på at de ikke følte seg skikket til å svare på en slik undersøkelse. Dette er litt merkelig i og med at tallene viser det de gjør. Hele fem personer tok seg tid til å sende meg en personlig e-post der det forteller at «Det ikke er slik vi jobber med sikkerhet..». Disse ble ikke besvart etter en forklarende mail fra meg. Hovedsakelig kom disse tilbakemeldingene fra personer i mindre virksomheter. Eksperter fra virksomheter som EDB Ergogroup og Mnemonic var på den andre siden veldig positive.

Det man kan ta ut fra kommentarfeltet er at sikkerhet og virksomhetsarkitektur kanskje ikke er et fagfelt som har kommet spesielt langt. Dette ser man ut i fra den tilgjengelige teorien også.

7.2 VIDERE ARBEID

Siden det ikke har blitt utført undersøkelser på samme problemområde før, med samme premisser kunne det vært bra å gjennomføre samme undersøkelse på personer utenfor ledelsessegmentet i virksomheten, for å se om de har samme oppfatning som ledelsen.

Det kan hende at ledelsen har vært med på å skape og definere mye av sikkerhetsarbeidet etterspurt i undersøkelsen, og dermed føler at disse tingene er på plass. Det kunne vært interessant å se om svarene hadde hatt en annen spredning om bare ansatte

The Open Group, som lager TOGAF, annonserte i april 2010 et samarbeid ned SABSA. De har satt sammen en gruppe med spesialister som skal fokusere på å transformere SABSA elementer om til TOGAF artefakter og i november 2011 kom whitepaperet «TOGAF and SABSA Integration».(TOGAF 2011) Det kunne derfor vært interessant å sett nærmere på denne sammenkoblingen og undersøkt hvordan virksomheter som i dag bruker TOGAF, som Helse-Vest, vil implementere SABSA prinsipper i sin virksomhetsarkitektur. SABSA, som kommentarene til spørreundersøkelsen viser er relativt ukjent i næringslivet i dag, vil forhåpentligvis også modne med dette.

VEDLEGG

Vedlegg inneholder utregninger produsert i SPSS.

KORRELASJON

Correlations

		Konseptuell_What	Konseptuell_Why	Konseptuell_How	Konseptuell_Who	Konseptuell_Where	Konseptuell_When	Logisk_What	Logisk_Why	Logisk_How	Logisk_Who	Logisk_Where	Logisk_When	Konseptuelt_nivå	Logisk_nivå
Konseptuell_What	Pearson Correlation	1	,777	,757	,563	,611	,726	,649	,685	,540	,514	,607	,540	,861	,720
	Sig. (2-tailed)		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	104,748	73,755	74,686	52,837	50,728	68,277	73,455	75,658	55,285	57,156	76,203	70,104	68,116	66,942
	Covariance	1,047	,738	,747	,528	,507	,683	,735	,757	,553	,572	,762	,701	,681	,669
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Konseptuell_Why	Pearson Correlation	,777	1	,726	,555	,648	,659	,640	,684	,595	,486	,643	,513	,847	,724
	Sig. (2-tailed)	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	73,755	85,990	64,879	47,160	48,711	56,196	65,589	68,433	55,181	48,938	73,094	60,292	60,661	60,967
	Covariance	,738	,860	,649	,472	,487	,562	,656	,684	,552	,489	,731	,603	,607	,610
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Konseptuell_How	Pearson Correlation	,757	,726	1	,588	,667	,725	,656	,665	,546	,552	,633	,554	,869	,733
	Sig. (2-tailed)	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	74,686	64,879	92,827	51,919	52,087	64,208	69,842	69,119	52,651	57,804	74,777	67,703	64,658	64,131
	Covariance	,747	,649	,928	,519	,521	,642	,698	,691	,527	,578	,748	,677	,647	,641
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Konseptuell_Who	Pearson Correlation	,563	,555	,588	1	,639	,589	,576	,553	,598	,413	,558	,352	,804	,626
	Sig. (2-tailed)	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	52,837	47,160	51,919	83,996	47,474	49,630	58,393	54,622	54,787	41,125	62,729	40,861	56,964	52,145
	Covariance	,528	,472	,519	,840	,475	,496	,584	,546	,548	,411	,627	,409	,570	,521
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Konseptuell_Where	Pearson Correlation	,611	,648	,687	,639	1	,644	,578	,554	,497	,416	,540	,449	,842	,617
	Sig. (2-tailed)	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	50,728	48,711	52,087	47,474	65,716	47,995	51,766	48,426	40,312	36,653	53,660	46,102	52,758	45,408
	Covariance	,507	,487	,521	,475	,657	,480	,518	,484	,403	,367	,537	,461	,528	,454
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Konseptuell_When	Pearson Correlation	,726	,659	,725	,589	,644	1	,728	,681	,573	,436	,606	,587	,844	,733
	Sig. (2-tailed)	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	68,277	56,196	64,208	49,630	47,995	84,450	73,990	67,507	52,619	43,535	68,267	68,356	59,938	61,193
	Covariance	,683	,562	,642	,496	,480	,845	,740	,675	,526	,435	,683	,684	,599	,612
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Logisk_What	Pearson Correlation	,649	,640	,656	,576	,578	,728	1	,768	,623	,521	,680	,613	,749	,865
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	73,455	65,589	69,842	58,393	51,766	73,990	122,198	91,601	68,874	62,557	92,153	85,871	64,016	86,849
	Covariance	,735	,656	,698	,584	,518	,740	1,222	,916	,689	,626	,922	,859	,640	,868
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Logisk_Why	Pearson Correlation	,685	,684	,665	,553	,554	,681	,768	1	,672	,585	,677	,617	,746	,890
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	75,658	68,433	69,119	54,622	48,426	67,507	91,601	116,361	72,532	68,520	89,510	84,347	62,184	87,189
	Covariance	,757	,684	,691	,546	,484	,675	,916	1,164	,725	,685	,895	,843	,622	,872
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Logisk_How	Pearson Correlation	,540	,595	,546	,598	,497	,573	,623	,672	1	,509	,609	,493	,663	,804
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000	,000
	Sum of Squares and Cross-products	55,285	55,181	52,651	54,787	40,312	52,619	68,874	72,532	100,015	55,317	74,658	62,545	51,198	73,068
	Covariance	,553	,552	,527	,548	,403	,526	,689	,725	1,000	,553	,747	,625	,512	,731
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Logisk_Who	Pearson Correlation	,514	,486	,552	,413	,416	,436	,521	,585	,509	1	,584	,545	,552	,772
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000	,000
	Sum of Squares and Cross-products	57,156	48,938	57,804	41,125	36,653	43,535	62,557	68,520	55,317	117,926	77,713	74,950	46,300	76,130
	Covariance	,572	,489	,578	,411	,367	,435	,626	,685	,553	1,179	,777	,750	,463	,761
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Logisk_Where	Pearson Correlation	,607	,643	,633	,558	,540	,606	,680	,677	,609	,584	1	,614	,704	,821
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000	,000
	Sum of Squares and Cross-products	76,203	73,094	74,777	62,729	53,660	68,267	92,153	89,510	74,658	77,713	150,356	95,475	66,704	91,390
	Covariance	,762	,731	,748	,627	,537	,683	,922	,895	,747	,777	1,504	,955	,667	,914
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Logisk_When	Pearson Correlation	,540	,513	,554	,352	,449	,587	,613	,617	,493	,545	,614	1	,579	,757
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000	,000
	Sum of Squares and Cross-products	70,104	60,292	67,703	40,861	46,102	68,356	85,871	84,347	62,545	74,950	95,475	160,634	56,700	87,153
	Covariance	,701	,603	,677	,409	,461	,684	,859	,843	,625	,750	,955	1,606	,567	,872
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Konseptuelt_nivå	Pearson Correlation	,861	,847	,869	,804	,842	,844	,749	,746	,663	,552	,704	,579	1	,813
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000		,000
	Sum of Squares and Cross-products	68,116	60,661	64,658	56,964	52,758	59,938	64,016	62,184	51,198	46,300	66,704	56,700	59,708	57,080
	Covariance	,681	,607	,647	,570	,528	,599	,640	,622	,512	,463	,667	,567	,597	,571
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101
Logisk_nivå	Pearson Correlation	,720	,724	,733	,626	,617	,733	,865	,890	,804	,772	,821	,757	,813	1
	Sig. (2-tailed)	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	,000	
	Sum of Squares and Cross-products	66,942	60,967	64,131	52,145	45,408	61,193	86,849	87,189	73,068	76,130	91,390	87,153	57,080	82,501
	Covariance	,669	,610	,641	,521	,454	,612	,868	,872	,731	,761	,914	,872	,571	,825
	N	101	101	101	101	101	101	101	101	101	101	101	101	101	101

FAKTORANALYSE

Principal Component Analysis

Pattern Matrixa

	Component			
	1	2	3	4
spørsmål_1	,763	-,085	-,180	-,171
spørsmål_2	,780	-,135	-,124	-,162
spørsmål_3	,672	-,129	,051	,029
spørsmål_4	,507	-,248	-,267	-,139
spørsmål_5	,802	-,108	-,016	-,160
spørsmål_6	,144	-,219	-,509	,294
spørsmål_7	,605	-,052	-,152	,254
spørsmål_8	,612	-,241	,241	,254
spørsmål_9	-,040	-,066	-,218	,881
spørsmål_10	,458	-,288	,328	,249
spørsmål_11	,102	-,033	-,721	,209
spørsmål_12	,857	,295	,042	,185
spørsmål_13	,786	,102	-,208	,125
spørsmål_14	,188	-,323	-,512	-,040
spørsmål_15	,256	-,534	-,220	-,046
spørsmål_16	,660	-,245	-,051	-,080
spørsmål_17	,407	-,436	-,163	-,003
spørsmål_18	,279	-,579	-,112	-,058
spørsmål_19	,019	-,681	,204	,147
spørsmål_20	,398	-,486	,147	,225
spørsmål_21	-,022	-,742	-,018	,133

spørsmål_22	-,151	-,823	-,161	-,061
spørsmål_23	,234	-,585	-,176	,058
spørsmål_24	,178	-,599	-,201	-,185

Principal Axis Factoring

Pattern Matrixa

	Factor			
	1	2	3	4
spørsmål_1	,200	-,098	-,060	-,721
spørsmål_2	,148	-,145	-,040	-,762
spørsmål_3	-,003	-,131	,234	-,506
spørsmål_4	,412	-,114	-,026	-,399
spørsmål_5	-,009	-,190	,036	-,746
spørsmål_6	,416	-,077	,129	-,149
spørsmål_7	,274	,090	,422	-,287
spørsmål_8	-,034	-,081	,671	-,219
spørsmål_9	,057	,027	,523	,062
spørsmål_10	-,162	-,189	,492	-,238
spørsmål_11	,356	-,087	-,059	-,228
spørsmål_12	,026	,249	,382	-,487
spørsmål_13	,289	,190	,271	-,519
spørsmål_14	,849	,049	-,052	-,024
spørsmål_15	,665	-,127	,198	,037
spørsmål_16	,351	-,038	,233	-,354
spørsmål_17	,449	-,156	,185	-,214
spørsmål_18	,375	-,321	,167	-,127
spørsmål_19	,258	-,204	,353	,126

spørsmål_20	,161	-,202	,556	-,083
spørsmål_21	-,019	-,649	,180	-,109
spørsmål_22	,138	-,746	-,069	-,056
spørsmål_23	,410	-,316	,215	-,093
spørsmål_24	,458	-,326	,002	-,101

Maximum-Likelihood

Pattern Matrixa

	Factor			
	1	2	3	4
spørsmål_1	,714	,110	-,007	-,160
spørsmål_2	,813	,179	-,015	-,071
spørsmål_3	,520	,113	,259	,011
spørsmål_4	,400	,092	-,045	-,426
spørsmål_5	,616	,152	,145	-,069
spørsmål_6	,244	,125	,044	-,334
spørsmål_7	,264	-,055	,422	-,270
spørsmål_8	,150	,035	,701	-,074
spørsmål_9	-,046	,023	,499	-,026
spørsmål_10	,168	,157	,542	,094
spørsmål_11	,166	,099	-,063	-,380
spørsmål_12	,435	-,228	,402	-,049
spørsmål_13	,475	-,165	,268	-,301
spørsmål_14	,138	-,013	-,169	-,757
spørsmål_15	-,136	,003	,160	-,863
spørsmål_16	,258	-,049	,244	-,496

spørsmål_17	,236	,096	,117	-,514
spørsmål_18	,075	,249	,161	-,476
spørsmål_19	-,132	,132	,268	-,376
spørsmål_20	,137	,168	,480	-,213
spørsmål_21	,078	,668	,191	-,004
spørsmål_22	,054	,785	-,060	-,118
spørsmål_23	,050	,261	,186	-,505
spørsmål_24	,084	,276	-,008	-,507

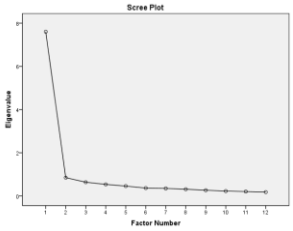
Faktoranalyse teoribasert indeks

Factor Score Coefficient Matrix

	Factor
	1
Konseptuell_What	,114
Konseptuell_Why	,111
Konseptuell_How	,140
Konseptuell_Who	,064
Konseptuell_Where	,076
Konseptuell_When	,116
Logisk_What	,127
Logisk_Why	,147
Logisk_How	,080
Logisk_Who	,053
Logisk_Where	,116
Logisk_When	,055

Communalities

	Initial
Konseptuell_What	,722
Konseptuell_Why	,704
Konseptuell_How	,706
Konseptuell_Who	,560
Konseptuell_Where	,583
Konseptuell_When	,701
Logisk_What	,700
Logisk_Why	,716
Logisk_How	,564
Logisk_Who	,471
Logisk_Where	,624
Logisk_When	,529



HIERARKISK KLYNGEANALYSE

Case Processing Summary[a]

Cases					
Valid		Missing		Total	
N	Percent	N	Percent	N	Percent
101	100.0	0	.0	101	100.0

a. Ward Linkage

Agglomeration Schedule

Stage	Cluster Combined		Coefficients	Stage Cluster First Appears		Next Stage
	Cluster 1	Cluster 2		Cluster 1	Cluster 2	
1	75	81	.681	0	0	16
2	30	82	1.486	0	0	37
3	40	69	2.514	0	0	26
4	54	95	3.569	0	0	56
5	19	52	4.625	0	0	12
6	32	36	5.736	0	0	36
7	13	18	6.917	0	0	15
8	79	80	8.139	0	0	13
9	26	99	9.375	0	0	51
10	14	16	10.778	0	0	14
11	35	46	12.250	0	0	59
12	19	83	13.750	5	0	52
13	76	79	15.417	0	8	36
14	14	55	17.125	10	0	38
15	13	88	18.833	7	0	34
16	7	75	20.542	0	1	55
17	45	63	22.264	0	0	64

18	48	49	23.986	0	0	77
19	15	72	25.722	0	0	28
20	37	71	27.472	0	0	30
21	43	60	29.361	0	0	42
22	50	68	31.472	0	0	38
23	8	24	33.653	0	0	58
24	31	74	35.847	0	0	58
25	5	66	38.125	0	0	43
26	34	40	40.449	0	3	62
27	4	17	42.880	0	0	52
28	15	33	45.440	19	0	56
29	2	59	48.093	0	0	71
30	37	78	50.806	20	0	43
31	22	101	53.542	0	0	68
32	21	96	56.347	0	0	75
33	86	93	59.153	0	0	65
34	13	38	61.965	15	0	57
35	1	10	64.813	0	0	54
36	32	76	67.679	6	13	49
37	30	44	70.633	2	0	49
38	14	50	73.600	14	22	63
39	62	87	76.711	0	0	61
40	42	77	79.961	0	0	70
41	47	65	83.211	0	0	79
42	39	43	86.544	0	21	69
43	5	37	89.959	25	30	59
44	12	53	93.403	0	0	73
45	56	100	96.889	0	0	76
46	70	91	100.375	0	0	65
47	84	92	103.973	0	0	62
48	51	57	107.653	0	0	50
49	30	32	111.347	37	36	67
50	29	51	115.092	0	48	84
51	11	26	118.838	0	9	60
52	4	19	122.696	27	12	72
53	25	89	126.626	0	0	70
54	1	28	130.575	35	0	80
55	7	20	134.617	16	0	82
56	15	54	138.899	28	4	64
57	13	23	143.442	34	0	74

58	8	31	148.074	23	24	74
59	5	35	152.724	43	11	95
60	9	11	157.735	0	51	68
61	3	62	162.883	0	39	93
62	34	84	168.068	26	47	66
63	14	64	173.471	38	0	85
64	15	45	178.917	56	17	80
65	70	86	184.383	46	33	87
66	34	98	189.851	62	0	78
67	27	30	195.433	0	49	82
68	9	22	201.352	60	31	81
69	39	41	207.664	42	0	83
70	25	42	214.005	53	40	88
71	2	85	220.482	29	0	87
72	4	73	227.183	52	0	89
73	12	94	234.832	44	0	78
74	8	13	243.031	58	57	90
75	21	58	251.596	32	0	81
76	6	56	260.239	0	45	92
77	48	67	269.406	18	0	94
78	12	34	278.934	73	66	86
79	47	97	288.517	41	0	86
80	1	15	298.316	54	64	85
81	9	21	308.137	68	75	83
82	7	27	318.587	55	67	97
83	9	39	329.487	81	69	88
84	29	90	340.707	50	0	91
85	1	14	353.594	80	63	89
86	12	47	367.552	78	79	90
87	2	70	383.800	71	65	94
88	9	25	401.009	83	70	93
89	1	4	418.363	85	72	91
90	8	12	438.996	74	86	95
91	1	29	459.973	89	84	97
92	6	61	482.948	76	0	96
93	3	9	508.748	61	88	98
94	2	48	539.607	87	77	99
95	5	8	570.626	59	90	96
96	5	6	607.028	95	92	98
97	1	7	658.063	91	82	100

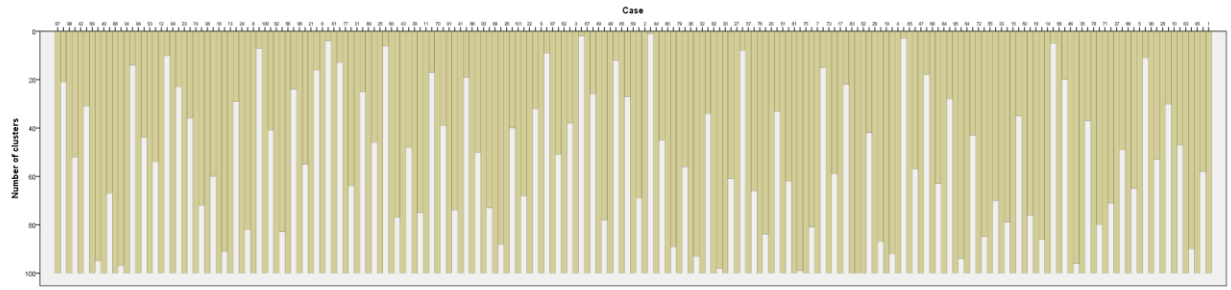
98	3	5	725.245	93	96	99
99	2	3	872.970	94	98	100
100	1	2	1385.969	97	99	0

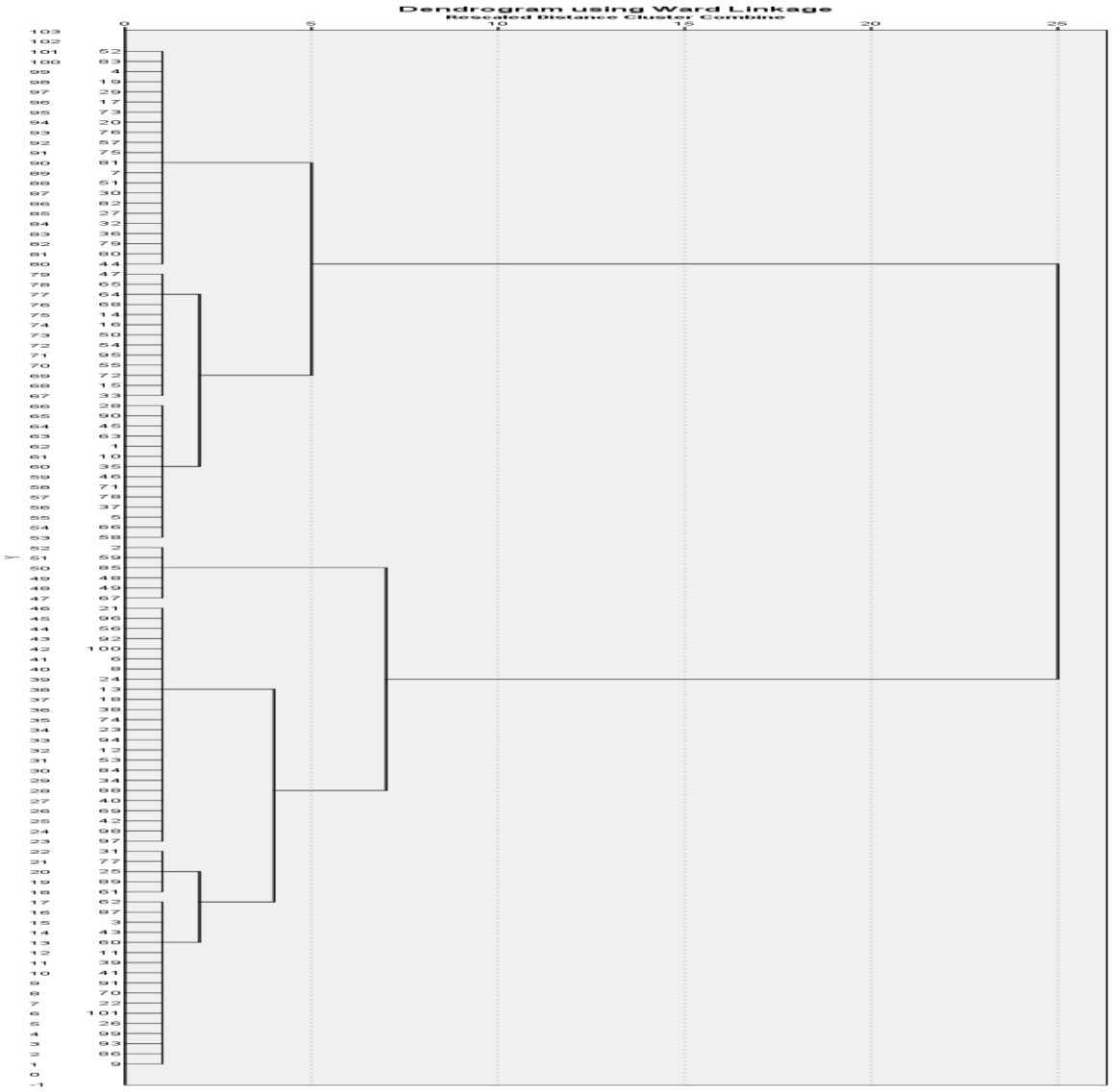
Cluster Membership

Case	4 Clusters
1	1
2	2
3	3
4	1
5	4
6	4
7	1
8	4
9	3
10	1
11	3
12	4
13	4
14	1
15	1
16	1
17	1
18	4
19	1
20	1
21	3
22	3
23	4
24	4
25	3
26	3
27	1
28	1
29	1
30	1
31	4
32	1

33	1
34	4
35	4
36	1
37	4
38	4
39	3
40	4
41	3
42	3
43	3
44	1
45	1
46	4
47	4
48	2
49	2
50	1
51	1
52	1
53	4
54	1
55	1
56	4
57	1
58	3
59	2
60	3
61	4
62	3
63	1
64	1
65	4
66	4
67	2
68	1
69	4
70	2
71	4
72	1

73	1
74	4
75	1
76	1
77	3
78	4
79	1
80	1
81	1
82	1
83	1
84	4
85	2
86	2
87	3
88	4
89	3
90	1
91	2
92	4
93	2
94	4
95	1
96	3
97	4
98	4
99	3
100	4
101	3





K-MEANS KLYNGEANALYSE

Initial Cluster Centers

	Cluster			
	1	2	3	4
Konseptuell_What	2.50	2.50	2.00	5.00

Konseptuell_Why	3.00	3.00	1.00	4.50
Konseptuell_How	2.50	3.50	1.00	5.00
Konseptuell_Who	5.00	2.00	1.00	5.00
Konseptuell_Where	4.33	2.67	1.00	5.00
Konseptuell_When	3.00	2.50	1.00	5.00
Logisk_What	4.50	3.50	1.00	5.00
Logisk_Why	2.50	2.50	1.00	5.00
Logisk_How	3.00	2.00	1.00	5.00
Logisk_Who	2.00	5.00	1.00	5.00
Logisk_Where	4.00	2.00	1.00	5.00
Logisk_When	1.00	5.00	1.00	5.00

Iteration History[a]

Iteration	Change in Cluster Centers			
	1	2	3	4
1	2.919	3.205	2.036	2.485
2	.288	.446	1.125	.323
3	.157	.339	.312	.000
4	.158	.200	.588	.000
5	.000	.162	.000	.085
6	.075	.107	.000	.000
7	.000	.000	.000	.000

a. Convergence achieved due to no or small change in cluster centers. The maximum absolute coordinate change for any center is .000. The current iteration is 7. The minimum distance between initial centers is 6.635.

Final Cluster Centers

	Cluster			
	1	2	3	4

Konseptuell_What	3.05	3.24	2.09	4.37
Konseptuell_Why	3.23	3.14	2.09	4.32
Konseptuell_How	2.93	3.10	2.14	4.21
Konseptuell_Who	3.86	3.60	2.94	4.64
Konseptuell_Where	3.30	3.06	2.45	4.07
Konseptuell_When	3.17	3.24	2.36	4.36
Logisk_What	2.97	3.10	1.82	4.37
Logisk_Why	2.97	3.05	1.50	4.24
Logisk_How	3.38	3.48	2.00	4.21
Logisk_Who	2.35	2.83	1.32	3.58
Logisk_Where	2.87	3.48	1.27	4.38
Logisk_When	2.27	3.90	1.27	4.10

Number of Cases in each Cluster

Cluster	1	30.000
	2	21.000
	3	11.000
	4	39.000
Valid		101.000
Missing		.000

REFERANSER

Cluster analysis.

Bishop, M. (2004). Introduction to Computer Security.

Buchanan, R. (2010). "Enterprise Architecture Program - Key Initiatives."

Forun, I. S. (2003). "Standard of Good Practice."

Gartner (2007). "Gartner Says CIOs Must Manage IT Risk as Business Risk."

Group, T. O. (2010). "TOGAF 9."

Hilliar, R. (2000). "Recommended Practice for Architectural Description of Software-Intensive Systems."

John Sherwood, A. C., David Lynas (2005). Enterprise Security Architecture: A Business-Driven Approach.

Joseph A. Gliem, R. R. G. (2003). Cronbach`s Alpha Reliability Coefficient for Likert-Type Scales. Research to Practice Conference in Adult, Continuing, and Community Education. Midwest.

Kessel, P. v. (2010). "Borderless security - Ernst & Young's 2010 Global Information Security Survey."

Lankhorst, M. (2009). Enterprise architecture at work: Modelling, communication and analasys.

M. Eric Johnson, E. G. (2007). "Embedding Information Security into the Organization."

Microsoft. (2011). "OSI Model." from http://technet.microsoft.com/en-us/library/cc959881.aspx.

NSR (2010). "Mørketallsundersøkelsen 2010."

OECD. (2011). from http://www.oecd.org/home/0,2987,en_2649_201185_1_1_1_1_1,00.html.

Osborne, A. B. C. J. W. (2005). "Best Practices in Exploratory Facotr Analysis: Four Recommendations for Getting the Most From Your Analysis." Practical Assessment Research & Evaluation.

Palmer, M. "Hypothesis-Driven and Exploratory Data Analysis."

Pedro Sousa, C. P., Rute Venderinho, Artur Caetano and José Tribolet (2007). "Applying the Zachman Framework Dimensions to Support Business Process Modeling."

Pontus Johnson, M. E., Enrique Silva, Leonel Plazaola (2004). "Using Enterprise Architectture for CIO Decision-makin: On the Importance of Theory."

PWC (2012). "Global State Information Security Survey."

Regjeringen. (2006). "Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007 - 2010." from http://www.regjeringen.no/Upload/FAD/Vedlegg/IKT-politikk/fad%20lav.pdf.

Ringdal, K. (2007). Enhet og mangfold.

Sambamoorthi, N. "Hierarchical Cluster Analysis - Some Basics and Algorithms."

Sannes, R. (2004). "Dataanalyse og statistikk - kvantitativ tilnærming."

Scheidell, M. (2008). "Three Undocumented Layers of the OSI Model and Their Impact on Security."

Sessions, R. (2007, May). "A Comparison of the Top Four Enterprise-Architecture Methodologies." from http://msdn.microsoft.com/en-us/library/bb466232.aspx.

TOGAF, S. (2011). "TOGAF and SABSA Integration."

University, C. M. (2011). "Software Architecture | Getting started | Glossary."

University, C. S. "Chapter Seven: Correlation and Regression." from http://www.csub.edu/ssricrem/spss/spss11-7/11-7.htm.

Watkins, A. C. S. A Manager`s Guide to Data Security and ISO27001/ISO 27002.

Wiik, R. "SOS 1002 Samfunnsvitenskapelig forskningsmetode."

Wikipedia (2011). "OSI model."

Young, E. (2010). "Global Information Security Survey: Borderless Security."

Zachman, J. A. "The Framework for Enterprise Architecture: Background, Description and Utility." Zachman Institute for Framework Advancement (ZIFA).

Zachman, J. A. (1987). "A framework for information systems architecture." IBM Syst. J. 26(3): 276-292.