Joakim N. Ellestad, Anders G. Gustad, Magnus L. Lilja, Espen S. Skuggerud

Sikkerhetskultur ved NTNU

Bacheloroppgave i IT-drift og informasjonssikkerhet
Veileder: Ernst Gunnar Gran
Juni 2019

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikajsonsteknologi

NTNU
Kunnskap for en bedre verden

Sammendrag av Bacheloroppgaven

Tittel:	**Sikkerhetskultur ved NTNU**
Dato:	19.05.2019
Deltakere:	Joakim Nereng Ellestad Espen Stårvik Skuggerud Anders Gjengstø Gustad Magnus Lien Lilja
Veiledere:	Ernst Gunnar Gran
Oppdragsgiver:	Norwegian University of Science and Technology
Kontaktperson:	Gaute Wangen, gaute.wangen@ntnu.no, 907 08 338
Nøkkelord:	Informasjonssikkerhet, måling, kultur
Antall sider:	116
Antall vedlegg:	11
Tilgjengelighet:	Åpen
Studiepoeng:	20 ECTS

Sammendrag:

Oppgaven har som hovedmål å gjøre en litteraturstudie av eksisterende rammeverk, finne bestepraksis, for måling av sikkerhetskultur og gjennomføre en måling på IT-avdelingen ved NTNU. Resultatet av målingen ligger i grunn for å utvikle tiltak for å bedre sikkerhetskulturen.
Oppgaven starter med å adressere relevant teori og begreper som vil ligge til grunn for videre arbeid med oppgaven. Videre vil litteraturanalysen og intervju med eksperter ligge til grunn for å adressere bestepraksis og valg av rammeverk. Det valgte rammeverket brukes for å gjennomføre en måling av sikkerhetskultur på IT-avdelingen ved NTNU. Til slutt konkluderer oppgaven med at bruken av rammeverket Information Security Culture Framework (ISCF) har vært vellykket. Bestepraksis for indikatorer kan sies å være stort sett basert på Schein og Robbins modeller og bruken av kvantiative måle metoder har vært brukt svært suksessfult i flere rammeverk. Resultatet fra målingen har identifisert flere viktige forbedringsområder: styring av informasjonsverdier, opplæring, kurs/trening og avdelingsstruktur.

Summary of Graduate Project

Title:	**Sikkerhetskultur ved NTNU**
Date:	19.05.2019
Authors:	Joakim Nereng Ellestad Espen Stårvik Skuggerud Anders Gjengstø Gustad Magnus Lien Lilja
Supervisor:	Ernst Gunnar Gran
Employer:	Norwegian University of Science and Technology
Contact Person:	Gaute Wangen, gaute.wangen@ntnu.no, 907 08 338
Keywords:	Information security, measure, culture
Pages:	116
Attachments:	11
Availability:	Open
Studypoints	20 ECTS

Abstract:

The purpose of this paper is to do a study of existing literature, identify best practice in the field of information security culture and conduct a survey on the IT-department at NTNU. Results from the survey is used to develop a set of actions to improve the security culture. The paper starts by adressing relevant theory and terms which creates the basis for assessing the research topics. The literature analysis together with interviews with experts are key elements for assessing best practice and choosing a framework. The chosen framework is used to conduct a information security culture survey on IT-departement at NTNU. The results show that using Information Security Culture Framework (ISCF) have been deployed successfully. Best practice for indicators can be said to be based on models by Schein and Robbins and quantitative methods have been used successfully by several frameworks. Results from the survey have identified room for improvements: asset management, education and training and program organisation.

Forord

Da arbeidet med bachelorprosjektet startet var vi svært blanke på hva begrepet sikkerhetskultur omhandlet og hvordan dette kunne måles. Vi forstod tidlig at vi trengte hjelp til å forstå konseptet og det holdt ikke bare med litteratur.

Vi vil herved rette en stor takk til alle som hjalp oss i arbeidet med bacheloroppgaven og hjalp oss i å navigere gjennom ukjent farvann av begreper og definisjoner.

Tusen takk til Roar Thon, Fagdirektør sikkerhetskultur i Nasjonal sikkerhetsmyndighet (NSM) og Bjarte Malmedal, Seniorrådgiver i Norsk senter for informasjonssikring, for at de delte sin kunnskap med oss. De hadde viktige innspill som bidro godt.

Tusen takk til Randi Utstrand, Rådgiver Sikkerhet og beredskap, HR- og HMS-avdelingen som holdt ut med oss gjennom en lang e-post korrespondanse underveis i prosjektet. Randi bidro med å styre arbeidet i riktig retning.

Takk til Håkon Alstad, IT-sjef for IT-avdelingen ved NTNU, som gav oss innsikt i IT-avdelingen. Vi håper resultatet blir verdiskapende for NTNU.

Vi må også takke Kai Roer for erfaringen han bidro med som gjorde forståelsen for måling av sikkerhetskultur litt enklere.

En stor takk går til oppdragsgiver Gaute Wangen, Seniorrådgiver for Digital Sikkerhet ved NTNU som kunne tilby oss denne veldig lærerike oppgaven. Analysen hadde vært noe tynn, hadde vi ikke fått opplæring i statistikk og SPSS.

Sist, men ikke minst, må vi rette en stor takk til veileder Ernst Gunnar Gran som kom med verdifull tilbakemelding på bacheloroppgaven.

Innhold

Figurer

Tabeller

1 Innledning

1.1 Bakgrunn

Sikkerhetsarbeid kan forklares med det arbeidet som nedlegges for å verne og forbedre helse, miljø og ressurser. Historisk sett har sikkerhetsarbeid blitt løst med teknologiske og organisatoriske tilnærminger, eksempelvis barrierebygging og ansvarsfordeling. Sikkerhetsarbeidet har i all hovedsak dreiet seg om utarbeiding av politikk og retningslinjer, samt adresserende teknologiske løsninger. I 2004 gjennomførte Shell *Hearts and Minds*, et vellykket prosjekt med mål for å redusere antall ulykker basert på kartlegging av adferd, holdninger og kultur [4]. Dette beregnes som springbrettet for hvordan man i nyere tid har tilnærmet seg sikkerhetsarbeid.

Informasjonssikkerhet handler generelt om å sikre informasjon ut ifra krav om konfidensialitet, integritet og tilgjengelighet, og kan ansees som en underliggende kategori av generelt sikkerhetsarbeid. Resultatet av *Hearts and Minds* samsvarer med rapporten, "Informasjonssikkerhet: atferd, holdninger og kultur" [2] utviklet av *SINTEF*, *Nasjonal Sikkerhetsmyndighet (NSM)* og *Norges Teknisk-Naturvitenskapelige Universitet (NTNU)* med at det ikke er tilstrekkelig med utforming av retningslinjer, men det må rettes større fokus på menneskelig adferd, holdninger og kunnskap for økt informasjonssikkerhet [2]. I den årlige rapporten utgitt av *Norsk senter for informasjonssikring (NorSIS)* i 2018 konkluderes det igjen med et behov for å bedre kunnskapen på sikkerhet og en positiv endring i adferd og holdnininger til informasjonssikkerhet [5]. Ut i fra disse kan vi se at det er enighet i hvordan kulturelle aspekter har stor innvirkning på sikkerhetsarbeid uavhengig av sektor og bransje. Ved sammenligning av rapportene til NorSIS fra 2017 og 2018 konkluderes det med at situasjonen ikke har blitt særlig bedre. Dette gjelder både for bedrifter og privatpersoner. Vi anser derfor at det eksisterer forbedringspotensiale i arbeidet med informasjonssikkerhet med perspektiv på menneskelige og kulturelle faktorer. Dette er bakgrunnen vi tar med oss inn i prosjektet.

1.2 Problem

Organisasjoner i dag er ofte avhengig av digitale løsninger og med digitale løsninger, samt alt annet, følger trusler. Organisasjoner implementerer tekniske kontroller slik som brannmurer, autentisering og lignende for å beskytte informasjonsverdier. Da følger kravet om kompetanse og erfaring til ansatte som implementerer eller bruker det med. Følgelig vil dette bety at ansatte blir en kritisk faktor i arbeidet med sikker bruk av digitale løsninger. Dette gjelder for de som implementerer og drifter samt også de som bruker løsningene. Når en ansatt arbeider med digitale informasjonsverdier blir personen automatisk det svakeste leddet, og sikkerheten til verdier blir avhengig av kunnskap, holdninger og adferd. En av utfordringene i beskyttelsen av informasjonsverdier er menneskelige faktorer. En tidligere bacheloroppgave ved NTNU avdekket en av disse utfordringene ved menneskelige faktorer. Bacheloroppgaven, *Mørketallsundersøkelsen* [6], avdekket at nærmere halvparten av deltagerne i undersøkelsen opplevde skreddersydde forsøk på utnyttelse. *von-Solmsom* forteller viktigheten av å ivareta og kontrollere menneskelige

faktorer ved informasjonssikkerhet [7].

1.3 Problemstilling

En konsekvens av dårlig sikkerhetskultur kan gå utover NTNU, blandt annet i form av økonomiske konsekvenser og tap av omdømme. I tillegg til de organisatoriske fordelene med måling, er NTNU underlagt eksterne krav om kontinuerlig forbedring og sikring av verdier [8]. NTNU sine egne retningslinjer for arbeid med sikkerhetskultur og opplæring innen informasjonssikkerhet sier at "ledere skal gjennom systematisk kartlegging bistå i å avdekke områder for nødvendig opplæring og kompetansehevende tiltak for å skape et kontinuerlig arbeid med utvikling av enhetens sikkerhetskultur."[1] Det finnes flere rammeverk for måling av kultur, men det er ikke kjent for NTNU hvordan disse kan benyttes i organisasjonen.

1.4 Problemformulering

Bacheloroppgaven skal på bakgrunn av problemstillingen gjøre en gjennomgang og analyse av beste praksis innenfor sikkerhetskultur, velge et rammeverk for måling av sikkerthetskultur og gjennomføre en måling på IT-avdelingen ved NTNU. Dernest skal resultatet fra målingen ligge til grunn for å foreslå tiltak for å bedre sikkerhetskulturen på IT-avdelingen.

- Gjennomgang og analyse av bestepraksis innenfor sikkerhetskultur
- Velge rammeverk og gjennomføre måling på IT-avdelingen
- Foreslå tiltak til å bedre sikkerhetskulturen på IT-avdelingen

1.5 Emne og rammer

Oppgaven er gitt av Seksjon for digital sikkerhet [2], ved Gaute Wangen [3], og har tittelen "Sikkerhetskultur ved NTNU". Oppgaven er i sin helhet gjengitt i vedlegg A. Oppgaven utføres fra februar måned og skal leveres 20. mai. Det skal i tillegg til den skriftlige bacheloroppgaven her gjennomføres en presentasjon av arbeidet mellom 4. juni og 6. juni.

Oppdragsgiver dekket eventuelle utgifter vi måtte ha ved utførelsen.

Oppdragsgiver sitt mål er å kunne ha et rammeverk som kan brukes av NTNU for å kartlegge sikkerhetskulturen. Dette gjøres gjennom oppgaven gitt til oss der målsetningen sammen med oppdragsgiver er satt i problemformuleringen nevnt ovenfor (se seksjon 1.4).

Sammen med oppdragsgiver ble det bestemt av vi avgrenser omfanget av måling til å gjelde IT-avdelingen [4].

1.6 Rapportens struktur

Rapporten inneholder 14 kapitler og 11 vedlegg.

[1] https://innsida.ntnu.no/documents/10157/2550717837/Retningslinje+for+arbeid+med+sikkerhetskultur+og+oppl%C3%A6ring.pdf/ee78e950-d96b-492d-b36b-b376d925603f - (03.05.2019)

[2] https://www.ntnu.no/adm/it/ansatte/digital-sikkerhet

[3] Seniorrådgiver i Digital Sikkerhet, NTNU

[4] https://www.ntnu.no/adm/it/ansatte - (04.05.2019)

Kapittel 1 - Innledning

Inneholder bakgrunnen for oppgaven og en diskusjon rundt problemområdet i tillegg til en konkret problemstilling.

Kapittel 2 - Teori

Inneholder en oversikt over hvordan bibliografien vi benytter omtaler relevante begreper. Videre går vi inn på teorier rundt måling av informasjonssikkerhetskultur og hva vi mener med rammeverk.

Kapittel 3 - Metode

Inneholder en beskrivelse av metoden vi brukte for å finne aktuell litteratur og filtrering og kvalitetsikring av disse. Det inneholder også fremgangsmåte for datainnsamling og analyse.

Kapittel 4 - Identifisering av bestepraksis

Kapittelet identifiserer områder i sikkerhetskultur som må ligge til grunn for valg av et rammeverk. Det forsøkes å kartlegge bestepraksis i områdene for å kunne gjøre vektede beslutninger i valg av rammeverk.

Kapittel 5 - Valg av rammeverk

Inneholder valg av rammeverk for måling av sikkerhetskultur ved NTNU. Dette kapittelet tar for seg hele denne prosessen fra den initielle vurderingen av hvert rammeverk, utvalgskriterier, til en dyptgående analyse av aktuelle rammeverk. Kapittelet avslutter med et valg av rammeverk.

Kapittel 6 - Information Security Culture Framework

Dette kapittelet inneholder en forklaring av oppbygningen til valgt rammeverk, slik at det er innforstått hvordan rammeverket virker før det taes i bruk.

Kapittel 7 - Tilpasninger av Information Security Culture Assessment til NTNU

Inneholder endringer gjort i utformingen av rammeverket for å kunne brukes i NTNU. Formålet med dette kapittlet er at endringene skal danne et grunnlag for å kunne bruke rammeverket på ulike avdelinger i NTNU.

Kapittel 8 - Steg 1 Forbredelse og planlegging

Inneholder involvering av interessenter, planlegging og konkret tilpasning av undersøkelsen til valgt avdeling.

Kapittel 9 - Steg 2 Gjennomføring

Inneholder utførelse av målingen på IT-avdelingen og oppfølging av undersøkelsen underveis i målingsperioden.

Kapittel 10 - Steg 3 Evaluering av undersøkelsen

Inneholder en beskrivelse av vårt arbeid med validering av undersøkelsen, samt en innledning til den statistiske undersøkelsen

Kapittel 11 - Steg 4 Dokumentasjon og tilbakemelding

Inneholder gjennomføringen av den statistiske analysen av undersøkelsen. Dette er en objektiv fremstilling av resultatene fra undersøkelsen.

Kapittel 12 - Steg 5 Handlingsplan

Inneholder en tiltakspakke basert på styrker og svakheter som ble avdekket ved målingen.

Kapittel 13 - Refleksjon

Inneholder erfaringer vi har gjort oss underveis i prosjektet og forbedringsområder ved en senere måling av sikkerhetskultur ved NTNU.

Kapittel 14 - Avslutning

Inneholder en konklusjon på oppgaven og svar på problemformuleringen. Det tas stilling til videre arbeid som bør gjennomføres ved måling av sikkerhetskultur.

2 Teori

Teorikapitlet er delt opp i seksjoner som tar for seg begreper og definisjoner, og diskuterer ulike tilnærminger litteraturen har. Her avklares og beskrives de essensielle begrepene innenfor emnet, slik at tolkningen av begrepene blir entydig.

2.1 Informasjonssikkerhetskultur

Begrepet informasjonssikkerhetskultur har mange ulike navn med den samme betydningen: Schlienger and Teufel [9] bruker begrepet *information security culture*, mens ENISA [10] har brukt begrepet *cyber security culture*. Begrepet *data security culture* har ikke blitt brukt i bibliografien som bacheloroppgaven benytter, men *data security* omtales av Bishop [11]. Det er vesentlig i forståelse av oppgaven å gå inn på hva dette betyr og se på hvordan litteraturen omtaler dette begrepet.

Kultur, eller organisasjonskultur forklarer noe om hvordan ting er gjort i en organisasjon og oppførselen til menneskene i organisasjonen Martins and Elofe [12, s. 204]. Denne forståelsen av kultur støttes opp av Schlienger and Teufel [9] som sier organisasjonskultur består av to kjerner, antagelser og oppfatninger. Videre sier de antagelser omhandler menneskelig natur, deres atferd og forhold. De påstår at organisasjonskultur vil være uttrykt som de samlede verdiene, normer og kunnskap i en organisasjon. De definerer normer og verdier som en samling av håndbøker, praksis og rapporter. Til slutt sier de at kultur har en enorm påvirkning på en organisasjons suksess. I intervju med Roar Thon forteller han at sikkerhetskultur og organisasjonskultur er sidestilt. Han påpeker viktigheten at man ikke skal ha et styringssystem for sikkerhet, men et styringssystem som inkluderer sikkerhet. Sikkerhet må være en del av den grunnleggende driften fra starten av og ikke være noe man gjør i tillegg. For enkelhets skyld brukes kultur og organisasjonskultur som synonymer videre i oppgaven. Når kultur omtales sammen med informasjonssikkerhet, datasikkerhet eller cybersikkerhet er det viktig å vite om det er noe som skiller dem.

Roar Thon sier videre i intervjuet at sikkerhetskultur er et relativt nytt begrep. Det var før et større fokus på fysisk sikkerhet og dokumentsikkerhet, men etter teknologiens innpass i organisasjoner har dette forandret seg. Han forteller at 22. juli-kommisjonen sin rapport tok i bruk begrepet sikkerhetskultur på en annen måte enn tidligere, og gjorde begrepet mer utbredt [13]. Han påpeker at rapporten fra 22. juli-kommisjonen og Statoil rapporten fra terror angrepet i In Amenas [14] gav en knusende dom i at enkeltpersoner har et bidrag å komme med i sikkerheten, noe som danner grunnlaget i hva som menes med sikkerhetskultur.

NTNU sin politikk for informasjonssikkerhet [8] definerer begrepet informasjonssikkerhet som:

> Informasjonssikkerhet handler om å sikre informasjon ut ifra krav om konfidensialitet, integritet og tilgjengelighet

Datasikkerhet blir beskrevet av Bishop [11] som beskyttelsen av integritet og konfidensialiteten i tillegg til å sørge for god tilgjengelighet av data. Dette er svært likt det NTNU formidler med betydningen av informasjonssikkerhet.

Schatz et al. [15, s. 66] bruker også konfidensialtet, integritet og tilgjengelighet, det såkalte *CIA*-triangelet[1] i sin beskrivelse om cybersikkerhet. Videre sier de at konseptet inkluderer retningslinjer, policyer og samlinger av sikkerhetstiltak, teknologi, verktøy og trening for å gi den beste beskyttelsen mot miljøet i cyber for brukerne. Beskrivelsene går godt inn i det som menes med informasjonssikkerhetskultur og cybersikkerhetskultur.
En forskningsrapport fra universiteten i Melbourne av Lim et al. [16] beskriver informasjonssikkerhetkultur som de ansattes sikkerhetsrelaterte oppfatninger og verdier, som kommer frem av ansattes handling og atferd i å beskytte organisasjonens informasjon.
Bruken av ordet informasjonssikkerhetkultur benyttes også i annen litteratur av Martins and Elofe [12], Schlienger [17] og Schlienger and Teufel [9]. Cybersikkerhetskultur benyttes av ENISA [10] og er beskrevet som

> "The concept of Cybersecurity Culture (CSC) refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behaviour with information technologies."

NTNU skiller seg noe ut i arbeidet med sikkerhetskultur fra litteraturen benyttet i oppgaven. I retningslinjer for arbeid med sikkerhetskultur og opplæring [2] defineres sikkerhetskultur og sikkerhetsklima. Med sikkerhetsklima menes

> "Resultatet fra et spørreskjema som kan avdekke kulturelle trekk, og som de felles verdier, normer og virkelighetsoppfatninger kan sammenstilles med andre sikkerhetsindikatorer for å ha oversikt og kontroll på egen sikkerhet." [2]

Med denne betydningen vil sikkerhetsklima være et tolket resultat av sikkerhetskultur, der sikkerhetskultur defineres av NTNU som

> "Innebærer en organisasjonskultur hvor de felles verdier, normer og virkelighetsoppfatninger som utvikler seg gjennom samhandling i omgivelsene, prioriterer høyt de sikkerhetsrelaterte antakelser, verdier og holdninger som gjelder for organisasjonen." [2]

Selv om ordlyden og begreper er forskjellige i definisjonene nevnt over er betydningen svært lik. Vi kan si at informasjonssikkerhetskultur kan forstås som holdninger, verdier og oppfatninger og hvordan dette påvirker adferden til ansatte og organisasjonen i sin helhet i forbindelse med informasjonssikkerhet. Videre i rapporten benyttes begrepet informasjonssikkerhetskultur, eller cybersikkerhetskultur, synonymt med sikkerhetskultur.

2.2 Måling av sikkerhetskultur

For å videre kunne diskutere praksisen innen sikkerhetskultur, og også si noe om en organisasjons sikkerhetskultur, er det viktig å drøfte begrepene brukt relatert til målingen av sikkerhetskulturen. En definisjon av måling i følge Hubbard [18, p. 71] er:

> **"Measurement**: A quantitatively expressed reduction of uncertainty based on one or more observations."

Målinger gjennomføres enten kvalitativt eller kvantitativt. Typisk for *kvalitativ* metode er intervju. Man får gjerne dypere innsikt i holdninger og adferd, men på bekostning av tidsressurser da det krever lengre tid å gjennomføre [1]. *Kvantitativ* metode for måling derimot kan være spørreundersøkelser. Det er mindre tidkrevende, og tillater gjerne større datainnsamling for økt representativitet i datasettet [19], i tilegg gir kvantitativt

[1] C = Konfidensialitet, I = Integritet, A = Tilgjengelighet https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet

[2] https://innsida.ntnu.no/documents/10157/2550717837/Retningslinje+for+arbeid+med+sikkerhetskultur+og+oppl%C3%A6ring.pdf/ee78e950-d96b-492d-b36b-b376d925603f - (18.05.2019)

tilnærming muligheten for å se statistiske sammenhenger, eksempelvis årsakssammenhenger og korreleasjonstester 3.3.2.

Ved en måling ser man gjerne på numeriske verdier, i form av eksempelvis antall, frekvens og tid for sammenligning med sine egne tidligere målinger eller en standard [20]. Sammenligning mot andre organisasjoner eller ved andre i bransjen er mindre typisk, da bedrifter eller organisasjoner flest ikke deler disse statistikkene da det formidler et dårlig bilde ovenfor bedriften selv [21].

For å måle en potensiell forandring og progresjon ved sikkerhetskulturen i en organisasjon, benyttes metrikker. European Network and Information Security Agency (ENISA) omtaler begrepet metrikk som et sett parametre av en kvantitativ vurdering. Disse metrikkene kan forandre og utvikle seg over tid, og de er typisk mulig å forandre ved å etablere tiltak [22, p. 73]. En måling er utført på ett enkelt tidspunkt, mens metrikker er sammenligning av to målinger gjort på forskjellige tidspunkt [23, p. 2]. Siden sikkerhetskultur omtales som en kontinuerlig utviklingsprosess [8], gjennomfører man målinger for å kontrollere endringer i kulturen. Man er nødt til å vite hva og hvordan noe skal endres, som forutsetter at man gjennomfører målinger av kulturen, og for å dokumentere at endringer har foregått, gjør man en senere måling og gjør en sammenligning av disse målingene (se vedlegg D).

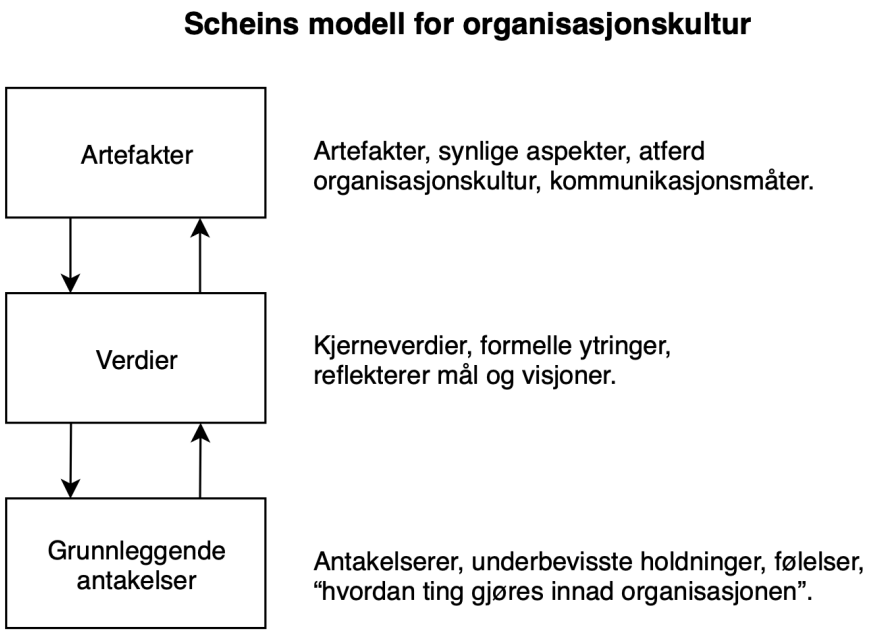
En måling av informasjonssikkerhetskultur hos en organisasjon anses da som noe en bedrift gjør ved egne, ofte tallbaserte målinger (kvantitativt). Ved å sammenligne disse over en lengre tidsperiode, vil man altså kunne se hvilke endringer i organisasjonen som finner sted, og man gjennomfører de nødvendige tiltakene for at endringene skal gå riktig vei.

2.3 Sentrale modeller for organisasjonskultur

Det er to modeller angående organisasjonskultur som er gjengangere i litteraturen vi benytter. Vi vil derfor adressere hva disse modellene går ut på her og bruke de som referanse når de nevnes senere i teksten.

2.3.1 Organisatorisk modell for kultur - Schein

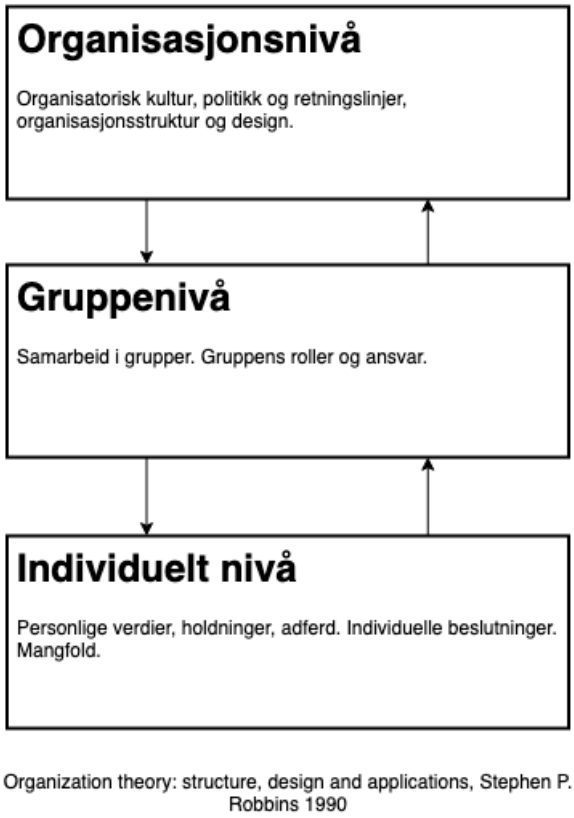
Edgar Schein har utviklet en modell med tre nivåer som organisasjonskultur deles opp i [24]. Modellen brukes for å beskrive og analysere hvilke som helst kulturelt fenomen. Schein sier ingenting om informasjonssikkerhetskultur, men forteller at modellen kan brukes for å beskrive sub-kulturerer, samt også organisasjonskultur. Modellen er vist i figur 1 og viser de tre nivåene *artefakter*, *verdier* og *grunnleggende antagelser*. Ser man på figuren 1 kommer det fram at nivåene påvirker hverandre.



Figur 1: Scheins modell for organisasjonskultur

2.3.2 Organisatorisk adferd - Robbins

Stephen Robbin har utviklet en trenivå-modell som benyttes for å beskrive organisasjonsadferd [25]. I teorien ser man på hvordan nivåene organisasjon, gruppe og individet påvirker hverandre. Dette er presentert i figur 2. Med denne teorien forklares det hvordan ansattes adferd påvirkes i henhold til hva som omfattes som “riktig” og “akseptabelt”. Effekten av dette kan observeres på de ulike nivåene.



Figur 2: Robbins trenivåmodell for organisasjonskultur

2.4 Rammeverk

I arbeidet med bacheloroppgaven ble det avdekket at definisjonen på rammeverk ikke var helt tydelig og ikke ble brukt likt i litteraturen. Generelt sett er et rammeverk en strukturert prosess som fungerer som en guide for å gjennomføre en oppgave.

Bacheloroppgaven benytter heretter begrepet *rammeverk* om litteratur som inneholder teoriforklaring, begreper, eventuelle empiriske studier og et *verktøy*. Begrepet verktøy brukes om en strukturert tilnærming for hvordan kulturelle trekk innenfor informasjonssikkerhetskultur kan synliggjøres eller måles på.

3 Metode

Dette kapittelet tar for seg beskrivelse og valg av metodebruk underveis i bacheloroppgaven.

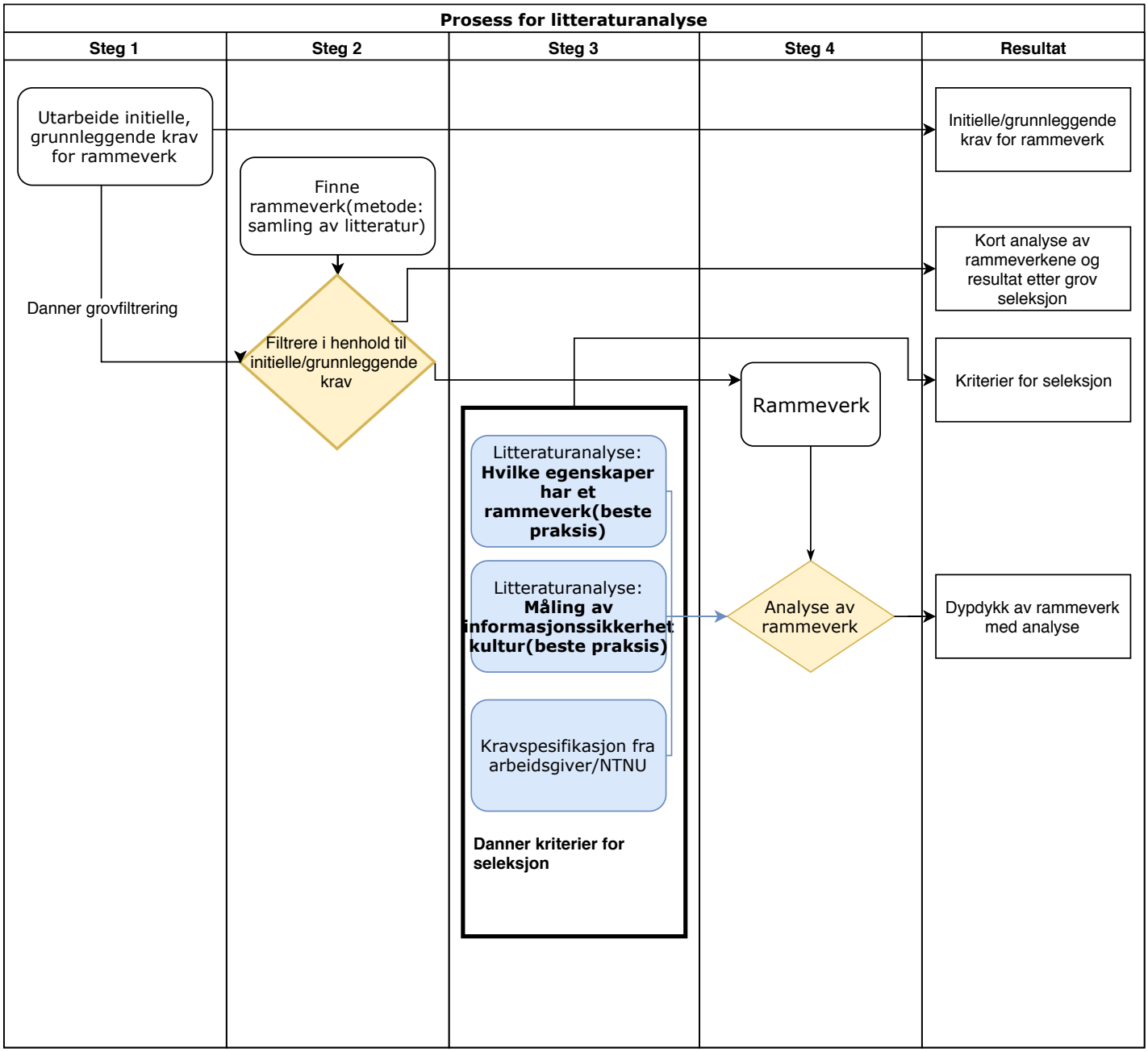
3.1 Litteraturanalyse

3.1.1 Valgt metodikk

Med litteraturanalyse menes metoden vi bruker for å foreta en analyse av rammeverk og prosessen rundt det. Analysen bygger på den initielle jobben med innsamling av litteratur som beskrevet i seksjon 3.2.

For å kunne besvare problemformuleringen vår om bestepraksis og valg av rammeverk benyttes litteraturanalyse da vi er nødt til å se på eksisterende litteratur og forskning om sikkerhetskultur.

Analysen starter først med å utarbeide initielle og grunnleggende krav for et rammeverk. Her er vi ute etter å kvalitetsikre rammeverket etter forfatters troverdighet og anerkjennelse i informasjonssikkerhetsmiljøet. Dette gjøres med en subjektiv vurdering, egne undersøkelser og oppdragsgivers krav. Etter grovfiltreringen vil vi stå igjen med flere rammeverk som kan være aktuelle kandidater. Før analysen tar for seg rammeverkene må det lages en rekke krav, egenskaper og retningslinjer som vil bidra til å velge det mest egnede rammeverket for vår situasjon. Kravene utarbeides sammen med oppdragsgiver, samt undersøkelser om hvilke krav NTNU som organisasjon har. I tillegg vil det gjøres en undersøkelse av litteratur angående beste praksis rundt emner som *måling av informasjonssikkerhetkultur* og *gode egenskaper til rammeverk*. Undersøkelsen skal også ta med kommentarer fra eksperter fra fagmiljø rundt informasjonssikkerhetskultur. I neste steg gjennomføres det et dypdykk av hvert rammeverk. Her vil rammeverkene bli vurdert oppimot krav og bestepraksis utarbeidet i forrige steg. Resultatet fra dypdykket vil være en rangering av rammeverk som tilfredsstiller krav fra arbeidsgiver, bestepraksis og andre egenskaper. Litteraturanalysen er illustrert i figur 3.



Figur 3: Prosess for litteraturanalyse

3.1.2 Alternativ metodikk

Istedenfor å utføre en grovanalyse av hvert rammeverk vi fant, er det en mulighet å gå rett på et dypdykk av hvert rammeverk. Dette kunne ha ført til at noen av de rammeverkene som ble utelatt videre vurdering i grovanalysen, egentlig er relevante ved en nærmere analyse. Noe av bakgrunnen for å ha en grovanalyse var å utelukke rammeverk som ikke oppfyller krav som vi anser som såpass viktige at rammeverkene ikke ville ha blitt vurdert uansett. Denne prosessen vil da også føre til effektivisering av arbeidet.

3.1.3 Metodekritikk

I forbindelse med arbeidet som ble utført ble det utviklet en egen metode for analyse av rammeverkene. Metoden er ikke utprøvd på forhånd og kan ha svakheter som ikke er kjent for oss.

3.2 Samling av litteratur

3.2.1 Valgt metodikk

For å sørge for effektivitet og forholdsmessighet i letingen etter litteratur og rammeverk er det viktig å arbeide strukturert. Kilder til litteratur i denne fasen har for det meste vært *Google Scholar* [1], Google's søkemotor for akademisk litteratur, og *Oria* [2], NTNUs universitetsbibliotek. I arbeidet ble det spesielt fokusert på disse kildene til litteratur fordi de vil kunne presentere resultater med høy troverdighet og god kvalitet. Dette gir en god start for å finne relevant litteratur, men kvaliteten og relevansen til hvert enkelt litterære verk må fortsatt vurderes.

Google Scholar er en søkemotor for å finne vitenskapelig litteratur [3]. Den har også funksjonalitet for å rangere resultatene ved å se på publikasjonssted, forfatter og hvor ofte dokumentet har blitt sitert i annen litteratur. En fordel med denne funksjonaliteten er at det gjør det lettere å sortere bort kilder med dårlig kvalitet. Derimot så er det også mulig at relevante dokumenter med lav rangering blir vanskeligere å finne.

Mange av resultatene fra Google Scholar vil man også finne ved søk i Oria. Noe av hovedforskjellen mellom disse to er at Oria gir tilgang til lisensbelagt litteratur. Oria gir også mulighet til å se litteratur som finnes på universitetsbiblioteket. En annen fordel med Oria er at det finnes flere filtreringsmuligheter enn Google Scholar tilbyr. Dette muliggjør spesifikke søk etter relevant litteratur med for eksempel filtrering på utgivelsesår, forfatter og emne.

Litteratur som ble vurdert som relevant og med god kvalitet ble lastet opp til en felles "teamsite" på SharePoint. Litteraturen ble fordelt på gruppedeltagerne og videre gikk arbeidet ut på å lese gjennom og markere viktig informasjon i teksten. Dette gjør prosessen med å lese litteraturen i etterkant mer effektiv, ved at man ikke trenger å lese hele teksten for å få med seg viktig informasjon.

I startfasen ble det hovedsaklig fokusert på norsk litteratur og det ble naturlig nok norske søkeord både på Google Scholar og Oria. Etterhvert i prosessen ble det vanskelig å finne rammeverk, og søket ble endret til å inkludere kilder på engelsk. I listen under finnes en oversikt over noen av søkeordene som ble benyttet:

- Organisasjonskultur
- Sikkerhetskultur
- Informasjonssikerhetskultur
- Sikkerhetskultur + rammeverk
- Måling av sikkerhetskultur
- Organizationalculture

[1] https://scholar.google.no/ - (19.05.2019)
[2] https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/search?sortby=rank&vid=NTNU_UB&lang=no_NO - (19.05.2019)
[3] https://scholar.google.com/intl/en/scholar/about.html - (19.05.2019)

- Measure security culture
- Information security culture
- Security culture framework

3.2.2 Alternativ metodikk

Det finnes mange kilder til litteratur. Metoden begrenser seg til to kilder og det kan være at enkelte rammeverk ikke finnes via disse kildene. En alternativ fremgangsmåte kan være å høre med flere forskjellige virksomheter for å undersøke hvilke rammeverk de benytter for å måle sikkerhetskultur med.

Mye av litteraturen vi har funnet refererer til de samme kildene. Det kunne ha vært interessant å ha laget et dokument som viser hvor mange ganger sentrale verk gjentar seg i forskjellig litteratur og rangert dem.

3.2.3 Metodekritikk

Vi er litt begrenset i måten vi leter etter litteratur på. Det kan være at det finnes rammeverk som er mye brukt, men som ikke er tilgjengelig via søkemotorene vi benyttet.

3.3 Statistisk analyse

I kapittel 11 som omhandler dokumentasjon og tilbakemedling benyttes statistisk analyse. Denne seksjonen beskriver metodene som blir brukt i analysen. Den statistiske analysen av spørreundersøkelsen skal være med på å tydeliggjøre mulige forbedringsområder og tilrettelegge for diskusjon av resultatene. Derfor er det viktig at den statistiske analysen utføres riktig.

Det finnes ulike metoder å analysere resultatene på. Oppdragsgiver satte rammene for hvilke statistiske analyse-metoder som kunne brukes, og er beskrevet nedenfor. Alt av analyser og tester ble utført i programmet SPSS[4].

3.3.1 Deskriptiv

Med *deskriptiv statistikk*, også kalt beskrivende statistikk, ønsker vi å presentere spredningen i datasettet og legge frem sentral tendens [26]. Flesteparten av påstandene i spørreundersøkelsen har likert-skala svaralternativer, med verdier fra 1 til 6 (svært uenig - svært enig). Andre påstander har "ja/nei" og eller "vet ikke" alternativer. Disse typer svaralternativer er diskrete variabler og går under kategorien *ordinale variable*. I ordinale variable finnes det ingen avstand mellom intervallene og man kan bare si at en verdi er større eller mindre enn en annen[5]. Derfor blir måling av gjennomsnitt, for sentral tendens, meningsløst. Man kan for eksempel ikke finne gjennomsnittet av enig og svært enig[5]. For analysen bruker vi median, typetall og variasjonsbredde for å beskrive ordinale data.
Nedenfor beskrives de ulike metodene vi bruker for i den deskriptive statistikken.

Median

Store Norske Leksikon (SNL) beskriver median på følgende måte:

> *"I statistikken er medianen den verdien av en variabel som ligger midt i det statistiske materialet, det vil si at like mange individer i materialet har verdier over medianen som*

[4] https://www.ibm.com/analytics/spss-statistics-software - (03.05.2019)
[5] https://www.st-andrews.ac.uk/media/capod/students/mathssupport/Likert.pdf - (30.04.2019)

under den." [6]

Typetall

SNL beskriver typetall (mode) på følgende måte:

> "*den observasjon som forekommer flest ganger*"[7]

Variasjonsbredde

SNL beskriver variasjonsbredde (range) på følgende måte:

> "*forskjellen mellom største og minste observasjonen*"[8]

Minimum og maksimum

Minimum og maksimum verdiene i datasettet beskriver henholdsvis den minste og den største observerte verdien i datasettet.

3.3.2 Korrelasjon

SNL beskriver korrelasjon som *"et statistisk mål på hvor mye to målbare størrelser henger sammen med hverandre"*[9]. Med andre ord er det stor korrelasjon jo flere respondenter svarer det samme på et spørsmål, svarer også likt på et annet spørsmål. Vi benytter oss av følgende metode for å måle korrelasjon.

Spearman's rho

Are Hugo Pripp beskriver Spearmans korrelasjonskoeffisient på en god måte i utgave 8 av Tidsskriftet for den Norske legeforening [27]. I artikkelen skriver Pripp at *"Spearman's rho (rang) er basert på verdiene til den relative rangeringen av observasjonene og ikke de observerte verdiene"*. Med andre ord så er Spearman's rho spesielt godt egnet for korrelasjonsanalyse av ordinale variable. I vårt tilfelle blir Spearman's rho brukt til korrelasjonsanalyse av ordinale variable.

Tolkning av resultat

Ved korrelasjonsanalyse med metoden beskrevet ovenfor, ender man opp med et tall mellom -1 og 1, kalt en korrelasjonskoeffisient (r). Det finnes ulike måter å tolke denne variabelen på. En forskningsartikkel publisert i 2018 [28], konkluderer med at tolkningen av korrelasjonskoeffisienten (r) er svært forskjellig blandt vitenskapelige forskningsområder og at det ikke finnes noen absolutte regler for tolkningen av dens styrke. På bakgrunn av dette benyttes en modell beskrevet i *Statistics How To*[10]. Intervallet -1 til 0 beskriver negativ korrelasjon, mens 0 til +1 beskriver positiv korrelasjon. De ulike gradene er beskrevet i tabell 1. Det er viktig å huske på at selv om to påstander korrelerer så tilsvarer ikke dette årsakssammenheng. Derfor må man være kritisk til resultatet og vurdere om korrelasjonen gir mening [27].

3.3.3 Metodekritikk

Det finnes mange måter å gjennomføre en statistisk analyse på og metoden vi har valgt er bare en av de. Vår erfaring på området er såpass begrenset at det blir vanskelig å

[6] https://snl.no/median - (30.04.2019)
[7] https://snl.no/typetall - (30.04.2019)
[8] https://snl.no/spredningsmål - (30.04.2019)
[9] https://snl.no/korrelasjon - (29.04.2019)
[10] https://www.statisticshowto.datasciencecentral.com/probability-and-statistics/correlation-coefficient-formula/ - (29.04.2019)

r		Beskrivelse
+1	-1	Perfekt
+0.7	-0.7	Veldig sterk
+0.4	-0.4	Sterk
+0.3	-0.3	Moderat
+0.2	-0.2	Svak
+0.1	-0.1	Ubetydelig
0	0	Ingen

Tabell 1: Tolkning av korrelasjonskoeffisient

vurdere alternative metoder. Vi har derfor basert oss i stor grad på oppdragsgivers ønsker og tidligere metodikk brukt av oppdragsgiver innen analyse av spørreundersøkelser, som ved f.eks. mørketallsundersøkelsen [6].

4 Identifisering av bestepraksis for måling av informasjonssikkerhetskultur

4.1 Innledning

En del av bacheloroppgaven går ut på å gjøre en gjennomgang og analyse av bestepraksis for måling av sikkerhetskultur, som bestemt i problemformuleringen, seksjon 1.4. Dette gjøres for å kunne ta godt begrunnet valg når det kommer til utvelgelse av rammeverk som skal benyttes for målingen. Det er to emner som fremkommer sentrale i litteraturen som bacheloroppaven ønker å belyse, *tindikatorer for informasjonssikkerhet* og *tilnærming til måling*. Arbeidet med å finne bestepraksis er gjort ut fra en litteraturanalyse og konsultasjon med ekspertene på fagfeltet Roar Thon og Bjarte Malmedal. Intervju med disse kan henholdsvis finnes i vedlegg D og E. For å finne bestepraksis vil da bacheloroppgaven prøve å finne fellesnevnere mellom litteraturen og ekspertenes erfaring.

4.2 Indikatorer for informasjonssikkerhetskultur

Et viktig element i utføringen av en måling er å ha gode indikatorer. Man bruker indikatorer for å angi eller beskrive forhold som er for kompliserte eller er for kostbare å måle direkte [29]. Litt enklere sagt betyr dette at indikatorer er "noe" som kan brukes for å måle kultur. Dette "noe" kan ofte være påstander eller spørsmål, avhengig av tilnærming til måling. Indikatorer kan være et forhold mellom demografiske data og en påstand som kan si noe om sikkerhetskultur. For eksempel kan påstanden, "Jeg låser datamaskinen når jeg går fra den" og demografiske variabelen "kjønn", si noe om informasjonssikkerhetskulturen. Indikatorer beskriver dermed en **relasjon** til sikkerhetskultur. Da det er for vanskelig og for omfattende å sammenligne indikatorer seg imellom, er det denne **relasjonen** vi skal identifisere og finne fellesnevnere til. Som et eksempel kan relasjonen fra eksempelet over være "compliance" mellom indikatoren og informasjonssikkerhetskultur.

Norsis har i sin rapport fra 2016, *Nordmenn og digital sikkerhetskultur*, påpekt usikkerheten i hva indikatorer for cybersikkerhetskultur virkelig er [30]. For å kunne bruke Norsis sine indikatorer som et sammenligningsgrunnlag er det viktig at deres definisjon på sikkerhetskultur er tilnærmet lik vår. Om Norsis definerte sikkerhetskultur som kun adferd, for eksempel hvorvidt ansatte klikker på phishing-linker, hadde vi ikke kunne brukt deres indikatorer som et sammenligningsgrunnlag da vår definisjon på sikkerhetskultur avviker fra denne. Delvis vil det da bety at vi ønsker å måle forskjellige ting. Norsis definerer dog sikkerhetskultur som holdninger, verdier og følelser, noe som treffer vår definisjon veldig godt. Norsis tok utgangspunkt i et sett med forskningspørsmål som dannet grunnlaget for hva de ønsket å finne ut av. Fra forskningsspørsmålene dannet de et sett med indikatorer, spørsmål, som forhåpentligvis kunne gi godt nok datagrunnlag for å svare på forskningspørsmålene. Indikatorene ble gruppert i åtte kjerneområder som cybersikkerhet består av: *collectivism, governance and control, trust, risk perception, techno-optimism and digitalization, competence, interest, behavior*.

Schlienger and Teufel [1] adresserer indikatorer ulikt Norsis, Schlienger og Teufel baserer sitt arbeid innen informasjonssikkerhetskultur på Schein sin lagdelte modell for

organisasjonskultur. Deres definisjon på informasjonssikkerhetskultur tar utgangspunkt i modellen og inneholder artefakter, felles verdier og grunnleggende antagelser og oppfatninger. Denne er beskrevet i teorikapitlet 2.3.1. De utførte også en spørreundersøkelse, lik Norsis, men deres indikatorer/spørsmål baserte seg på Schein sin modell og metoder for å evaluere informasjonssikkerhet. Se figur figur 5 for hvordan disse henger sammen. Det er krysningen mellom laget i modellen sammen med metode som danner relasjonen til informasjonssikkerhetskultur. Man ser umiddelbart at denne metoden gir lite bredde i relasjonen til informasjonssikkerhet, men potensiell mer nøyaktig i måling. En metode for evaluering som Schlienger og Teufel utførte var analyse av sikkerhetspolitikken. Fra denne politikken avledet de spørsmålet "The computer and electronic communications systems should be used for Orange's business activities only". Respondenter fikk tre svaralternativer (sant, usant, vet ikke) og måtte ta stilling til spørsmålet ut ifra (Dette er illustrert figur 4)

- hva man selv trodde
- hva det offisielle/uttalte svaret var
- hvis man selv var ansvarlig, ta stilling til hva man trodde var best

En annen tilnærming er Robbins [25] trenivåmodell 2 for organisasjonskultur, den deler kultur på tre nivåer: individuell, gruppe og organisatorisk nivå. Denne tilnærmingen har blitt brukt av Adele Da Veiga [3]. Derfor forskjellig fra Schlienger og Teufel der relasjonen mellom informasjonssikkerhetskultur og de organisasjonsnivåene blir bredere ved å videre dele opp hvert nivå videre inn i kategorier og komponenter. Veiga har også brukt spørreundersøkelse, med påstander som indikatorer, og endt opp med syv kjerneområder for informasjonssikkerhet; *ledelse og styring, sikkerhetsledelse og drift, sikkerhetspolicy, sikkerhetsprogramledelse, brukersikkerhetsstyring, teknisk sikkerhet og drift og endring*. Disse igjen deles opp i komponenter som er det som påvirker adferd og danner kulturen. Man kan se likheter mellom Adele Da Veiga sine kjerneområder og Norsis sine, men de skiller seg klart fra metoden til Schlienger og Teufel.

I intervjuet, vedlegg D, med Roar Thon legger han vekt på at indikatorer må velges ut ifra hva slags organisasjon man er. Følgelig vil dette bety for oss at et rammeverk vil antageligvis ikke kunne brukes ut av boksen, men samtaler med ledelse i IT-avdelingen kan forme indikatorene som kan brukes. Et annet viktig moment, som Bjarte Malmedal forteller i intervju, vedlegg E, er å benytte seg av sikkerhetsansvarlig i organisasjonen for å skaffe seg et oppdatert bilde på organisasjonens ståsted. For eksempel kan sikkerhetspolitikken være utdatert og ikke reflektere dagens ønsker for adferd.

Kai Roer, en ekspert på feltet, benytter seg av syv kjerneområder som informasjonssikkerhet består av: *attitude, cognition, behavior, communication, norms, responsebility, compliance* [31, s. 16]. Man ser her også likheter mellom Roer, Norsis og Adele Da Veiga sine kjerneområder.
Litteraturen vi har sett på er ikke enige i hvilke indikatorer man bør benyttes, ei heller hvordan man kommer fram til de. Det er noen fellesnevnere i gjennomgangen av indikatorer. Uten å ha inkludert annen litteratur som benytter Robbins modell her, vet vi at denne er mye brukt i arbeid med organisasjonskultur. Det samme gjelder for Schein sin modell. Annen fellesnevner er bruken av kjerneområder som beskriver informasjonssikkerhetskultur. Det kan derfor tyde på at Schein og Robbins modell er bestepraksis når det kommer til å velge indikatorer.

Method / Item	Analysis of documents	Questionnaire	Group session	Interview	Observation
Artefacts	Analysis of the security policy			Interview with the Chief Security Officer (CSO)	Audit
Official values		Questioning all level of employees			
True values					

Figur 5: Forholdet til Scheins modell fra Schlienger og Teufel

***Table 2.* Example question**

2	The computer and electronic communications systems should be used for Orange's business activities only.			
	a) Personally I think, this is	True	False	I don't know
	b) Orange regards this as	True	False	I don't know
	c) If I were responsible, I would regard this as	True	False	I don't know

Figur 4: Eksempel spørsmål fra [1]

4.3 Tilnærming til måling

Det finnes to metoder for tilnærming til måling av sikkerhetskultur, kvalitativ og kvantitativ måling. Den kvantitative metoden ble nevnt i seksjon 2.2 og handler om kvantifiserbar informasjon, som for eksempel antall, frekvens og tid. Kvalitativ metode derimot omhandler en deskriptiv innsamling og/eller fremstilling av en måling. Det er viktig å påpeke at ved å kun se på for eksempel datainnsamlingen eller analysen av målingen isolert sett, avgjør ikke om selve undersøkelsen er kvalitativ eller kvantitativ. For eksempel så går det an å gjennomføre et intervju hvor man i analysen etterpå baserer seg på tallbaserte verdier. Når vi i denne seksjonen beskriver et rammeverk som kvalitativt eller kvantitativt så er det hele undersøkelsen som er kvalitativ eller kvantitativ og ikke bare datainnsamling, utføring eller analyse av resultater som enkeltstående deler.

For å finne bestepraksis har vi sett på et utvalg av de rammeverkene som ble samlet inn etter metodikk beskrevet i seksjon 3.2. Bakgrunnen for dette er at det er vanskelig å finne ut hvilke rammeverk som er mest brukt i praksis for å måle sikkerhetskultur. Siteringer og rangering på sider som for eksmpel Google Scholar kan gi oss en pekepin på hvilke rammeverk som er mye brukt, men det sier ingenting om hvilke rammeverk de fleste virksomhetene bruker, som igjen tilsvarer bestepraksis. Videre i denne seksjonen gjør vi en undersøkelse av hvilke tilnærminger til måling som blir brukt av rammeverkene vi har sett på. Vi vil også undersøke hvorfor de ulike tilnærmingene til måling er valgt. Ut ifra denne undersøkelsen ønsker vi å få en indikasjon på hva bestepraksis kan være.

Schlienger og Teufel bruker en kvantitativ fremgangsmåte i sitt rammeverk *Tool Supported Management of Information Security Culture* [1]. Schlienger og Teufel mener at

ved bruk av spørreundersøkelse burde man benytte digitale hjelpemidler for utdeling av undersøkelsen og aggregering av innsamlet data da det er mer tidseffektivt og man trenger mindre ressurser for å gjennomføre prosessen. Tolkningen av dataen baserer seg på en statistisk analyse.

Adéle da Veiga undersøkte i "Cultivating and Assessing Information Security Culture" flere rammeverk og kom fram til at kvantitativ metode fungerte godt. For sin egen empiriske studie ble også en kvantitativ spørreundersøkelse benyttet [3]. For å analysere den innsamlede dataen ble det brukt programvare for statistisk analyse.

Yngve Nordby og Christian Waale Hansen ved "Informasjonssikkerhet atferd, holdninger og kultur" legger frem fremgangsmåter for å utføre både en kvalitativ og en kvantitativ undersøkelse. De har to metoder for innsamling av data: spørreundersøkelse (papirbasert eller web-basert) og intervjuer. Det forklares at at en web-basert undersøkelse vil være en god framgangsmetode om man ønsker nå større deler av en organisasjon og få ett mer helhetlig bilde av sikkerhetskulturen. Anonyme spørreundersøkelser gir potensielt mer ærlige svar enn ved identifiserbare undersøkelser eller intervjuer. Intervjuer gir mulighet for utdyping av svarene og kan gi mer nøyaktige svar og mindre rom for feiltolkning, dog er intervju veldig tidkrevende. Som nevnt mister deltakerene også anonymitet ved identifiserbare undersøkelser eller intervjuer, man kan da risikere at respondene oppgir svar som ikke reflekterer den sanne verdien [2, 9].

NorSIS har siden 2015 gjennomført kvalitative undersøkelser om sikkerhetskultur i befolkningen, på skoler og bedrifter i Norge[1]. Undersøkelsene ble gjennomført ved hjelp av en spørreundersøkelse, der man benyttet standardiserte spørsmål som ga tallbaserte svar [5]. Ved å gjennomføre en årlig undersøkelse, kan man se hvorvidt det er en forbedring eller forverring.

ENISA sier i "How to raise information security awareness" [22] at i store virksomheter ønsker man å gjennomføre kvantitative undersøkelser med spørreundersøkelse da dette skaper større statistisk grunnlag og er mer hensiktsmessig og effektivt enn intervjuer. Basert på budsjetter, hva virksomheten arbeider med og størrelsen, kan det argumenteres for bruk av en kvalitativ undersøkelse [22].

Magnus Alsaker skriver i "Indikatorer for informasjonssikkerhet" [32] at det kan være en svakhet rundt bruk av spørreundersøkelser i kvantitative fremgangsmåter, da de kan beskrive situasjonen feilaktig ved å fremstille den som annerledes enn faktum. På bakgrunn av dette mener Alsaker at det burde vurderes å benytte kvalitative metoder. Samtidig påpekes det at målingsmetoden også burde være enkel og lite tidkrevende, dersom man ser behov for å gjøre periodvise målinger for best mulig oppfølging av innførte tiltak og endringer.

Ut ifra en gjennomgang av disse rammeverkene kan det tyde på at de fleste rammeverkene benytter en kvantitativ undersøkelse for å måle sikkerhetskultur. De rammeverkene som bruker en kvantitativ undersøkelse bruker stort sett spørreundersøkelser for å samle inn data og statistisk analyse for å tolke den innsamlede dataen. Det argumenteres for å bruke kvantitative undersøkelser i større organisasjoner for å effektiviserse datainnsamlingen, men det kommer ikke frem hva som menes med større organisasjoner. Det er derfor vanskelig å avgjøre når det er hensiktsmessig å bruke kvantitative over kvalitative undersøkelser bare på organisasjonsstørrelsen. De rammeverkene som bruker en kvanti-

[1] https://norsis.no/nordmenn-og-digital-sikkerhetskultur-2018/ - (16.05.2019)

tativ undersøkelse ser ut til å foretrekke bruk av intervjuer for å samle inn data. Det er ikke forhåndsbestemt at våres sluttvurdering vil benytte seg av kvantitativ undersøkelse basert på dette, men punkter fra denne drøftingen taes med videre ved dypdykket i seksjon 5.5.

5 Valg av rammeverk

Som en del av arbeidet med denne oppgaven ble det gjennomført en omfattende litteraturanalyse av rammeverk for måling av informasjonssikkerhetskultur. Litteraturanalysen er å finne i sin helhet i vedlegg H. Litteraturanalysen som ble gjennomført i forbindelse med vår oppgave er svært sentral og essensiell, men vi finner det hensiktsmessig å adskille denne i et vedlegg da det er resultatet av analysen som benyttes videre i dette dokumentet. Vi vil derfor komme frem med de store linjene av analysen gjennom dette kapitlet, og oppsummere litteraturanalysen her.

Metoden beskrevet i seksjon 3.2 ble brukt til å finne rammeverkene som utgjør utgangspunktet for selve litteraturanalysen. For å effektivisere selve prosessen med å velge et rammeverk delte vi prosessen inn i flere steg. Seksjon 5.1 viser rammeverkene som er vurdert. Det første steget i valgprosessen presenteres i seksjon 5.2, som omhandler fundamentale krav for rammeverkene som skal vurderes. Videre kommer grovanalysen i seksjon 5.3, som videre avgrenser antall rammeverk som er funnet. I kravspesifikasjonen i seksjon 5.4, presenteres krav fra oppdragsgiver som vi forholder oss til, samt noen lovpålagte retningslinjer. Til slutt vil vi gjøre et en dyptgående analyse av hvert rammeverk i seksjon 5.5. I seksjon 5.6 og 5.7 blir rammeverkene sammenliknet og ett rammeverk for måling av sikkerhetskultur ved NTNU blir valgt.

5.1 Utvalg av rammeverk

Nedenfor presenteres rammeverkene som har blitt vurdert fra tabell 2 til tabell 9. Videre er all fakta fra rammeverkene hentet fra sin respektive kilde som oppgis her. Vi vil derfor ikke henvise i teksten til hvert rammeverk.

Navn	Informasjonssikerhet – atdferd, holdninger og kultur
Forfatter	Yngve Nordby, Christian Waale Hansen
Publisert	NTNU(ROSS)
Publikasjonsår	2005
Brukt av	NSM, Telenor, Rikstrygdeverket og Statens forvaltningstjeneste

Tabell 2: Rammeverk: Informasjonssikerhet - atdferd, holdninger og kultur - informasjon

Navn	The Security Culture Framework
Forfatter	Kai Roer
Publisert	Security Culture Framework Forum
Publikasjonsår	2015
Brukt av	N/A

Tabell 3: Rammeverk: The Security Culture Framework - informasjon

Navn	Understanding An Measuring Information Security Culture
Forfatter	Mohammed Alnatheer, Taizan Chan, karen Nelson
Publisert	Pan, S & Cao, T (Eds.) Proceedings of the 16th Pacific Asia Conference on Information Systems (PACIS), 11 - 15 July, 2012, Vietnam
Publikasjonsår	2012
Brukt av	N/A

Tabell 4: Rammeverk: Understanding An Measuring Information Security Culture - informasjon

Navn	Cultivating and Assessing Information Security Culture
Forfatter	Adéle da Veiga, Jan Eloff
Publisert	(phd thesis)
Publikasjonsår	2008
Brukt av	N/A

Tabell 5: Rammeverk: A framework and assessment instrument for information security culture - informasjon

Navn	Information Security Culture
Forfatter	Adéle da Veiga, Jan Eloff
Publisert	Kluwer Academic Publishers, Rand Afrikaans University, Springer - Boston MA
Publikasjonsår	2002
Brukt av	N/A

Tabell 6: Rammeverk: Information Security Culture - informasjon

Navn	Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture
Forfatter	Thomas Schlienger, Stephanie Teufel
Publisert	14th International Workshop on Database and Expert Systems Applications, 2003
Publikasjonsår	2003
Brukt av	Privat bank(Sveits) [1]

Tabell 7: Rammeverk: Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture - informasjon

Navn	Information security culture: A Behaviour Compliance Conceptual Framework
Forfatter	Salahuddin Alfawaz, Karen Nelson & Kavoos Mohannak
Publisert	8th Australiasaian Information Security Conference (AISC) Brisbane Australia
Publikasjonsår	2010
Brukt av	N/A

Tabell 8: Rammeverk: Information security culture: A Behaviour Compliance Conceptual Framework - informasjon

Navn	A comprehensive human factor framework for information security in organizations
Forfatter	Areej Alhogail, Abdurrahman Mirza & Saad Haj Bakry
Publisert	Journal of Theoretical and Applied Information Technology
Publikasjonsår	2015
Brukt av	N/A

Tabell 9: Rammeverk: A comprehensive human factor framework for information security in organizations - informasjon

5.2 Grunnleggende krav

Den initielle vurderingen av de aktuelle rammeverk ble gjort fortløpende etterhvert som vi fant rapporter som omhandler måling av sikkerhetskultur. Vurderingen ble gjort ut i fra kravene spesifisert i liste 10, initielle krav. Disse kravene er laget for tidlig å filtrere bort rapporter som ikke er verdt å bruke tid på i en dyptgående analyse. Kravene omhandler blant annet publiseringstid på rapporten, kredibiliteten til forfatterne og bruken av rammeverket. Videre er den initielle vurderingen for hvert rammeverk diskutert. Totalt syv rammeverk har blitt vurdert i dennne initielle vurderingen. De grunnleggende kravene er følgende fem nummererte krav listet opp i liste 10.

i. **Alder:** Rammeverket kan ikke være eldre enn 15 år.
ii. **Tredjeparter:** Rammeverkets utbytte må være under eierskap av NTNU.
iii. **Struktur:** Rammeverket har en logisk god struktur.
iv. **Kvalitet, kredibilitet:** Rammeverket er et resultat av forskning fra anerkjente forskere i informasjonssikkerhetsmiljøet, eller har opphav i bedrifter som har godt renomé.
v. **Kilder, referanser:** Rammeverkets rapport skal benytte refereranser og kilder.

Liste 10: Initielle krav for rammeverk

De ulike kravene blir forklart nedenfor.

i. **Alder** - Det er tenkt at rammeverket skal bli brukt fremover på NTNU for å måle sikkerhetskultur. Det ble da satt en grense på at rammeverket ikke skulle være eldre enn 15 år gammelt. Denne aldersbegrensningen ble satt på bakgrunn av at begrepet sikkerhetskultur har blitt forandret i takt med teknologien i de senere årene, som nevnt i tidligere i teorikapittelet (se seksjon 2.1). Dette kravet er ikke et "absolutt-krav". Dersom rammeverket er på grensen til alders-kravet, men gjør det bra på andre krav blir det tatt med videre.
ii. **Bruk av tredjeparter** - Med dette menes det at informasjon ikke kan deles med tredjeparter eller andre enn eier av informasjon, i henhold til ”Sentrale lover og forskrifter” på informasjonssikkerhetsområdet under NTNU’s Politikk for informasjonssikkerhet [8]. Det er et krav at rammeverket skal være en in-house løsning for NTNU. Rammeverket må da være publisert under en lisens som gjør det *open source*. Dersom et rammeverk ikke oppfyller dette kravet blir det direkte utelukket fra vuderingen.

iii. **Struktur** - Strukturen til rammeverket blir subjektivt vurdert. Dersom et rammeverk virker dårlig strukturert blir det ikke utelukket øyeblikkelig, men det teller negativt i den samlede vurderingen. Hensikten med dette kravet er å sørge for at rammeverket enkelt kan benyttes av oss og brukes videre på NTNU.

iv. **Kvalitet og kredibilitet** - Kredibiliteten til rammeverket og forfatterne blir i stor grad vurdert ut i fra hvor rammeverket er publisert og hvor mange siteringer forfatterne har på sider som Researchgate[1] og Google Scholar [2]. Det er ønskelig med et rammeverk som er anerkjent og viser til dokumentert bruk.

v. **Kilder** - Rammeverket benytter seg av kilder. Dette innefatter også at kildene er valide, delvis at disse eksisterer og de kan synes er gode. Kildene som benyttes gjennom rammeverkets rapport bør også inneha kredibilitet.

5.3 Grovanalyse

I listen nedenfor gis en kort beskrivelse av hvert rammeverks status mot de initielle kravene fra liste 10.

Figur 6 som følger listen nedenfor av rammeverkene, er en oppsummering av resultatet av rammeverksvurderingen.

- **Informasjonssikkerhet - atferd, holdninger og kultur (IAHK)**
  Dette er et rammeverk som skiller seg ut umiddelbart ved at det har meget god struktur. Rammeverket ble laget på bakgrunn av ett tidligere samarbeidsprosjekt mellom NSM og NTNU, som igjen har inspirasjon fra *Hearts and minds* [4]. Dette gjør at rammeverket fremstår som meget troverdig og scorer høyt på struktur og validitet. Det er noe gammelt og er på grensen til hva vi har satt i kravene. På bakgrunn av dette taes IAHK allikevel med til en videre vurdering.
- **The security culture framework**
  Dette er et relativt nytt rammeverk som er laget av Kai Roer. Dette rammeverket finnes i to versjoner. Den ene er en tjeneste som selskapet CLTRe[3] tilbyr. Her får man blandt annet en metode å måle sikkerhetskultur på. Dette er en tjeneste som blir utført av CLTRe, og overholder ikke kravene for bruk av tredjeparter. Den andre versjonen av rammeverket er en open source versjon, som er veldig dårlig dokumentert med tanke på hvordan det skal taes i bruk [4]. Dette rammeverket blir ikke med til videre vurdering basert på at det ikke overholder krav til bruk av tredjeparter og manglende dokumentasjon.
- **Understanding and measuring information security culture**
  Forfatterne av denne rapporten er personer som fremstår med høy troverdighet. Rammeverket ble publisert i en anerkjent publikasjon for forskere (PACIS)[5]. Strukturen anses som noe dårlig. Rammeverket er dog open source og overholder alderskravet. På bakgrunn av dette er rammeverket med til videre vurdering.
- **Cultivating and assessing information security culture**
  Denne publikasjonen er et resultat ev Adéle Da Veiga sin forsking mot sin PhD. Publikasjonen illustrerer et rammeverk for måling av sikkerhetskultur og legger

[1] https://www.researchgate.net/
[2] https://scholar.google.no/
[3] https://get.clt.re
[4] https://securityculturеframework.net/
[5] https://aisel.aisnet.org/pacis/

frem en meget godt struktur og beskrivelse av metoden for gjennomføring. Teori og fremgangsmåte bygges opp med grunnlag i valide ressurser og kildebruken er god. Førsteinntrykket av dette rammeverket er meget godt og det blir med til videre vurdering.

- **Analyzing information security culture**
  Thomas Schlienger og Stephanie Teufel er to forskere som fremstår som troverdige med blant annet et høyt antall siteringer, som blir brukt i annen forsking og artikler innenfor organisasjonskultur. De har laget dette rammeverket hvor det er meget god kildebruk og argumentasjon. Rammeverket er noe gammelt, men en mer avgjørende negativ faktor er mangel på god struktur. Detaljer rundt rammeverket er spredt på flere rapporter, som gjør det vanskelig å arbeide med og kan resultere i feil bruk. Vi ønsker ikke arbeide videre med dette rammeverket, men tar med oss deler av teorien herfra, da dette er relevant.
- **Information security culture: A behavior and compliance conceptual framework**
  Forfatterne til dette rammeverket har, basert på antall siteringer tilknyttet deres tidligere publikasjoner, liten kredibilitet. Men argumentasjonen i rammeverket og bakgrunnsteorien er fremdeles god og bygger på tidligere anerkjente pubilikasjoner som også går igjen i flere andre rammverk i denne analysen. Strukturen til rammeverket er god men prosessen rundt gjennomføring av en måling er fraværende. Dette gjør det vanskelig å bruke rammeverket slik det er tenkt å brukes. På bakgrunn av dette blir ikke dette rammeverket med til videre vurdering.
- **A comprehensive human factor framework for information security in organizations**
  En fordel med dette rammeverket er at det bygger på teori som er anerkjent. Det er i tillegg fra 2015, noe som trekker opp i vurderingen. Rammeverket legger vekt på kompleksiteten rundt måling av sikkerhetskultur. En stor svakhet ved dette rammeverket er at rapporten sier lite konkret om hvordan kartleggingen skal gjennomføres i praksis. Dette er grunnen til at det ikke kommer med for videre vurdering.

Figur 6 nedenfor, har de initielle kravene i hver kolonnene og rammeverkene i hver rad. Den uthevede kolonnen til høyre viser konklusjonen, altså hvilke rammeverk som blir med til en videre vurdering i dypdykket (se seksjon 5.5). I figur 6 er det brukt farger for å beskrive en tre-nivå skala, hvor fargene grønn, gul og rød beskriver en skala med nivåene god, dårlig og ikke tilstrekkelig. I tillegg er det tekst i enkelte ruter som kommenterer ytterligere hvordan rammeverket stiller seg til gjeldene krav.

Navn på rammeverk	i. Alder	ii. Bruk av tredjeparter	iii. Struktur	iv. Kvalitet og kredibilitet	v. Kilder	KONKLUSJON (grønn taes med i dypdykk)
Informasjonssikerhet – atdferd, holdninger og kultur (sjekkIT)	14					Ja
The Security Culture Framework	4		Ukjent		Ukjent	Nei
Understanding and Measuring Information Security Culture	7					Ja
Cultivating and Assessing Information Security Culture	11					Ja
Analyzing Information Security Culture	16					Nei
Information security culture: A Behaviour Compliance ConceptualFramewor	9					Nei
A comprehensive human factor framework for information securityin organizations	4					Nei

Figur 6: Oversikt over hvordan rammeverkene stiller seg til de initielle kravene. Høyre kolonne med tykk ramme, *konklusjon*, svarer på hvilke rammeverk som tas med i dypdykket.

5.3.1 Oppsummering av grovanalyse

På bakgrunn av gjennomgangen av rammeverkene opp imot de initielle kravene, kom vi frem til tre rammeverk som blir med videre til vurdering i dypdykket (se seksjon 5.5).

5.4 Kravspesifikasjon

For å legge til rette for et godt sammenlikningsgrunnlag mellom rammeverkene, kreves det at vi har tatt høyde for eksterne krav, retningslinjer og regelverk på forhånd. Dette vil i tillegg til å sørge for at valgt rammeverk forholder seg til gjeldene anordninger, også legge til rette for at rammeverket vi presenterer kan bli brukt aktivt innad i organisasjonen for å kartlegge sikkerhetskultur. I denne seksjonen presenteres eksterne rammer og ønsker for hva et rammeverk skal oppnå og forholde seg til.

5.4.1 Krav fra oppdragsgiver

1. Rammeverket skal være lett å forstå for ansatte som ikke har erfaring fra denne typen kartlegginger fra før. Det er ikke et krav at en person uten noen kunnskap om cyber og informasjonsikkerhetskultur skal kunne utføre målingen. Her menes det at rammeverket skal være entydig og lett å forstå for personer med noe IT-relevant utdannelse. For å unngå at dette blir en subjektiv mening for den enkelte, skal vi se på i hvor stor grad rammeverket som vurderes forklarer begreper.
2. Fremgangsmetoden for målingen skal være tydelig. Her skal det vurderes grad av

usikkerhet som foreligger rundt prosessen for gjennomføring av måling med bruk av det aktuelle rammeverket. Målet er at fremgangsmåten skal være så tydelig forklart som mulig.
3. Ønskelig med kvalitativ undersøkelse.
4. Lett å tolke resultat og komme med relevante tiltak.
5. Foreslå tiltak basert på alle faktorer ved resultatet av målingen. Med dette menes det at rammeverket skal ha en tiltakspakke som henger sammen med styrker og svakheter som analysen av målingen fører til. I de avdelingene hvor kartleggingen blir gjennomført er det ikke sikkert at alle har de samme styrkene og svakhentene når det gjelder sikkerhetskultur. Derfor er det viktig og komme med forslag til tiltak på alle elementene som er resultatet av målingen, og ikke bare svakhetene etter den første målingen vi gjennomfører.

5.4.2 Lovpålagte retningslinjer

1. Anonymisering av resultat og måling. Det skal ikke foretas en granskning av enkeltpersoner, men være en helhetlig måling på avdelingsbasis. For å sørge for at dette blir ivaretatt skal en eventuell spørreundersøkelse være anonym i tillegg til å ikke inkludere for mange demografiske opplysninger, slik at man indirekte kan identifisere enkeltpersoner. [6]
2. Undersøkelsen skal ha klare rammer for hvilke opplysninger som er relevante å samle inn [6].

5.5 Dypdykk

Denne seksjonen er et dypdykk i rammeverkene som kom videre fra den initielle vurderingen i seksjon 5.3. Målet med denne seksjonen er at den skal legge til rette for en diskusjon rundt valg av rammeverk i seksjon 5.6. Dypdykket baserer seg på krav listet i seksjon 5.4 og bestepraksis diskutert i teorikapittelet med seksjonene 4.2 og 4.3. For å forenkle navnene på rammeverkene har vi valgt å bruke følgende akronymer i resten av dette kapittelet.

Navn	Akronym
Informasjonssikkerhet - atferd, holdninger og kultur	IAHK
Understanding And Measuring Information Security Culture	UMISC
Information Security Culture Framework	ISCF

Videre forklares strukturen til dypdykket på hvert rammeverk. I dypdykket vil de tre rammeverkene presenteres med en *introduksjon* til selve rammeverket. En *målsetning* som presenterer hva rammeverket ønsker å oppnå. En *bakgrunn* som forklarer hvorfor rammeverket er laget og teori og studier som ligger bak arbeidet. *Indikatorer* tar for seg hvordan rammeverket måler kulturen og hvordan disse forholder seg til bestepraksis omtalt i kapittel 4.2. I *tilnærming til måling* vektes rammeverkets metode for måling opp mot bestepraksisen omtalt i teorikapitlet 4.3. *Styrker og svakheter* er en oppsummering av det vi mener er de beste og dårligste punktene med rammeverket.

[6] https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/personvern-pa-arbeidsplassen/?id=1333 - 15.02.2019

5.5.1 Informasjonssikkerhet - atferd, holdninger og kultur

Introduksjon

Rammeverket IAHK [2] presenterer et verktøy kalt SjekkIT. Dette er et verktøy for måling og forbedring av sikkerhetskultur, med fokus på menneskelige og organisatoriske faktorer i relasjon med sikkerhetsarbeid.

Målsetning

Hovedmålet med rammeverket IAHK er å tilby et konkret verktøy som kan brukes for å måle en virksomhets sikkerhetskultur. Det er også laget for å kunne nå bredt ut til alle typer virksomheter. Verktøyet SjekkIT har to bruksområder, med forskjellige målsetninger.

1. **Diagnostiseringsverktøy:** Her er målsetningen å kartlegge tilstanden i virksomheten, for å da avdekke sterke og svake sider relatert til sikkerhet.
2. **Forbedringsverktøy:** Målsetningen her er at spørsmålene fra undersøkelsen skal gi grunnlag for diskusjoner rundt sikkerheten og problemområder i bedriften ved å videreutvikle kultur gjennom å heve kompetansenivå, for å unngå unødvendige produksjonsopphold eller problemer.

Bakgrunn

IAHK er et rammeverk som er et resultat av et samarbeid mellom Nasjonal Sikkerhetsmyndighet (NSM) og NTNU. Prosjektet ble startet på bakgrunn av et tidligere samarbeid mellom NTNU og NSM, som resulterte i en rapport kalt Informasjonssikkerhet og innsideproblematikk [33]. Denne rapporten gikk ut på å kartlegge holdninger, adferd og kultur i forbindelse med informasjonssikkerhet. Informasjonssikkerhet og innsideproblematikk er igjen basert på *Hearts and Minds*[7] Hearts and Minds er et verkøy som ble brukt av Shell fra 1986 - 2001 og kan vise til dokumentert forbedret sikkerhetskultur. IAHK har en solid bakgrunn og bygger på mange års forskning og forbedringer. De konkrete forbedringspunktene er videreført fra Informasjonssikkerhet og innsideproblematikk [33] og har dannet grunnlaget for utviklikngen av IAHK.

Indikatorer

Rammeverket IAHK baserer seg i stor grad på Scheins trenivåmodell av kultur, som forklart i teorikapitlet (se seksjon 2.3.1). IAHK har spesielt fokus på de to øverste nivåene i modellen: artefakter og observerbare verdier, hvor rammeverket prøver å måle rutiner og prosedyrer. Det gjenværende nivået, grunnleggende antakelser vil kun endres når de nye adferdsmønstrene blir tatt for gitt som riktige [2]. IAHK har videreutvilket målingsmetoden fra Kufås og Mølmann [33] med tilbakemeldinger fra brukere, samarbeidspartnere og sentrale teorier [2]. Det er også fokus på å forankre spørsmålene i relevante teorier, policier og standarder, slik som IAEA [34], ISO 17799 [35] og elementer i god IKT-sikkerhetspolitikk. Det er svært godt dokumentert i rammeverket hvor hvert enkelt spørsmål er hentet fra. IAHK's indikatorvalg er lik annen praksis, som skrives om i bestepraksis kapittelet (se seksjon 4.2).

[7] http://heartsandminds.energyinst.org - (10.05.2019)

Tilnærming til måling

Hovedsakelig gjennomføres IAHK som en kvantitativ undersøkelse. På lik linje med de andre rammeverkene nevnt i seksjon 4.3, så bruker også IAHK en spørreundersøkelse for å gjennomføre målingen. Denne spørreundersøkelsen kan tolkes ulikt avhengig av bruksområdet til rammeverket. Dersom man bruker SjekkIT som et diagnostiseringsverktøy utfører man en statistisk analyse av svarene. IAHK advarer mot å ikke dra konkrete slutninger basert på svarene fra den statistiske analysen [2, s. 36]. Det er ikke sikkert at full score på hvert spørsmål er det som er riktig for bedriften. Man må benytte skjønn for å avgjøre hva man kan forvente fra hvert spørsmål [2, s. 43].

Velger man heller å benytte SjekkIT som et forbedringsverktøy får man en litt mer kvalitativ tilnærming til bearbeidingen av undersøkelsen. Etter undersøkelsen er gjennomført skal resultatet diskuteres gruppevis. Her skal det også foreslåes relevante tiltak. Denne fremgangsmåten er basert på organisasjonsutvikling med samskapt læring hvor sjansen for gjennomføring øker dersom folk får være med på å bestemme selv [2, s. 45]. Ved bruk av IAHK er det mulighet for en å utføre en kvantitativ undersøkelse, som følger bestepraksis. Det er også mulighet for å tilrettelgge for en kvalitativ måling dersom dette er ønskelig.

Styrker og svakheter

IAHK er et rammeverk som har en solid bakgrunn. Det er tatt høyde for forbedringspunkter fra andre rammeverk i utviklingen av IAHK, som anses som et pluss. Rammeverket er godt dokumentert og har en tydelig gjennomgang av teoretien bak utformingen av indikatorer og spørsmål. IAHK ble utviklet via et samarbeid mellom NTNU, NSM og SINTEF, som gir økt kredibilitet til rammeverket. Det er også positivt at rammeverket kommer med 30 spørsmål som en basispakke, med muligheter for å legge til eller bytte ut spørsmål fra en forhåndslagd tilleggspakke eller tilpasset til virksomheten. En annen styrke er at det er mulighet for å benytte IAHK som både en kvalitativ og en kvantitativ undersøkelse. Ved å ta høyde for begge disse tilnærmingene til måling kan rammeverket ytterligere tilpasses avdelingens behov og ønsker.

IAHK har også noen svakheter. Som nevnt i IAHK så favner det ikke alle ledelsesperspektivene, men velger å ha fokus på byråkratiske ledelsesstrukturer, som innebærer fokus på kontroll og overvåkning [2, s. 9]. Det er ikke sikkert at alle lederne har dette ledelsesfokuset og det kan derfor bli litt feil for enkelte avdelinger. En annen svakhet ved rammeverket er at det kan synes å konkludere for mye i svaralternativene på spørsmålene. Det kan være lett for respondenten å finne ut hva som er det "riktige svaret" basert på alternativene. Et eksempel på et slikt spørsmål er vist i figur 7 nedenfor.

		Atferd				
10	B/L	Hvilke vaner har du for valg og bruk av brukernavn og passord?	Skifter aldri passord. Enkelhet prioriteres framfor sikkerhet.		Bruker samme passord på forskjellige tjenester. Skifter passord av og til.		Skifter passord ut fra en risikovurdering. Benytter passord som er en kombinasjon av tall og store/små bokstaver som er over 7 tegn.
11	B/L	Hvilke e-postvaner har du?	Åpner og videresender e-post med vedlegg uten å tenke på sikkerheten. Tenker aldri over at e-post kan komme uvedkommende i hende.		Det er laget regler for god e- post skikk som beskriver hvordan e-post skal benyttes.		Er klar over at e-post er et usikkert medium. Avsender kan forfalskes, og vedlegg og lenker kan være skadelige eller feilaktige. Det er laget regler som beskriver hvordan e-post kan brukes sikkert for å sikre at bare rett person får korrekt informasjon uten at andre får innsyn i det.

Figur 7: Eksempel på spørsmål i IAHK [2, p. ~100]

I enkelte tilfeller kan svaralternativene også være litt for spesifikke. I svaralternativet til høyre i figur 7 beskrives det en spesifikk passord-policy. Dette gjør at spørsmålet ikke nødvendigvis er relevant for virksomheten som utfører undersøkelsen, men dette er noe som enkelt kan tilpasses.

5.5.2 Understanding and measuring information security culture

Introduksjon

Rammeverket UMISC [36] er utledet ved Queensland University of Technology i Australia, som ved bruk av både kvalitative og kvantitative metoder adresserer sikkerhetskultur.

Målsetning

Målsetningen til UMISC er å utvikle en metode for måling av informasjonssikkerhetskultur som tydelig skiller mellom hvilke faktorer som danner sikkerhetskultur og hvilke faktorer som påvirker sikkerhetskulturen.

Bakgrunn

Utviklingen av UMISC baserer seg på en litteraturanalyse som konkluderte med mangel på et skille mellom faktorer som er med på å danne sikkerhetskultur og faktorer som påvirker sikkerhetskultur. Disse forskjellene er utgangspunkt i tilnærmingen til dette rammeverket. Utviklingen startet med et kvalitativt intervju for å finne ut hvilke faktorer som utgjør og påvirker sikkerhetskultur. Ut i fra en analyse av disse intervjuene endte de opp med to hypoteser:

1. Sikkerhetskultur består hovedsaklig av to reflekterende faktorer: bevissthet og eierskap til sikkerhet.
2. Ledelsens innvirkning, informasjonssikkerhetspolitikken og opplæring i informasjonssikkerhet er faktorer som har positiv og betydelig innflytelse på sikkerhetskulturen.

Spørsmålene i intervjuet de gjennomførte benytter en fem-nivå likert skala, som er tilsvarende brukt i andre rammeverk og spørreundersøkelser. Utviklingsprosessen til undersøkelsen er omfattende og er etter vår vurdering gjort på en måte som sørger for god validitet og reliabilitet. De startet med å samle påstander og brukte informasjonssikkerhetseksperter til å sortere påstandene etter metodikk fra Moore and Benbasa [37]. Målet med prosessen var å finne ut hvordan spørsmålene konvergerer og hvor representative de er. De foretok flere runder med eksperter for å få flere synspunkter på vurderingen av spørsmålene. Prosessen ble avsluttet med en ny gjennomgang av påstandene med de initielle intervjuobjektene for å sørge for at de er relevante for arbeidsmiljøet. Dette resulterte i 18 påstander.

Indikatorer

Indikatorene er hentet ut ifra de initielle intervjuene i rammeverket. Resultatet fra bearbeidingen av disse intervjuene førte til fem kategorier, som igjen er underkategorier av de to hypotesene rapporten bygger på:

- **Faktorer som danner sikkerhetskultur**
    - *Security awareness*
    - *Security ownership*

- **Faktorer som påvirker sikkerhetskultur**
  - *Top management involvement in information security*
  - *Information security policy enforcement*
  - *Information security training*

Det er vanskelig å avgjøre om disse indikatorene er bedre egnet for NTNU enn andre. Indikatorene fokuserer mye på retningslinjer og policier, som nevnt i seksjon 4.2 kan være uheldig å benytte. Dette rammeverket skiller seg ut fra de to andre rammeverkene i dypdykket ved at det bruker sin egen metode for å hente ut indikatorer til undersøkelsen. De to andre rammeverkene har enten Schein eller Robbins sin organisasjonsmodell i grunn. Indikatorene eller kjerneområdene ligner på andre, omtalt i bestepraksis kapitlet, men det vil være vanskelig å si om disse er bedre egnet enn andre. Det som er positivt er at kjerneområdene ser ut til å reflektere organisasjonen de ble brukt i siden de nettop brukte intervju for å hente de ut. Dette er noe som ble omtalt i bestepraksis kapitlet som viktig.

Tilnærming til måling

UMISC bruker en kvantitativ tilnærming til måling. Spørreundersøkelsen analyseres ved hjelp av statistiske metoder. Her er det lagt vekt på validitet og reliabilitet med bruk av ulike statistiske verktøy. Videre i rammeverket brukes det statistisk analyse for å svare på de initielle hypotesene, omtalt i *bakgrunn* ovenfor. På dette punktet følger UMISC bestepraksis ved å benytte en kvantitativ undersøkelsesmetode.

Styrker og svakheter

NTNU er en organisasjon bestående av mange ulike avdelinger og dermed også mange ulike arbeidsområder. I de initielle intervjuene i dette rammeverket har de oppsøkt bedrifter med ulik demografisk sammensetning. Både privat og offentlig sektor, med organisasjonsstørrelse fra 100 - 3100 ansatte og ulike typer industri. Dette gjør at spørsmålene som resulterte fra disse intervjuene kan ha stor relevanse for NTNU. En annen styrke er at spørsmålene viser til kildene de ble hentet fra.

UMISC har også noen svakheter. De spørsmålene som ikke ble med i undersøkelsen ble ikke vedlagt i rammeverket deres. Disse kan fremdeles være relevante for bedrifter i et annet miljø, selv om de ble utelukket i undersøkelsen rammeverket ble brukt i. Det kunne også ha vært interessant å sett på dokumentasjonen fra intervjuene. Det kan være uheldig at rammeverket ikke bruker en modell i grunn, slik som Schein eller Robbins, så man kan spå usikkerhet i validiteten til indikatorene. Indikatorene sin relevanse og nøyaktighet må i så fall testes for å kunne brukes i de i en undersøkelse. En av de utfordringene ved å benytte dette rammeverket er at det er skrevet på en måte der man innledende trenger god forståelse for statistikk. Selve forklaringen rundt analysen og valideringen av spørreundersøkelsen kan derfor være krevende å forstå. Dette gjør det til en utfordring ved bruk av rammeverket. UMISC inneholder heller ingen klart definert fremgangsmåte for gjennomføring av måling.

5.5.3 Information Security Culture Framework

Introduksjon

Rammeverket ISCF [3] er resultatet av Adéle Da Veiga sin forskning mot sin PhD grad hos University of Pretoria. Rammeverket inneholder en empirisk studie som danner grunnlaget for utviklingen av Information Security Culture Assessment (ISCULA), som er verktøyet for å måle informasjonssikkerhetskultur.

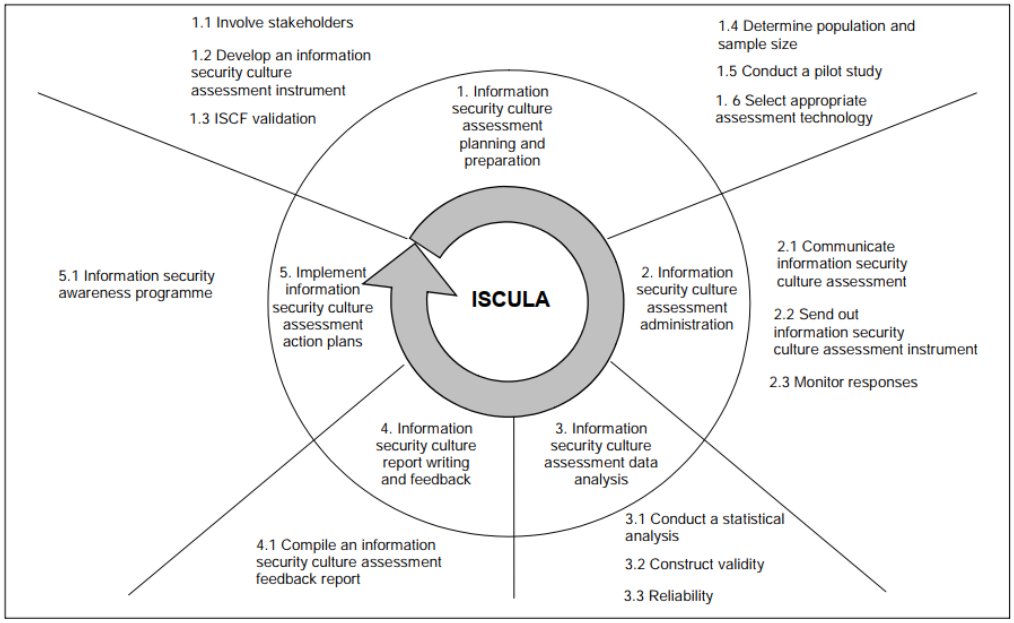
Målsetning

Hovedmålet med dette rammeverket er å fremme og forbedre sikkerhetskulturen i en virksomhet, ved å redusere risikoen menneskelig adferd har mot beskyttelsen av informasjonsverdier. Det skal også adressere hvilket nivå sikkerhetskulturen ligger på og om det er på et akseptabelt nivå. Underveis i rapporten blir det svart på flere forskningsspørsmål. Ett av disse omhandler utviklingen av rammeverket og går ut på at rammeverket skal fungere som et grunnlag for vurderingen av informasjonssikkerhetskultur.

Bakgrunn

ISCF innleder med en detaljert forklaring av begreper og gjennomgang av eksisterende forskning rundt sikkerhetskultur. Da Veiga sammenliknet 14 forskjellige rammeverk på kriterier som omhandler måling av sikkerhetskultur og validiteten til denne målingen. Da Veiga vurderte også hvilken rapport som gir det mest komplette bildet på sikkerhetskultur ut i fra forhåndsbestemte kriterier som for eksempel Schein sin trenivåmodell for kultur [38], som forklart i seksjon 2.3.1. Det blir konkludert med at det ikke finnes ett rammeverk som oppfyller alle disse krieriene. Dette danner grunnlaget for utviklingen av dette rammeverket.

ISCULA inneholder en fremgangsmåte for hvordan en måling skal gjennomføres. Dette er illustrert i figur 8. I grove trekk omhandler denne prosessen alt fra planlegging og gjennomføring av en spørreundersøkelse til analyse av dataene og skriving av rapport. Det legges vekt på involvering av interessenter og validering av komponenter (hvilke deler i organisasjon som påvirker adferd).



Figur 8: *Information Security Culture Assessment process* ***(ISCULA)*** [3]

Indikatorer

Utviklingen av rammeverket startet med å identifisere de informasjonssikkerheskomponentene som kan påvirke informasjonssikkerhetskulturen i en organisasjon. Rammeverket ble senere utviklet rundt disse. Indikatorene ble identifisert ut i fra følgende kilder: ISO/IEC 17799 og ISO/IEC [35] FDIS 27001 [39], PROTECT [3, chap. 4.2.3], Capability Maturity Model[8], ISA [40] og Standard of Good Practice for Information Security (SOGP) [41]. Indikatorene som ble identifisert i kildene ovenfor ble sammenliknet og valgt ut i fra hvilke som forekommer flest ganger. Til slutt blir indikatorene kategorisert i syv kategorier:

1. Ledelse og styring
2. Sikkerhetsledelse og drift
3. Sikkerhetspolicy
4. Sikkerhetsprogramledelse
5. Brukersikkerhetsstyring
6. Teknisk sikkeret og drift
7. Endring

En full versjon av de ulike hovedkategoriene og deres underkategorier (komponenter) er illustrert i vedlegg F. ISCF presenterer en unik tilnærming til inndeling av indikatorene. De deles inn i organisatorisk, gruppe og individuelt nivå, som er Robbins [25] sin trenivåmodell for organisasjonsstruktur. Adferd over tid innenfor disse nivåene fører til en kultur som er synlig i observerbare artefakter, verdier og grunnleggende antakelser, som er nivåene i Schein sin trenivåmodell for kultur [38]. Denne klassifiseringen ved hjelp av både Schein og Robbins modell gjør at man kan måle spesifikt opp mot den

[8] https://www.itgovernance.co.uk/capability-maturity-model- (19.04.2019)

enkelte komponenten for å se hva den påvirker.

Indikatorene er opprinnelig hentet ut ifra kjente standarder, noe som nevnt i bestepraksis kan være uheldig (se kapittel 4). Ved at ISCF kategoriserer indikatorene i etterkant av identifiseringen så viser rammeverket hvordan de ulike indikatorene påvirker adferd, som igjen danner kultur. På bakgrunn av denne inndelingen av indikatorene i Schein og Robbins modell så er dette likt andre tilnærminger som beskrevet i bestepraksis, kapittel 4.2.

Tilnærming til måling

Undersøkelsesmetoden til ISCF er en kvantitativ spørreundersøkelse av sikkerhetskulturen i en virksomhet. I undersøkelsen som ble gjort i rammeverket er det brukt surveytracker[9] for å analysere dataene. Det er ikke definert en kvalitativ undersøkelsesmetode i rammeverket. Ved at ISCF bruker en kvantitativ undersøkelsesmetode, stemmer dette med hva bestepraksis tilsier.

Styrker og svakheter

Noen styrker ved ISCF er at definisjonen av sikkerhetskultur som blir presentert i rammeverket er et resultat av en strukturert analyse av eksisterende litteratur. Definisjonen er lik den vi har definert i kapittel 2. Rammeverket er detaljert og godt forklart i rapporten. Det er i tillegg brukt språk som gjør det lett å forstå, selv for personer med liten teknisk bakgrunn. Klassifiseringen av komponentene gjør det lettere å finne målrettede tiltak for hver enkelt komponent. ISCF er lik andre tilnærminger i bestepraksis på både indikatorvalg og tilnærming til måling.

ISCF har også noen svakheter. Den delen av rammeverket som beskriver den statistiske analysen og valideringen av undersøkelsen er litt lite detaljert og har ingen klart definert fremgangsmåte.

5.6 Sammenlikning og diskusjon av rammeverk

Denne seksjonen sammenlikner de tre rammeverkene fra dypdykket over. Målet er å ende opp med ett rammeverk for måling av sikkerhetskultur ved NTNU. Sammenlikningsgrunnlaget er kravspesifikasjonen, bestepraksis når det gjelder tilnærming til måling og valg av indikatorer, i tillegg til diskusjon av hvorvidt rammeverkene passer til NTNU.

Som forklart i seksjon 5.4 ble det definert noen krav til rammeverkene. Tabell 11 oppsummerer hvordan de ulike rammeverkene stiller seg til de bestemte kravene. En "*X*" betyr at rammeverket oppfyller kravet, mens en "∼" betyr at rammeverket delvis oppfyller kravet.

Som tabellen viser så finnes det ikke ett rammeverk som oppfyller alle kravene vi har satt. Dersom et rammeverk ikke oppfyller et krav, betyr det ikke umiddelbar utelukkelse av rammeverket. Flere av kravene er noe som kan tilpasses i etterkant og i enkelte rammeverk er også dette intensjonen, fordi det må tilpasses til virksomheten og arbeidsmiljøet. Dette gjelder for eksempel kravene til tiltak. Ingen av rammeverkene vi har vurdert sier noe om hvilke tiltak som passer til det enkelte spørsmålet, eller eksempler på tiltak for å forbedre sikkerhetskulturen i en bedrift. Ingen av rammeverkene har dette i sin målsetning eller forskningsspørsmål og det er rimelig å anta at dette i mange tilfeller er

[9] Verktøy for utstedelse av web-basert spørreundersøkelse. Nettsiden finnes ikke lengre. - (21.03.2019)

Krav	IAHK	UMISC	ISCF
Inget krav om forkunnskaper før gjennomføring	X		X
Tydelig fremgangsmetode	X	~	X
Benytter kvalitativ undersøkelse	~		
Lett å tolke data og å foreslå tiltak	X	X	X
Tiltak basert på resultat av undersøkelse			
Anonymisert resultat og måling			
Klarhet i hvilke opplysninger som er relevant å lagre	X		~

Tabell 11: Oppsummering av krav for rammeverkene

en separat prosess fra måling av sikkerhetskultur. Videre følger en forklaring til hvordan hvert av rammeverkene stiller seg opp imot kravene i tabell 11.

Bakgrunnen for at IAHK delvis oppfyller kravet til bruk av kvalitativ undersøkelse er at det avhenger av bruksområdet til rammeverket om undersøkelsen er kvalitativ eller kvantitativ. IAHK beskriver en tydelig fremgangsmåte for hvordan man kan gjennomføre en måling og har god forklaring av sentrale begreper. Prosessen for hvordan analysen av undersøkelsen skal gjennomføres er noe fraværende, men det er lett å kunne foreslå tiltak basert på indikatorene rammeverket deler spørsmålene inn i. IAHK presenterer et forslag til demografiske opplysninger som kan være relevante å samle inn, men sier ingenting om hvordan man skal gjennomføre undersøkelsen anonymt.

UMISC oppfyller færrest av kravene sammenliknet med de andre rammeverkene. Det er en rapport som er vanskelig å forstå med liten til fraværende forklaring av begreper. Beskrivelse av fremgangsmetoden er god i enkelte deler av rammeverket. Spesielt når det gjelder analysen av undersøkelsen. UMISC foreslår ingen demografiske opplysninger. Dette fører til uklarhet i hvilke opplysninger som er relevante å lagre. Fremgangsmåten for anonymisering av undersøkelsen blir ikke nevnt.

ISCF er det mest detaljerte rammeverket blandt de tre som er vurdert. Det har en meget detaljert fremgangsmåte og en god struktur. Ordbruken som er valgt fører til at rapporten er lettlest. Valgene som er gjort er godt dokumentert og argumentert for i rapporten. ISCF benytter en kvantitativ undersøkelse. Tolkningen av undersøkelsen gjennomføres ved hjelp av en statistisk analyse. Det nevnes så vidt hvilke demografiske opplysninger som kan samles inn, men det sies ingen ting om prosessen for anonymisering av undersøkelsen. En stor fordel med dette rammeverket er at det er veldig lett å foreslå tiltak til indikatorene for hvert spørsmål. ISCF har den mest forseggjorte inndelingen av indikatorene sammenliknet med de andre rammeverkene i dypdykket. Dette gjør at det er lett å finne ut hvilket område indikatorene adresserer og komme med spesifikke og målrettede tiltak.

5.6.1 Styrker og svakheter

Fra kravspesifikasjonen er det IAHK og ISCF som oppfyller flest av kravene, med fire av kravene oppfylt. UMISC oppfyller to av kravene i kravspesifikasjonen. Videre i dette kapittelet diskuteres de ulike styrkene og svakhetnene til hvert av rammeverkene for å se hvordan rammeverkene stiller seg til bestepraksis (se kapittel 4).

IAHK og ISCF skiller seg ut med en godt forklart og dokumentert bakgrunn for valg som er gjort i rammeverket. Her er ISCF noe bedre enn IAHK fordi den foretar en dypere

analyse i teorikapittelet. UMISC er svakere enn de andre rammeverkene på dette punktet. Rapporten til UMISC er ikke like detaljert som de andre og har i liten grad forklaring av begreper og gjør antakelser om at leseren innehar en viss bakgrunnskunnskap om emnet. UMISC har derimot en mulig større relevanse for NTNU på bakgrunn av intervjuene som ble gjort med en målgruppe, som vurderes som representativ for NTNU's ansatte. IAHK har også relevanse til NTNU fordi den er utviklet med mål om å kunne brukes som et verktøy for måling i et bredt utvalg virksomheter. ISCF har relevanse til NTNU ved det måler et bredt spekter av indikatorer.

5.7 Valg av rammeverk

Fordi målingen av sikkerhetskultur er tenkt å foregå på avdelingsbasis er det viktig at rammeverket er lett å forstå for den som utfører målingen ved en senere anledning. Dette fører til at kravet til forståelse av rammeverket stilles sterkere enn de andre. ISCF sin metode for å klassifiere indikatorene er unik og gir etter vår vurdering en større mulighet for tilpasning av rammeverket til NTNU. Dette styrker totalinntrykket av ISCF. Indikatorene som er brukt i ISCF passer bedre til NTNUs retningslinjer for informasjonssikkerhet[10], da begge er derivert fra blandt annet ISO27001. Vi vurderete det lettere for oss å tilpasse spørsmålene i henhold til NTNUs retningslinjer og organisasjonsstruktur ved bruk av ISCF enn med de andre rammeverkene. ISCF presenterer også en av de mest strukturerte fremgangsmåtene for å måle sikkerhetskultur. På bakgrunn av dette valgte vi rammeverket *Information Security Culture Framework - (ISCF)* som rammeverk for måling av sikkerhetskultur ved NTNU.

[10] https://innsida.ntnu.no/wiki/-/wiki/norsk/informasjonssikkerhet - Krever tilgangsnivå: intern

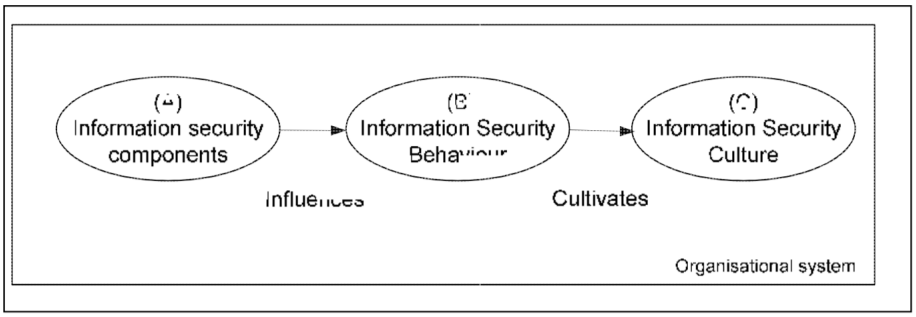
6 Information Security Culture Framework

6.1 Innledning

I seksjon 5.7 ble det konkludert med at rammeverket Information Security Culture Framework (ISCF) skal brukes for å måle sikkerhetskultur ved NTNU. Dette kapitlet forklarer hvordan rammeverket er bygd opp og fungerer i praksis. Informasjon om ISCF er hentet fra Da Veiga sin doktorgradsavhandling [3].

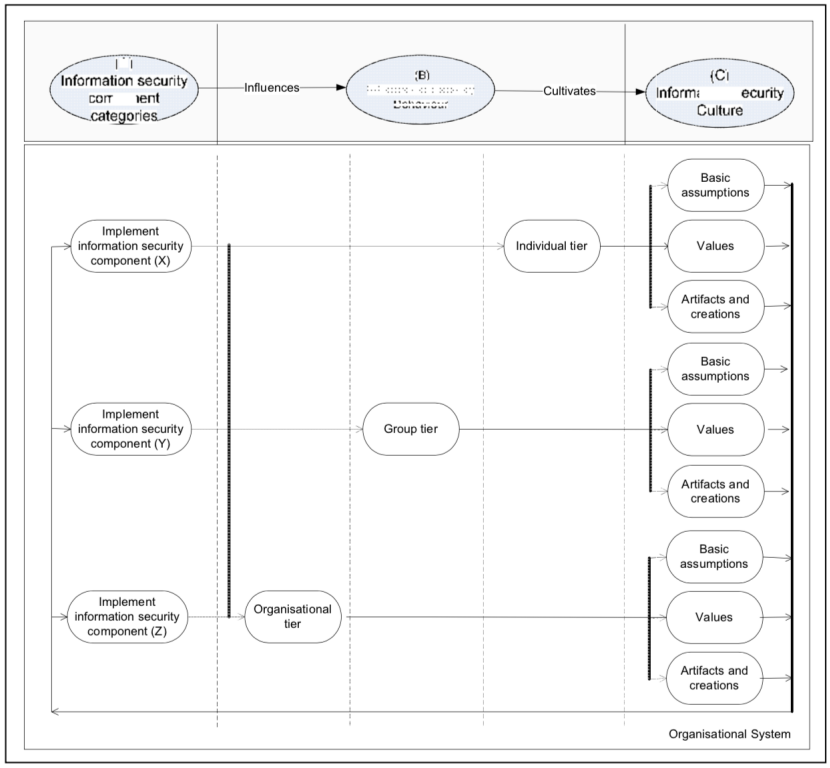
6.2 Forklaring til rammeverket

Rammeverket bygger på Robbins modell, som er forklart i teoridelen (se seksjon 2.3.2). Dette betyr at rammeverket forsøker å måle kultur på flere nivåer: organisatorisk, gruppe og individuelt nivå. I hvert av de tre nivåene er det visse informasjonssikkerhetskultur-"komponenter" som påvirker adferden og adferden danner informasjonssikkerhetskulturen. Man kan se denne utviklede kulturen i artefakter, verdier og underliggende grunnleggende antakelser som Schein har oppdelt organisasjonskultur i (se seksjon 2.3.1). For eksempel stadfester politikk eller prosedyrer hva ledelsens forventninger til handling er, dette påvirker de ansattes adferd. Ansattes adferd danner igjen kulturen, som vist i figur 9.



Figur 9: Nivå 1: Komponenter påvirker adferd, som danner kultur. - Figur hentet fra ISCF [3]

For å illustrere relasjonen mellom A, B og C i figur 9 kan vi se på en komponent, for eksempel politikk. En politikk uttrykker blant annet ledelsens forventinger til ansatte når det gjelder sikker bruk av informasjonsverdier. Den angir akseptabel oppførsel og bidrar til sikringen av informasjonsverdier innad i organisasjonen. Uten en politikk, vil ikke ansatte ha noe konkret å ved bruk av informasjonsverdier, og kan derfor utgjøre en risiko mot disse informasjonsverdiene.



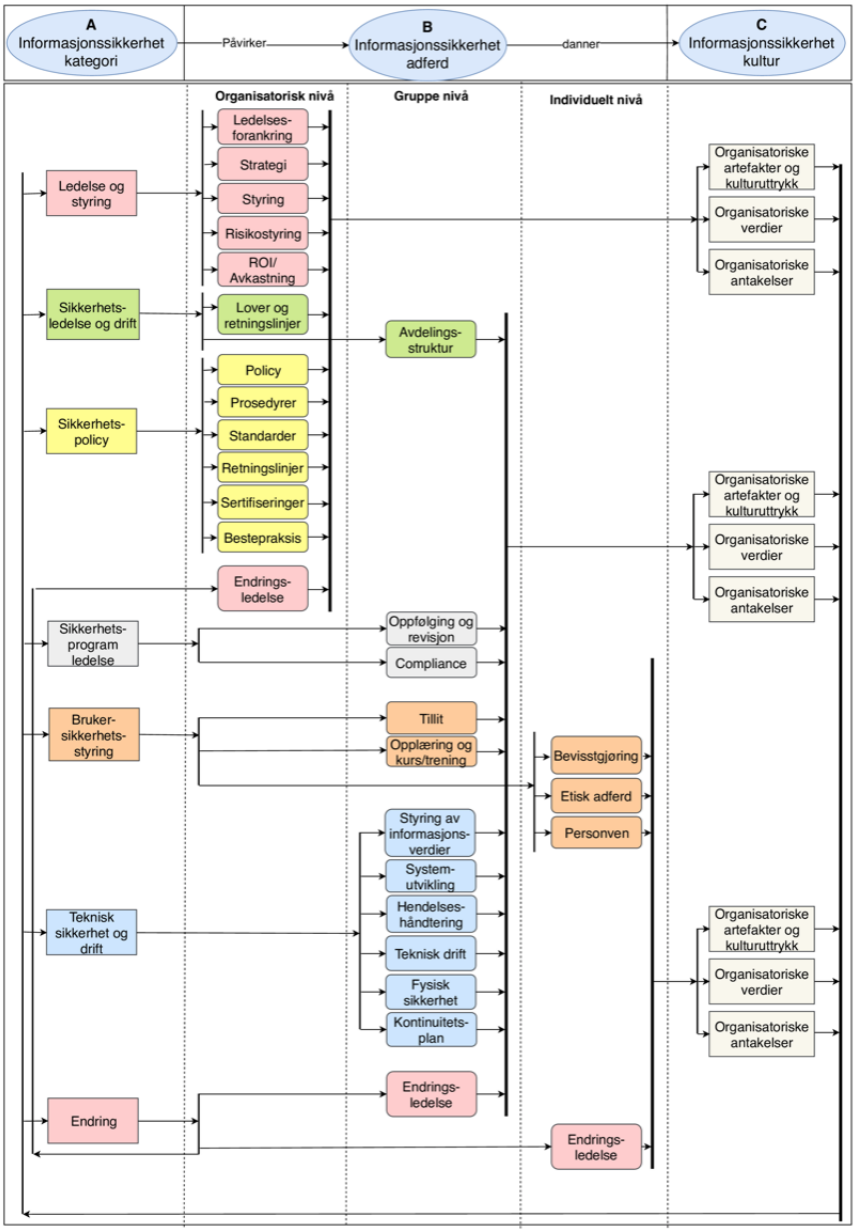
Figur 10: Nivå 2: Komponenter påvirker adferd, som utvikler kultur. - Figur hentet fra ISCF [3]

Figur 10 illustrerer relasjonene mellom kategorier for sikkerhetskomponentene (A), adferd (B) og kultur (C). Man kan gruppere komponentene (B) i forskjellige kategorier (A), referert til som X, Y og Z i figur 10. Kategoriene som er identifisert i rammeverket er listet opp i tabell 12, sammen med en forklaring. Komponentene er benyttet i en organisasjon på organisatorisk, gruppe eller individuelt nivå, (B).

Organisatorisk nivå omhandler organisasjonens struktur, om for eksempel organisasjonen fungerer sentralisert eller desentralisert. Det kan også omhandle beskyttelsesmekanismer for informasjonsverdier som er tatt i bruk, eller verktøy som utvikles for å bidra i ansattes arbeid.

Gruppenivå dreier seg om adferd mellom ansatte i for eksempel en seksjon. En gruppes syn på antakelige riktige valg kan overkjøre individuelles meninger og syn. [3, p.93].

Ved det individuelle nivået ser man på personkarakteristikk som kan påvirke adferd på arbeidsplassen. Personlighetstype kan påvirke adferd; to forskjellige personer med ulik personlighet kan ha ulik adferd ved etterlevelse av organisasjonspolitikk [25].



Figur 11: Nivå 3: Komponenter påvirker adferd, som utvikler kultur. - Figur oversatt fra ISCF [3]

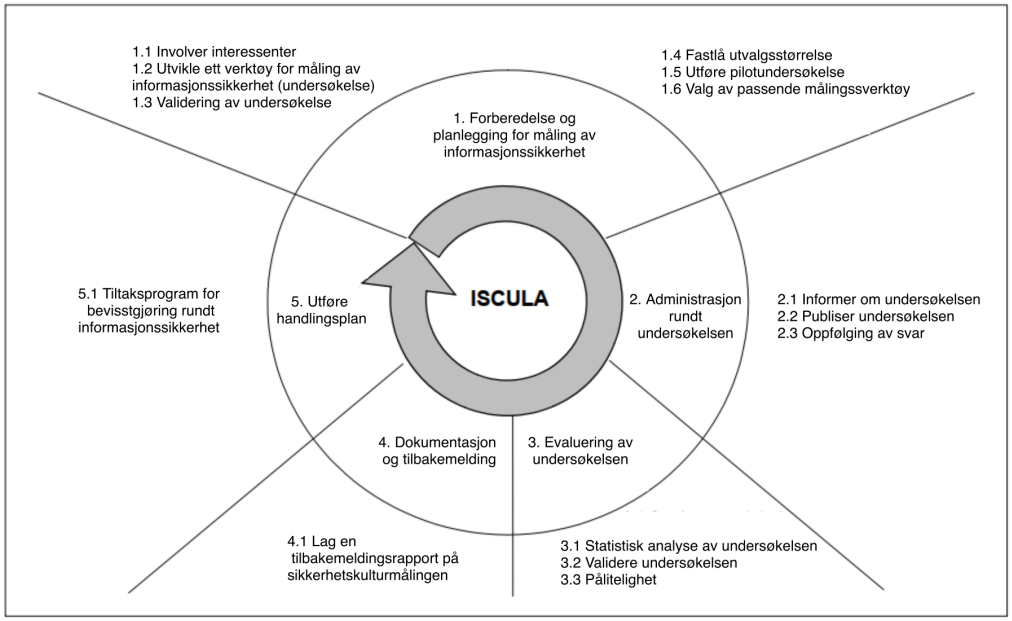
Adferd kan derfor sies at utvikles over tid til en kultur, som er synlig i artefakter, verdier og grunnleggende antakelser hos de ansatte. Hovedfiguren for ISCF i figur 11, viser til hvilke komponenterer som påvirkes på hvilke nivå i Robbins organisasjonsmodell. Vi gjør en mer detaljert forklaring av komponentene som blir benyttet i spørreundersøkelsen i tabell 15.

6.3 Prosessen for gjennomføring

ISCF legger grunnlaget for verktøyet *Information Security Culture Assessment* (ISCULA) som beskriver prosessen for å utføre en måling av sikkerhetskultur. Den originale figuren som viser ISCULA finnes i dypdykket, kapittel 5.5, se figur 8. Vi har produsert en norsk

versjon av dette verktøyet i figur 12, nedenfor.

ISCULA illustrerer en stegvis prosess, bestående av fem steg for gjennomføring av måling for informasjonssikkerhet. ISCULA fungerer som en prosessbasert veileder for gjennomføring. Prosessen bidrar til planlegging, tildeling av roller, kvalitetssikring av data og identifisering av handlingsplaner. En norsk versjon som forklarer alle stegene i rammeverket finnes i vedlegg G.



Figur 12: ISCULA prosessen [3] - Oversatt til norsk

Kategori	Definisjon
Ledelse og styring	Styrer hvordan komponenter implementeres i andre kategorier. En definert strategi bidrar til gjennomføring av de andre komponentene. Risikostyring er essensielt ved å definere risikonivåer, utføre vurderinger og håndteringer, og gjennomføre den satte strategien. Risiko vil være sett på med forskjellig syn avhengig av hvilke mål organisasjon har. ROI, og underliggende målinger bidrar til å vurdere tilstanden rundt informasjonssikkerheten.
Sikkerhetsledelse og drift	Inneholder komponenter som hjelper ved styring av informasjonssikkerhet, og omtaler lover og retningslinjer som en organisasjon må forholde seg til.
Sikkerhetspolicy	Inneholder dokumenterte krav som er definert av organisasjonen, standarder eller guidelines for å styre ansattes atferd.
Sikkerhetsprogramledelse	Referer til komponentene brukt som sørger for effektivt håndtering av informasjonssikkerhet. Oppfølging, revisjon og compliance inkluderes i denne kategorien, som del av sikkerhetsprogrammet.
Brukersikkerhetsstyring	Omhandler de komponentene som forholder seg til de ansatte og deres adferd. Prosesser som er essensielle her er opplæring, for styringens del, men også tillit, som relaterer direkte til forholdet mellom ansatte.
Teknisk sikkerhet og drift	Involverer tekniske, og også fysiske verktøy som sikrer informasjonsverdier, og håndtering av disse. Kategorien omhandler styring av informasjonsverdier, systemutvikling, hendelseshåndtering og kontinuitetsplan og prosesser relatert til disse.
Endring	Endringsledelse er en prosess som i tillegg til innsikt i ansattes verdier og holdninger krever forankring. Dette er med å skape eierskap og bidrar til at prosessen lykkes. Derfor ansees endring som en prosess på tvers av alle komponent-kategoriene.

Tabell 12: Kategorier i ISCF

7 Tilpasninger av Information Security Culture Assessment til NTNU

Dette kapittelet handler om hvordan rammeverket ISCF tilpasses NTNU som organisasjon, for bruk på avdelinger. Merk forskjellen mellom dette kapittelet og neste kapittel. Kapittel 8 viser *bruken* av rammeverket og tar for seg spesifikke tilpasninger vi har gjort for gjennomførelse på IT-avdelingen. Rammeverket tilpasses NTNU etter beste evne ved å inkludere tilbakemeldinger fra oppdragsgiver og Randi Utstrand[1].

7.1 Valg av demografiske opplysninger

Det kommer frem i ISCF at demografiske data kan være nyttig å bruke i en spørreundersøkelse med tanke på kostnadseffektivitet. Videre forklares dette ved at man kan identifisere en spesifik g ruppe basert på demografiske data, eksempelvis alder og ansiennitet og deretter komme med målrettede tiltak. På denne måten kan man muligens redusere kostnader om det er mindre hensiktsmessig å innføre tiltak på en større målgruppe. Størrelsesordenen på målgruppen ved spørreundersøkelsen er derfor avgjørende ved valg av demografiske spørsmål. Dersom utvalget ved en uthentet demografisk egenskap ikke er representativt, vil man ikke kunne benytte denne demografiske opplysningen. Det må derfor taes en beslutning basert på den enkelte avdelingens størrelse. Hvis avdelingen er liten, vil muligens respondendter miste anonymitet da man gjerne kan "peke ut" en respondent ut i fra de demografiske egenskapene man spør om. Det er uheldig om individuelle føler de mister anonymitet grunnet dette og vi anser at det som et viktig punkt som bør taes hensyn til.

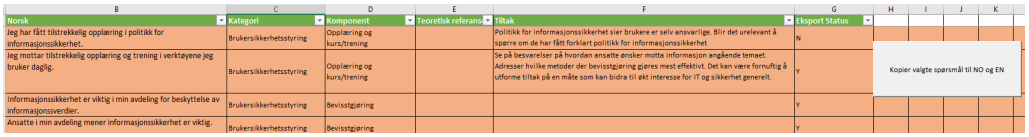
7.2 Tilgjengelighet til rammeverket

Vi ønsker at den norske versjonen av ISCULA (se vedlegg G) kan benyttes av personer som innledningsvis ikke behøver å sette seg inn i ISCF. Vår versjon av ISCULA følger den samme strukturen og formålbeskrivelsen som orginalen, men fjerner teoretisk bakgrunn, argumentasjoner og diskusjoner. Dette øker lesbarheten, som igjen påvirker sannsynligheten for at prosessen blir gjennomført. Spørmålene adskilles fra rammeverket for å forenkle videre arbeid og tilpasninger av spørsmål. Vi utviklet en arbeidsbok i Excel, som inneholder over 80 påstander som kan filtreres etter kategori og komponent (se figur 13 for et utsnitt). Videre utviklet vi en macro[2] i arbeidsdokumentet, som kan ta de valgte påstandene (Y/N i egen kolonne) og eksportere disse til et nytt Excel-ark (se vedlegg C). Macroen kopierte over valgte spørsmål og satte disse i en slik rekkefølge, med konfigurasjonsparametere slik det kunne eksporteres til applikasjonen for distribusjon av spørreundersøkelsen, *SelectSurvey*[3].

[1] https://www.ntnu.no/ansatte/randi.utstrand - (19.04.2019)

[2] https://support.office.com/en-ie/article/quick-start-create-a-macro-741130ca-080d-49f5-9471-1e5fb3d581a8 - (18.05.2019)

[3] https://innsida.ntnu.no/wiki/-/wiki/Norsk/Sp%C3%B8rreunders%C3%B8kelser



Norsk	Kategori	Komponent	Teoretisk referans	Tiltak	Eksport Status
Jeg har fått tilstrekkelig opplæring i politikk for informasjonssikkerhet.	Brukersikkerhetsstyring	Opplæring og kurs/trening		Politikk for informasjonssikkerhet sier brukere er selv ansvarlige. Blir det urelevant å spørre om de har fått forklart politikk for informasjonssikkerhet	N
Jeg mottar tilstrekkelig opplæring og trening i verktøyene jeg bruker daglig.	Brukersikkerhetsstyring	Opplæring og kurs/trening		Se på besvarelser på hvorden ansatte ønsker motte informasjon angående temaet. Adresser hvilke metoder der bevisstgjøring gjøres mest effektivt. Det kan være fornuftig å utforme tiltak på en måte som kan bidra til økt interesse for IT og sikkerhet generelt.	Y
Informasjonssikkerhet er viktig i min avdeling for beskyttelse av informasjonsverdier.	Brukersikkerhetsstyring	Bevisstgjøring			Y
Ansatte i min avdeling mener informasjonssikkerhet er viktig.	Brukersikkerhetsstyring	Bevisstgjøring			Y

Kopier valgte spørsmål til NO og EN

Figur 13: Utsnitt av Excel-arbeidsbok

7.2.1 Språkvalg og fremmedord for spørreundersøkelse

Ved oversettelse av spørreundersøkelsen er det viktig at budskapet og definisjoner ivaretas. Fordi NTNU primært er norsk så ble det valgt sammen med oppdragsgiver å oversette påstandene til norsk. Dette vil også bidra med at det kan gjennomføres en ny måling av sikkerhetskulturen på et senere tidspunkt. For å sørge for at innholdet og formulering ble ivaretatt ved oversettelse, ble de oversatte påstandene validert i samarbeid med oppdragsgiver. Det er også viktig at begreper og definisjoner ikke er ukjente for ansatte i NTNU, som var noe oppdragsgiver fokuserte på under valideringen av påstandene. For eksempel så benytter ISCF ulik gradering av informasjon i forhold til hva NTNU benytter seg av [4]. Generelt vil denne prosessen gjelde for all ordlyd som spriker fra hva respondente er kjent med. Prosessen gjøres ved å benytte informasjon og begrepsavklaringer som befinner seg på NTNUs nettsider, samt veiledning fra oppdragsgiver Gaute Wangen.

7.3 Krav til lengde og antall spørsmål på undersøkelsen

Rammeverket stiller ingen krav til lengde på undersøkelsen fra før. I samarbeid med oppdragsgiver og Randi Utstrand[5] har vi kommet fram til at en undersøkelse ikke må overskride ti minutter, hvor det beste er å holde seg innenfor seks til åtte minutter. Dette inkluderer selve spørreundersøkelsen og lesing av introduksjon. Dette er grunnet det er ønskelig at flest mulig gjennomfører undersøkelsen for best mulig datagrunnlag.

7.4 Valg av graderingskala for spørreundersøkelse

Rammeverket deler spørreundersøkelsen opp i tre deler, demografiske spørsmål, kunnskapspåstander og påstander som adresserer kultur. Kunnskapsspåstandene besvares i ISCF med bruk av svaralternativene ja og nei. I samråd med oppdragsgiver var det hensiktsmessig å i enkelte tilfeller legge til vet ikke som svaralternativ. ISCF sier at en fem nivå likert skala, med nivåene svært uenig, uenig, vet ikke, enig, svært enig, skal benyttes ved likert-skala som svaralternativ. Sammen med oppdragsgiver ble det bestemt å bruke en seks-nivå likert skala, hvor vi ønsker å tvinge respondenten til å ta stilling til påstanden. Dette betyr at vi fjerner "vet ikke" som alternativ og introduserer nivåene "noe enig" og "noe uenig" [42].

[4] https://innsida.ntnu.no/wiki/-/wiki/Norsk/Kanaler+for+informasjon+og+nyheter#section-Kanaler+for+informasjon+og+nyheter-Informasjonssikkerhet+&+klassifisering

[5] https://www.ntnu.no/ansatte/randi.utstrand - (19.04.2019)

8 Steg 1 - Forberedelse og planlegging

De neste kapitlene omhandler steg 1 til steg 5 i ISCULA (figur 12) som beskriver hvordan vi utfører målingen av sikkerhetskultur på IT-avdelingen. Vi følger prosessen som beskrevet i rammeverket vi har tilpasset til NTNU (se vedlegg G). Steg 1 omhandler innvolvering av interessenter, planlegging og tilpassning av undersøkelsen for IT-avdelingen.

8.1 Bakgrunn

Rammeverket har i kapittel 7 blitt tilpasset for å kunne bli brukt på avdelinger ved NTNU. Siden avdelinger har varierende størrelse, kompetanse, risiko, trusselbilde og retningslinjer må rammeverket derfor tilpasses til avdelingen det utføres på. Etter konsultasjon med oppdragsgiver og Randi Utstrand[1] valgte vi å utføre undersøkelsen på IT-avdelingen. Med den begrensede tiden vi har er det hensiktsmessig å gjennomføre det på den avdelingen oppdragsgiver er tilknyttet for å kunne hurtig lansere undersøkelsen da byråkratiet rundt lansering av spørreundersølelser på NTNU kan ta en del tid. IT-Avdelingen har rundt 200 ansatte og er delt opp i seks seksjoner. Det kan være noe uheldig å gjennomføre en måling av sikkerhetskultur på en avdeling som antageligvis allerede har god kjennskap til sikkerhet. For erfaringen sin skyld og for at rammeverket skal best mulig kunne brukes på hele NTNU hadde det vært hensiktsmessig å gjennomføre målingen på en avdeling som har noe mindre kjennskap til sikkerhet, da det antas at de fleste avdelinger på NTNU har mindre kompetanse enn IT-avdelingen på det området. Det hadde gjort at erfaringene fra undersøkelsen kunne blitt brukt til å bedre rammeverket for flertallet av avdelingene i NTNU og ikke blitt begrenset til de med IT-kompetanse. Det vil si at ved senere anledninger må det gjøres en god jobb for å sørge for at også ansatte med mindre IT-kompetanse forstår undersøkelsen på den måten at målingen faktisk blir en ressurs for de og ikke en byrde. Dette vil også sørge for validitet og pålitelighet på målingen.

8.2 Steg 1.1 - Innvolvere interessenter

Dette steget handler om å involvere interessenter og å få støtte i ledelsen for gjennomføring av en måling. I Retningslinjer for arbeid med sikkerhetskultur og opplæring innen informasjonssikkerhet [2] på NTNU står det at leder for HR- og HMS-avdelingen er ansvarlig for arbeidet med sikkerhetskultur. Arbeidet starta derfor tidlig med å ta forbindelse med Randi Utstrand for å få gode føringer for undersøkelsen. I tillegg ble leder for IT-avdelingen, Håkon Alstad, involvert for støtte og veiledning for gjennomføring av undersøkelsen på avdelingen. Oppdragsgiver Gaute Wangen er også med på å gi føringer for målingen.

8.3 Steg 1.2 - Fokusområdet for undersøkelsen

Denne seksjonen omhandler å finne fokusområder for undersøkelsen og da spesifikt hvilke komponenter som er mest relevant.

[1] https://www.ntnu.no/ansatte/randi.utstrand - (19.04.2019)
[2] https://innsida.ntnu.no/wiki/-/wiki/norsk/informasjonssikkerhet - intern (19.05.2019)

Undersøkelsen består av generelle påstander som omhandler sikkerhetskultur og vil bli derivert fra de komponentene interessentene mener er mest gjeldene eller interessante for IT-avdelingen. De andre påstandene er derivert fra hypoteser utviklet i samarbeid med interessentene, såkalte *industry input* som Da Veiga kaller det. Hypotesene vil være gjeldende for hele NTNU eller spesifikt for IT-avdelingen. Hypotesene vil også naturligvis være tilhørende én eller flere komponenter.

En utfordring med å velge fokusområder er å holde oss innenfor tidskravet på maks 10 minutter. Rammeverket spesifiserer 27 komponenter som sikkerhetskultur består av. Bare de 41 generelle påstandene vil overgå tidskravet. Det er derfor viktig å bruke interessentene til å finne de komponentene som er gjeldene for IT-avdelingen.

Prosessen for å prioritere komponenter er basert på kryssreferanser i e-postkorrespondanse med personer i NTNU, blant annet Håkon Alstad og Randi Utstrand. Vi brukte også intervjuet med Roar Thon, hva vi som prosjektgruppe mener er viktig, samt hva selve kjernen i informasjonssikkerhet og kultur dreier seg om (se seksjon 2.1). I tillegg benyttet vi hendelsedata[3] og mørketallsundersøkelsen [6]. I underseksjonene nedenfor beskrives hvilke fokusområder vi har hentet fra de ulike områdene. Til slutt presenteres komponentene som brukes for å måle sikkerhetskultur på IT-avdelingen.

Konsultasjon med Håkon Alstad

I arbeidet med avgrensingen har vi forhørt oss med Håkon Alstad, for å få informasjon om hva han kunne tenke seg interessant å se på. Vi spurte også om det er spesielle områder som har hatt fokus i det siste og som kunne tenkes adresseres for å se forandringer eller effekt. Alstad kom fram til 13 komponenter som er viktig for IT-avdelingen: Ledelsesforankring, strategi, styring, risikostyring, avkastning, avdelingsstruktur, sertifisering, tillit, systemutvikling, hendelseshåndtering, teknisk drift, fysisk sikkerhet og kontinuitetsplan. Alstad påpeker at avdelingen ikke har noe strategi, men strategi burde vært på plass og kommunisert videre til de ansatte. Videre sier Alstad at styringen gjerne kunne blitt kommunisert bedre, ledelsen har god fokus på risikostyring, men opplæring av ansatte er noe manglende.

Intervju av Roar Thon

I et intervju med Roar Thon spurte vi om hvilke indikatorer et rammeverk burde ta med (se vedlegg D). På det spørsmålet svarte han blant annet at faktorer at man kan se på er: “Føler du får nok informasjon om sikkerhet”,“Vet du hva virksomheten utsettes for til daglig?” og “Forstår du hva konsekvensene er om sikkerheten kompromitteres?”. Disse spørsmålene kobler vi til komponentene compliance og hendelseshåndtering, som omhandler konsekvenser og den ansattes forståelse av sikkerhet i virksomheten. Ut ifra dette ble følgende spørsmål tatt med i spørreundersøkelsen.

- Jeg får nok informasjon om sikkerhet (se figur 23)

Konsultasjon med Randi Utstrand

Innledende til spørreundersøkelser er det viktig å kartlegge problemområdet. Dette sørger for at spørsmålene forblir relevante ettersom hva man ønsker kartlegge. I dialog med Randi Ustrand ble det identifisert flere interessante temaer som vi ved bruk av rammeverket mappet tilbake til komponenter av interesse. Listen under presenterer de identifiserte

[3] Utlevert fra oppdragsgiver

temeaene.

- Oversikt verdier (eks. system)
- Gjennomføring av risikovurderinger
- Implementering av identifiserte tiltak
- Håndtering av avvik
- Utvikling av IKT-systemer/tjenester der disse direkte understøtter prosesser som eksempelvis: Behandling av personopplysninger (innebygget personvern) i eks. tilsettingsprosesser, personalsaker
- Sporbarhet og dokumentasjon (kontrollerende del)

Disse temaene kobler vi sammen med komponentene: risikostyring, systemutvikling og styring av informasjonsverdier. Ut ifra dette blir følgende spørsmål derivert.

- Jeg mener retningslinje for sikker utvikling brukes ved innføring eller utvikling av systemer (se figur 50)
- Jeg kjenner til arbeidsprosessene ved andre fakulteter i NTNU (se figur 43)
- Jeg klassifiserer informasjon jeg jobber med (se figur 53)
- I seksjonen jeg jobber i har vi oversikt over hvilke informasjonsverdier vi behandler (se figur 42)
- Seksjonen jeg jobber i implementerer risikoreduserende tiltak (se figur 42)
- Lederen min er opptatt av at vi kan lære og forbedre oss av de avvik som meldes inn (se figur 40)

Analyse av hendelsesdata

Ved begrensing av komponenter har vi tatt utgangspunkt i hendelsesdata fra NTNU [43]. Her har vi sett på hvilke hendelsesårsaker som økte fra 2017 til 2018. Dette gir grunnlag for å prioritere komponenter i undersøkelsen. Ved kobling mellom hendelsesdata og komponent har vi sett på definisjonen av komponenten og sårbarheten til hendelsesårsaken for å se hvilke komponenter som passer til hendelsen. Dette er viktig at dette forstås som en subjektiv vurdering, da tolkning er en vurdering som gjøres subjektivt og kan føre til ulikt resultat ut ifra hvem som utfører tolkningen. Denne vurderingen resulterte i tilsammen ti komponenter. I tabell 13 lister vi opp hendelsesdata og tilhørende komponenter, samt en forklaring til hvorfor denne komponenten ble valgt. Tabell 14 viser hvor ofte hver komponent ble knyttet sammen med en årsak i hendelsesdataen.

Hendelsesdata	Komponent	Begrunnelse
Phishing	Bevisstgjøring, Teknisk Drift	Veldig høye nivåer i 2017 og 2018. Økning i 2018.
Vulnerable software	Systemutvikling, Bestepraksis, Risikostyring	Økning fra 2017 til 2018
Regular user compromise	Policy, Retningslinjer, Oppfølging og Revisjon, Bevisstgjøring	Gått litt ned fra 2017 til 2018, men generelt mange hendelser som har denne årsaken
IT-Policy violation	Policy, Compliance	Markant nedgang fra 2017 til 2018. Kan være aktuelt å fjerne fra undersøkelsen
Misconfiguration	Teknisk drift	Økning fra 2017 til 2018
Trojan	Etisk adferd, Teknisk drift, Bevisstgjøring, Retningslinjer	Holdt seg omtrent lik fra 2017 og 2018.

Tabell 13: Hendelsesdata og komponenter det tilhører

Komponent	Frekvens i hendelsesdata
Bevisstgjøring	2
Teknisk drift	3
Systemutvikling	1
Bestepraksis	1
Risikostyring	1
Policy	2
Oppfølging og revisjon	1
Compliance	1
Etisk adferd	1

Tabell 14: Frekvens av komponenter i hendelsesdata

Analyse av mørketallsundersøkelsen

I konklusjonen på mørketallsundersøkelsen [6] sies det at det finnes et stort forbedringspotensiale når det kommer til rapportering av sikkerhetshendelser og avvik på NTNU. Dette kan knyttes opp mot komponenten hendelseshåndtering. Videre er det konkludert med at det er svak praksis når det kommer til både fysisk og logisk sikring av sensitiv informasjon. Denne konklusjonen kan knyttes sammen med komponenten styring av informasjonsverdier. I tillegg til komponentene identifisert ovenfor er endringsledelse svært sentral i rammeverket.

Valg av komponenter

Basert på tidsbegrensingen til spørreundersøkelsen er det nødvendig at de relevante komponenter med tilhørlige påstander blir identifisert. Denne prosessen forklares også i rammeverket til da Veiga [3, chap. 6.4.1.2] som et innledende arbeid.

Tabell 15, gjenspeiler resultatet av arbeidet med identifisering og prioritering av komponenter. Resultatet av prosessen for å velge ut komponenter førte til en metrikk som kan brukes for å velge de mest relevante komponentene. “Antall” kolonnen i tabellen, viser hvor mange ganger den enkelte komponenter er knyttet opp mot ulike interessenter.

De komponentene som ble brukt i undersøkelsen er uthevet i tabell 15. Komponentene som har har størst nummer i "Antall" kolonnen ble naturligvis brukt i undersøkelsen, fordi de er nevnt av flere interessenter som viktige områder. Det er ønskelig å dekke flest mulig komponenter, samtidig som varigheten på undersøkelsen overholder kravet på ti minutter. Dersom man bare velger de komponentene med antall ≥ 2 fra tabellen, vil det ikke dekke over nok komponenter til å få et helhetlig bilde av kulturen. Derfor må det tas med noen flere komponenter. De komponentene som ble valgt ut med 1 i antall-kolonnen, ble valgt ut ifra bachelorgruppens subjektive mening om hva som kunne passe for IT-avdelingen. I tillegg til disse ble også komponentene "opplæring og kurs/trening" og "personvern" tatt med i undersøkelsen. Dette var på bakgrunn av Håkon Alstad og Randi Utstrand nevnte disse som mulige forbedringsområder for IT-avdelingen. De utvalgte komponentenes påstander, sammen med påstander derivert fra Intervju med Roar Thon og hypoteser fra Randi Utstrand gav oss påstandene som skal brukes for å måle sikkerhetskultur på IT-avdelingen. Totalt fører dette til at spørreundersøkelsen inneholder 37 påstander.

Komponent	Definisjon	Antall
Ledelsesforankring	Formel støtte av ledelse på strategisk nivå for arbeid med informasjonssikkerhet. Skal gi retningslinjer for arbeid med informasjonssikkerhet i organisasjonen.	1
Strategi	En strategisk plan for informasjonssikkerhet med visjon og plan for håndtering av risiko knyttet til informasjonssikkerhet. 2) Strategien møter organisasjonens forretningsmessige mål og knyttes opp imot eksisterende organisatoriske- og IT –strategier som sørger for at kort- og langsiktige mål ivaretas.	1
Styring	Omhandler settet med policyer og retningslinjer som definerer hvordan organisasjonen styrer og kontrollerer bruken av teknologi og beskyttelse av informasjon.	1
Risikostyring	Risikostyring handler om kartlegging av sannsynlighet og konsekvenser ved uønskede hendelser. Prosessen innebærer risiko- og sårbarhetsvurdering for å oppnå akseptabel risiko.	3
Avkastning	Begrepets betydning i rammeverket omhandler forvaltning av ressurser og verdiøkning. Dette kan være kapital, tid og arbeidsinnsats.	1
Avdelingsstruktur	Referer til avdelingsens struktur innenfor IT, sammensetning og rapporterings hierarki (eks. Sentralisert eller desentralisert). Komponenten innebærer også roller, ansvar, ferdigheter og erfaring.	1
Politikk	I NTNU er det politikk for informasjonssikkerhet som er førende for arbeid med informasjonssikkerhet. ISO 2700 definerer policy som “den overordnede intensjon og styring utarbeidet av ledelse”. Med andre ord et dokument som utrykker ledelsens forventninger til ansatte i forhold til tema som “sikker bruk av informasjonsverdier”. Sikkerhets Policy er et eksempel som sier at tilgang til verdier skal være kontrollert. Retningslinjer er dokumenter som assisterer ledelse i arbeidet for implementering av informasjonssikkerhet.	1
Sertifiseringer	Ved sertifisering kan organisasjoner imøtekomme bransjekrav og de regulativer organisasjonen må forholde seg til.	1
Bestepraksis	Ved å sørge for at organisasjonen benytter erfaringer opparbeidet over tid innen bransjen kan organisasjonen tilegne seg eksisterende kunnskap og erfaringer. Standarder fornyes over tid som sørger for å adressere trender og utvikling innen fagfeltet. Ved å benytte eksisterende bestepraksis kan man mitigere kjente risikoer.	1
Oppfølging og revisjon	Organisasjonen må holde seg oppdatert på ny lovgivning siden disse endrer seg over tid. Organisasjonsendringer og nye regulativer må etterfølges. Ansatte må følges opp siden de ikke alltid følger kravene som er satt.(...)	1
Compliance	I denne sammenheng dreier dette seg om å holde organisasjonen oppdatert på nasjonale og internasjonallovgivning og regulativer som for bransjen for å beskytte informasjonsverdier. Det er essensielt å måle og håndheve compliance. Teknologi og ansatte oppfølges slik at policier som dreier seg om informasjonssikkerhet etterfølges, og fungerer effektivt på hendelser.	2

Tillit	Tillit er viktig når man implementerer informasjonssikkerhet. Det påvirker ansattes selvtillit når de foretar beslutninger.	1
Bevisstgjøring	Bevisstgjøring kan forklares ut ifra de aktivitetene en ansatt utfører for å forholde seg til sikkerhetskravene, og ansattes ansvar som kreves gitt i en informasjonssikkerhetspolicy. Dette er ansattes egenskaper som effektivt kan forbedre organisasjonen med tanke på informasjonssikkerhet. Ulike tiltak kan iverksettes for å bevisstgjøre ansatte.	1
Etisk adferd	Etisk atferd omtales som de verdier og regler som adskiller rett fra galt. Eksempelvis, ikke prate om konfidensiell informasjon i offentlige settinger.	1
Styring av informasjonsverdier	Dette relateres til beskyttelse av organisasjonens verdier, inkludert identifisering av verdier og føring av inventarliste. Dette inkorporerer også beskyttelse av informasjonsverdiene ved klassifisering av verdiene basert på sensitivitet og kritikalitet.	2
Systemutvikling	Denne komponenten adresserer sikkerhet i filsystemer og utviklingen av nye applikasjoner. Den forsikrer også at det ved endringer ivaretas sikkerhet som tema	3
Hendelseshåndtering	Hendelseshåndtering er prosessen som benyttes for å identifisere, respondere og overvåkning av sikkerhetshendelser. Det skilles mellom hendelser og avvik	3
Teknisk drift	Teknisk drift referer til teknologien som benyttes for å beskytte miljøet og informasjonsverdier, eksempelvis antivirus og brannmurer.	2
Kontinuitetsplan	En kontinuitetsplan dreier seg om å håndtere brudd på normal drift og gjennomretting av tilstand. En katastrofeplan er en del av kontinuitetsplanen. En organisasjon må identifisere kritisk infrastruktur og systemer og opprette en plan for å gjennomrette ønsket tilstand.	1
Endringsledelse	Ved implementering av sikkerhetskomponenter vil organisasjonens prosesser og arbeidsmønster for ansatte endres. Endringer i informasjonssikkerhet må aksepteres og styres på en måte slik at de ansatte kan fremdeles gjennomføre sine oppgaver. Ansattes oppførsel vil over tid bli mer fokusert på å beskytte informasjonsverdier. Endringer i oppførsel relatert med compliance og verning omkring verdier er viktig når graden av suksess skal måles.	1

Tabell 15: Liste over komponenter som skal brukes i undersøkelsen

8.4 Steg 1.3 - Validering av undersøkelsen

For best mulig datagrunnlag er det essensielt at påstandene gitt i undersøkelsen er betydningsmessig klare og kortfattede. Påstandene er konsultert i samarbeid med oppdragsgiver og Randi Utstrand. Oppdragsgiver validerte bruken av begreper og fagterminologi slik at dette skulle være forståelig for målgruppen. Sammen med Utstrand fjernet vi 23 påstander og la til seks påstander (se seksjon 8.3). Påstandene som ble kuttet dreide seg stort sett om påstander ansatte ikke trenger å forholde seg til, i følge Randi.

8.5 Steg 1.4 - Kunnskapspåstander

For delen av undersøkelsen som omhandler Kunnskapspåstander er det viktig at disse faktisk er relevante for IT-avdelingen. ISCF presenterer originalt 13 Kunnskapspåstander, som kan brukes i spørreundersøkelsen. De påstandene som ikke var relevante ble fjernet og begrepsbruken ble endret for å passe til avdelingen. Videre ble oppdragsgiver brukt for å verifsere at kunnskapsspørsmålene adresserte relevante temaer for IT-avdelingen. Dette resulterte i ni kunnskapsspørsmål listet i tabell 16 nedenfor.

Kunnskapsspørsmål
Jeg har lest politikk for informasjonssikkerhet
Jeg vet hvor jeg kan lese politikk for informasjonssikkerhet
Jeg forstår innholdet gitt i politikk for informasjonssikkerhet
Jeg vet hva informasjonssikkerhet omhandler
Jeg vet risikoene ved å åpne e-post fra ukjente sendere, spesielt hvis den inneholder vedlegg
Jeg låser for det meste datamaskinen min når jeg forlater den
Jeg mottar meldinger om informasjonssikkerhet helst i følgende kanaler
Jeg får nok informasjon om sikkerhet?
Jeg vet hvilke ansvar jeg har angående informasjonssikkerhet

Tabell 16: Kunnskapsspørsmål brukt i undersøkelsen

8.6 Steg 1.5 - Demografisk data

Etter dialog med oppdragsgiver finner vi det lite relevant å benytte demografiske data utover *seksjonstilhørlighet*. Dette baseres på at seksjoner i IT-avdelingen inneholder få ansatte som gjør det mulig å identifisere respondenter ut i fra mer enn ett demografisk spørsmål. Ved avdelinger med få ansatte er det hensiktsmessig å se på mer seksjonspesifikke karakteristikka som grunnlag for forbedringer eller tiltak. Beslutningsgrunnlaget baserte seg også på oppdragsgiver tidligere erfaring, som foreslo å prioritere anonymitet.

8.7 Steg 1.6 - Utvalgsstørrelse

Det er vanskelig å beregne antall spørsmål i undersøkelsen for å holde seg innenfor kravet på 10 minutter. I følge HealthGuidance[4] så er gjennomsnittlig lesehastighet for voksne 250 ord i minuttet (L). Med en antakelse om at hvert spørsmål (S) inneholder maksimalt 50 ord (O) så får vi følgende regnestykke:

$$V = S \times \frac{O}{L}$$

For å ta høyde for tenketid i hvert spørsmål senkes gjennomsnittelig lesehastighet til 200 ord i minuttet. For denne undersøkelsen har vi valgt ut 37 spørsmål. Beregnes antatt tidsbruk på undersøkelsen med disse variablene får vi følgende utregning:

$$\underline{9.25} = 37 \times \frac{50}{200}$$

Fra denne utregningen kan vi anta at varigheten på undersøkelsen er mellom ni og ti minutter med 37 spørsmål. Ved å ta høyde for at hvert spørsmål inneholder maksimalt 50 ord, vil vi med utregningen prøve å ta høyde for en maksimal tidsbruk på undersøkelsen.

[4] https://www.healthguidance.org/entry/13263/1/What-Is-the-Average-Reading-Speed-and-the-Best-Rate-of-Reading.html - (23.03.2018)

8.8 Steg 1.7 - Pilotundersøkelse

Steg 1.7 i ISCULA omhandler en pilotundersøkelse, men på grunn av tidsbegrensingen med bacheloroppgaven så ble det bestemt å utføre en annen form for pilotundersøkelse, en liten kvalitetssikring. Hensikten er å avdekke svakheter ved selve undersøkelsen. Kvalitetssikringen ble gjennomført av foresatte til prosjektgruppen. Tilbakemeldingene gir en pekepinn på hvordan undersøkelsen vil bli mottatt. En slik kvalitetssikring vil avdekke svakheter i språkvalget og uklarheter i hva spørsmål som kan revideres før undersøkelsen sendes ut. I tillegg vil testen bekrefte om undersøkelsen la seg gjennomføre innenfor akseptabel tid, og om designet av spørreundersøkelsen er akseptabelt. Kandidatene er representative innenfor det som ansees som relevant for målgruppen og det stilles ingen krav til forkunnskaper.

Etter å ha kjørt pilotundersøkelsen på foreldrene våre, fikk vi følgende tilbakemeldinger:

- Vanskelig å forstå innledning og definisjon av begreper.
- Hensikt og målsetning burde komme tydligere frem og være lett forståelig.
- Ser i hovedsak bra ut.
- Ønsket "vet ikke" som svaralternativ da det kunne være vanskelig å ta stilling til enkelte påstander.

Vi tok til oss tilbakemeldingene og valgte å omformulere innledning og begreper. Vi valgte ikke å ta med "vet ikke" alternativ da hensikten var å tvinge respondenter til å ta stilling(se seksjon 7.4).

8.9 Steg 1.8 - Bruk av SelectSurvey

Veiledningen i bruk av SelectSurvey, sendt på e-post fra Orakeltjenesten på NTNU [5] beskriver fremgangsmåten for hvordan man skal utføre en anonym spørreundersøkelse. Dersom denne prosessen følges er det ikke meldeplikt til Norsk senter for forskningsdata (NSD), registreringsplikten i NTNUs databaser for helseforskningsprosjekter eller behandling av personopplysninger. Denne fremgangsmåten innbærer at det ikke finnes noen spørsmål som medfører mulighet for direkte eller indirekte personidentifikajson. Indirekte personidentifikasjon innebærer spørsmålskombinasjoner som fører til en unik sammensetning av demografiske opplysninger. Dette har vi lagt vekt på ved valg av demografiske opplysninger (se seksjon 7.1).

På SelectSurvey finnes det funksjonalitet for å distribuere spørreundersøkelsen til deltakerne pr e-post. Dette fører til større kontroll over besvarelsene. Man kan få oversikt over hvem som har svart i tillegg til å sikre at respondenten kun avgir én besvarelse. Det er da også muligheter for selektiv purring, slik at man kun varsler de som ikke har avgitt svar. Dersom man følger prosessen for gjennomføring spørreundersøkelser med anonyme respondenter på SelectSurvey kan ikke denne funksjonaliteten benyttes. Den vil knytte respondentenes e-postadresse opp mot responsene. Dette medfører noen ulemper ved at hver respondent kan svare så mange ganger den vil. Muligheten for selektiv purring faller bort og dersom man skal sende ut en påminnelse til deltakerne, så må denne sendes ut til alle deltakerne.

Vi ønsker den funksjonaliteten SelectSurvey tilbyr med bruk av e-postlister. Dette

[5] https://innsida.ntnu.no/wiki/-/wiki/Norsk/Orakeltjenesten - (21.03.2019)

medfører at kravet til anonymitet ikke overholdes. Denne problemstillingen ble diskutert med oppdragsgiver på møtet den 22. mars. Her ble det kommet frem til at oppdragsgiver melder inn prosjektet til NSD or å unngå mulige feiltolkninger av reglelverket. På den måten blir ikke spørreundersøkelsen fullstendig anonym og det er teoretisk mulig å knytte svar til hver respondent. Det skal derimot fremgå i innledningen til undersøkelsen at svarene behandles anonymt. Vi kommer til å skille svarene fra e-postadressene før de analyseres.

9 Steg 2 - Gjennomføring

9.1 Steg 2.1 - Informer om undersøkelsen

Informasjon om undersøkelsen gikk ut til seksjonslederne i IT-avdelingen fredag 22. mars (uke 12) via e-post. E-posten ble sendt ut av Gaute Wangen og Randi Utstrand og kort fortalt ble det informert spørreundersøkelse, samt forklaring av NTNU sitt arbeid med sikkerhetskultur. Dette forteller målgruppen at undersøkelsen har forankring i ledelsen, noe som styrker gjennomslagskraften av undersøkelsen og poengterer dens viktighet, som øker sannsynligheten for at flere gjennomfører undersøkelsen.

9.2 Steg 2.2 - Publisere undersøkelsen

Undersøkelsen ble publisert via SelectSurvey sin e-postfunksjon. Vi valgte å lage et skript i Python[1] som hentet e-poster som lå ute på nettsiden til NTNU. Skriptet er lagt i vedlegg B. Undersøkelsen gikk ut til 227 ansatte i IT-avdelingen. Hele undersøkelsen slik den fremstod for deltakerne er lagt i vedlegg I.

9.3 Steg 2.3 - Oppfølging og svar

Etter utsendelse av undersøkelsen kom det første svaret inn etter under tre minutter. Videre fikk vi cirka 15 respondenter innen de første 10 minuttene, dette gav oss indikasjoner på at vi hadde estimert lengde på undersøkelsen bra.

Vi valgte å gjennomføre en purring på mandag 8. april, 10 dager etter undersøkelsen har vært ute. Mandag morgen ble vurdert som en optimal dag å purre på, da flere undersøkelser[2] [3], viser til høy svarprosent den dagen.

Undersøkelsen var ute fra 29.03.2019 kl. 08:45 til 11.04.2019 kl. 08:30.

[1] Objektorientert programmeringsspråk - https://www.python.org
[2] https://www.checkmarket.com/blog/survey-invitations-best-time-send/
[3] https://www.surveymonkey.com/curiosity/day-of-the-week/

10 Steg 3 - Evaluering av undersøkelsen

Steg 3 i ISCULA omhandler hvilke statistiske metoder man skal bruke for å analysere resultatet. Dette er gjort i metodekapitlet (se seksjon 3.3). Vi presenterer resultatet av den statstiske analysen i kapittel 11. I tillegg foreslår ISCULA bruk av ulike valideringsmetoder for å finne ut om kategoriene er statistisk valide å bruke.

11 Steg 4 - Dokumentasjon og tilbakemelding

Følgende kapittel tar for seg steg 4 i ISCULA-modellen, som er oppsummering av funn og resultater fra undersøkelsen.

Her presenteres hva som er gjort etter at spørreundersøkelsen er gjennomført. Først presenteres grunnlagsdata og feilmargin. Videre adresseres forbredelser gjort før analysen og tolkning av data. Evaluering av tilbakemeldingene gjøres før analysen, slik at man tar forbehold til andre tolkninger eller lignende ved selve analysen (se seksjon 11.6).

11.1 Datagrunnlaget

Spørreundersøkelsen ble sendt ut til totalt 227 ansatte på IT-avdelingen ved NTNU. Totalt var det 137 (60%) respondenter som fullførte undersøkelesen. Det var 30 respondenter som ikke fullførte undersøkelsen. Det vil si at det var totalt 167 respondenter, medregnet de som ikke fullførte. Etter det første spørsmålet i undersøkelsen var det allerede 18 respondenter som ikke hadde svart. I statistikken er respondentene som ikke fullførte undersøkelsen utelatt. Det vil si at N=137 gjennom hele analysen av spørreundersøkelsen, hvis ikke annet er oppgitt. Hadde det vært flere respondenter som delvis fulllførte undersøkelsen hadde det blitt vurdert på nytt hvorvidt delvis-fullførte svar skal medregnes eller ikke. Slik situasjonen er nå, ser vi ingen nytte av å ta med svaret til de respondentene som har delvis fullført undersøkelsen.

11.2 Innsamling av grunnlagsdata

Det er viktig å se forskjellen på grunnlagsdata og demografi. Grunnlagsdataen presenterer den reelle sammensetningen av ansatte i IT-avdelingen, mens de demografiske opplysningene presenterer sammensetningen av ansatte i resultatet av spørreundersøkelsen. Grunnlagsdataen ble hentet ned 11.april 2019 - 08:22, gjennom informasjon om ansatte fordelt på seksjoner i IT-avdelingen, som ligger åpent på innsida[1]. For å hente ned informasjon om hvilken seksjon de ansatte hører til, ble det utarbeidet et skript i Python som knytter den ansatte opp mot den seksjonen de tilhører på innsida. Her er det en mulig feilkilde, ved at seksjonstilhørligheten den ansatte står oppført med på innsida ikke stemmer med faktisk seksjonstilhørlighet. Bakgrunnen for at det er 228 ansatte i grunnlagsdataen og 227 ansatte undersøkelsen ble sendt ut til, er at det er en tidsforskjell mellom innsamling av e-post adresser før lansering av undersøkelsen og da de ansatte ble knyttet opp mot seksjonstilhørlighet. I løpet av denne perioden kan det virke som om det har skjedd noen utskiftninger av ansatte på IT-avdelingen på innsida. Vi ser ingen nytte av å ta med ytterligere grunnlagsdata, annet en det som er brukt som demografiske opplysninger i spørreundersøkelsen (se seksjon 7.1).

11.3 Grunnlagsdata

Tabell 17 nedenfor viser en sammenlikning mellom data innhentet fra grunnlagsdataen og de kategoriske variablene fra resultatet på spørreundersøkelsen. Antallet i grunnlags-

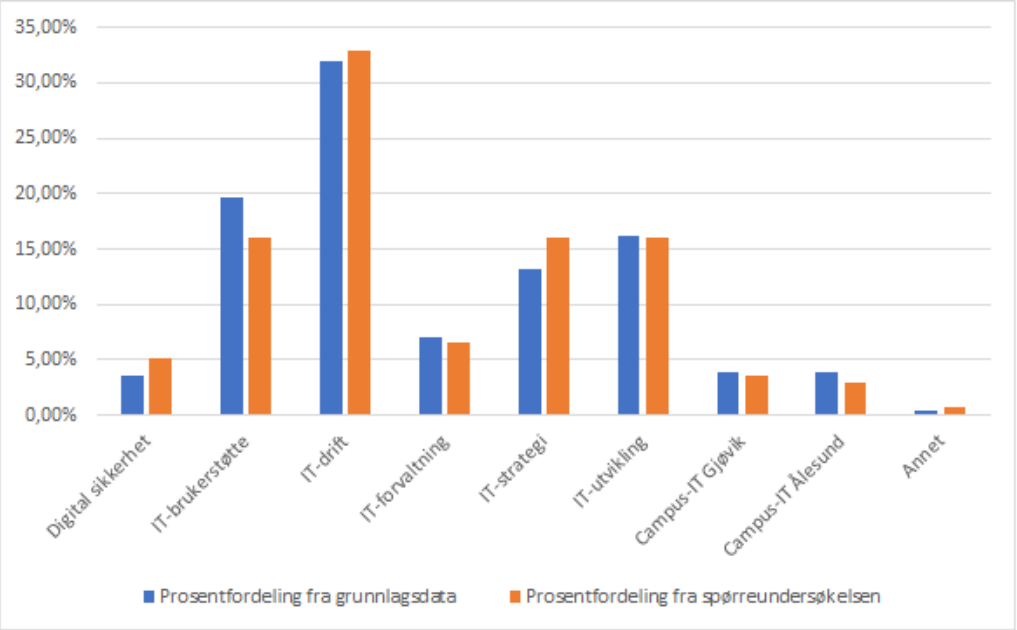
[1] https://www.ntnu.no/adm/it/ansatte

dataen beskriver hvor mange som faktisk jobber i hver seksjon i IT-avdelingen. Prosentandelen beskriver hvor mange prosent denne seksjonen utgjør i det totale antallet ansatte på IT-avdelingen. Antallet i resultatet fra spørreundersøkelsen angir hvor mange som svarte fra hver seksjon i spørreundersøkelsen. Her beskriver prosentandelen hvor mange prosent denne avdelingen utgjør blant alle svarene fra undersøkelsen. For eksempel så utgjør Seksjon for digital sikkerhet 3.5% av IT-avdelingen i grunnlagsdataen og 5.10% i resultatene fra spørreundersøkelsen. Dette sier noe om hvor representative seksjonene er i undersøkelsen.

	Grunnlagsdata		**Tall fra spørreundersøkelsen**	
Seksjonsnavn	Antall	Prosentandel	Antall	Prosentandel
Digital sikkerhet	8	3.51%	7	5.11%
IT-brukerstøtte	45	19.74%	22	16.06%
IT-drift	73	32.02%	45	32.85%
IT-forvaltning	16	7.02%	9	6.57%
IT-strategi	30	13.16%	22	16.06%
IT-utvikling	37	16.23%	22	16.06%
Campus-IT Gjøvik	9	3.95%	5	3.65%
Campus-IT Ålesund	9	3.95%	4	2.92%
Annet	1	0.44%	1	0.73%
Total	228	100%	137	100%

Tabell 17: Datagrunnlaget fra spørreundersøkelsen sammenlignet med grunnlagsdata

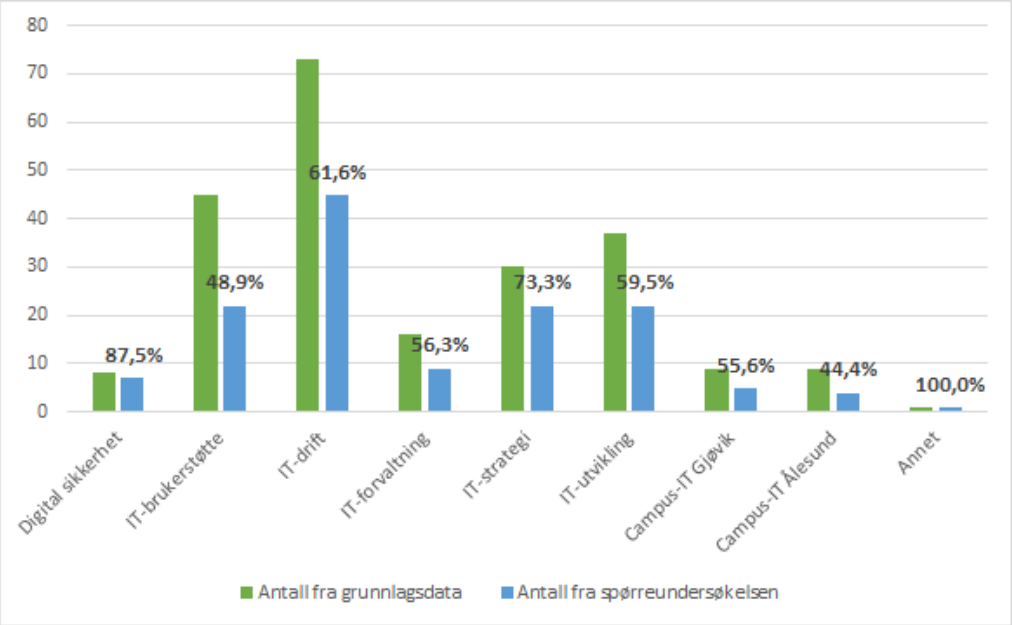
Figur 14 viser prosentvis fordeling av seksjonene i grunnlagsdataen sammenliknet med resultater fra spørreundersøkelsen. Ved å legge disse prosentandelene oppå hverandre i én figur kan man få et inntrykk av hvor representativ avdelingen er i undersøkelsen, sammenliknet med hvordan fordelingen faktisk er. Figuren viser at vi er svært nærme fordelingen i grunnlagsdataen, og at vi generelt sett har fått et representativt utvalg ansatte fra IT-avdelingen. Ved å se på om søylen til variabelen i resultatet fra målingen er høyere eller lavere enn den tilhørende søylen i grunnlagsdataen, kan vi vurdere om seksjonen er over- eller underrepresentert i undersøkelsen. IT-brukerstøtte er noe underrepresentert, hvor grunnlagsdataen viser en fordeling på 19.73%, mens resultatene fra undersøkelsen sier 16.05%. IT-strategi er noe overrepresentert i undersøkelsen, hvor differansen er 16.05% i resultatene fra undersøkelsen, mot 13.15% i grunnlagsdataen.



Figur 14: Sammenlikning mellom prosentvis seksjonsfordeling i grunnlagsdata og prosetvis seksjonsfordeling i resultatet fra spørreundersøkelsen

Figur 15 illustrerer en sammenlikning mellom antallet som faktisk jobber i hver seksjon og antallet som svarte fra hver seksjon. Dette vil ikke vise hvor representativ hver seksjon er i resultatet fra undersøkelsen, men kan gi oss et bilde på hvor mange som svarte sammenliknet med totalt antall ansatte i hver seksjon. Figuren viser også hvor stor prosentandel ansatte som er representert fra hver seksjon, sammenliknet med grunnlagsdataen. For eksempel så har 7 av 8 fra seksjon for digital sikkerhet svart på undersøkelsen, som utgjør 87.5% av totalt ansatte i seksjon for digital sikkerhet.

Alt i alt fikk vi god respons på undersøkelsen fra alle seksjoner, og man har oppnåd et representativt utvalg til analysen.



Figur 15: Sammenlikning mellom antallet i hver sesksjon og antallet som svarte på undesøkese

11.4 Feilmargin

For å beregne feilmargin har vi brukt en kalkulator på *Creative Research Systems*[2]. Vi valgte denne over andre metoder fordi denne har større nøyaktighet, ved bruk av to desimaler og forholdsvis enkel i bruk. I denne undersøkelsen er populasjonen på 227 personer hvorav 137 har fullført undersøkelsen (utvalg). Med et konfidensintervall på 95% vil vi få en feilmargin på 5.28%.

11.5 Forberedelser

For at SPSS skal kunne tolke svaralternativene våres, må de konverteres de til en numerisk verdi. Vi benytter følgende verdier for svaralternativene våre, gitt i tabell 18 og 19 nedenfor. Eksempelvis ved kunnskapspåstandene med svaralternativene ja, nei og vet ikke, vil "ja" mappes til numerisk verdi "1".

For å sørge for at integriteten ivaretas, og dataen før konverteringen er i overenstemmelse med data etter endring, gikk vi igjennom dataen for å sjekke samsvar ved å sammenligne datasettene.

Svaralternativ	**Verdi**
Ja	1
Nei	2
Vet ikke	3

Tabell 18: Svaralternativ for kunnskapspåstander konvertert

[2] https://www.surveysystem.com/sscalc.html - (01.05.2018)

Svaralternativ	Verdi
Svært enig	1
Uenig	2
Noe uenig	3
Noe enig	3
Enig	5
Svært uenig	6

Tabell 19: Svaralternativ for enighetsgrader konvertert

11.6 Evaluering av tilbakemeldinger på undersøkelsen

I forbindelse med spørreundersøkelser er det viktig å gi respondentene muligheten for å komme til ordet. Her kan respondenten fortelle om uklarheter, begreper som ble oppfattet som fremmed, utdype bakgrunn for svar og hva respondenten selv mener mangler. Tilbakemeldinger kan benyttes som grunnlag for å forbedre undersøkelsen ved en senere annledning. I tillegg fungerer tilbakemeldinger som en "temperaturmåler", hvor vi får et innblikk i hvordan respondenten opplevde undersøkelsen. Tilbakemeldingsdata kan behandles frittstående som eget datasett, men også tas i betraktning når selve påstandsdataen skal tolkes. Ved å benytte tilbakemeldinger i tolkningen håper vi å kunne sette oss inn i hvordan påstandene ble oppfattet av målgruppen, slik at vi kan med større sikkerhet presentere tolkning av data.

Det ble valgt følgende løsning for å håndtere tilbakemeldinger. Alle tilbakemeldninger med substans knyttet til en påstand eller problemområde (Eksempelvis fremmedord) ble kategorisert og rangert ut ifra hva som går igjen (trend). Dette gjenspeiler hva de fleste mener og derav størst forbedringspotensiale.

Det kom inn totalt 26 tilbakemeldninger fra 137 respondenter som fullførte undersøkelsen.

- 7 av 26 mener likert-skalaens intervaller er uheldig, da det kommer fram at respondentene ønsker å kunne svare "vet ikke" som et nøytralt alternativ.
- 7 av 26 mener det benyttes tunge fagutrykk og begreper (videre utdypet i seksjon 11.6.1).

Man kan se ut ifra foregående liste at flere ønsker å svare nøytralt. Valg av skala var et problemområde vi innledene i utforming av spørreundersøkelsen var klar over (se seksjon 7.4). I tillegg kommer det fram at språket oppfattes tungt. Dette kan skyldes manglende kunnskap hos respondenten, dårlig formulering eller hva vi mener er allment for målgruppen ikke er riktig.

11.6.1 Uklarhet i spørsmål og påstander

Flere respondendter forstod ikke påstand 30, "Jeg bruker private applikasjoner for å utføre arbeid relatert til jobben min". Her var det ønsket å adressere hvorvidt man *ikke* benytter applikasjoner som NTNU supplerer til arbeid man gjør knyttet til NTNU og behandling av NTNUs informasjonsverdier. Ett eksempel er dokumentlagring ved bruk av applikasjoner som *ikke* er tilbudt av NTNU, for eksempel Dropbox; da NTNU tilbyr Office 365 med skylagring via OneDrive. Det kan være rimelig å anta at applikasjoner blir benyttet på grunn av brukervennlighet, og man utelater bruke eksisterende, supplerte verktøy

om det mangler ved behov. Påstanden kunne da vært formulert på en klarere måte.

Påstand 27, "Jeg mener retningslinjer som berører mitt daglige arbeid er tilstrekkelig" ble omtalt av to respondenter som utydelig. En ønsket tolkning av påstanden var hvorvidt man kan støtte seg til dokumenterer som angir retningslinjer når man utfører daglig arbeid, og at disse angir godt nok hva en ansatt trenger forholde seg til og gjøre. Påstanden kunne derfor vært formulert på en annen måte.

11.7 Analyse av undersøkelsen

I de kommende avsnitt presenteres statistikken fra undersøkelsen, og påstandene benyttet i spørreundersøkelsen, med tilhørende graf og tolkning. Oppdelingen av påstandene skjer i kategorier med tilhørende komponenter. Komponentene er forklart i 11.8.2.

11.7.1 Deskriptiv statistikk

Forklaringen av statistikken finnes i kapittel 3.3. *N* i kolonne nummer to er antall respondender som har svart på påstanden. Tabell 20 beskriver fordelingen og legger frem sentral tendens for påstandene i undersøkelsen.

Påstand nr	N	Min	Max	Median	Variasjonsbredde	Typetall
2	137	1	3	2	2	1
3	68	1	2	1	1	1
4	67	1	2	1	1	1
5	137	1	6	5	5	5
6	137	1	6	6	5	6
7	137	1	2	1	1	1
9	137	1	2	2	1	2
10	137	1	2	1	1	1
11	137	1	6	4	5	4
12	137	3	6	6	3	6
13	137	1	6	5	5	5
14	137	1	6	5	5	5
15	137	1	6	5	5	6
16	137	1	6	4	5	5
17	137	1	6	5	5	5
18	137	1	6	4	5	4
19	137	1	6	5	5	5
20	137	1	6	5	5	5
21	137	1	6	4	5	4
22	137	1	6	5	5	5
23	137	3	6	6	3	6
24	137	1	6	4	5	4
25	137	1	6	5	5	5
26	137	1	6	5	5	5
27	137	1	6	4	5	5
28	137	1	6	4	5	4
29	137	1	6	5	5	5
30	137	1	6	2	5	2
32	137	1	6	3	5	2
33	137	1	6	4	5	4
34	137	1	6	4	5	4
35	137	1	6	5	5	5
36	137	1	6	4	5	5

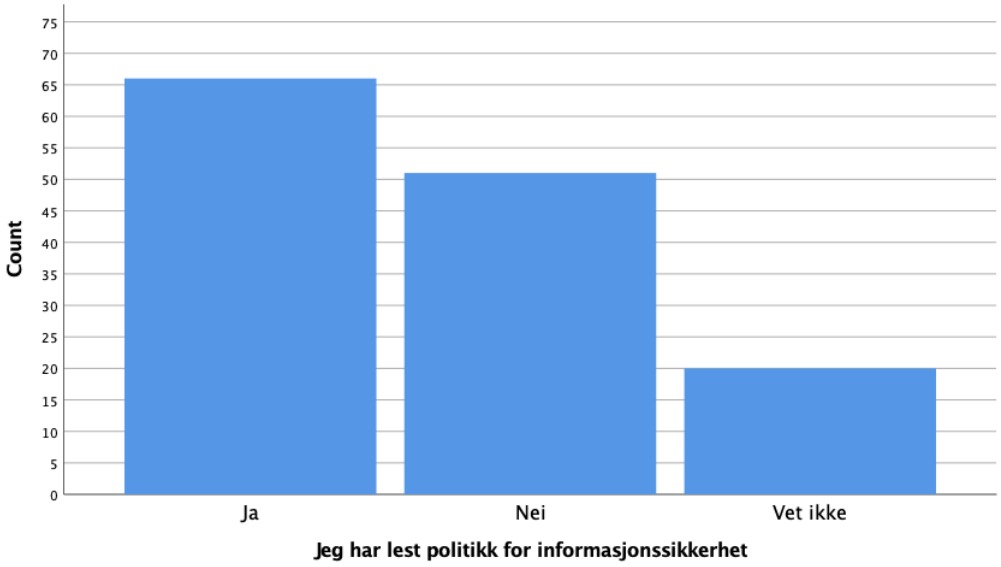
Tabell 20: Deskriptiv statistikk over resultatet fra undersøkelsen med ordinale data

11.7.2 Kunnskapspåstander

Videre er hver kunnskapspåstand i undersøkelsen, nummer 2-10, listet opp. Vi starter opplistingen på påstand nummer to for ryddighets skyld, da påstand nummer en i undersøkelsen omhandler demografi. Hver kunnskapspåstand vil presenteres med en deskriptiv forklaring av resultatet, en graf som viser svarene i prosentvis fordeling, og deretter en tolkning av resultatet.

2. Jeg har lest politikk for informasjonssikkerhet

På denne påstanden (se figur 16) svarte totalt svarte 48% at de faktisk har lest politikk for informasjonssikkerhet. 37% svarte at de ikke har lest politikk for informasjonssikkerhet, og resterende 15% svarte at de ikke vet om de har lest den.

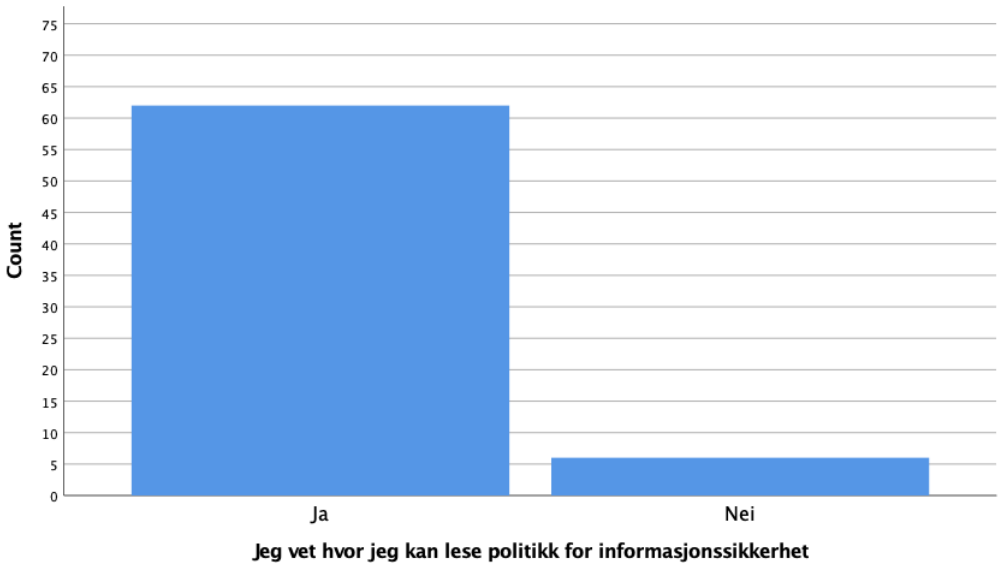


Figur 16: Jeg har lest politikk for informasjonssikkerhet

Nærmere halvparten, 48% mener de har lest politikk for informasjonssikkerhet. Det er rimelig å anta at respondenter som svarer at de ikke vet om de har lest dokumentene mener de har mindre sikkerhet i kunnskapen de sitter med angående hva politikk for informasjonssikkerhet omhandler. Man kan derfor anta at over halvparten svarer at de ikke vet om de har lest den eller at de faktisk ikke har lest den. Det er usikkert om respondentene som svarte “vet ikke” ikke forstod påstanden. Det var derimot ingen som adresserte påstanden som uforståelig og det antas derfor at påstanden stort sett blir tolket som at man har lest det. Påstanden adresserer ikke hvorvidt det er bekjent for ansatte at det finnes skreven politikk for informasjonssikkerhet, men det adresserer hvorvidt man har lest politikk for informasjonssikkerhet, og det er ønskelig at svarraten er større enn den utgir seg for å være.

3. Jeg vet hvor jeg kan lese politikk for informasjonssikkerhet

Denne påstanden (se figur 17) er knyttet foregående påstand, "Jeg har lest politikk for informasjonssikkerhet". Det vil si at respondentene kan svare på på denne påstanden *bare* om de svarte ja på forrige påstand. Det er viktig å merke seg at 68 respondenter har besvart denne påstanden (N = 68). Ut av 68 respondenter svarte 91% at de vet hvor de kan lese politikk for informasjonssikkerhet. Bare 9% svarte nei til at de vet hvor de kan lese politikk for informasjonssikkerhet.



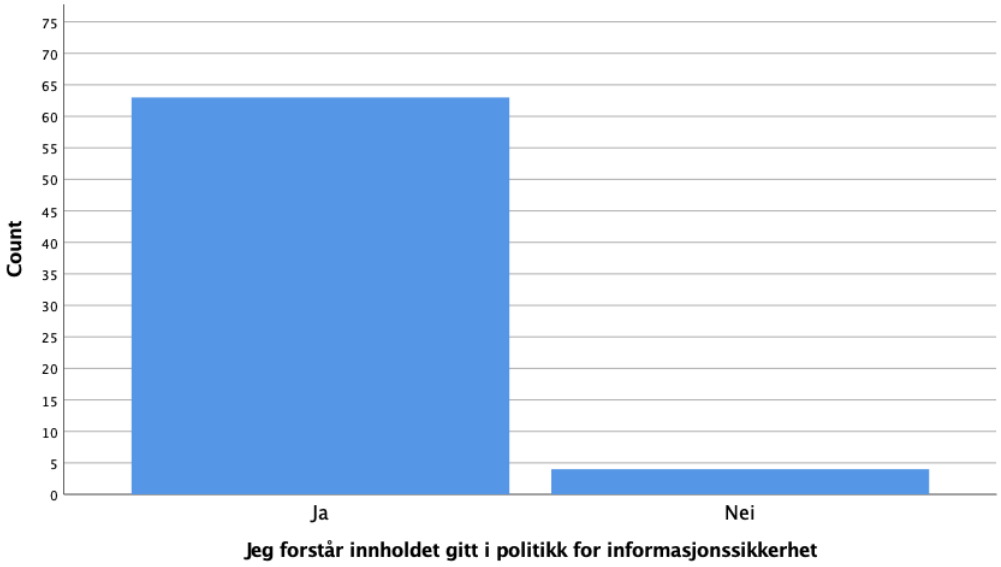
Figur 17: Jeg vet hvor jeg kan lese politikk for informasjonssikkerhet

Det ønskes at informasjonssikkerhet skal være et sentralt tema gjennom ansattes arbeidsprosesser og kommunikasjonsflyt ved NTNU, og derfor anses det som viktig at sentrale dokumenter vedrørende informasjonssikkerhet er lett å finne for ansatte. Med tanke på prosentandelen som svarer ja, så utgir svarraten her for å være på den positive siden når det kommer til at dokumenter er enkle å finne.

Her kunne det vært interessant å sett på om de som har svart "nei" på forrige påstand vet hvor de kan finne dokumentet. Dersom de ikke vet hvor de kan finne dokumnetet og ikke har lest politikken kan dette tyde på at det for eksempel er dårlig opplyst på innsida om hvor dokumentene ligger. I andre tilfellet, hvis de vet hvor de kan finne det og ikke har lest det, så kan dette tyde på dårlig holdning.

4. Jeg forstår innholdet gitt i politikk for informasjonssikkerhet.

På denne påstanden (se figur 18) svarte totalt svarte 94% at de forstår innholdet gitt i politikk for informasjonssikkerhet, og bare 6% av respondene at de ikke forstår innholdet.

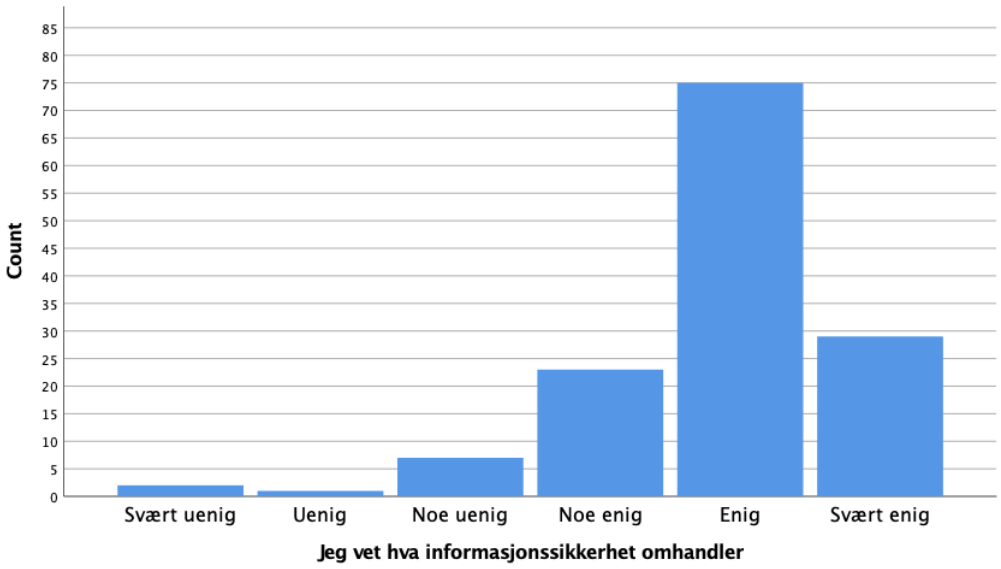


Figur 18: Jeg forstår innholdet gitt i politikk for informasjonssikkerhet

Denne påstanden er avhengig av foregående påstand, nummer to om "Jeg har lest politikk for informasjonssikkerhet". Dette lar respondenter svare på om de har forstått innholdet i dokumentene om politikk for informasjonssikkerhet bare om de tidligere svarer at de har lest dokumentene (N=67). Det er altså ett fåtall som mener de ikke forstår innholdet gitt i politikk for informasjonssikkerhet. Dette er en sterk indikasjon på at dokumentet er lett forståelig.

5. Jeg vet hva informasjonssikkerhet omhandler

På denne påstanden (se figur 19) svarte 54.7% svarte at de var enig, 21.2% at de er svært enig, og 16.8% at de var noe enig. Dette skiller seg fra svært uenig til noe uenig, med samlet 7.3%. Figur 19 nedenfor viser en skjev fordeling med størsteparten som svarer at de vet hva informasjonssikkerhet omhandler.

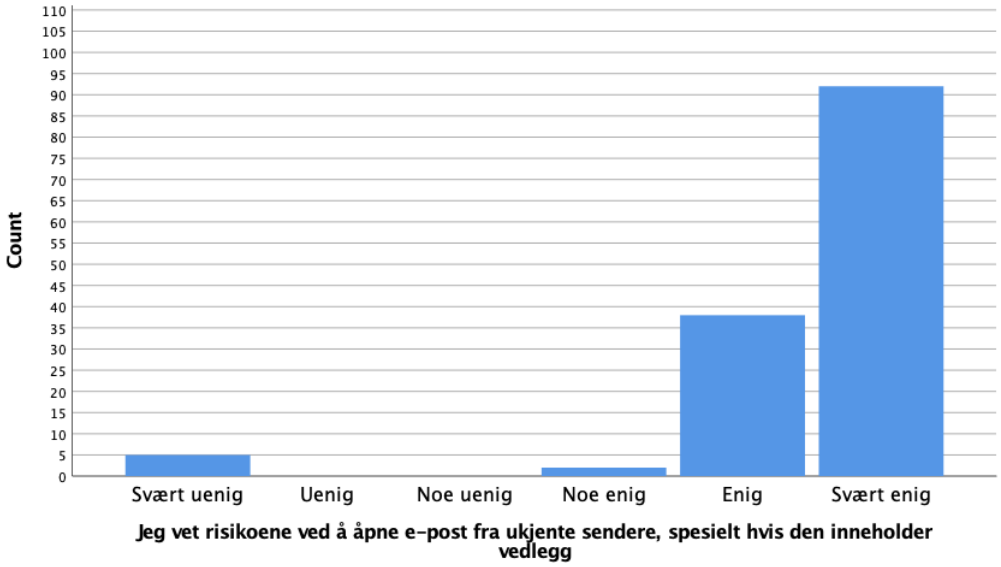


Figur 19: Jeg vet hva informasjonssikkerhet omhandler

Totalt svarte 7.3% at de er noe uenig til svært uenig i utsagnet om at de vet hva informasjonssikkerhet omhandler. Grafen antyder derfor at 9 av 10 underlagt IT-Avdelingen har god eller bedre forståelse for informasjonsssikkerhet. Vi gjør en antakelse på at det er en større andel som svarer “enig” i steden for “svært enig”, da man antar at man ved større kunnskap om informasjonssikkerhet også forstår hvor komplekst temaet er, og derfor unnlater svare “svært enig” ved ydmykhet.

6. Jeg vet risikoene ved å åpne e-post fra ukjente sendere, spesielt hvis den inneholder vedlegg.

På denne påstanden (se figur 20) svarte totalt 66% svarte at de var svært enige i at de vet risikoene ved åpning av e-post fra ukjente sendere. 28% svarte enig, 1% svarer noe enig. Samlet svarte totalt 4% at de var noe uenig til svært uenig.



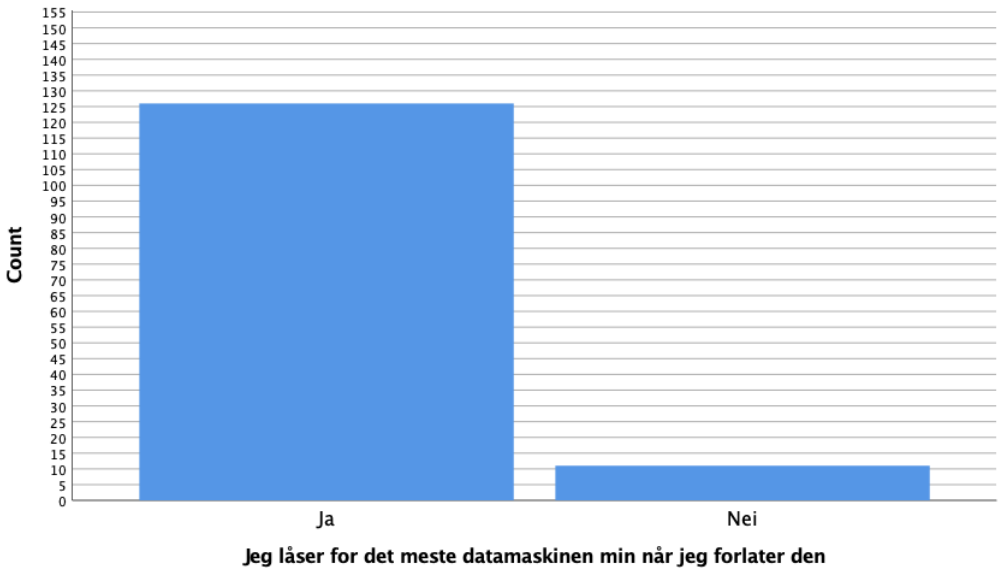
Figur 20: Jeg vet risikoene ved å åpne e-post fra ukjente sendere, spesielt hvis den inneholder vedlegg

Samlet svarte de aller fleste at de kjenner til risikoene ved å åpne e-post fra ukjente. Distribusjonen er på den positive siden, og det kan anses som at ansatte stort sett har kunnskap ved risikoene man utsettes for ved å åpne e-post fra ukjente sendere. En liten andel mener derimot at de er svært uenig i utsagnet. Hvorvidt disse respondentene kjenner til at e-postvedlegg kan utjøre en risiko, eller hvilke risiko man utsettes for, er usikkert. Man kan ved usikkerhet anta at disse respondentene ikke kjenner til risikomomentene vedrørende e-postvedlegg, eller at de er klar over at det finnes risikoer, men ikke nødvendigvis hvilke risikoer man står ovenfor.

I følge mørktetallsunderøkelsen har antall phishinghendelser på NTNU de siste årene har vært høy [6]. På bakgrunn av dette kunne det ha vært hensiktsmessig å omformulert det til å også dekke risikoen ved å klikke på linker. Selv om det nevnes at phishing har vært en av de hyppigste sikkerhetshendelsene, er det viktig å bemerke at mørketallsundersøkelsen ble gjort på tvers av fakulteter, og ikke trengs sees i sammenheng med besvarelsenene i påstanden gitt i figur 20, da undersøkelsen er utført på IT-avdelingen.

7. Jeg låser for det meste datamaskinen min når jeg forlater den.

På denne påstanden (se figur 21) svarte totalt svarte 92% at de for det meste låser datamaskinen sin når de forlater den. 8% svarte nei til at de låser maskinen når de forlater den.



Figur 21: Jeg låser for det meste datamaskinen min når jeg forlater den

De aller fleste, 92%, svarte at de for de meste låser datamaskinen sin når de forlater den. Det er rimelig å anse dette som et sterkt tall, da prosentandelen som benytter låsefunksjonen er høy. Opplåsing av en datamaskin krever i en stor del tilfeller passord, men det tas forbehold om at man ikke har tatt passordstyrke og lignende i betrakning når man stilte påstanden.

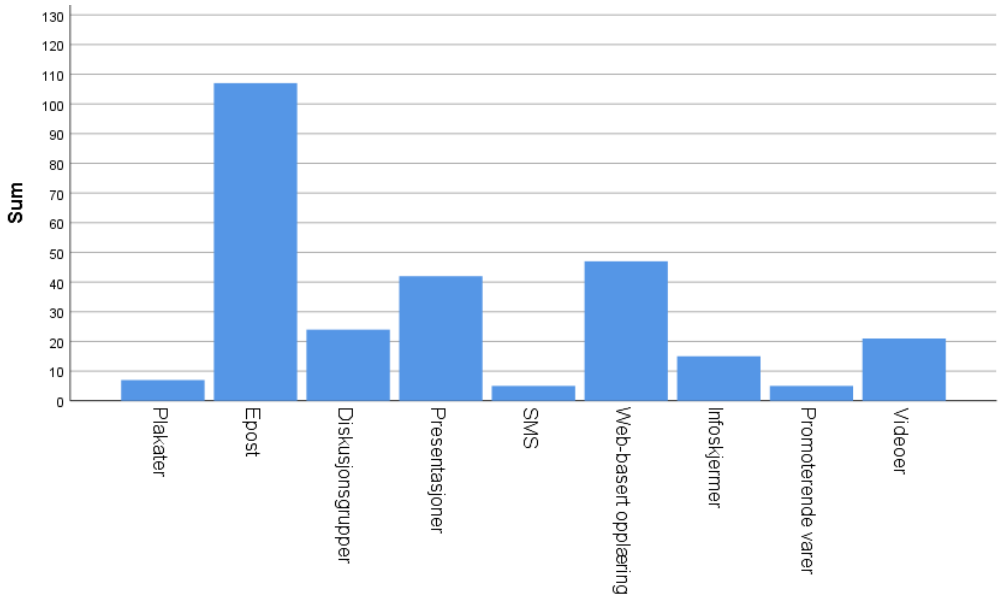
Denne påstanden kan gi rom for tolkning av hva som menes med “for det meste”. Det er rimelig å anta at ansatte låser maskinen med hensikt. Om man alltid utelater låse maskinen, antas det at man ikke kjenner til risikoer, men kan anta at man forstår risikoene man utsettes for hvis man faktisk velger bruke låsefunksjonen.

Man kan gjøre en antakagelse ved at ansatte med egne kontorer unnlater låse datamaskinen fordi de låser kontordøren, og derfor ikke “trenger” låse datamaskinen.

Påstanden sier heller ikke direkte om man kjenner til risikoer ved å forlate datamaskinen ulåst. Dett kan være rimelig å anta at ansatte kjenner til at det faktisk finnes risikoer ved å forlate datamaskinen ulåst, da en såpass stor andel velger å bruke låsefunksjonen i de fleste tilfeller.

8. Jeg mottar meldinger om informasjonssikkerhet helst i følgende kanaler. Du kan velge étt eller flere alternativ.

På dette spørsmålet (se figur 22) svarer en større del på 76% av ansatte ønsker å motta meldinger om informasjonssikkerhet via e-post. En stor del på 33% mottar gjerne web-basert opplæring, og en nesten like stor andel på 29% ved presentasjoner.



Figur 22: Jeg mottar meldinger om informasjonssikkerhet helst i følgende kanaler

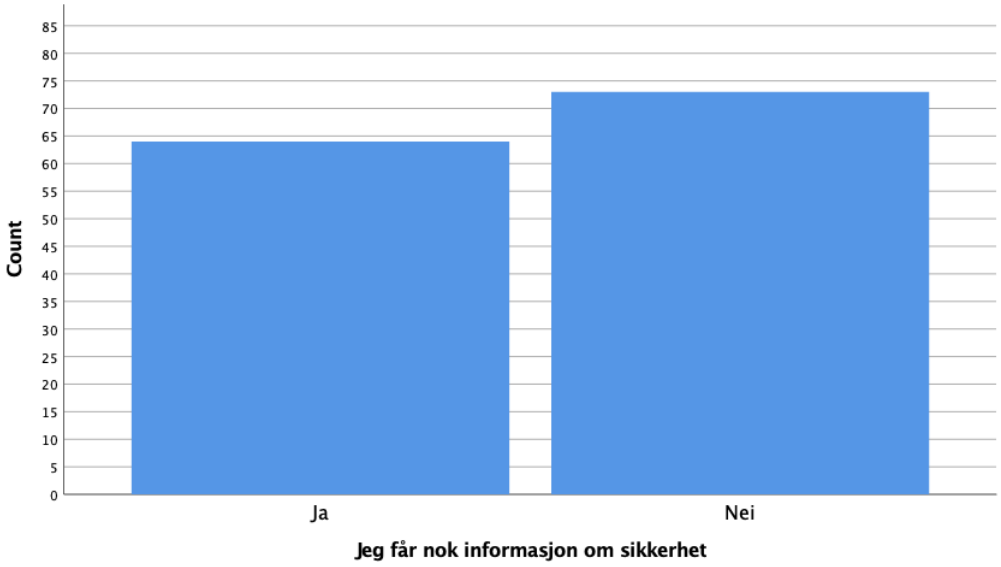
Man kan tolke den nåværende påstanden som hvordan man faktisk mottar meldinger om informasjonssikkerhet, men ved en annen formulering av påstanden, der man spør om hvordan det er *ønskelig* å motta meldinger om informasjonssikkerhet, får man en annen betydning av påstanden. Det er derfor antatt at man kan ha fått svar på både hvordan ansatte faktisk mottar meldinger, og hvordan ansatte *ønsker* å motta meldinger om informasjonssikkerhet.

I tillegg til flervalgsalternativene, svarer 22 ansatte i kommentarboks, at de mottar meldinger gjennom NTNUs intranett, ved spesifikt meldinger gjennom Innsida. Det nevnes av en respondent at det faller naturlig at Innsida brukes til meldinger om informasjonssikkerhet, da Innsida kan brukes til å adressere alle ansatte, og informasjonssikkerhet er relevant for alle ansatte.

Alternativt nevnes det også blant respondenter at man benytter seg av seksjonsmøter, eller eksterne seminarer. Egne kommunikasjonsmidler eller kanaler nevnes også, ved Slack, IRC eller lignende midler. Det kan tyde på at det ikke er noen stor felles enighet om foretrukket valg av kanal.

9. Jeg får nok informasjon om sikkerhet

På denne påstanden (se figur 23) svarte totalt svarte 47% av ansatte at de får nok informasjon om sikkerhet, men en større del på 53% svarte at de ikke får nok informasjon om sikkerhet.



Figur 23: Jeg får nok informasjon om sikkerhet

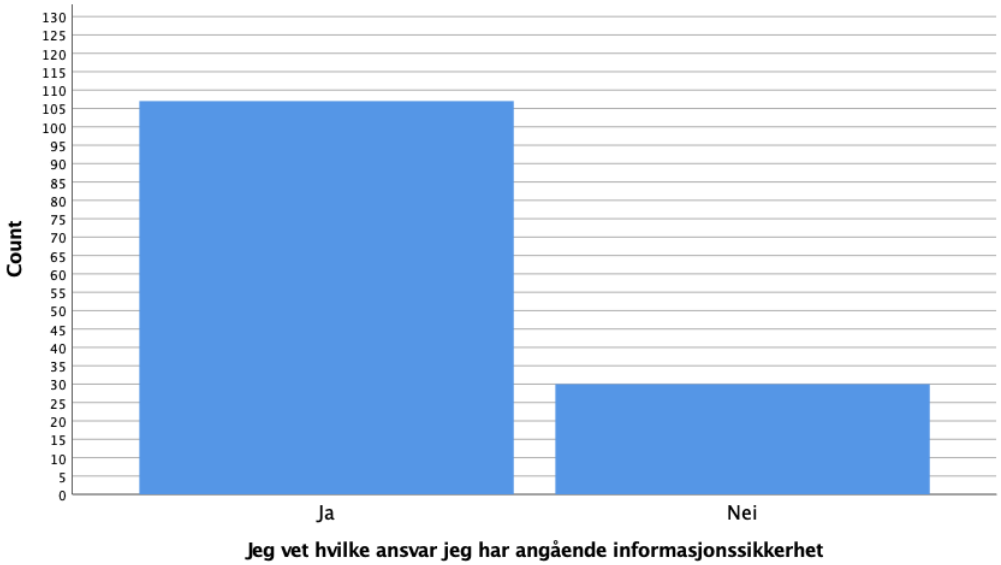
Over halvparten, 53% mener de ikke mottar nok informasjon om sikkerhet. En ulempe er her at påstanden kan også tolkes som at respondenten ikke *ønsker* mer informasjon om sikkerhet, uavhengig av kunnskapsnivå til respondenten. Selv om man kan anta at en respondendt muligens har *behov* for å motta informasjon, kan en respondent ha svart "nei", basert på personlig ønske.

Man kan se på interessen for å motta informasjon i sammenheng med spørsmålet angående hvor man ønsker motta meldinger om informasjonssikkerhet. Ved spørsmål nummer åtte er det et flertall som helst mottar meldinger ved e-post, web-basert opplæring eller presentasjoner. Flere ansatte nevnte også Innsida, NTNUs intranett, som en måte å motta meldinger.

Påstanden stilles da det er interessant å vite om ansatte mener de får nok informasjon om sikkerhet. Man kan anta at de som svarer "ja" føler de får nok informasjon, eller innehar nok kunnskap til at denne formidlingen ikke behøves. Det kan derimot også antas at det finnes et behov for denne kunnskapsformidlingen til individuelle, selv om disse kan ha svart "nei" grunnet manglende interesse for temaet.

10. Jeg vet hvilke ansvar jeg har angående informasjonssikkerhet

På denne påstanden (se figur 24) svarte over tre fjerdedeler, 78% svarte at de vet hvilke ansvar de har angående informasjonssikkerhet. 22% svarte at de ikke vet hvilke ansvar de har angående informasjonssikkerhet.



Figur 24: Jeg vet hvilke ansvar jeg har angående informasjonssikkerhet

Over en femtedel, 22% av ansatte, svarte at de ikke vet hvilke ansvar de har angående informasjonssikkerhet. Selv om flesteparten har svart ja på dette, anser vi fortsatt at 22% for de som har svart nei er et relativt høyt tall, da det er ønskelig at alle vet hvilke ansvar man har ovenfor informasjon man behandler.

Påstanden i figur 24, "Jeg vet hvilke ansvar jeg har angående informasjonssikkerhet" korrelerer sterkt med spørsmålet om man forstår innholdet gitt i politikk for informasjonssikkerhet, illustrert i figur 18 ($r = 0.583$). Denne korrelasjonen gir mening ved at politikk for informasjonsikkerhet omtaler de ansattes ansvar angående informasjonssikkerhet. Ut fra korrelasjonen er det rimelig å anta at ansatte som har svart "ja" på forståelse for innholdet gitt i politikk for informasjonssikkerhet, også har høyere andel "ja"-svar på "Jeg vet hvilke ansvar jeg har angående informasjonssikkerhet".

11.7.3 Sikkerhetskulturpåstander - innledning

Tidligere har vi sett på kunnskapsspørsmålene i undersøkelsen. Nå vil rapporten gå over til å se på sikkerhetskulturpåstandene. Påstandene blir kategorisert under sin tilhørende komponent og komponentene under den tilhørende kategorien. Dette gjøres fordi det enkelte steder gjøres tolkninger og oppsummering per komponent.

11.7.4 Kategori - Brukersikkerhetsstyring

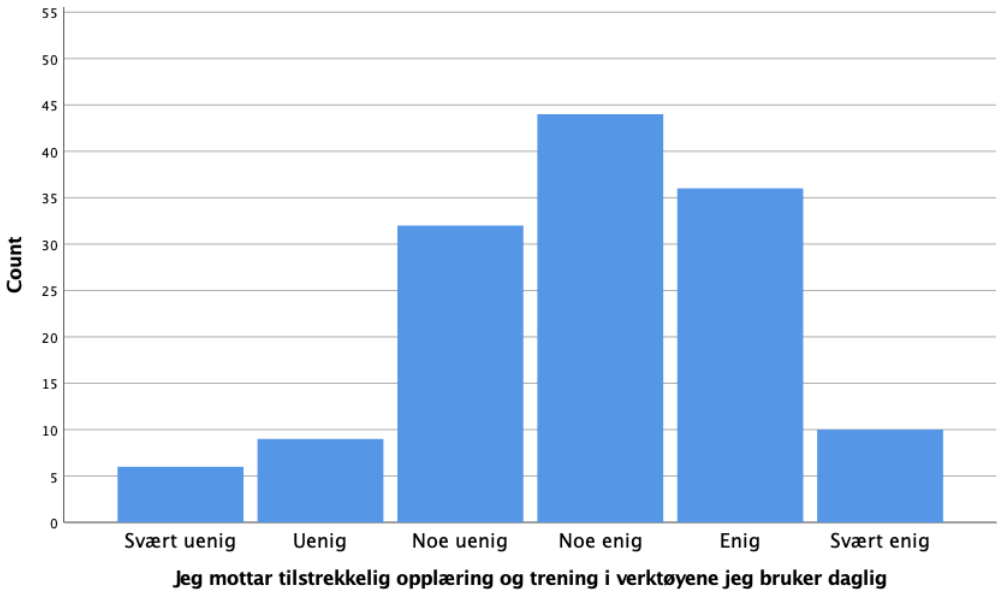
Påstand 11 til 16 i undersøkelsen omhandler kategorien brukersikkerhetsstyring. Komponentene i kategorien brukt i undersøkelsen var opplæring og kurs/trening, bevisstgjøring, etisk adferd og personvern. Videre er påstandene under kategorien brukersikkerhetsstyring listet opp under sin respektive komponent. Påstandene har deskriptive data følgende etter, graf og en tolkning.

Komponent - Opplæring og kurs/trening

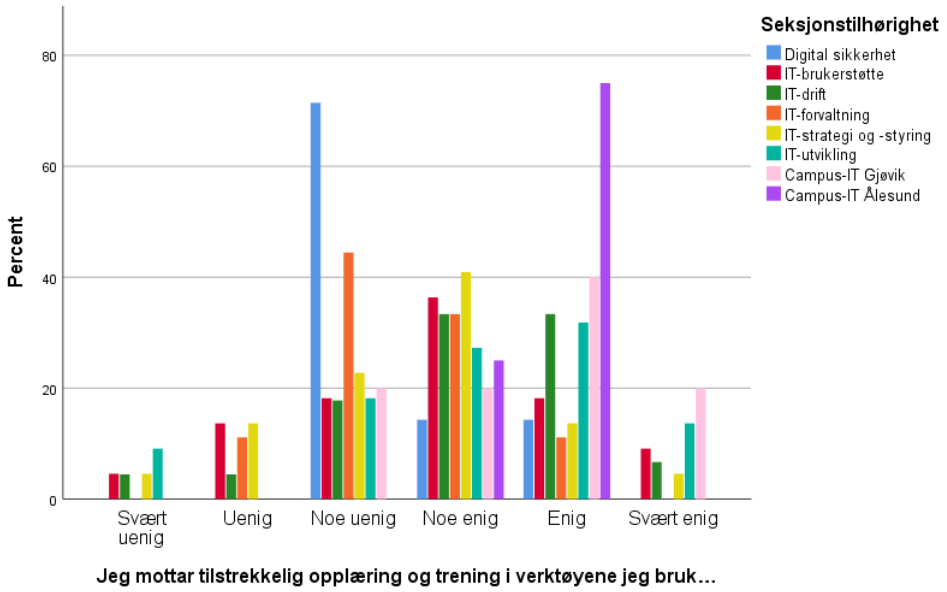
11. Jeg mottar tilstrekkelig opplæring og trening i verktøyene jeg bruker daglig

Påstanden er tiltenkt å avdekke om brukere føler de får den opplæringen og treningen de føler de trenger. Tanken bak påstanden er at om brukere ikke får god opplæring/trening blir de usikre i bruken av programmet og det kan forårsake feil bruk. Feil bruk av programmer kan gjøre arbeidsoppgaver svært tidkrevende og feil eller sikkerhetsrelaterte problemer kan oppstå.

Figur 25 viser at flest (44) respondenter svarer “noe enig”. 6 er “svært uenig”, så øker det til 9 “uenig” og det øker ytterligere til 32 som er “noe uenig”. Videre er 44 “noe enig”, 36 “enig” og så synker det til 10 som er “svært enig“. Distribusjonen er sentrert rundt “noe uenig“ til “enig”.



Figur 25: Jeg mottar tilstrekkelig opplæring og trening i verktøyene jeg bruker daglig



Figur 26: Jeg mottar tilstrekkelig opplæring og trening i verktøyene jeg bruker daglig sammen med seksjonstilhørighet

Det kan tyde på at flere ansatte, 90 respondenter, mener de får tilstrekkelig opplæring. Det er 65,7%, noe som ikke er veldig betryggende da man fortsatt har 47(34,3%) respondenter som føler de ikke får tilstrekkelig opplæring. Ser man resultatet distribuert per seksjon ser man ingen klar forskjell på seksjonene.

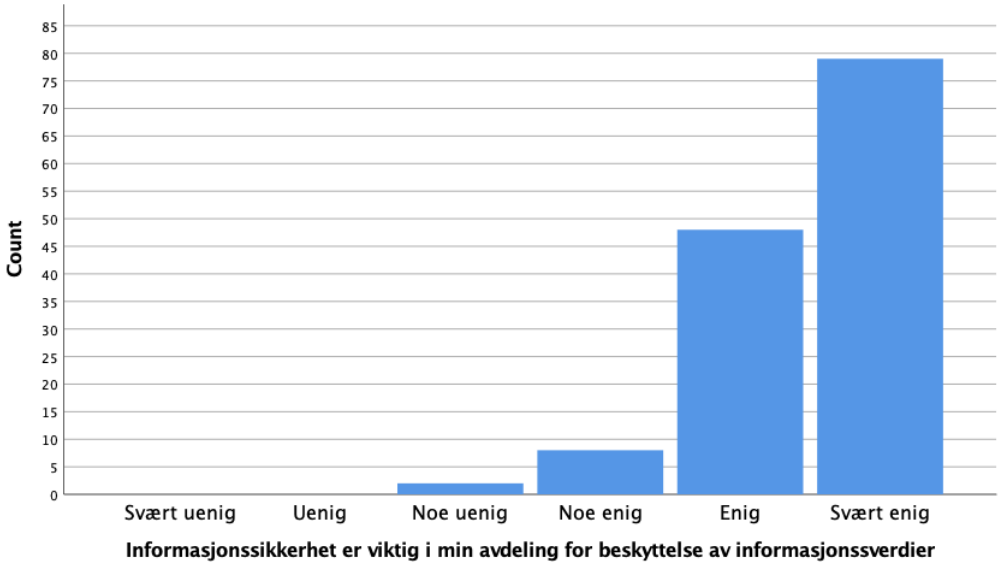
Basert på tilbakemeldinger (uklarhet i hva som menes) kan det tyde på at flere av respondentene svarte “noe uenig”/“noe enig” når de ønsket å være nøytrale. Om vi fjerner “noe uenig” og “noe enig” fra datasettet blir det 46 respondenter på “enig”/“svært enig” og 15 respondenter på “svært uenig”/“uenig”. Dette gjør ikke distribusjonen noe enklere å arbeide med, men det kan tyde på at det er forskjeller innad i en seksjon og at flere ansatte føler de ikke mottar tilstrekkelig opplæring.

Komponent - Bevisstgjøring

De følgende påstandene, 12, 13 og 14 prøver alle å avdekke grunnleggende holdninger i komponenten “bevisstgjøring”. Tolkningen av påstandene kommer i slutten av komponenten.

12. Informasjonssikkerhet er viktig i min avdeling for beskyttelse av informasjonssverdier

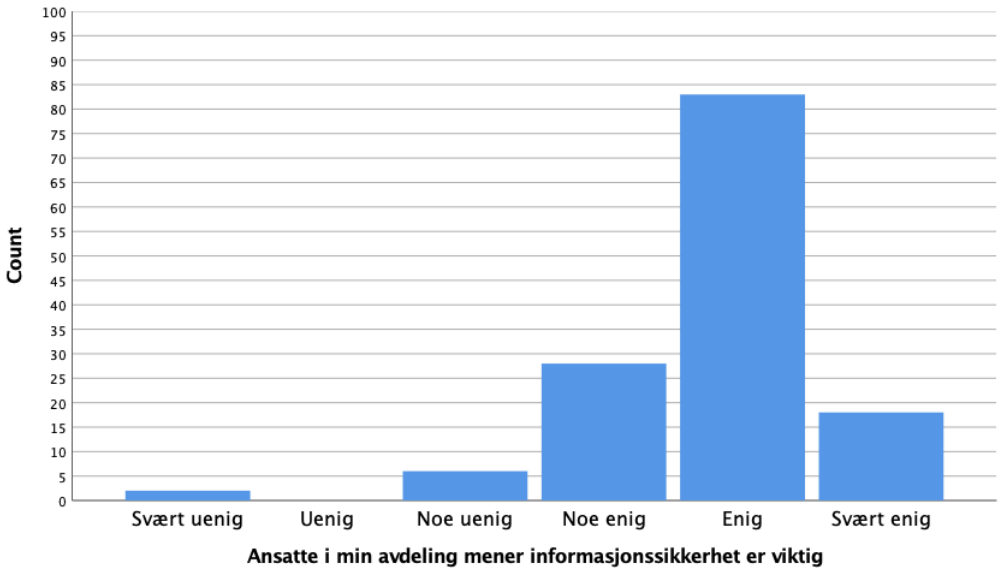
Figur 27 viser at respondentene har svart svært likt på spørsmålet. På venstredelen av distribusjonen har 2 svart at de er noe uenig. Videre øker det til 8 på noe enig, 48 på enig og 79 på svært enig. Flest respondenter har svart at de er svært enig.



Figur 27: Informasjonssikkerhet er viktig i min avdeling for beskyttelse av informasjonssverdier

13. Ansatte i min avdeling mener informasjonssikkerhet er viktig

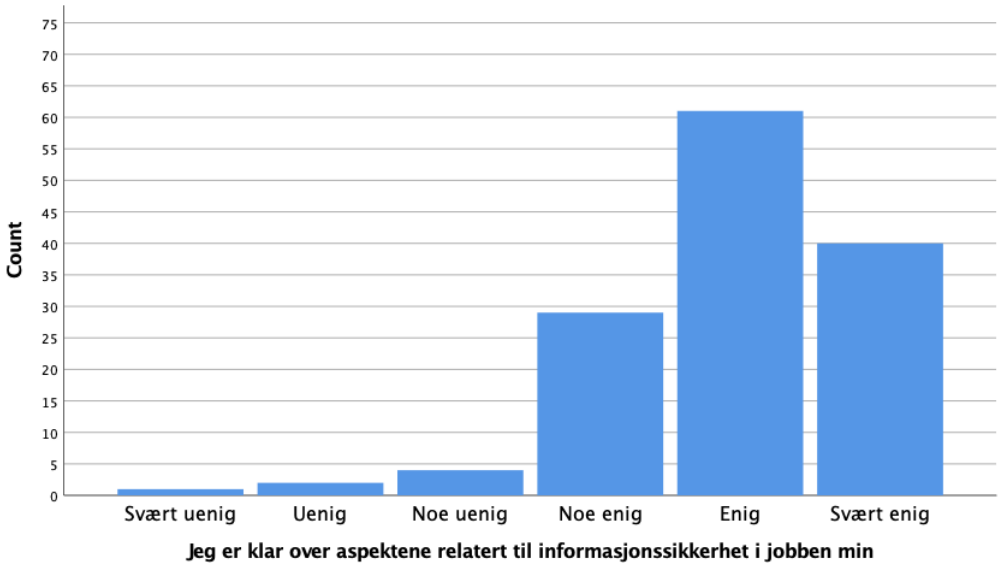
Distribusjonen gitt i figur 28 viser at flest respondenter, hele 68, nesten 50%, svarer enig i påstanden. 2 respondenter sier de er svært uenig, 1 er uenig, 2 er noe uenig. Videre sier 12 at de er noe enig, 68 enig(nesten 50%) og 52 er svært enig.



Figur 28: Ansatte i min avdeling mener informasjonssikkerhet er viktig

14. Jeg er klar over aspektene relatert til informasjonssikkerhet i jobben min

Figur 29 viser at majoriteten av respondenter svarer at de er enig i påstanden. Fra venstre svarer kun 1 at de er svært uenig, 2 er uenig og 4 er noe uenig. Videre sier 29 at de er noe enig, 61 er enig og 40 er svært enig i påstanden.



Figur 29: Jeg er klar over aspektene relatert til informasjonssikkerhet i jobben min

Correlations

			Informasjons sikkerhet er viktig i min avdeling for beskyttelse av informasjons verdier	Ansatte i min avdeling mener informasjons sikkerhet er viktig	Jeg er klar over aspektene relatert til informasjons sikkerhet i jobben min
Spearman's rho	Informasjonssikkerhet er viktig i min avdeling for beskyttelse av informasjonsverdier	Correlation Coefficient	1,000	,435**	,405**
		Sig. (2-tailed)	.	,000	,000
		N	137	137	137
	Ansatte i min avdeling mener informasjonssikkerhet er viktig	Correlation Coefficient	,435**	1,000	,377**
		Sig. (2-tailed)	,000	.	,000
		N	137	137	137
	Jeg er klar over aspektene relatert til informasjonssikkerhet i jobben min	Correlation Coefficient	,405**	,377**	1,000
		Sig. (2-tailed)	,000	,000	.
		N	137	137	137

**. Correlation is significant at the 0.01 level (2-tailed).

Figur 30: Korrelasjon for spørsmål i bevissthet komponenten.

Påstandene 12, 13 og 14 hører til under komponenten "bevisstgjøring". Disse påstandene angriper komponenten fra henholdsvis organisatorisk, gruppe og individuelt nivå i Robbins modell for organisasjonsstruktur. Et delmål med tolkningen er å avdekke om

det kan foreligge forskjeller mellom nivåene. Videre blir påstandene tolket hver for seg og det blir forsøkt å avdekke om det finnes et mønster i nivåene.

Påstand nummer 12, viser tydelig at det er stor enighet blant respondentene at informasjonssikkerhet er viktig i IT-avdelingen. Det er hele 98.5% som er "noe enig" til "svært enig". Her er det rimelig å samle sammen den øvre delen av skalaen, noe som tydelig viser stor enighet blant respondentene. Videre skulle man da ønske at respondentene sier at de ansatte mener informasjonssikkerhet er viktig i avdelingen, siden det er enighet at det er viktig.

Påstand 13 viser at hele 49.6% er enig at ansatte i avdelingen ser på informasjonssikkerhet som viktig. Samler man opp de som svarer "noe enig" og "svært enig", havner man på 96.4%. Ser man dette i sammenheng med foregående påstand så ser det ut til at ansatte etterlever viktigheten av informasjonssikkerhet. Det er fire respondenter som svarer "svært uenig" til "noe uenig", om at ansatte ikke mener informasjonssikkerhet er viktig. Dette utgjør en liten del totalt og kan være relatert til enkeltsituasjoner der andre faktorer har spilt inn for respondenten sin oppfatning. Man skal likevel ikke feie det under teppet at enkeltpersoner kanskje må arbeide med sin holdning til informasjonssikkerhet, om dette er relevant for personen sitt arbeid og er ønskelig av ledelsen.

Påstand nummer 14, handler om at respondenten er klar over aspektene relatert til informasjonssikkerhet i jobben sin. Det kan se ut til at det er en tendens fra de tidligere grafene om at flere har svart på venstre delen av skalen, fra "svært uenig" til "noe uenig". Ser man på tallene viser dette en økning fra 2, til 5, til 7 respondenter som svarer på fra "svært uenig" til "noe uenig". Tallene er mindre gode, men med et større antall respondenter så kunne man kanskje sett tendenser til impostor syndrom [3], redselen av å bli oppfattet som en bedrager. Hadde forskjellene vært større kunne dette betydd at respondentene føler at ansatte i avdelingen og organisasjonen har større styrke rundt informasjonssikkerhet enn det man selv har. Det er likevel mange respondenter (94.9%), som mener de er klar over aspektene relatert til informasjonssikkerhet i jobben sin. Det kan tyde på at ansatte føler noe usikkerhet rundt det å identifisere aspekter (arbeidsoppgaver, programmer, rutiner) som er viktig å tenke på for å arbeide godt med informasjonssikkerhet.

Som et scenario kan det hende en ansatt ikke er klar over hvordan bruken av Sharepoint relaterer til informasjonssikkerhet. En oppgave i faget IMT2008 med Gaute Wangen ved NTNU identifiserte nettopp dette. Flere ansatte hadde ikke tilstrekkelig tilgangskontroll for sine Sharepoint-sider. Dette gjorde sidene tilgjengelige for potensielt uvedkommende personer.

Det er også viktig å tenke på ved tolkningen, at kanskje ikke alle forstår hva som menes med "aspektene". Dette kan også være grunnen til en skjevere fordeling, enn ved spørsmål 12 og 13. Selv om det er et veldig fåtall (5.1%), som er "svært uenig" til "noe uenig" så er det viktig å merke seg at man arbeider som oftest som individer og det er individenes styrke som utgjør sikkerheten til organisasjonen. Det vil derfor være hensiktsmessig å arbeide for at alle ansatte kjenner til aspektene rundt informasjonssikkerhet relatert til jobben sin for å redusere risikoen for hendelser.

Et eksempel er det nylige angrepet Hydro stod ovenfor der løsepengeviruset Lockergoga herjet på systemet deres. NRK skriver at angrepet kan har startet med noe så enkelt

[3] https://en.wikipedia.org/wiki/Impostor_syndrome - (02.05.2019)

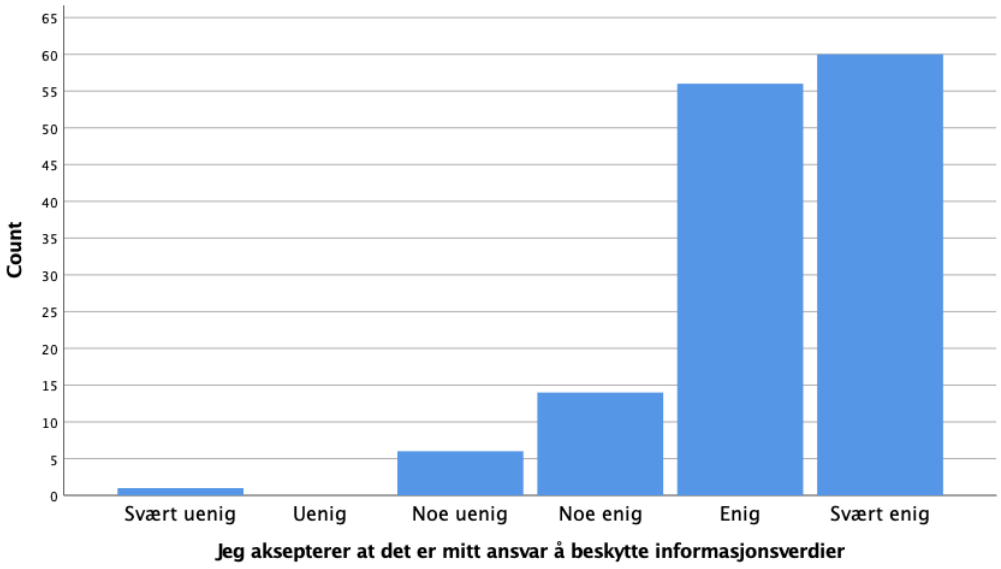
som en e-post [4]. Dette viser at selv om flertallet kan være bevisste, så er fortsatt individets handlinger svært viktig, noe som i Hydro sin sammenheng kostet dem en halv milliard [5].

Det er også interessant å se om det finnes korrelasjon mellom spørsmålene. Figur 30 viser korrelasjon mellom påstandene 12, 13 og 14. Vi kan lese av i figur 30 at det er moderat korrelasjon mellom påstand 12, og påstand 13, men en sterk korrelasjon med påstand 14. Videre ser vi også moderat korrelasjon mellom påstand 13 og 14. Siden det var sterk enighet blant respondentene at informasjonssikkerhet er viktig i IT-avdelingen så korrelerer det også sterkt (r=0.405) med at de selv er klar over aspektene relatert til informasjonssikkerhet. Dette kan tyde på at de som svarte at informasjonssikkerhet ikke er viktig i avdelingen sin, heller ikke selv er klar over aspektene relatert til informasjonssikkerhet. Dette utgjør dog et lite antall (7) av respondentene, men er uansett viktig å påpeke. Ut fra figuren tyder det mer på en sammenheng mellom organisatorisk, gruppe og individuelt nivå enn at det ikke er en sammenheng.

Komponent - Etisk adferd

15. Jeg aksepterer at det er mitt ansvar å beskytte informasjonsverdier

Det kommer frem i figur 31 at flest respondenter er svært enige i påstanden. Hele 60 svarer de er svært enige og 56 svarer de er enig. Sammen med 14 respondenter som svarer noe enig utgjør dette 94.9% av respondentene. En respondent svarte svært uenig, ingen uenige og 6 er noe uenig i påstanden.



Figur 31: Jeg aksepterer at det er mitt ansvar å beskytte informasjonsverdier

Totalt 7 respondenter har svart at de er enten "svært uenig" eller "noe uenig". Majoriteten ligger på den andre siden med over 94% av respondentene. Det betyr ikke så

[4] https://www.nrk.no/norge/slik-fungerer-losepengeviruset-som-rammet-hydro-1.14481782 - (01.05.2019)

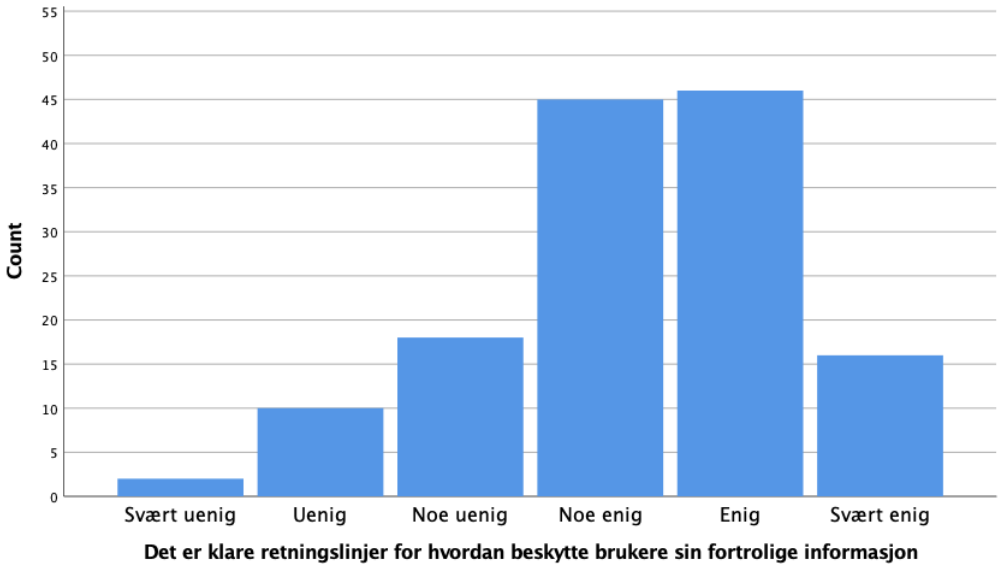
[5] https://www.dn.no/marked/hydro/norsk-hydro/svein-richard-brandtzag/cyberangrepet-koster-hydro-en-halv-milliard-i-forste-kvartal/2-1-594949 - (01.05.2019)

mye om retningslinjene sier om ansvaret ligger på brukeren. Her er det uansett positivt for IT-avdelingen at resultatet kan tyde på at ansatte aksepterer ansvaret for å beskytte informasjonsverdier selv. Man skal likevel ikke glemme respondentene som er uenige i påstanden. Det er viktig for NTNU og ansatte at informasjonsverdier er tilstrekkelig sikret. Det er vanskelig å si noe om adferden til de ansatte. For øvrig kan det tyde på at respondentene aksepterer ansvaret. For de fåtall av respondenter som svarer "svært uenig" til "noe uenig" er det ønskelig at de behandler informasjonsverdier korrekt, selv om de nødvendigvis ikke aksepterer det innebærer.

Komponent - Personvern

16. Det er klare retningslinjer for hvordan beskytte brukere sin fortrolige informasjon

Påstanden i figur 32 viser at flest respondenter svarer enten "noe enig" (45 stk) eller "enig" (46 stk), sammen utgjør det 66.4% av svarene. 2 respondenter svarer "svært uenig", 10 sier "uenig" og 18 er "noe uenig". 16 svarer de er "svært enig".



Figur 32: Det er klare retningslinjer for hvordan beskytte brukere sin fortrolige informasjon

Det kan synes at det er noe usikkerhet rundt retningslinjer for å beskytte brukere sin fortrolige informasjon. Man må tenke på at kanskje mange ikke arbeider med fortrolig informasjon og ikke kjenner til disse retningslinjene. Det kan være at de da har havnet mot midten, noe man kanskje kan se en tendens på i figuren på søyle "noe enig".

Det er 21.5% som svarer at de er "svært uenig" til "noe uenig". Dette utgjør 30 respondenter. Om det er rimelig å anta at de som svarte "noe uenig" eller "noe enig" ønsket å svare nøytralt, vil det være 8.8% (12 respondenter) som sier de er "svært uenig" til "uenig". Det er viktig å merke at folk er forkjellige og kan forstå og lære forskjellig. Det kan da være hensiktsmessig å arbeide for at flere skal forstå retningslinjene. Videre vil de som svarer "enig" til "svært enig" utgjøre 45.3%, noe som kan tyde på vanskeligheter med retningslinjene. Andre faktorer som relevanse og arbeidsoppgaver spiller inn her,

men det kan tenkes at de som da har svart enten “svært uenig” til “uenig” og “enig” til “svært enig” vil være de som har en mening på retningslinjer. Da er det rimelig å anta at majoriteten mener at retningslinjene er klare. Hvorvidt disse faktisk følges er en annen sak og bør følges opp innad i avdelingen.

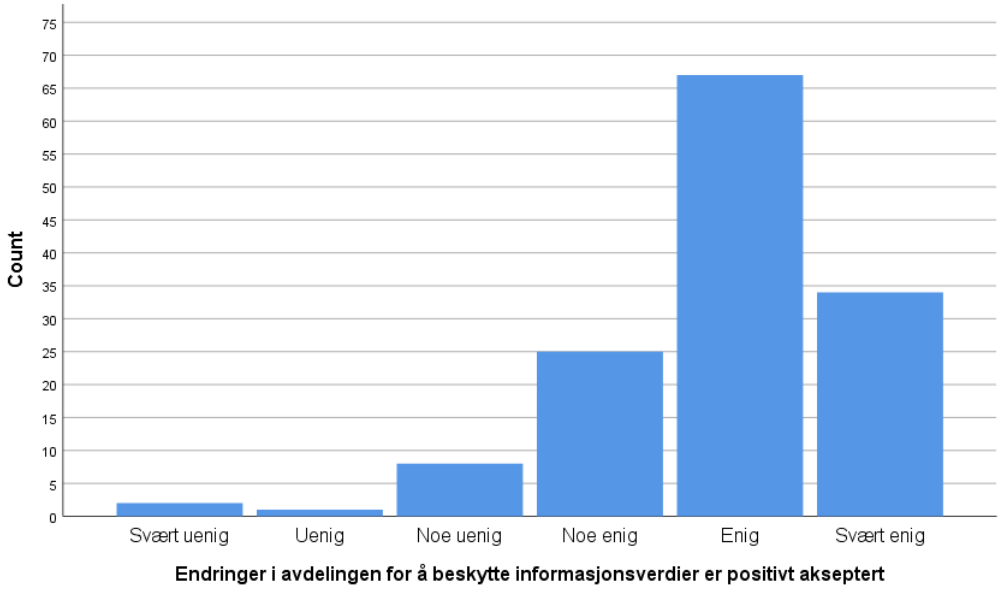
11.7.5 Kategori - Endring

Komponent - Endringsledelse

17. Endringer i avdelingen for å beskytte informasjonsverdier er positivt akseptert

Denne påstanden sier noe om hvordan avdelingen opplever endringer og om endringer oppfattes som positivt eller negativt. Påstanden sier også noe om hva respondentene mener om avdelingen som en helhet.

På denne distribusjonen så svarer de fleste at de er enig. Det var 34 som svarte at de var "svært enig", 67 oppgir at de er "enige" og 25 oppgir at de er "noe enig" i påstanden. Det er til sammen 11 som er "noe uenig", "uenig" eller "svært uenig".



Figur 33: Endringer i avdelingen for å beskytte informasjonsverdier er positivt akseptert

Ut ifra resultatet i figur 33 kan det virke som om at IT-avdelingen hånterer enderinger på en god måte eller at endringer er positivt motatt blant de ansatte i avdelingen. Ekstremverdiene, som i dette tilfellet er "svært uenig" og "uenig" kan tyde på enkelttilfeller hvor endringer har blitt dårlig mottatt. Spredningen i svarene kan også tyde på at det er noe usikkerhet blant respondentene, eller at de ikke vet om enderinger blir positivt akseptert i IT-avdelingen. Da er det naturlig å tenke at de kan ha svart "noe uenig" og "noe enig", som er de sentrale verdiene i likert-skalaen. Fjerner man disse fra resultatet viser responsen fremdeles en tendens mot "enig". I dette spørsmålet er Robbins organisasjonsmodell sentral, ved at gruppens handlinger påvirker individet og i dette tilfellet vil en positiv tendens i gruppa kunne bli med å heve de individuelles oppfatning av endringer.

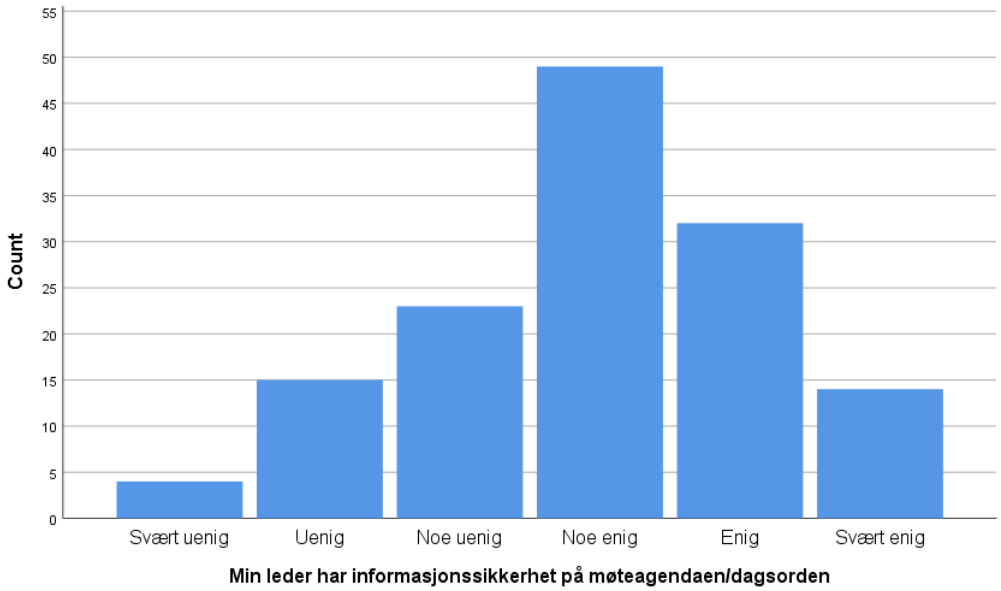
11.7.6 Kategori - Ledelse og styring

Komponent - Ledelsesforankring

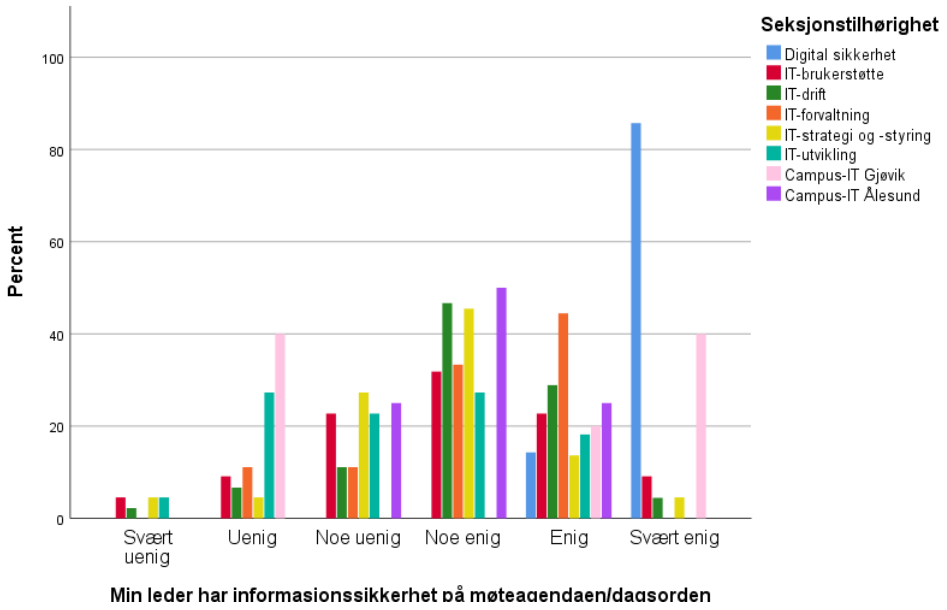
Denne komponenten inneholder to påstander. Tolkningen av begge påstandene blir gjort i slutten av komponenten.

18. Min leder har informasjonssikkerhet på møteagendaen/dagsorden

På denne påstanden (se figur 34) svarte 4 personer at de var "svært uenige", 15 oppga at de var "uenige", 23 "Noe uenig". Tilsammen så utgjør svarene fra "Svært uenig" tom. "Noe uenig" 30.7% av svarene. Når det gjelder de som er enige så svarte 49 at de var "noe enige", 32 "enige" og 14 "svært enig".



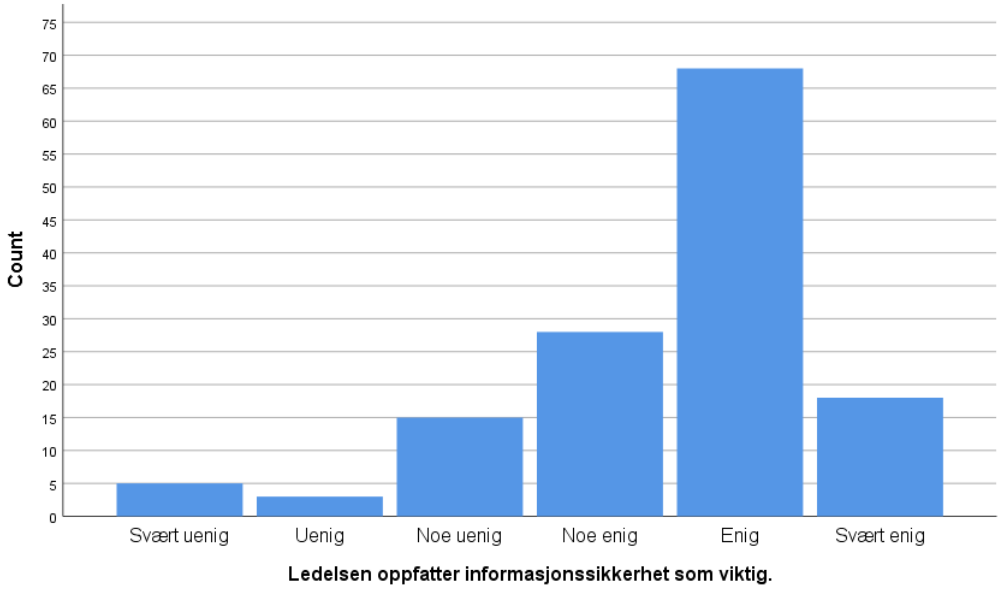
Figur 34: Min leder har informasjonssikkerhet på møteagendaen/dagsorden



Figur 35: Seksjonstilhørlighet til påstanden "Min leder har informasjonssikkerhet på møteagendaen/dagsorden"

19. Ledelsen oppfatter informasjonssikkerhet som viktig

Respondentene er generelt enige i denne påstanden, figur 36. Til sammen så svarer 83.1% av respondentene at de er "noe enige", "enige" eller "svært enige" i påstanden. Det er 5 respondenter som er "svært uenig", 3 som er "uenig" og 15 respondenter er "noe uenig" i påstanden.



Figur 36: Ledelsen oppfatter informasjonssikkerhet som viktig

På påstand 18 er respondentene rimelig spredt utover hele skalen, med en sentral tendens mot "noe enig". Det er interessant å se på spredningen i svarene til en seksjon, som vist ved figur 35. For eksempel så har IT-brukerstøtte avgitt svar på alle nivåene i likert-skalaen. Ut i fra figuren kan vi observere stor spredning i opplevelsen hos respondentene innad i enkelte seksjoner om hvorvidt lederen kommuniserer informasjonsikkerhet og om informasjonsikkerhet tas opp eller ikke. Det at det er stor spreding i besvarelsen innad i en seksjon kan også tyde på at informasjonssikkerhet blir kommunisert på ulike måter til de ansatte. Det er rimelig å anta at det er meningen at informasjonssikkerhet skal bli kommunisert og at informasjonssikkerhet er noe som burde ha vært tatt opp. På grunn av at det er noen som stiller seg "svært enig" og "svært uenig" i påstanden fra den samme avdelingen, så kan det virke som at enkelte har inntrykket at lederen formidler informasjonssikkerhet mens andre ikke har det samme inntrykket.

Påstand 18 kan tolkes på flere måter. Det kan enten forståes som at lederen kommuniserer sikkerhet, om lederen tar opp informasjonssikkerhet ved møter el. eller om informasjonssikkerhet taes opp i seksjonen generelt. Dersom enkelte ikke forstod meningen med spørsmålet er det naturlig å tro at de oppga svar mot "midten" av skalen i intervallene, "noe uenig" og "noe enig". Ekskluderer vi disse to intervallene får vi at 29.2% er "svært uenig" og "uenig" mens 70.8% er "enig" og "svært enig", som fremdeles er en tendens mot generell enighet i påstanden.

Påstand 19 korrelerer sterkt med påstanden om "*min leder har informasjonssikkerhet på møteagendaen/dagsorden*", illustrert i figur 34 (r = 0.562). Med påstand 19 er vi ute etter de ansattes mening på om ledelsen prioriterer og holder seg oppdatert på informasjonssikkerhet og synes det er viktig. På grunn av likheten mellom denne påstanden og den forrige, kan det være noe usikkerhet i om respondentene oppfatter påstandene riktig. Korrelasjonen kan tyde på at en del respondenter svarer det samme på begge påstandene. Det er også sterk korrelasjon med påstanden om "*jeg mener NTNU gir tilstrekkelig oppmerksomhet til informasjonssikkerhet*", i figur 38 (r = 0.576).

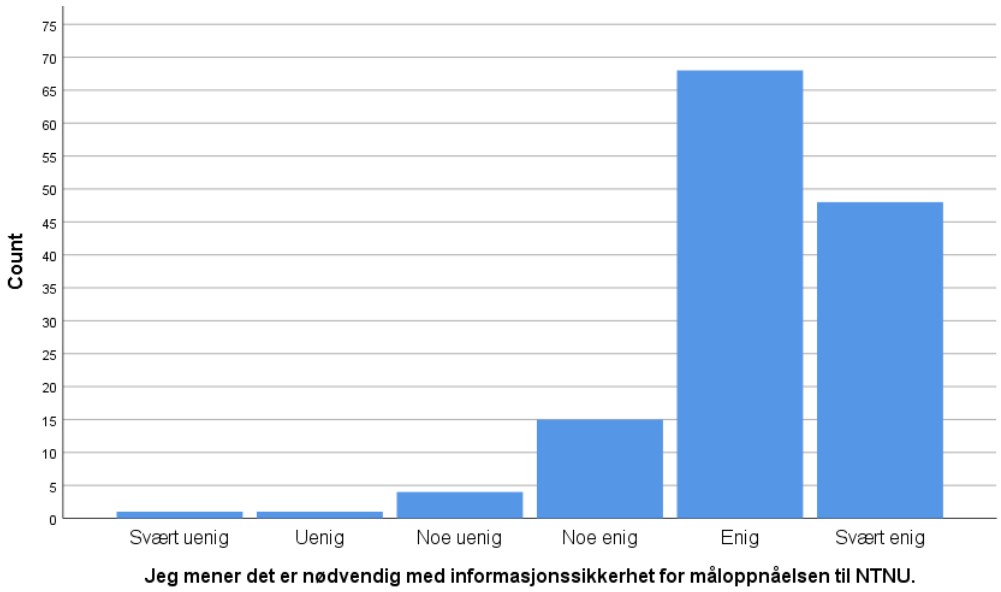
I besvarelsen av påstand 19 kan kunnskapsnivået om informasjonssikkerhet til den ansatte påvirke graden av enighet i besvarelsen. Det er rimelig å anta at dersom den ansatte allerede innehar mye kunnskap om informasjonssikkerhet, så føler man kanskje at ledelsen ikke oppfatter informasjonssikkerhet som viktig nok. Har man derimot lite kunnskap om informasjonssikkerhet så er det mulig at man synes ledelsen bruker mye tid på det.

Komponent - Strategi

Denne komponenten inneholder to påstander. Tolkningen av begge påstandene blir gjort i slutten av komponenten.

20. Jeg mener det er nødvendig med informasjonssikkerhet for måloppnåelsen til NTNU

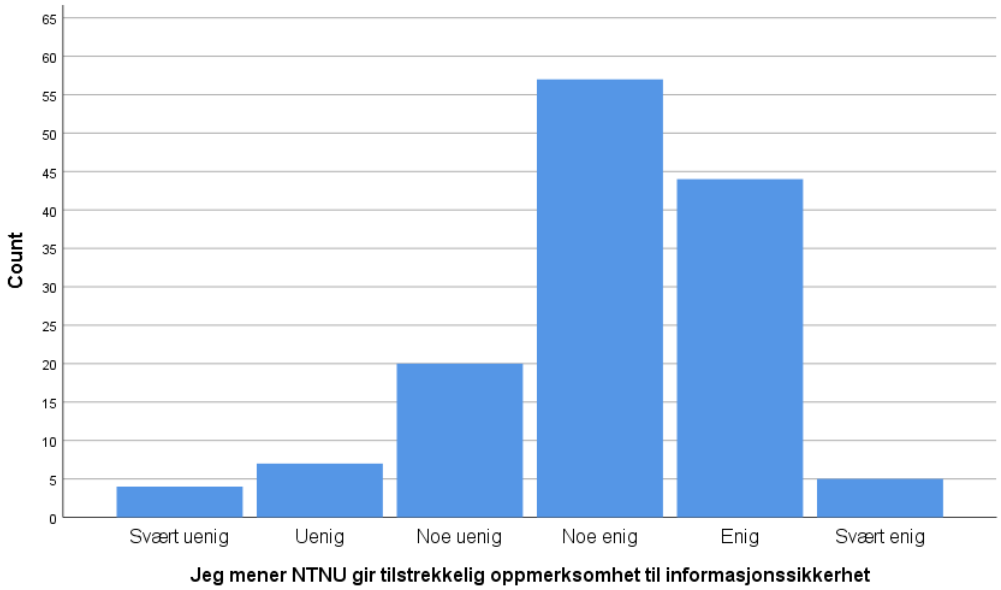
I denne påstanden (se figur 37) er de fleste respondentene "enig"(49.6%) og "svært enig"(35.0%). 15 respondenter er ogå "noe enig" i påstanden. Det er 1 respondent som er "svært uenig", 1 som er "uenig" og 4 respondenter er "noe uenig".



Figur 37: Jeg mener det er nødvendig med informasjonssikkerhet for måloppnåelsen til NTNU

21. Jeg mener NTNU gir tilstrekkelig oppmerksomhet til informasjonssikkerhet

På påstanden i figur 38, svarer de fleste at de er "noe enige" i påstanden. 4 respondenter er "svært uenig", 7 "uenig" og 20 er "noe uenig". Denne halvdelen av svarene utgjør 22.6%. Videre svarer 57 respondenter at de er "noe enige", 44 "enige" og 5 svarer "svært enig". Totalt utgjør den andre halvdelen av svarene 77.4% av respondentene.



Figur 38: Jeg mener NTNU gir tilstrekkelig oppmerksomhet til informasjonssikkerhet

I påstand 20 antyder resultatet at det er en stor enighet i at informasjonssikkerhet er viktig for måloppnåelsen til NTNU. Det er også rimelig å anta at respondentene også er klar over hva måloppnåelsen til NTNU går ut på. Isåfall er dette et meget godt resultat.

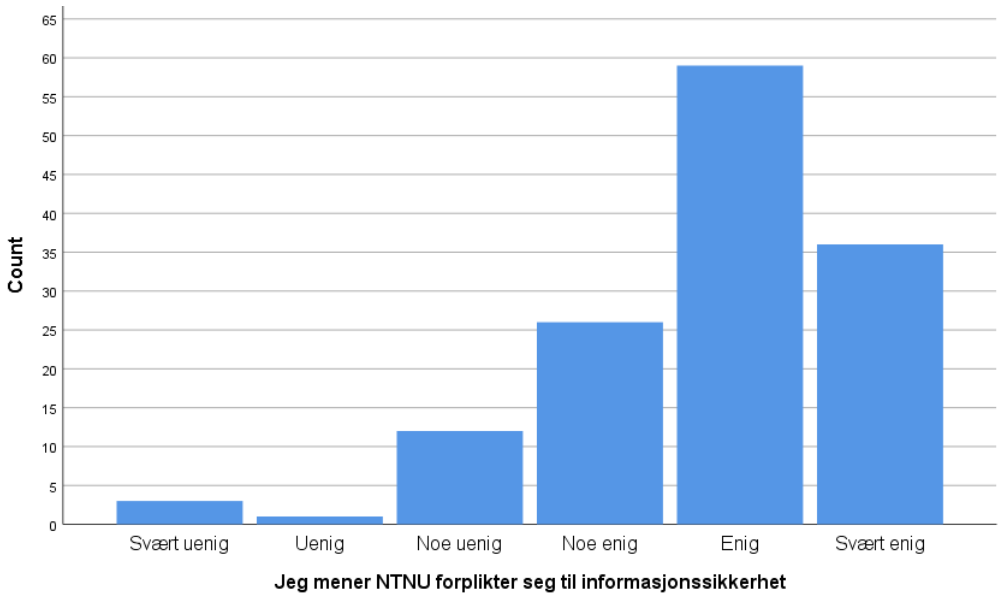
Påstand 21 derimot, sier noe om IT-avdelingens oppfattning av NTNU sin oppmersomhet til informasjonssikkerhet. Ut ifra Robbins organisasjonsmodell så vil denne påstanden påvirke det organisatoriske nivået. Det organisatoriske vil da igjen påvirke gruppe-nivået og tilslutt enkeltindividene. Det er derfor viktig at ledelsen prioriterer informasjonssikkerhet for å kunne påvirke de ansatte i en positiv retning. I påstand 21 er det overvekt av antall respondenter som er "svært enig" i påstanden. Det er allikevel 22.6% av svarene på den venstre halvdelen av skalaen. Det er vanskelig å si om nivået i resultatet er aksepterbart eller ikke. NTNU er en organisasjon med flere målsetninger og det er naturlig at ikke alt av tiden brukes på informasjonssikkerhet. Det er viktig å huske på at dette er bare synspunktet til IT-avdelingen om NTNU vier nok oppmerksomhet til informasjonssikkerhet. Det kan være at NTNU bruker en del tid på informasjonssikkerhet, men dette blir kommunisert dårlig til IT-avdelingen. Det kan også hende at IT-avdelingen er en av de avdelingene som får informasjonssikkerhet kommunisert best.

Komponent - Styring

Denne komponenten inneholder to påstander. Tolkningen av begge påstandene blir gjort i slutten av komponenten.

22. Jeg mener NTNU forplikter seg til informasjonssikkerhet

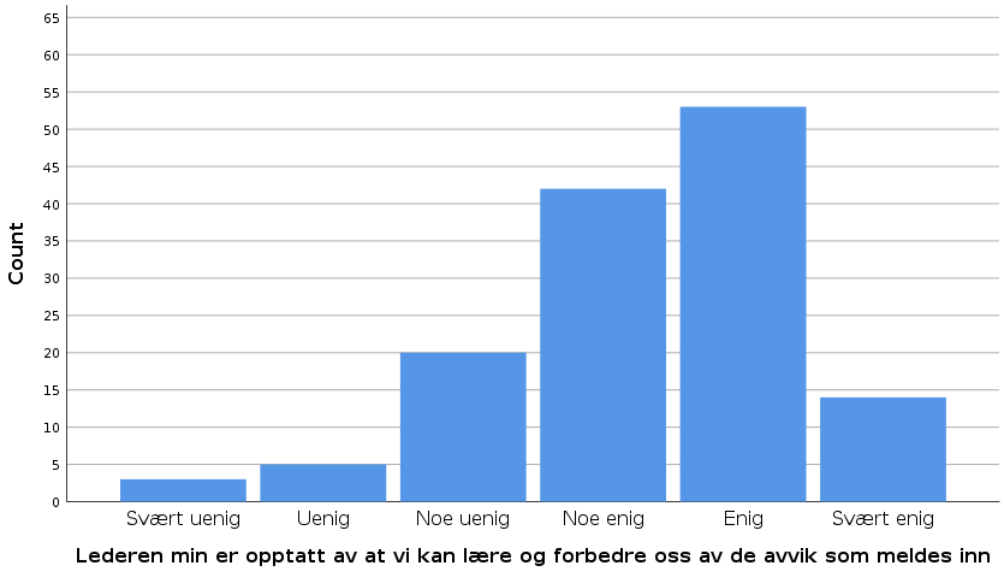
Ved påstanden i figur 39 er de fleste respondentene "enige". Det er 36 respondenter som svarer at de er "svært enige", 59 svarer at de er "enige" og 26 respondenter er "noe enige". Tilsammen utgjør disse svarene hele 88.3%. På den andre siden så svarer 3 respondenter at de er "svært uenige", 1 er "uenig" og 12 respondenter er "noe uenige" i påstanden.



Figur 39: Jeg mener NTNU forplikter seg til informasjonssikkerhet

36 - Lederen min er opptatt av at vi kan lære og forbedre oss av de avvik som meldes inn

På denne påstanden (se figur 40) svarte 3 respondenter "svært uenig", 5 "uenig", 20 "noe uenig", 42 "noe enig", 53 "enig" og 14 svarte at de var "svært enig".



Figur 40: Lederen min er opptatt av at vi kan lære og forbedre oss av de avvik som meldes inn

I påstand 22 er vi ute etter de ansattes mening på hvorvidt NTNU prioriterer informasjonssikkerhet. Det er også da rimelig å anta at dersom respondentene er enige i denne påstanden så har de kunnskap om avgjørelser ledelsen i NTNU gjør relatert til informasjonssikkerhet. Det kan være muligheter for ulik forståelse av denne påstanden ved at det tolkes som at NTNU er nødt til å forholde seg til informasjonssikkerhet på papiret mot opplevd forpliktelse blant de ansatte som svarte på dette spørsmålet. Det er interessant å se på mulige grunner til at de ansatte opplever at NTNU ikke forplikter seg til informasjonsikkerhet, altså de som er "svært uenig", "uenig" og "noe uenig" i denne påstanden. En mulig grunn til dette er ulik tolkning av påstanden, men det er også mulig at respondentene ikke har nok kunnskap om avgjørelser ledelsen gjør angående informasjonssikkerhet.

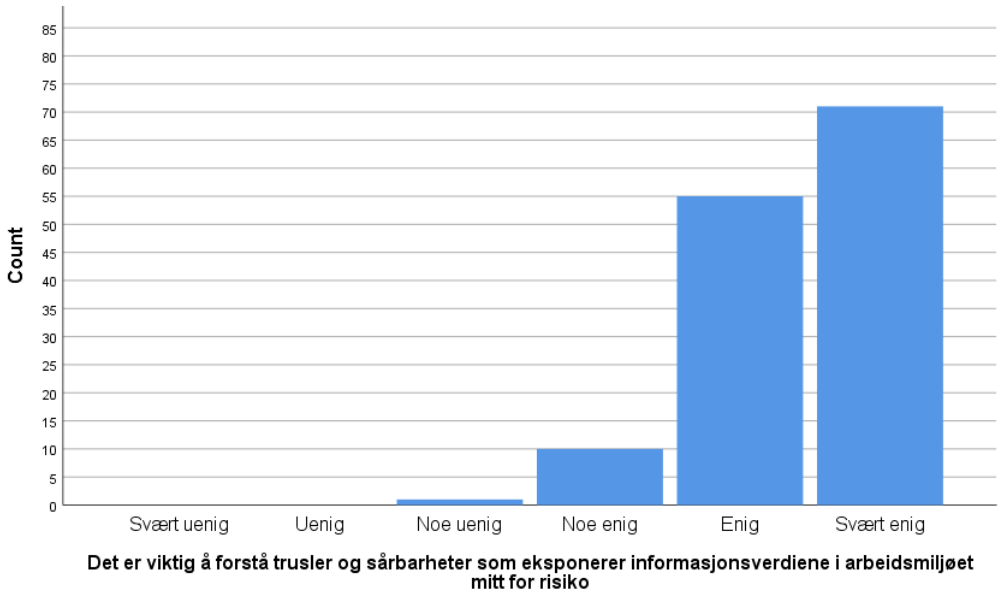
I påstand 36 kan man se en høyreskjøvet fordeling hvor 95 respondenter (69.4%) svarte enten "noe enig" eller "enig". Påstanden forteller hvordan de ansatte oppfatter sin leder med tanke på læring ved innrapporterting av innmeldte avvik. Vanligvis oppfattes ordet avvik negativt ladet, men la oss anta at ansatte har en positiv holdning til avvik på bakgrunn av at ved rapportering av avvik kommer forbedringer. Med denne antakelsen kan man videre tenke seg at i avdelinger hvor avvik knyttes til noe positivt vil rapportering forekomme hyppigere og man unngår underrapportering som baseres på "det skjer ikke noe allikevel". Videre kan man også tenke seg at ledelseforankring ikke nødvendigvis tilsier at rapportering vil forekomme. Det skyldes at det i tillegg må det være aksept på gruppenivå for at rapportering skal forekomme.

Komponent - Risikostyring

Denne komponenten inneholder to påstander. Tolkningen av begge påstandene blir gjort i slutten av komponenten.

23. Det er viktig å forstå trusler og sårbarheter som eksponerer informasjonsverdiene i arbeidsmiljøet mitt for risiko

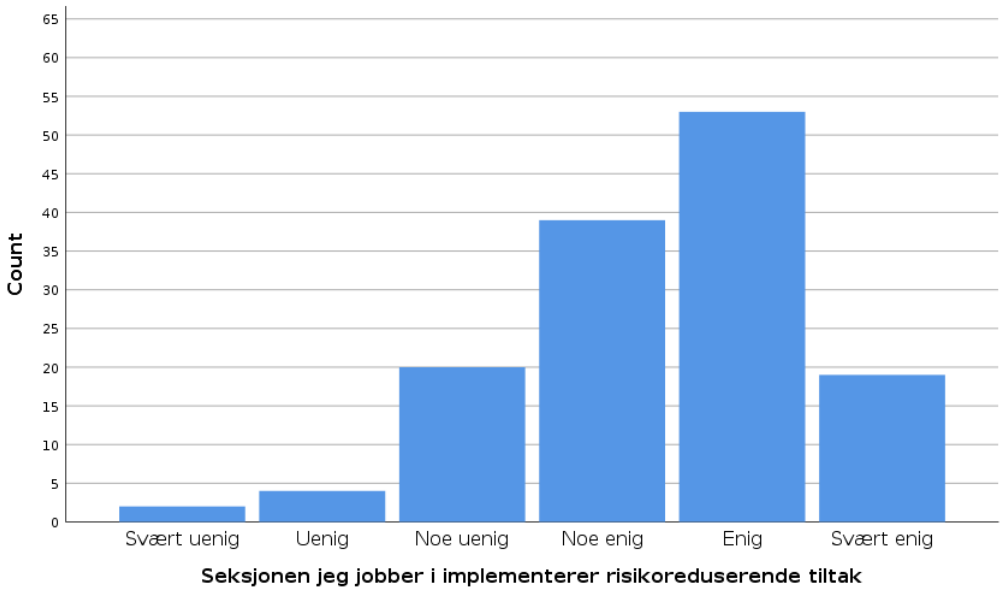
I denne påstanden (se figur 41) svarer de fleste respondentene at de er svært enige. Hele 71 respondenter svarer svært enig og 55 er enige i denne påstanden. Disse to svaralternativene utgjør 91.9%. 1 svarer “noe uenig”, mens 10 svarer “noe enig”.



Figur 41: Det er viktig å forstå trusler og sårbarheter som eksponerer informasjonsverdiene i arbeidsmiljøet mitt for risiko

35 - Seksjonen jeg jobber i implementerer risikoreduserende tiltak

Ved påstand 35 vist i figur 42 nedenfor svarer 2 “svært uenig”, 4 “uenig”, 20 “noe uenig”, 39 “noe enig”, 53 “enig” og 19 “svært enig”.



Figur 42: Seksjonen jeg jobber i implementerer risikoreduserende tiltak

Gjennom påstand 23 ønsker vi å finne ut om de ansatte forstår viktigheten av risiko- og sårbarhetsvurderinger (ROS). Vi vil imidlertid ikke nødvendigvis finne ut om de ansatte vet hva som er truslene og sårbarhetene. Men påstanden kan si noe om at de ansatte synes at risikovurderinger er viktig. Ut ifra dette kan man antyde at de ansatte er motiverte for å drive med risikovurderinger. Dette er isåfall en gruppe som er mottagelig for læring, dersom de ikke innhar kunnskap om trusler og sårbarheter. Det er rimelig å anta at påstand 23 er meget sentral for IT-avdelingen spesielt. Det kan være noe av grunnen til det gode resultatet.

Påstanden 35 forteller hvordan respondenten opplever seksjonen vedkommende jobber i. Politikk for Informasjonssikkerhet sier:

> ... ansatte og studenter i stand til å klassifisere informasjonen de behandler, gjennomføre risikovurderinger og velge nødvendige **tiltak** for å beskytte informasjonen i arbeidsprosessene [8].

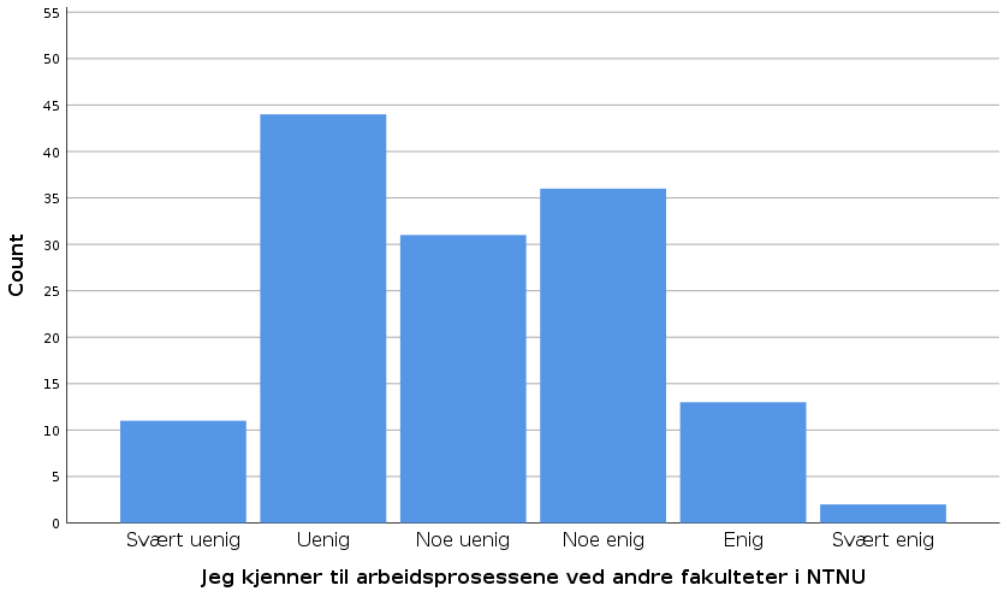
På bakgrunn av at det er den enkelte selv som er ansvarlig for å gjennomføre risikoreduserende tiltak føler vi at fordelingen i påstand 35, er mer spredt enn ønskelig. Man kan tenke seg at å gjennomføre tiltak ikke nødvendigis er en prosess som alle er involvert i, men hvor en ansatt er utnevnt uoffisielt med “ansvaret”. En annen antakelse på hvorfor fordelingen er spredt kan skyldes at selv om respondenten eksempelvis kommer med tiltaksforslag blir ikke disse fulgt opp. Generelt kan det virke naturlig at det vil være færre hendelser i en avdeling med hyppigere proaktive tiltak.

11.7.7 Kategori - Sikkerhetsledelse og drift

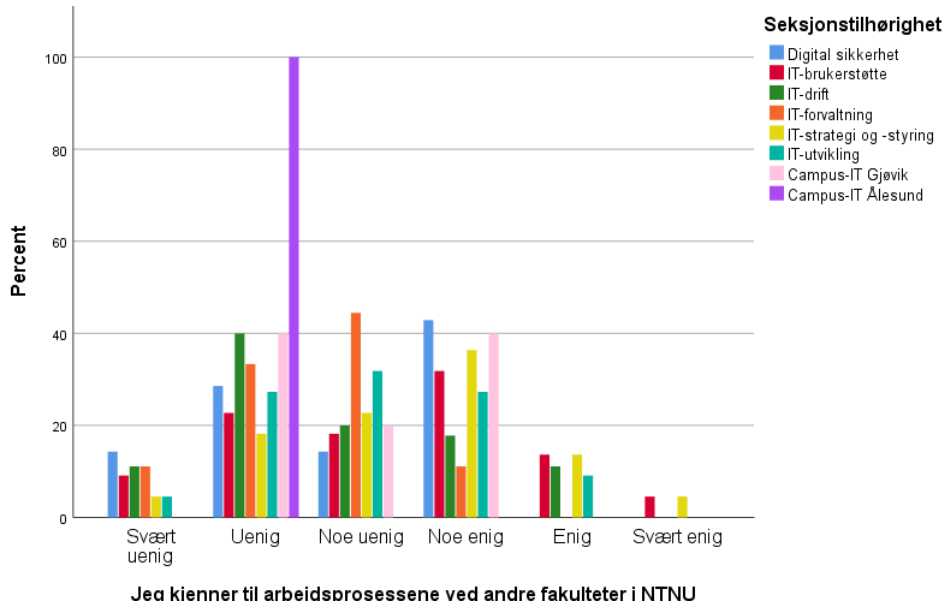
Komponent - Avdelingstruktur

32 - Jeg kjenner til arbeidsprosessene ved andre fakulteter i NTNU

På denne påstanden (se figur 43) har respondentene svart følgende: 11 “svært uenig”, 44 “uenig”, 31 “noe uenig”, 36 “noe enig”, 13 “enig” og 2 “svært enig”



Figur 43: Jeg kjenner til arbeidsprosessene ved andre fakulteter i NTNU



Figur 44: Jeg kjenner til arbeidsprosessene ved andre fakulteter i NTNU - Tilhørlighet

Her kan vi se at svarene er relativt spredt. Hvor viktig det er å kjenne til andre fakulteters arbeidsprosesser kan diskuteres i hvorvidt det er nødvendig med krav til samarbeid. Med tanke på at denne undersøkelsen tok for seg IT-avdelingen kan det være interessant å se nærmere på resultatet. Videre kan også årsaken til spredt resultat for IT-utvikling skyldes at det primært er én person med hovedoppgave å lytte til de kravene som stilles til programvaren. Videre analyse skyldes at IT-avdelingen i tillegg til sine interne arbeidsoppgaver fungerer som kontaktpunkt, som bidrar til å løse utfordringer i ulike fakulteter[6]. Ved nærmere analyse av figur 44, kan det tyde på at respondenter som tilhører seksjon for IT-utvikling også svarer relativt ulikt. Dette er interessant med tanke på at en av arbeidsoppgavene for IT-utvikling er å tilrette og løse utfordringer som kommer fra ulike fakulteter. Eksempelvis kan det foreligge ønske om et nytt program. Man kan anta at det vil være svært vanskelig å imøtekomme de ønskene som blir stilt uten å vite hvordan arbeidsprosessene og de systemer som benyttes i fakultet fungerer. Dette kan eksempelvis dreie seg om at det blir benyttet ulike operativsystemer og derfor må programvaren være uavhengig av operativsystemene. Hvis man antar at overnevnte påstand er riktig kan dette være en årsak til at det benyttes programvareløsninger som ikke er produsert eller godkjent av NTNU. Derfor kan man anta at påstand nummer 32 korrelerer med påstand 30, "Jeg bruker private applikasjoner for å utføre arbeid relatert til jobben min". Noe det viser seg å ikke gjøre (r=-0.004). Ut ifra denne korrelasjonen kan det tyde på at en mulig konsekvens at IT-avdelingens verktøy ikke nødvendigvis påvirker ansatte i IT-avdelingen til å bruke alternative verktøy. Det kan på en annen side være muligheter for at andre fakulteter utfører arbied på siden av systemer, men det er vanskelig å si noe om dette i denne undersøkelsen. Med ønske fra Randi ble påstand nummer 32 lagt til i undersøkelsen, på bakgrunn av en hypotese om at IT-avdelingen ikke kjenner så godt til kjerneviksomheten og de administrative støtteprosessene i NTNU. Hypotesen går også ut på at IT-avdelingen tilbyr verktøy som ikke er godt nok tilpasset NTNUs prosesser som kan medføre at medarbeidere utfører arbeidet sitt på siden av systemer.

[6] "...alt fra rådgivning, utvikling og IT-drift. Sammen jobber vi alle for å forenkle, fornye og forbedre arbeids- og studiehverdagen for alle på NTNU." https://www.ntnu.no/adm/it

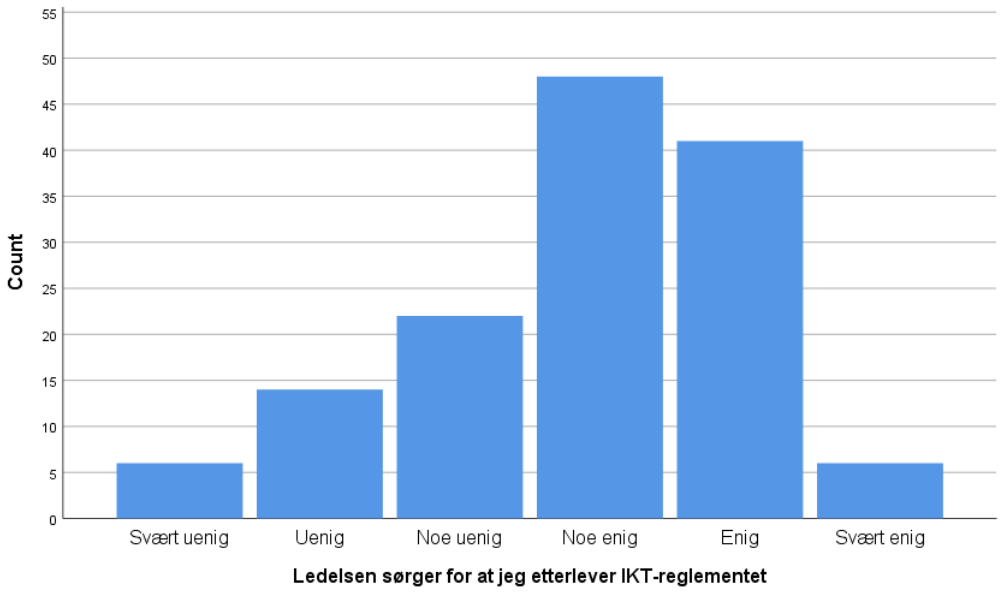
11.7.8 Kategori - Sikkerhetsprogramledelse

Komponent - Compliance

Denne komponenten inneholder fire påstander. Tolkningen av påstandene blir gjort i slutten av komponenten.

24. Ledelsen sørger for at jeg etterlever IKT-reglementet

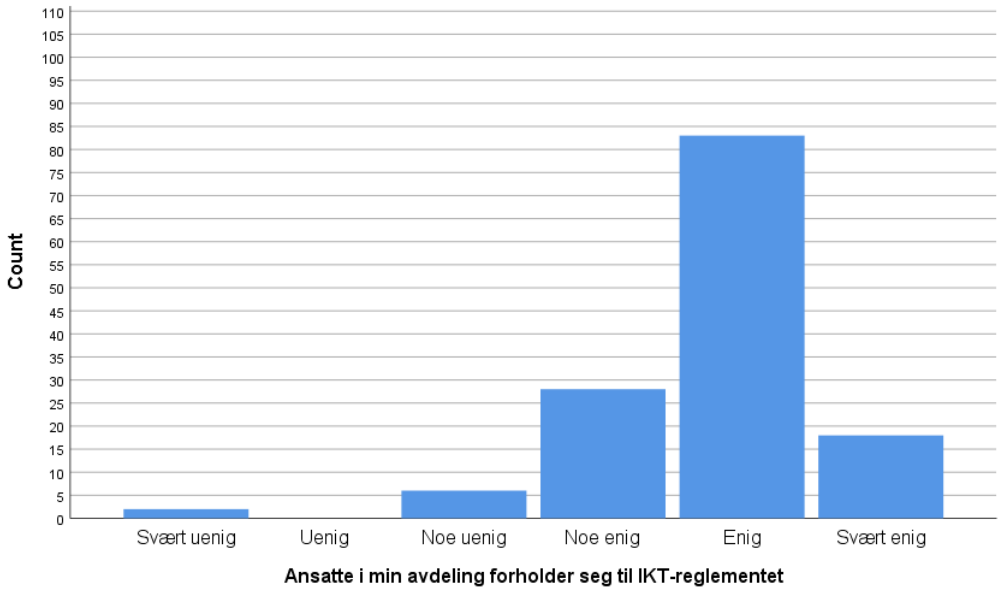
På denne påstanden (se figur 45) svarer 6 respondenter at de er "svært uenig", 14 er "uenig" og 22 er "noe uenig". Denne uenige halvdelen av likert-skalen tilsvarer 30.7% av svarene. De resterende 69.3% har følgende fordeling: 48 respondenter er "noe enig", 41 er "enig" og 6 er "svært enig" i påstanden. Dette spørsmålet korrelerer sterkt med spørsmålet om *ansatte i min avdeling forholder seg til IKT reglementet*, illustrert i figur 46 (r = 0.482).



Figur 45: Ledelsen sørger for at jeg etterlever IKT-reglemente

25. Ansatte i min avdeling forholder seg til IKT-reglementet

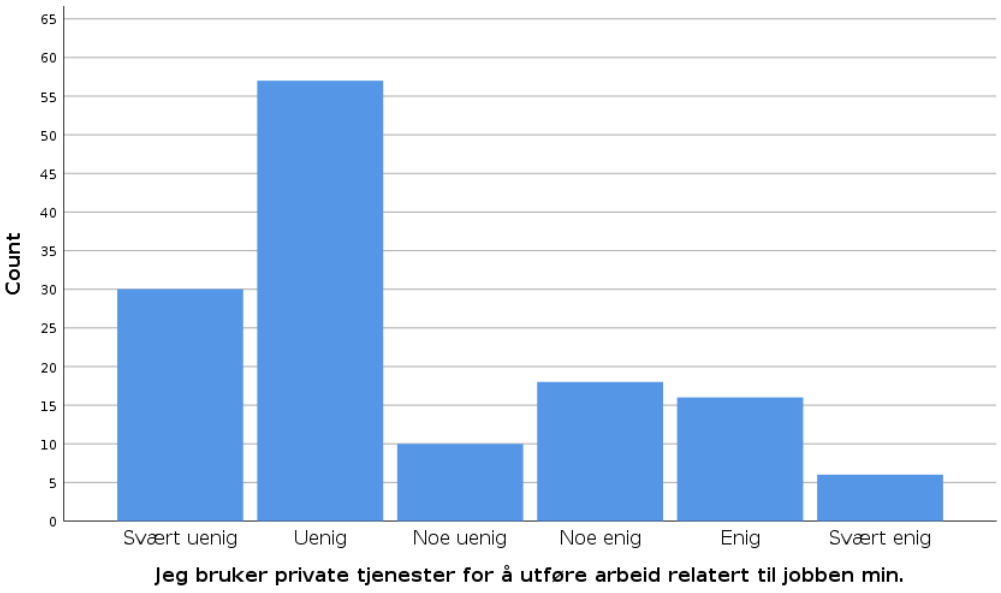
Med denne påstanden (se figur 46) ønsker vi å finne ut hva den enkelte mener om avdelingen som helhet. I denne påstanden er de fleste "enige", med 83 respondenter (60.6%). 18 respondenter er "svært enige" og 28 er "noe enige" i påstanden. Hele 94.2% av svarene er fordelt på "noe enig", "enig" eller "svært enig". På den andre siden så har 2 respondenter svart "svært uenig" og 6 svarer at de er "noe uenig".



Figur 46: Ansatte i min avdeling forholder seg til IKT-reglementet

30 - Jeg bruker private applikasjoner for å utføre arbeid relatert til jobben min

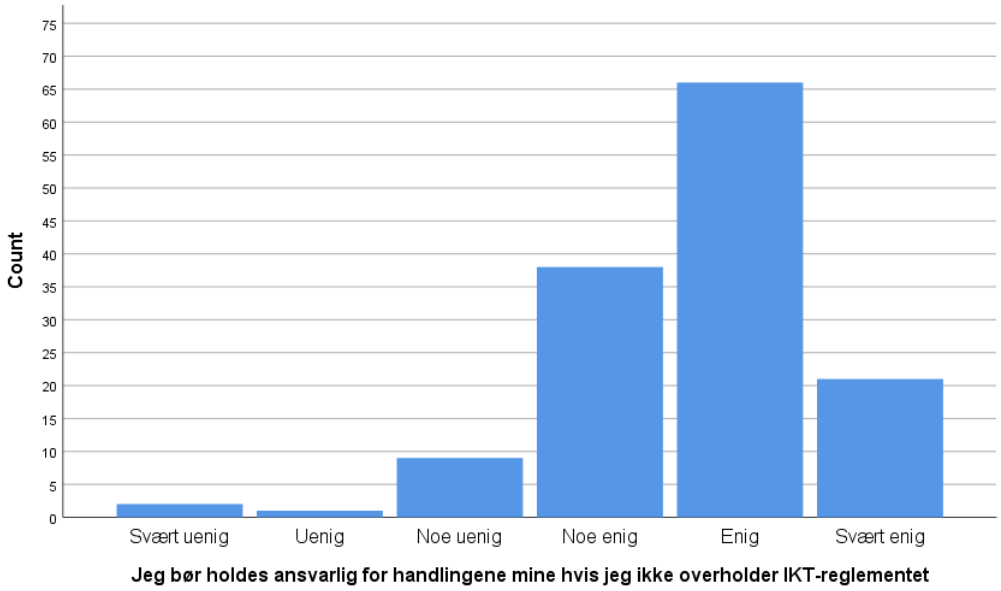
I denne påstanden (se figur 47) svarer 30 respondenter "svært uenig", 57 svarer "uenig", 10 svarer "noe uenig", 18 "noe enig", 16 "enig" og 6 respondenter stiller seg "svært enig" til påstanden.



Figur 47: Jeg bruker private applikasjoner for å utføre arbeid relatert til jobben min

26. Jeg bør holdes ansvarlig for handlingene mine hvis jeg ikke overholder IKT-reglementet

I denne påstanden (se figur 48) svarer 2 respondenter at de er "svært uenige", 1 svarer "uenig", 9 svarer "noe uenig", 38 svarer "noe enig", 66 svarer "enig" og 21 svarer at de er "svært enige". Dette spørsmålet korrelerer sterkt med spørsmålet om ansatte i min avdeing forholder seg til IKT-reglementet, illustrert i figur 46 (r = 0.457).



Figur 48: Jeg bør holdes ansvarlig for handlingene mine hvis jeg ikke overholder IKT-reglementet

Oppsummering compliance

På påstand 24, "ledelsen sørger for at jeg etterlever IKT-reglementet", så er de fleste respondentene "noe enig" og "enig". IKT-reglementet. Det er en mulighet for at denne påstanden kan tolkes ulikt, ved at det er forskjellig oppfatning om hva som menes med å etterleve. Påstanden kan tolkes som at ledelsen sørger for at man etterlever IKT-reglementet hvis man signerer på dokumentet. En annen tolkningsmetode er at ledelsen aktivt sørger for at den ansatte etterlever IKT reglementet, selv etter at dokumentet er signert.

I påstand nummer 25, om *ansatte i min avdeling forholder seg til IKT-reglement* kan det tyde på en enighet om at avdelingen som helhet forholder seg til IKT-reglementet. Denne påstanden prøver å finne ut hva respondenten tenker om avdelingen som gruppe og hvilke oppfatninger den har om avdelingen. Det kan være mulig å anta at lite sikkerhetshendelser gjør at folk tror de etterlever IKT-reglementet. Dersom man svarer "svært uenig" på denne påstanden så kan det tyde på at man er ganske klar over tilfeller hvor ansatte har brutt IKT-reglementet. På grunn av sterk korrelasjon mellom påstand 24 og 25 så kan det tyde på at mange av de som har svart et gitt svar på påstand 24 har svart det samme i påstand 25. Det kan tyde på at noen av de som er "svært uenig" i påstand 24 og da mener at ledelsen ikke sørger for at de ansatte etterlever IKT-reglementet også er svært uenig i at de ansatte i avdelingen følger det. Det samme gjelder også for andre en-

den av skalaen. Grunnen til at mange svarer “svært enig” kan være at de ikke vet konkret de ansattes forhold til IKT-reglementet, men heller har en antakelse om at det følges.

HI påstand nummer 30 kan fordelingen tolkes som at NTNU stort sett dekker de behovene respondenten har til applikasjoner for å utføre sine arbeidsoppgaver. Det er viktig å bemerke seg at påstanden ikke sier noe om hvorvidt det eksisterer programvare for arbeidsprosessene utstedt av NTNU. En antakelse kan være at selv om det eksisterer programvare så finnes det bedre private tjenester som respondenten foretrekker eksempelvis grunnet bedre kjennskap eller utfører arbeidsprosessen enklere. Her ser vi i etterkant av spørreundersøkelsen at det burde foreligget et tilstandskrav i fobindelse med påstand nummer 31 i spørreundersøkelsen: “I såfall hvilke privateapplikasjoner er det du anser som viktig”. Dette fritekst-spørsmålet burde vært avgrenset til kun de som svarte “noe uenig“ eller lavere i påstand 30. Forøvrig, ved å kategorisere de mest svarte svaralternativene i påstand 31, kommer vi fram til følgende gjentagelse: (5)Teksteditorer m/ IDE-støtte. (4)Skylagringstjenester som Dropbox og Google Drive og (4)e-postklienter for både Windows og Linux.

I påstand 26, “Jeg bør holdes ansvarlig for handlingene mine hvis jeg ikke overholder IKT- reglementet”, tyder det på at det er en stor enighet blant de ansatte om at de selv burde holdes ansvarlige. Selv om den ansatte ikke nødvendigvis er ansvarlig for brudd på IKT-reglementet, så er det rimelig å anta at resultatet reflekterer at de ansatte er ansvarsfulle i den forstand at de selv føler seg ansvarlige for sine handlinger. Dette er en kollektiv god etisk atferd for en gruppe, og det kan virke som at de ansatte har en stolthet til arbeidsplassen sin.

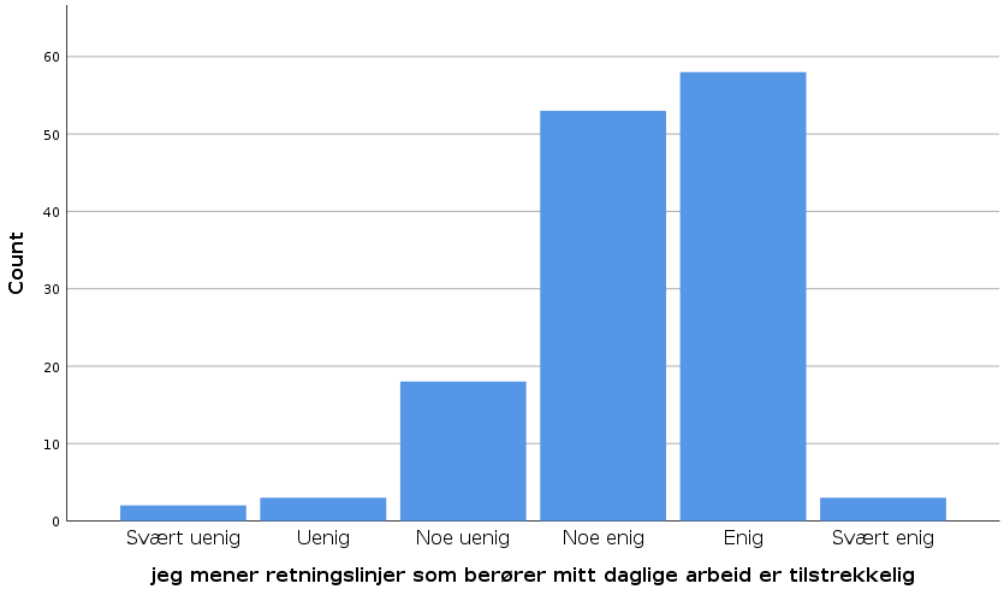
Disse fire påstandene måler komponenten Compliance fra ulike perspektiver. Påstand 24 sier noe om hva hver ansatt mener om organisasjonen som helet, påstand 25 sier noe om hva den ansatte synes om gruppa, påstand 30 og 26 sier noe om hva hver enkelt ansatt mener om seg selv. Det er interessant å se om synspunktet til den ansatte forandres ettersom de skal mene noe om gruppa som helhet eller seg selv. I dette tilfellet er det ingen merkbare forskjeller.

11.7.9 Kategori - Sikkerhetspolitikk

Komponent - Politikk

27 - Jeg mener retningslinjer som berører mitt daglige arbeid er tilstrekkelig

I denne påstanden (se figur 49) svarer 2 “svært uenig”, 3 “uenig”, 18 “noe uenig”, 53 “noe enig”, 58 “enig” og 3 “svært enig”.



Figur 49: Jeg mener retningslinjer som berører mitt daglige arbeid er tilstrekkelig

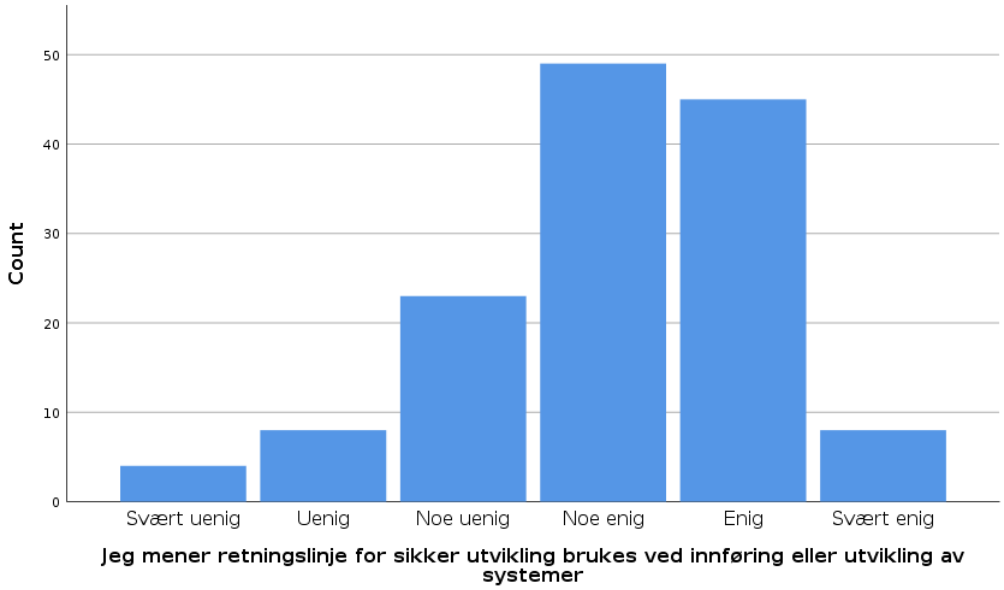
Hele 81% svarte enten “noe enig” eller “enig”.
På bakgrunn av spredningen kan det virke som om de fleste opplever at arbeidsprosesser er godt identifiserte og dokumenterte. Man kan anta at avdelinger med en høyere frekvens av nye arbeidsoppgaver vil kunne oppleve retningslinjene mangefull og derfor stille seg mer uenig til påstanden. En annen antakelse er at respondentene var usikre ved tolkningen av spørsmålet, noe som kommer fram i tilbakemeldingen fra undersøkelsen og derfor holdt seg nøytrale til påstanden som påvirker resultatet.

11.7.10 Kategori - Teknisk sikkerhet og drift

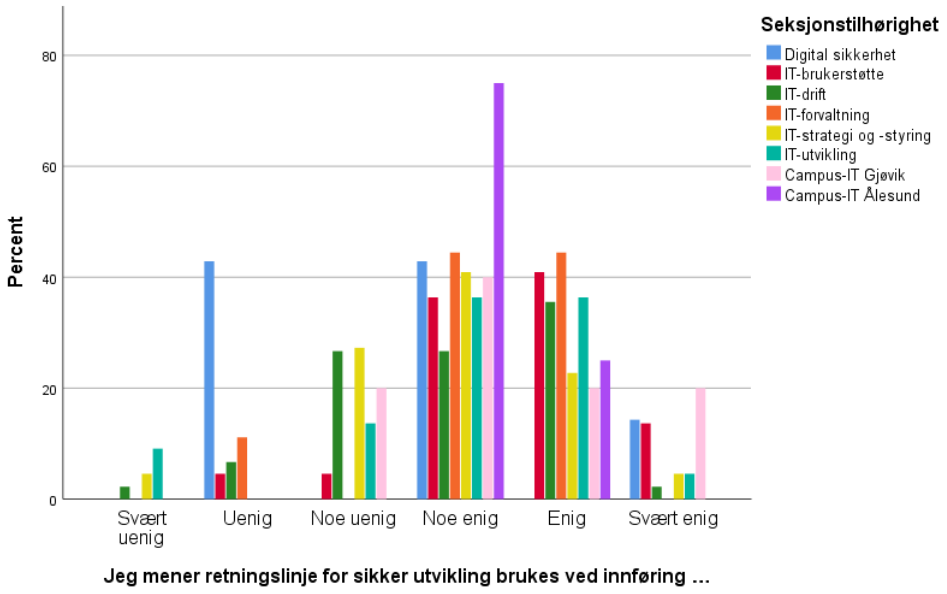
Komponent - Systemutvikling

28 - Jeg mener retningslinje for sikker utvikling brukes ved innføring eller utvikling av systemer

På denne påstanden (se figur 50) svarer 4 respondenter "svært uenig", 8 "uenig", 23 "noe uenig", 49 "noe enig", 45 "enig" og 8 respondenter er "svært enig".



Figur 50: Jeg mener retningslinje for sikker utvikling brukes ved innføring eller utvikling av systemer



Figur 51: Jeg mener retningslinje for sikker utvikling brukes ved innføring eller utvikling av systemer - Fordeling

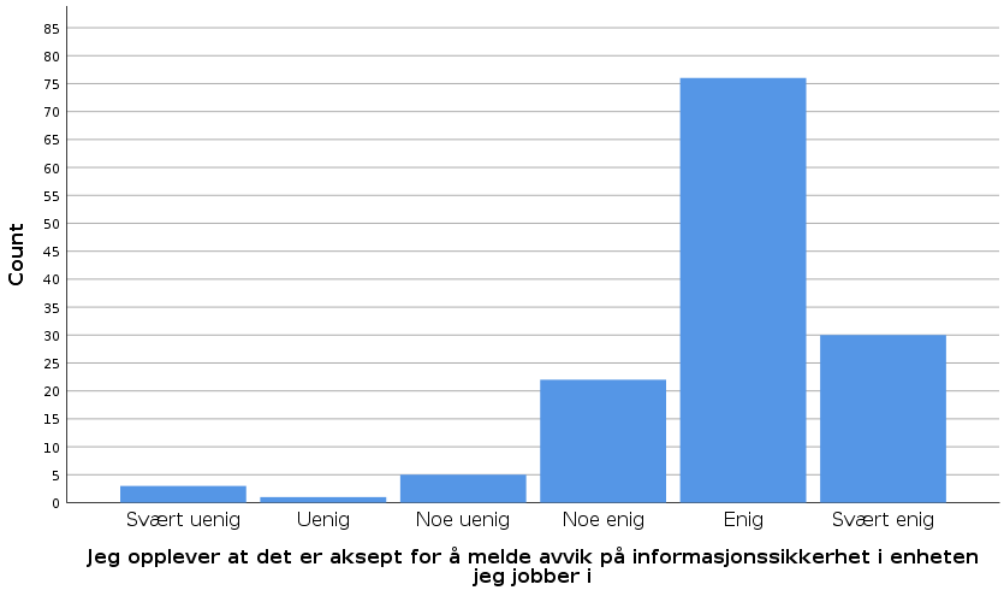
Her tyder fordelingen av data på usikkerhet knyttet til spørsmålet. Dette kan skyldes tolkning og hvor relevant dette er i sammenheng med respondentens jobb. Svaret blir derfor noe nøytralt (sentralisert i figuren).

Det er interessant er at resultatet til IT-utvikling er sentrert noe høyere på skalaen (se figur 51). Dette kan knyttes opp imot at avdelingens arbeidsprosesser er direkte knyttet til utvikling, som igjen kan tyde på at retningslinjene for IT-Utvikling er i tråd med sikker utvikling. En antakelse kan være at ikke alle har de samme arbeidsprosessene innad og derfor ikke direkte knyttet opp til arbeid med utvikling (figur 51).

Komponent - Hendelseshåndtering

29 - Jeg opplever at det er aksept for å melde avvik på informasjonssikkerhet i seksjonen jeg jobber i

I denne påstanden (se figur 52) svarer respondentene, 3 “svært uenig”, 1 “uenig”, 5 “noe uenig”, 22 “noe enig”, 76 “enig” og 30 “svært enig”.



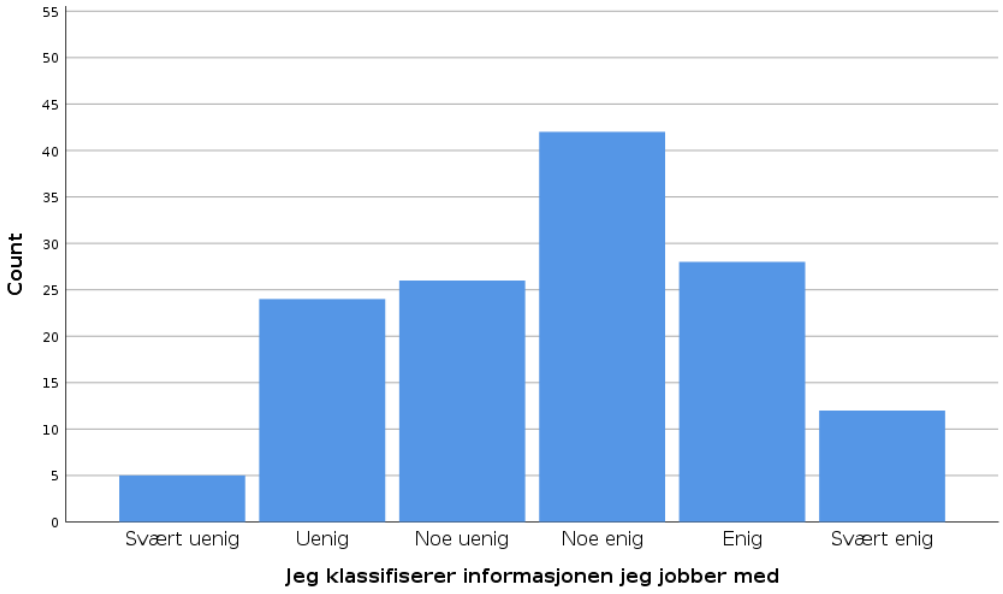
Figur 52: Jeg opplever at det er aksept for å melde avvik på informasjonssikkerhet i seksjonen jeg jobber i

Hele 78% av respondentene (106) svarte “enig” eller “svært enig”. Dette forteller noe om hvordan respondenten oppfatter holdningene blant sine medarbeidere. Generelt kan datafordelingen tyde på at takhøyden for å melde avvik er god. Man kan anta at avdelinger med lav aksept for å melde avvik har et potensielt høyere antall tilfeller hvor avvik ikke er rapportert og mister derfor muligheten for å utbedre disse avvikene.

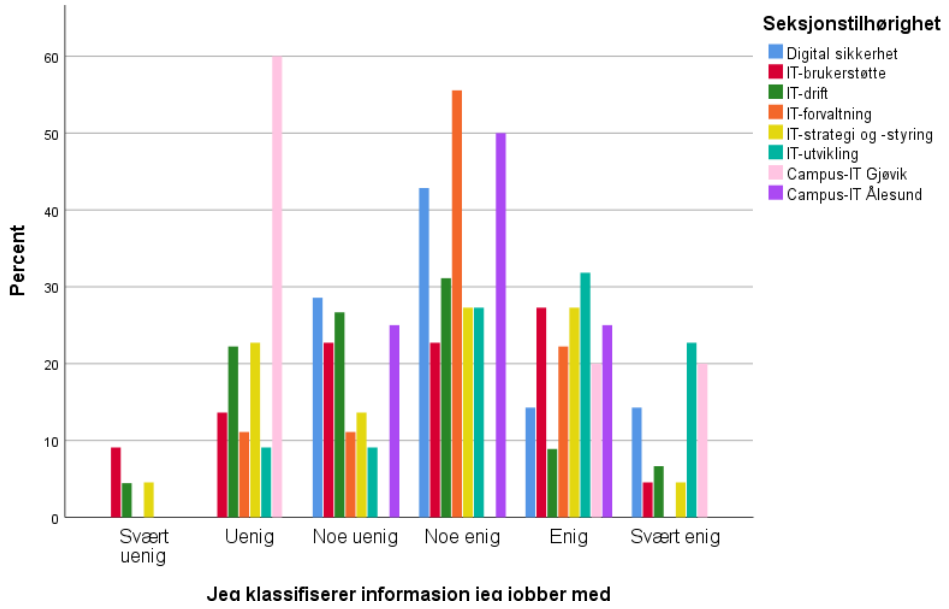
Komponent - Styring av informasjonsverdier

33 - Jeg klassifiserer informasjon jeg jobber med

I denne påstanden (se figur 53) svarer 5 respondenter “svært uenig”, 24 “uenig”, 26 “noe uenig”, 42 “noe enig”. 28 “enig”, og 12 “svært enig”. Denne påstanden korrelerer sterkt med påstand nr 34. “I seksjonen jeg jobber i har vi oversikt over hvilke informasjonsverdier vi behandler"($r = 0.603$)”



Figur 53: Jeg klassifiserer informasjon jeg jobber med



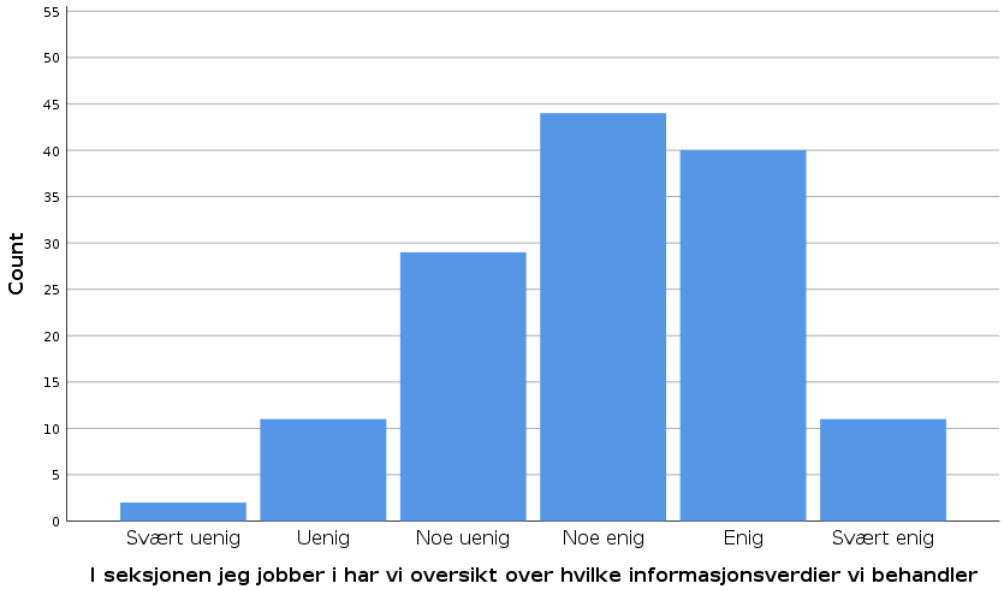
Figur 54: Jeg klassifiserer informasjon jeg jobber med - Fordeling

Påstand 33 forteller oss om respondenten selv klassifiserer informasjonen som benyttes. For oss virker det interessant at data er så spredt som baseres på at klassifisering er en prosess som man enten gjennomfører eller ikke. Derfor burde kanskje et alternativ til likert-skala vært vurdert, da man kan anse at man enten faktisk *klassifiserer informasjon man jobber med*, eller *ikke klassifiserer informasjonen*. Respondentens svar kan skyldes *til hvilken grad* dette gjøres på bakgrunn av nye informasjonsverdier som dukker opp.

Hvis en avdeling ofte opplever å behandle nye verdier er klassifisering en prosess som gjennomføres oftere. Med foregående antakelse om at hyppighet er avgjørende, tyder fordelingen i figur 54 på at IT-utvikling er de som hyppigst må forholde seg til klassifisering av informasjonen det jobbes med.

34 - I seksjonen jeg jobber i har vi oversikt over hvilke informasjonsverdier vi behandler

I denne påstanden (se figur 55), svarer 2 respondenter “svært uenig”, 11 “uenig”, 29 “noe uenig”, 44 “noe enig”, 40 “enig”, 11 “svært enige”.



Figur 55: I seksjonen jeg jobber i har vi oversikt over hvilke informasjonsverdier vi behandler

Påstand 34 gir oss de ansattes perspektiv på seksjonen. Her kan det virke som fordelingen av dataen kan skyldes ulik tolkning av påstanden. Dersom man ser kun på én avdeling, så er fremdeles dataen spredt. Dette er interessant å se på, da det virker naturlig at ansatte i samme avdeling burde ha svart det samme og at ansatte i samme seksjon, spesielt de mindre, håndterer de samme informasjonsverdiene. Dette kan igjen skyldes tolkningen av påstanden, eller at en ansatt har fått utvidet ansvar for å identifisere informasjonsverdiene. I tillegg kan man også anta at ved større avdelinger behandles det flere typer informasjonsverdier og derav mindre kontroll. Det er interssant å sammenligne IT-Campus-Gjøvik og -Ålesund. Hvis man kan anta at disse benytter de samme informasjonsverdiene og hvorfor Ålesund skiller seg ut ved med betydlig mindre spredning. Dette kan skyldes lite utvalg.

11.8 Styrker og svakheter ved kulturen i IT-avdelingen

Denne seksjonen omhandler utvalg av sterke og svake sider ved sikkerhetskulturen til IT-avdelingen. Det vil først være en gjennomgang av hver komponent sine spørsmål for å finne ut om det er forbedringspotensiale eller ikke. Til slutt er det en oppsummering

som viser tydelig hva som er de største styrkene og svakhetene vi har funnet.

11.8.1 Kunnskapspåstander

I kunnskapsspørsmålene ble det avdekket noen områder med mulig forbedringpotensiale. Ved spørsmål om respondenten har lest politikk for informasjonssikkerhet, så svarer 37% at de ikke har lest den og 15% at de ikke vet. Det er ønskelig at en større andel ansatte leser politikk for informasjonssikkerhet, fordi den gir oversikt over definisjoner og begreper knyttet til informasjonssikkerhet, lover og regler man må forholde seg til og mål og strategier som NTNU har satt. Videre så kan det synes at ansatte føler de ikke får nok informasjon om sikkerhet. Her er det også muligheter for forbedring, selv om dette spørsmålet ikke tar hensyn til inneværende kunnskap om informasjonssikkerhet.

Det er også noen sterke sider blant kunnskapspåstandene. Nesten alle de ansatte vi har spurt låser for det meste datamaskinen sin når de forlater den. De ansatte er også godt kjent med risikoen ved å åpne e-post med vedlegg fra ukjente avsendere. Det tyder også på at de aller fleste ansatte vet hva informasjonssikkerhet omhandler. Stort sett så tyder det på at de som har lest politikk for informasjonssikkerhet, både vet hvor dokumentet finnes og forstår innholdet. Flesteparten av respondentene vet også hvilke ansvar de har angående informasjonssikkerhet.

Det virker som om flesteparten av de deltakerne i undersøkelsen vår ønsker å motta meldinger om informasjonssikkerhet via digitale virkemidler slik som E-post, presentasjoner og web-basert opplæring. Dette er et viktig hjelpemiddel i vår prosess med å velge ut riktig virkemiddel for formidling av tiltak. Alt i alt så tyder det på at de ansatte ved IT-avdelingen sitter inne med et godt kunnskapsnivå om informasjonssikkerhet, ut ifra påstandene vi har i denne undersøkelsen.

11.8.2 Komponenter

Videre følger en gjennomgang av hver komponent brukt i spørreundersøkelsen.

Opplæring og kurs/trening

Komponenten “opplæring og kurs/trening” avdekket at det kan synes som om enkelte ansatte ikke får den opplæringen på programmer eller verktøy de mener er tilstrekkelig. Rammeverket sier at opplæring og kurs brukes som virkemiddel for å styrke gruppens bevisstgjøring og at det skal gjennomføres periodevise relevante kurs. Denne komponenten inneholdt én påstand. Basert på resultatet fra denne påstanden er det rom for forbedring på komponenten opplæring og kurs/trening.

Bevisstgjøring

I rammeverket beskrives bevisstgjøring som “de ansattes egenskaper som effektivt kan forbedre organisasjonen med tanke på informasjonssikkerhet”. Denne komponenten gikk i undersøkelsen ut på beskyttelse av informasjonsverdier og kan synes å være tilstrekkelig. Individuelle ansatte, ansatte som en gruppe og avdelingen kan synes å ha veldig lik adferd, noe som ligger i grunn for å kunne si at “bevissthet” som en komponent i informasjonssikkerhetskultur er sterk.

Etisk adferd

I undersøkelsen ble denne komponenten målt med ett spørsmål som handlet om hva den individuelle mener om sine egne handlinger i forbindelse med informasjonsverdier

NTNU besitter. Ut ifra hva som kunne avdekkes i komponenten "etisk atferd" kunne det synes som om de ansatte har gode verdier og ønsker å bidra positivt til beskyttelse av informasjonsverdier.

Personvern

På denne komponenten kan det virke som om de ansatte er noe usikre når det gjelder retningslinjer for å beskytte brukere sin fortrolige informasjon. Rammeverket sier at personvern kan diskuteres som en faktor av tillit: Uten personvern eksisterer ikke tillit. Det kan være noe urovekkende at det er såpass stor spredning i svaret, men det kan tolkes som at ikke alle ansatte behandler sensitive personopplysninger.

Endringsledelse

Denne komponenten måler hvordan de ansatte opplever endringer i avdelingen. Denne komponenten omhandler hva de ansatte tenker om avdelingen som en helhet og ikke nødvendigvis bare hva de mener om seg selv. Resultatet kan tyde på at avdelingen har en positiv holdning til endringer.

Ledelsesforankring

Denne komponenten måler om det er støtte i ledelsen for arbeid med informasjonssikkerhet. Denne komponenten ble målt med to spørsmål som omhandler hva hver enkelt respondent mener om ledelsen sin oppfatning rundt viktigheten av informasjonssikkerhet. Resultatet kan tyde på at det er forbedringspotensiale når det gjelder formidling av informasjonssikkerhet fra ledelsen til de ansatte. Spesielt interessant er det å se at der er stor spredning i svarene internt i flere sekjsoner. Her kan det virke som om seksjon for IT-brukerstøtte, IT-drift, IT-strategi og -styring og IT-utvikling har potensiale for å kunne kommunisere informasjonsikkerhet tydeligere til alle de ansatte i seksjonene. På en annen side så er det en styrke at de ansatte oppfatter at ledelsen ser på informasjonssikkerhet som viktig. Ett viktig prinsipp kan hentes ut i fra Organisasjonskultur - for ledere (NTNU)[7]

> "Vær en rollemodell. Ønsket kultur er mer oppnåelig gjennom å vise ønsket atferd og verdier enn å kommunisere de ut i organisasjonen."

Ved å vise ønsket atferd, kan man motivere andre til å gjøre det samme. Det er altså viktig for ledere å vite hvordan man kan påvirke kultur, da man som leder har stor innflytelsesverdi ovenfor ansatte.

Strategi

Denne komponenten måler om NTNU som organisasjon gir oppmerksomhet til informasjonssikkerhet og om de ansatte vet om at det finnes en strategi for informasjonssikkerhet. Her er det en stor styrke at flesteparten av de ansatte er klar over at det er viktig med informasjonssikkerhet for måloppnåelsen til NTNU. Da er det rimelig å anta at de ansatte også er klar over hva måloppnåelsen til NTNU omhandler. Det er noe større uenighet om hvorvidt NTNU gir tilstrekkelig oppmerksomhet til informasjonssikkerhet, men alt i alt så ligger det på et akseptabelt nivå.

Styring

Denne komponenten måler hva de ansatte synes om NTNUs avgjørelser i forbindelse med informasjonssikkerhet. Ut i fra svarene på spørsmålene i denne komponenten kan

[7] https://innsida.ntnu.no/wiki/-/wiki/Norsk/Organisasjonskultur+-+for+ledere - (19.05.2019)

det virke som at de ansatte har kunnskaper om avgjørelser NTNU gjør knyttet til informasjonssikerhet. Det er en styrke at de ansatte har kunnskap om organiasjonen som helhet, spesielt når det gjelder ansatte i IT-avdelingen.

Risikostyring

Denne komponenten måler kunnskapen til de ansatte rundt viktigheten av risikoanalyser og implementasjon av risikoreduserende tiltak. Her er det stor enighet i at dette er viktig. Det er på den annen side større uenighet når det kommer til om seksjonen implementerer riskoreduserende tiltak, men utfallet er i all hovedsak positivt her også.

Avdelingstruktur

Denne komponenten måler om avdelingen har kjennskap til andre fakulteters struktur og sammensetning. Det kan argumenteres for at det er viktig for IT-avdelingen spesielt, å vite litt om arbeidsprosessene til andre avdelinger i NTNU. Resultatet fra denne komponenten viser at det kan tyde på at det er liten kjennskap til arbeidsprosessene i andre fakulteter blant de ansatte i IT-avdelingen generelt. Her er det stort forbedringspotensiale.

Compliance

Denne komponenten handler om å holde avdelingen oppdatert på lovgiving og regulativer for å beskytte informasjonsverdier. I denne sammenhengen gjelder det spesifikt IKT-reglementet. Resultatene tyder på at de ansatte mener at avdelingen forholder seg til IKT-reglementet og at de er klar over ansvaret sitt dersom reglementet ikke overholdes. Det kan tyde på noe større uenighet rundt hvorvidt ledelsen sørger for at den ansatte etterlever IKT-reglementet. Med etterlevelse menes det om ledelsen sørger for å følge opp de ansatte i etterkant av signert dokument. Her kan det virke om at det noe uenighet blant de ansatte på IT-avdelingen og mulig forbedringspotensiale. Alt i alt er det vurdert til å være på et akseptabelt nivå.

Politikk

Denne komponenten ser på om det foreligger relevante retninglinjer for den enkelte ansattes daglige arbeid, i tillegg til forståelsen og aktualiteten til disse. Vi fikk noen tilbakemeldinger på uklarhet i påstanden som innegår i denne komponenten. Det er naturlig å tro at de som ikke forstår spørsmålet svarer “noe uenig” eller “noe enig”. Fjerner vi disse to alternativene fra spørsmålet tyder det på en generell enighet om at det finnes tilstrekkelig med retningslinjer for det daglige arbeidet.

Systemutvikling

I denne komponenten addresseres ikke bare sikkerhet i utviklingen av applikajsoner, men også en forsikring om at sikkerhet prioriteres ved endringer. Denne komponenten måles med ett spørsmål som omhandler bruk av retningslinjer for sikker utvikling. Dette spørsmålet er litt mer aktuelt for enkelte seksjoner enn andre, slik som for eksempel seksjon for IT-utvikling. Resultatet fra dette spørsmålet kan tyde på de ansatte enten ikke synes spørsmålet er relevant eller at de er enige i påstanden.

Hendelseshåndtering

Denne komponenten omhandler prosessen for å identifisere, respondere og overvåke sikkerhetshendelser. Spørsmålet som måler denne komponenten går spesifikt på identi-

fisering av sikkerhetshendelser ved å spørre om de ansatte opplever aksept for å melde avvik innad i seksjonen. Dette spørsmålet er tenkt å se på de ansattes oppfattning av seksjonen som en helhet, men kan fort bli oppfattet til å bare gjelde en selv. Alt i alt er det meget positivt at det virker som om at det er aksept for å melde inn avvik.

Styring av informasjonsverdier

Denne komponenten relateres til beskyttelse av avdelingens verdier, spesielt når det kommer til oversikt og identifisering av verdier. Resultatet fra denne komponenten tyder på at det er forbedringspotensiale når det kommer til om hver enkelt ansatt klassifiserer verdiene de jobber med. Dette er knyttet til om de ansatte i seksjonen har oversikt over hvilke informasjonsverdier de behandler. Her tyder det på at det er en generell enighet i at de ansatte har oversikt over verdiene sine, men det er rom for forbedring på dette punktet.

11.8.3 Oppsummering

Ut ifra gjennomgangen av komponentene ovenfor har vi kommet frem til sterke og svake sider ved sikkerhetskulturen på IT-avdelingen ved NTNU. Nedenfor presenteres de fire områdene som har forbedringspotensiale og de fire sterkeste sidene ved listen nedenfor og visuelt i figur 56. De resterende komponentene som ikke blir nevnt i listene nedenfor har vi vurdert til å være tilfredsstillende.

Forbedringspotensiale

Listen nedenfor presenterer komponenter, som vi mener har forbedringspotensiale

- Opplæring og kurs/trening
- Ledelsesforanking
- Avdelingsstruktur
- Styring av informasjonssverdier

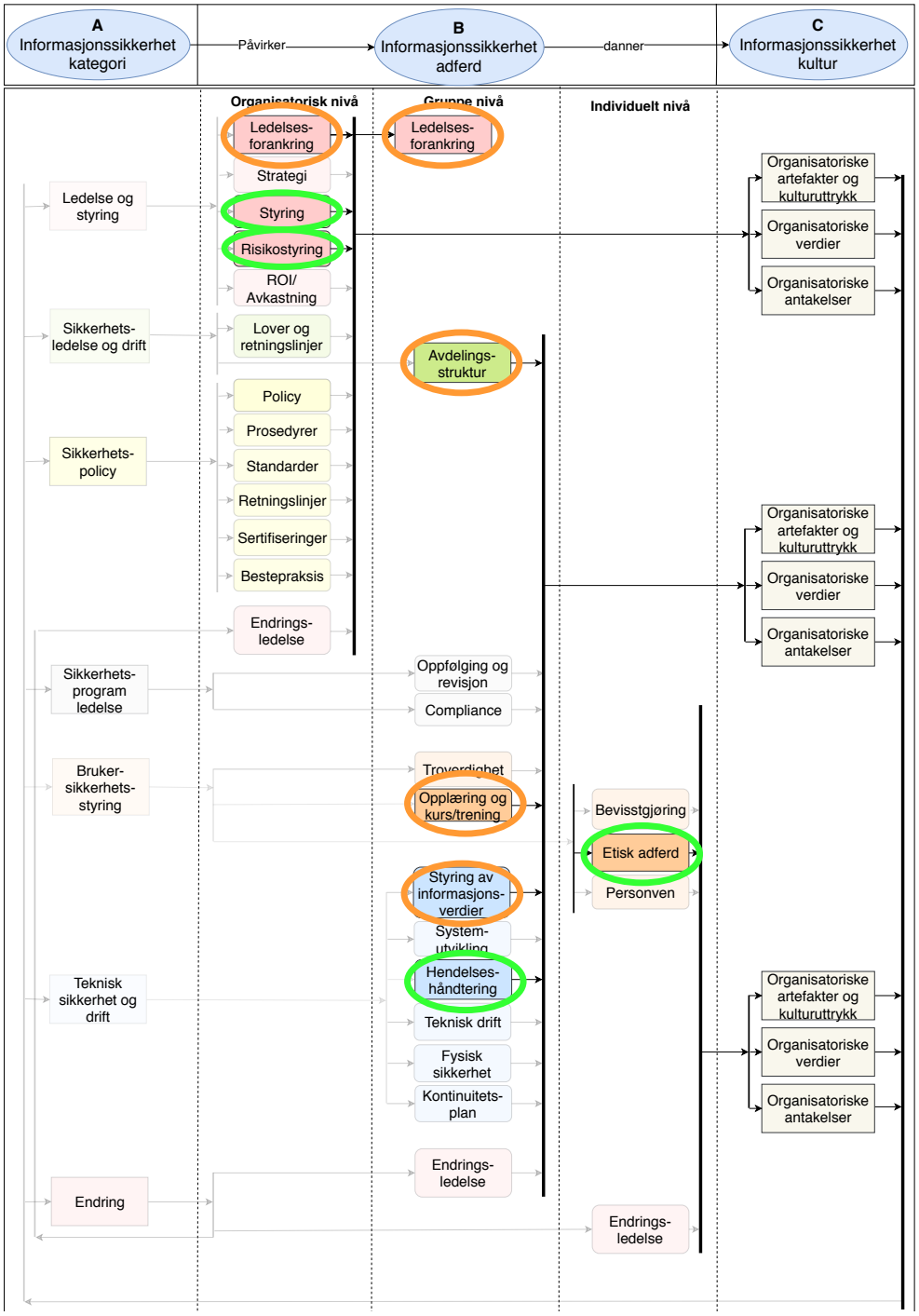
Disse komponentene vil få laget tilpassede tiltak i kapittel 12, "*handlingsplan*". Med andre ord kan vi si at det er forbedringspotensiale når det kommer til formidling av informasjonssikkerhet fra ledelsen til de ansatte, kunnskap om andre fakulteter i NTNU og oversikt over informasjonsverdier.

Sterke sider

Listen nedenfor presenterer komponenter, som vi mener utgjør de sterkeste sidene ved sikkerhetskulturen på IT-avdelingen.

- Styring
- Risikostyring
- Hendelseshåndtering
- Etisk atferd

Det er viktig å trekke frem de sterkeste sidene ved sikkerhetskulturen og ikke bare de svake. Dette er for å motivere og skryte av de ansatte, som også kan være med på å vise de at de faktisk har en betydning for å styrke informasjonssikkerheten i avdelingen. I figur 56 nedenfor er de sterke sidene uthevet ved grønn sirkel, og de komponentene som anses som de svakeste sirklet oransje.



Figur 56: Komponentene ved fokus; forbedringspotensiale med oransje sirkel, sterke sider med grønn sirkel.

12 Steg 5 - Handlingsplan

I dette kapittelet bygger vi videre på de identifiserte svake sidene ved IT-Avdelingen når det gjelder sikkerhetskultur, og presenterer en handlingsplan som adresserer disse. Målet av handlingsplanen er å redusere de svake sidene som igjen reduserer sannsynlighet for sikkerhethendelser. Det er også viktig å huske på at selve spørreundersøkelsen er et tiltak i seg selv for å øke bevisstheten til informasjonssikkerhet for de ansatte.

12.1 Steg 5.1 - Tiltaksprogram

Tiltaksprogrammet tar utgangspunkt i funnene gjort i kapittel 11.7. Videre er tiltak delt opp i kategori og eventuelt komponent. Der det er hensiktsmessig har flere kategorier, komponenter eller påstander dannet et tiltak som kan brukes på de alle.

Det grunnleggende målet med tiltaksprogrammet er å forbedre eller øke bevisstheten til de grunnleggende verdiene som ligger til grunn i komponenten. Som skrevet tidligere i teorikapittelet er kultur akseptabel adferd og oppfatninger av ansatte og organisasjonen i sin helhet i forbindelse med informasjonssikkerhet.

1. Opplæring av ansatte i verktøy og programmer de bruker til daglig

Basert på påstand nummer 11 i undersøkelsen kan det virke som om enkelte ansatte ikke har fått den opplæringen de anser som tilstrekkelig i verktøy og programmer de bruker daglig. Da undersøkelsen ikke gikk videre inn på hvilke programmer dette gjaldt er det vanskelig å avgjøre hvordan dette kan forbedres.

En mulighet kan være at ledelsen kartlegger hvilke verktøy og programmer dette gjelder. Det kan vurderes å utføre kartleggingen anonymt da det er mulig at bakgrunnen for at enkelte ikke har mottatt den opplæringen er fordi de ikke ønsker å være en "byrde". Et annet perspektiv er jo at dette gjelder økonomiske eller tidsmessige årsaker. Etter verktøy og programmer er kartlagt kan et påmeldingsskjema opprettes og ansatte kan melde seg på.

Det er svært vanskelig å avgjøre kostnaden for dette. Det kommer helt an på om opplæringen kan skje internt kontra eksternt og om hvor omfattende opplæringen er, samt antall deltagere.

Om undersøkelsen gjennomføres på nytt er det ønskelig å se en reduksjon på antallet som sier de ikke mottar tilstrekkelig opplæring. Man må også ved senere undersøkelser tenke på nyansettelser og ansatte som ikke arbeider der lenger som kan endre forventet resultat ved ny undersøkelse. Ved senere undersøkelser kan det være interessant å ha demografiske data med nyansettelser innen for eksempel ett år og se hvordan resultatet blir. Da kan man kanskje avdekke manglende opplæring av nyansatte.

En opplæring som dette anses som rimelig å gjennomføre på seksjons eller avdelingsnivå. Avhengig av kartleggingen av hvilke programmer dette gjelder kan det være hensiktsmessig at dette gjennomføres på avdeling eller internt på seksjon. Enkelte programmer er kanskje ikke relevant for alle på avdelingen.

Det anbefales å gjennomføre den nevnte kartleggingen snarest mulig for å få en over-

sikt over omfanget. Det vil være rimelig at ansatte snarest får den opplæringen de trenger, men det vil være lite hensiktsmessig å sette en tidsfrist før overnevnte kartlegging er på plass.

2. Forbedre ledelsens kommunikasjon av informasjonssikkerhet

Komponenten "ledelsesforankring" avdekket at ledelsen kan forbedre sin formidling rundt informasjonssikkerhet. Det er vanskelig å avgjøre hvorvidt det er relevant for en leder å formidle informasjonssikkerhet, så dette tiltaket gir et grunnlag som kan benyttes for generel forbedring. Fra kunnskapspåstand nummer ni kom det fram at ansatte generelt ønsker å vite mer om informasjonssikkerhet og antageligvis hvordan informasjonssikkerhet påvirker ansatte sitt daglige arbeid.

Eksempelvis kan ledere møtes, diskutere hvordan de formidler informasjonssikkerher og prøve å komme fram til metoder som fungerer og hva som ikke fungerer. Målet med diskusjonen vil være å drøfte egne erfaringer, ved hvordan de kan formidle informasjonssikkerhet inn den daglige driften som en integrert del og ikke som en separert del. Her er det også et poeng at seksjoner som gjør det godt på denne målingen kan formidle til de andre seksjonene hva de gjør slik at man kan lære av hverandre.

Om man går ut ifra et møte mellom seksjonslederne og it-sjefen, med en varighet på én til to timer kan dette ha en kostnad på mellom 8000 og 10 000kr om dette fører til ekstra arbeid. (Det kan også tenkes at dette kan gjennomføres i arbeidstiden, som en del av arbeidsoppgavene og derav ingen ekstra kostnader). Det kan virke som dette er dyrt, men det kan ha betydelig påvirkning på ansatte og hvordan fremtidige avvik eller hendelser blir håndtert, noe som kan bli svært dyrt. For eksempel kan eksempelet om Hydro som nevnt tidligere brukes her også. Sammenlignet med kostnaden for Hydro sin hendelse blir kostnaden for dette tiltaket småpenger.

Siden det var noe spredning på denne målingen, kan det tyde på at enkelte kommuniserer sikkerhet bedre enn andre. I ettertid, ved senere måling, vil det være ønskelig å se en større enighet innad i seksjonene.

Tiltaket vil være for ledelsen i seksjonene og IT-sjefen, men resultatet fra tiltaket vil påvirke kunnskapen og adferden til de ansatte.

Det er ikke viktig at dette tiltaket gjennomføres omgående, da målingen ikke ga indikasjon på at dette er kritisk. Det er ønskelig at tiltaket gjennomføres innen seks måneder. Seksjonene er lokalisert på ulike geografiske lokasjoner, og det vil være hensiktsmessig å gjennomføre dette møtet ved bruk at digitale hjelpemidler.

3. Øke kjennskap til arbeidsprosesser ved andre fakultet ved NTNU

Fra påstand nummer 32 ble det tydelig at ansatte har lite kjennskap til andre arbeidsprosesser ved NTNU, spesielt gjelder dette for ansatte i IT-utvikling. Tiltaket går ut på å få kjennskap til arbeidsprosesser som en naturlig del i arbeidet med å levere tjenester til andre ansatte i NTNU. Ved å øke samarbeidet mellom de som leverer tjenester og sluttbrukerne, vil brukere som benytter disse tjenestene få større verdiøkning av utbedrede tjenester. Hvordan dette kan gjøres vil være en utfordring, men det handler om å være bevisste på det ved innføring av IT-tjenester.

Hvis det er ønskelig å øke den generelle kunnskapen hos alle i IT-avdelingen om andre fakultet burde dette komme tidlig i en ansettelsefase. Det vil antageligvis være

for omfattende og lite relevant å utføre en opplæring på arbeidsprosesser hos andre i NTNU når det ikke er sikkert man får bruk for det. Men det vil være viktig å tenke på sluttbrukeren ved innføring av IT-tjenester og sørge for at dette vil fungere godt i sluttbrukeren sin arbeidsprosess.

Ved en senere måling vil det være ønskelig å se en større kunnskap om andre fakulteter i NTNU, og at hypotesen om forbedringspotensial knyttet til påstand 43 av Utstrand blir svekket. Det hadde også vært interessant å sett på hva andre avdelinger i NTNU mener om verktøyene IT-avdelingen tilbyr passer behovet.

Tiltaket vil nok påvirke arbeidstiden det tar å innføre og utvikle it-tjenester. Det er vanskelig å si noe om hvor mye tid dette tar og vi kan derfor ikke komme med en estimering av kostnad.

For ansatte som påvirker arbeidsprosessene til andre ved NTNU vil det være spesielt viktig for de å gjennomføre dette tiltaket, dvs. benytte seg av innføring av ny retningslinje.

Tiltaket kan enkelt beskrives som en retningslinje ved innføring av IT-tjenester og kan innføres omgående.

4. Kunnskap om informasjonsverdier

Ut ifra komponenten "styring av informasjonsverdier" kan det tyde på at påstandene om de ansatte har oversikt over informasjonsverdiene de jobber med og om de klassifiserer informasjonen de jobber, med henger sammen. Ved at de ansatte får bedre oversikt over informasjonsverdiene de jobber med kan det føre til at de også klassifiserer informasjonen og motsatt.

Derfor anser vi det som viktig at seksjonen først får oversikt over sine informasjonsverdier før de arbeider med klassifiseringen. Man må rett og slett lage en prosess der man får oversikt over eksisterende informasjonsverdier. Man må også bygge inn klassifiseringen inn den i daglige driften og opplære ansatte på hva som inngår i hvilken klassifisering(åpen, internt, fortrolig, strengt fortrolig) og hvordan klassifiseringen kan utføres. Dette budksapet kan formidles ved bruk av ulike virkemidler. Et eksempel er bruk av *dilemmatrening* [1] fra direktoratet for forvalting og IT (DIFI), et opplæringsverktøy som adresserer krav til informasjonssikkerhet og hvorfor dette gjelder dem (ansatte). Håkon Styri i DIFI, forteller om positive tilbakemeldinger fra virksomhetene som fikk brettspillet (dilemmatrening). Videre sier Styri også at dilemmaene har en egenverdi ved at de bidrar til diskusjon, refleksjon, innsikt og bedre forståelse for problemstillinger knyttet til dilemmaet.

Klassifisering bør være en integrert del av arbeidet, slik som politikken tilsier [8]. Her kan det foreligge kostnad knyttet til utvikling eller forbedring av retningslinjer for klassifisering. Ved bevisstgjøring av ansatte ved bruk av dilemmatrening, blir kostnaden noe høyere. Dilemmatrening er en gratis ressurs, men det vil gå med en del tid til gjennomføring. Dersom halvparten av de ansatte i IT-avdelingen bruker én time på å gjennomføre brettspillet vil dette bli estimert til å koste mellom 30 000 og 35 000kr.

Ved senere måling er det ønskelig at flere ansatte får kunnskap om informasjonsverdier og på bakgrunn av dette klassifiserer informasjonsverdiene de jobber med. I intervjuet med Roar Thon sier han at i akademia så er forståelsen av deling en utfordring. Man må

[1] https://www.difi.no/node/2341/dilemmatrening-informasjonssikkerhet

prøve å identifisere hva som er sikre områder og hva man kan dele. Ved å klassifisere informasjonsverdiene de ansatte jobber med kan det føre til bedre tilgangskontroll og etterlevelse av relevant lovgiving og regelverk, samt en økt forståelse for hvilke data som er greit å dele.

En opplæring som dette gjelder alle de ansatte på hele IT-avdelingen. Det var ingen seksjoner i målingen som skilte seg merkverdig ut, men tiltaket er hensiktsmessig å gjennomføre av hver seksjonsleder innad i sin respektive seksjon.

Tiltaket burde utføres omgående da fordelene med det er store og det kan straffe seg dyrt å ikke ha denne delen på stell. Informasjonsverdier på avveie kan koste NTNU dyrt med tanke på for eksempel GDPR[2]. Dette skal da være en integrert del av arbeidet. Hva dette vil koste for NTNU er vanskelig og si.

[2] https://www.dn.no/teknologi/personvern/gdpr/bergen-kommune/datatilsynet-varsler-millionbot-til-bergen-kommune/2-1-503797 - (08.05.2019)

13 Refleksjon

Hensikten med dette kapittel er å legge fram erfaringene oppbygget underveis i prosjektet. Dette kan benyttes i ettertid ved liknende arbeid for å unngå de samme fallgruvene.

13.1 Erfaringer med SelectSurvey

Spørsmålsbasen ble utarbeidet i et Excel dokument for lett å kunne håndtere utvikling av spørsmålene. Vi gjorde dette i god tro om at importfunksjonen til SelectSurvey med CSV filer skulle fungere, noe det viste seg å ikke gjøre. Driftsansvarlig ble varslet, men har ikke fulgt oss opp på dette (per 18.05.19). Derfor ble prosessen med å overføre spørsmålene til SelectSurvey et veldig manuelt arbeid som var tidkrevende. Spørsmålene ble laget i tre forskjellige biblioteker i SelectSurvey: kultur, hypoteser og kunnskapspørsmål.

Bibliotekene i SelectSurvey har mulighet for å legge til eiere og gruppens medlemmer ble eier av bibliotekene. Men når undersøkelsen skulle lages var det kun kontoen som hadde opprettet biblioteket som kunne bruke biblioteket til å hente spørsmål til undersøkelsen. I tillegg var det bare mulig å importere ett og ett spørsmål fra biblioteket og med nesten 40 spørsmål ble dette igjen veldig tidkrevende.

Vi skulle helst ønsket oss et verktøy som i større grad tillot samarbeid på tvers av brukerkontoer og mer smidigere i utvikling av undersøkelsen.

13.2 Valg av verktøy til spørreundersøkelse

Det ble ikke sett på hvilke muligheter som fantes rundt valg av verktøy for lansering av spørreundersøkelser på NTNU. Det ble nevnt tidlig av oppdragsgiver at SelectSurvey var en mulighet. Etter dette ble SelectSurvey regnet som eneste mulighet uten at vi hadde gjort videre undersøkelser rundt hvilke alternativer som finnes. Ved et søk på innsida ble vi klar over at det finnes pimært to vertøy for spørreundersøkelser på NTNU[1]: Questback og SelectSurvey. Førsteinntrykket av Questback er at det kan løse mange av utfordringene vi har med SelectSurvey når det gjelder import av spørsmål, manuelt arbeid og samarbeid på tvers av brukerkontoer. Mye av dette kommer av at Questback har et mye mer brukervennlig grensesnitt og som følge av en større kundegruppe også flere funksjoner og muligheter enn SelectSurvey. Nå har vi imidlertid ikke satt oss nok inn i Questback til å ha et sammenlikningsgrunnlag, men i retrospekt så kunne vi med fordel ha vurdert hvilke muligheter som fantes før vi bestemte oss for en løsning.

13.3 Finne styrker og svakheter ved sikkerhetskulturen på IT-avdelingen

Da vi ikke fikk mulighet til å diskutere funnene med relevante personer i IT-avdelingen, blir vår mening om hva som er god sikkerhetskultur kombinert med vår oppfattning av IT-avdelingen med på å avgjøre sterke sider og mulige forbedringsområder ved sikkerhetskulturen. Det vil bli opp til oppdragsgiver og ledelse i avdelingen å ta en avgjørelse på hva som er akseptabelt i avdelingen. Det hadde vært svært interessant å tatt denne avgjørelsen sammen med ledelsen, men på grunn av begrenset med tid fra ledelsen sin

[1] https://innsida.ntnu.no/wiki/-/wiki/Norsk/Sp%C3%B8rreunders%C3%B8kelser - (23.04.2019)

side og tidsbegrensingen på bacheloroppgaven ser vi det som hensiktsmessig å la vurderingsformen blir vår subjektive oppfatning av akseptabel adferd.

13.3.1 Utvidet pilotundersøkelse

Vår pilottest av spørreundersøkelsen begrenset seg til noen få personer. Ved en gjentakelse av en spørreundersøkelse kan det med fordel brukes lengre tid på "syretesting" av spørsmålene, slik at de er enkle å forstå og samtidig har ønsket resultat. Vi foretok bare en kvalitetstest av de spørsmålene vi brukte i undersøkelsene.

14 Avslutning

14.1 Videre arbeid

14.1.1 Oversatt spørreundersøkelse

Hvis spørreundersøkelsen ønskes utstedt på en målgruppe som er flerspråklig, kan det være nødvendig å utstede spørreundersøkelsen på de nødvendige språkene. I mange tilfeller vil det holde med en norsk- og en engelskspråklig variant. Det er da svært viktig at man sørger for at spørsmål eller påstand har helt samme betydning på begge språkene. Dersom ikke dette er tilfellet kan man risikere at man får dårlig validitet på dataen. I verste fall kan ikke resultatet fra den norsk- og den engelskspråklige versjonen sammenslåes.

14.1.2 Flere målinger

Det hadde vært interessant å gjennomført en ny måling av sikkerhetskulturen på IT-avdelingen om ett år. Da kan man kartlegge nye områder av sikkerhetskulturen eller se endringer i sikkerhetskulturen ved å benytte samme spørreundersøkelse. Et annet interessant område hadde vært å sett på sikkeretskulturen i andre avdelinger. Dette vil kunne skape et bedre helhetlig bilde av hva sikkerhetskulturen er på NTNU som organisasjon og ikke bare i én avdeling.

14.1.3 Implementasjon av tiltak

Denne bacheloroppgaven gikk ut på å foreslå tiltak for å forbedre sikkerhetskulturen på NTNU. Det hadde vært interessant å implementert disse tiltakene i tillegg til å sette målsetninger sammen med ledelsen i IT-avdelingen for å se om sikkerhetskulturen forbedres over tid. Et annet interessant poeng hadde vært å se om tiltakene er verdt kostnaden ved å kjøre en kost-nytte analyse.

14.2 Konklusjon

I denne bacheloroppgaven skulle vi gjennom en analyse av bestepraksis innenfor sikkerhetskultur, velge et rammeverk for måling av sikkerhetskultur på NTNU. Deretter skulle vi utføre en måling basert på rammeverket, og fra resultatet av målingen foreslå tiltak for å forbedre sikkerhetskulturen.

Gjennom hele arbeidsprosessen våres har vi hatt fokus på å finne en prosess for måling av sikkerhetskultur som skal være lett anvendelig for NTNU, og gjenbrukbar for å kunne utføre senere målinger. Dette ledet fram til rammeverket ISCF. ISCULA-prosessen og tilhørende spørsmål ble oversatt til norsk for å gjøre det enklere å forstå fremgangsmåten for å måle sikkerhetskultur. Det ble laget en arbeidsbok i Excel for å forenkle arbeidet med å importere spørsmål til spørreundersøkelsen inn i SelectSurvey.

Vi kom frem til at riktig valg av indikatorer danner grunnlaget for måling av sikkerhetskultur. En analyse av bestepraksis på dette området kom frem til at det ikke finnes noen fasit på hvilke indikatorer som er riktig å bruke, men en felles enighet om at Robbins og Scheins modell var sentrale på dette området. Rammeverket vi endte opp med å bruke benytter både Robbins og Scheins modell for klassisfisering av indikatorer. Oppdragsgiver ønsket en kvalitativ tilnærming til måling, men etter en analyse av bestepraksis kan det konkluderes med at en kvantitativ måling er mest bruk ved måling av sikkerhetskultur. Etter å ha fulgt fremgangsmåten for måling av sikkerhetskultur som beskrevet i rammeverket (ISCULA), kom vi frem til at sikkerhetskulturen på IT-avdelingen er relativt god. Vi fant allikevel noen forbedringsområder, spesielt når det gjelder informasjonsverdier og ledelsesforanking. På de punktene som ble vurdert som de fire svakeste kom vi med tilpassede tiltak for å forbedre sikkerhetskulturen ytterligere. Tiltakene baserer seg i stor grad på å øke de ansattes kunnskap om informasjonsverdier og programmer som blir brukt daglig. Et annet viktig tiltak er å samordne ledelsens kommunikasjon om sikkerhet til de ansatte i seksjonene.

Alt i alt føler vi at vi har svart på problemforuleringen på en god måte og bidratt positivt med en forenklet metode for å kartlegge sikkerhetskultur, som kan brukes igjen senere for å måle sikkerhetskultur ved NTNU.

Vårt læringsutbytte gjennom hele denne prosessen har vært stort, spesielt når det gjelder vitenskapelig fremgangsmetode og akademisk skriving. Vi har fått et inblikk i prosessen med å skrive en oppgave, argumentasjon og jobbe strukturert sammen i en gruppe. Vi har kommet frem til at sikkerhetskultur er et komplekst emne som det ikke finnes noen konkret fasit på hvordan man skal forbedre og måle. Vi har fått erfaring i forståelse av organisasjoner og hvordan kultur faktisk definerer hvordan de fungerer. I tillegg har vi lært statistisk analyse og bruk av verktøyet SPSS for å distribuere spørreundersøkelser.

Bibliografi

[1] Thomas Schlienger and Stephanie Teufel. Tool supported management of information security culture. In *IFIP International Information Security Conference*, pages 65–77. Springer, 2005.

[2] Yngve Nordby and Christian Waale Hansen. *Informasjonssikkerhet : atferd, holdninger og kultur*, volume 200504 of *ROSS (NTNU) (trykt utg.)*. NTNU, Institutt for produksjons- og kvalitetsteknikk, Trondheim, 2005. ISBN 8277062222.

[3] Adéle Da Veiga. *Cultivating and Assessing Information Security Culture*. Thesis, 2008. URL https://repository.up.ac.za/bitstream/handle/2263/24117/Complete.pdf.

[4] Patrick Hudson. The hearts and minds project. 01 2004. URL https://www.researchgate.net/publication/281236607_The_Hearts_and_Minds_Project.

[5] Hanne Eggen Røislien and Bjarte Malmedal. Nordmenn og digital sikkerhetskultur 2018. page 56, 09 2018. URL https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf.

[6] Even Østby Brodin Christopher Berglind Gaute Wangen, Bent Håkon Skari. Mørketallsundersøkelsen ved ntnu 2018, 2019.

[7] B. Von Solms. Information security -the third wave? *Computers and Security*, 19 (7):615–620, 2000. ISSN 01674048. doi: 10.1016/S0167-4048(00)07021-8.

[8] NTNU. Politikk for informasjonssikkerhet. 2018. URL https://innsida.ntnu.no/wiki/-/wiki/Norsk/Politikk+for+informasjonssikkerhet.

[9] Thomas Schlienger and Stephanie Teufel. Analyzing information security culture: increased trust by an appropriate information security culture. In *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*, pages 405–409. ISBN 1529-4188. doi: 10.1109/DEXA.2003.1232055. URL https://ieeexplore.ieee.org/ielx5/8719/27592/01232055.pdf?tp=&arnumber=1232055&isnumber=27592.

[10] ENISA. *Cyber security culture in organisations*. ENISA, Heraklion, 2017. ISBN 9789292042455. URL http://publications.europa.eu/publication/manifestation_identifier/PUB_TP0617472ENN.

[11] M. Bishop. What is computer security? *Security & Privacy, IEEE*, 99(1):67–69, 2003. ISSN 1540-7993.

[12] Adéle Martins and Jan Elofe. Information security culture. In *Security in the information society*, pages 203–214. Springer, 2002.

[13] Alexandra Bech Gjørv. Rapport fra 22. juli-kommisjonen. 2012. URL https://www.regjeringen.no/no/dokumenter/nou-2012-14/id697260/sec1.

[14] Equinor (Tidl. Statoil). In amenas rapport. URL https://www.equinor.com/content/dam/statoil/documents/In%20Amenas%20report.pdf.

[15] Daniel Schatz, Rabih Bashroush, and Julie Wall. Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*, 2017. ISSN The Journal of Digital Forensics, Security and Law.

[16] Joo S. Lim, Shanton Chang, Sean Maynard, and Atif Ahmad. Exploring the relationship between organizational culture and information security culture, 2009.

[17] Stephanie og Sasaki Ryoichi og Qing Sihan og Okamoto Eiji og Yoshiura Hiroshi Schlienger, Thomas og Teufel. *Tool Supported Management of Information Security Culture*, volume 181 of *IFIP International Federation for Information Processing*. 2005. ISBN 9780387256580,038725658X.

[18] Douglas W Hubbard. *How to measure anything: Finding the value of intangibles in business*. John Wiley & Sons, 2014.

[19] Adéle Da Veiga and Jan H.P. Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, 2010. URL https://www.sciencedirect.com/science/article/pii/S0167404809000923.

[20] Adele da Veiga and Jan H.P. Elof. Information security culture, part five: Social and ethical aspects of information security. 2006. URL https://link.springer.com/content/pdf/10.1007%2F978-0-387-35586-3_16.pdf.

[21] Andrej Volchkov. How to measure security from a governance perspective. *ISACA Journal*, 5, 2013.

[22] ENISA. The new users' guide: How to raise information security awareness. 2010. URL https://www.enisa.europa.eu.

[23] Shirley C Payne. A guide to security metrics. *SANS Security Essentials GSEC Practical Assignment Version*, 1, 2001.

[24] Edgar H. Schein. Organizational culture and leadership, 2017. URL https://books.google.no/books?hl=en&lr=&id=DlGhlT34jCUC&oi=fnd&pg=PR9&dq=Organizational+culture+and+leadership,&ots=-dr36o_eEP&sig=njJxcaxP7uelmCxCf2Nyk4tcOE8&redir_esc=y#v=onepage&q=Organizational%20culture%20and%20leadership%2C&f=false.

[25] Stephen P. Robbins. *Organizational Behavior*. Prentice Hall, 2001. ISBN 9780130184191. URL https://books.google.no/books?id=fEPUIjNddhUC.

[26] Gaute Wangen. Statistisk analyse av spørreundersøkelsen. 04 2019.

[27] AH Pripp. Pearsons eller spearmans korrelasjonskoeffisienter. *Tidsskrift for den Norske laegeforening: tidsskrift for praktisk medicin, ny raekke*, 138(8), 2018.

[28] Haldun Akoglu. User's guide to correlation coefficients. *Turkish journal of emergency medicine*, 2018.

[29] Dahlum. Sirianne. Indikator, 2014. URL https://snl.no/indikator. Accessed 17.02.2019.

[30] Hanne Eggen Røislien Bjarte Malmedal. The norwegian cyber security culture. 2016. URL https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf.

[31] Kai Roer and Dr. Gregor Petrič. To measure security culture: A scientific approach. Report, 2018.

[32] Magnus Alsaker. Indikatorer for informasjonssikkerhet. 2004. URL https://sh.ehelse.no/hkode/arkiv/Delte%20dokumenter/KITH/upload/1177/R08-04IndikatorerInformasjonssikkerhet.pdf.

[33] Ivar Kufås and Roy Are Mølmann. Informasjonssikkerhet og innsideproblematikk, 2003.

[34] *Nuclear Security Culture*. Number 7 in Implementing Guides. INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, 2008. ISBN 978-92-0-107808-7. URL https://www.iaea.org/publications/7977/nuclear-security-culture.

[35] *ISO 17799: A Standard for Information Security Management*. ITRG, 2003. URL https://books.google.no/books?id=VPySnQAACAAJ.

[36] Leanne Ngo, Wanlei Zhou, and Matthew Warren. Understanding transition towards information security culture change. In *AISM*, pages 67–73, 2005.

[37] Gary C Moore and Izak Benbasat. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information systems research*, 2(3):192–222, 1991.

[38] Ingvild Sagberg. Edgar schein. URL https://snl.no/Edgar_Schein.

[39] *ISO 27001: Information technology – Security techniques – Information security management systems – Requirements*. International Organization for Standardization, 2013. URL https://www.iso.org/standard/54534.html.

[40] Jan Killmeyer Tudor. *Information Security Architecture: An Integrated Approach to Security in the Organization*. CRC Press, Inc., Boca Raton, FL, USA, 2000. ISBN 0849399882.

[41] *The 2011 Standard of Good Practicefor Information Security*. Information Security Forum Limited, 2011. URL https://www.uninett.no/sites/default/files/webfm/ISF%20Standard%20of%20Good%20Practice%20for%20Information%20Security%202011.pdf.

[42] 5 point- vs 6 point likert scale. URL http://www.infosurv.com/wp-content/uploads/5-point-vs-6-point-Likert-Scales.pdf.

[43] Gaute Wangen. Statistikk over hendelser ved ntnu 2016 til 2018, 2019.

A Oppg. 38. Sikkerhetskultur ved NTNU

Oppdragsgiver

Oppdragsgiver: IIK, Seksjon for Digital Sikkerhet, NTNU
Kontaktperson: Gaute Wangen
Adresse: NTNU i Gjøvik, Kontor A128
Telefon: 9070883
Epost: gaute.wangen@ntnu.no

Sikkerhetskultur ved NTNU

NTNU Seksjon for Digital Sikkerhet arbeider kontinuerlig med innføring av styringssystem for informasjonssikkerhet. En sentral del av dette er arbeid med sikkerhetskultur. Som en offentlig og akademisk institusjon er balansen mellom tilstrekkelig frihet og åpenhet versus krav til sikkerhet i cyber et utfordrende mål. En gjennomgang av informasjonssikkerhetskulturen dreier seg i hovedsak om å kartlegge hvilke svakheter og styrker som finnes internt. En konsekvens av dårlig sikkerhetskultur kan gå utover bedriften i forskjellige former, blant annet økonomiske tap og dårlig omdømme. Dette kan igjen være med på å utsette de eventuelle konkurransefortrinn bedriften har i forhold til markedet.

Oppgaven

Formålet med denne oppgaven er å gjøre en måling av sikkerhetskultur på NTNU. Oppgaven går ut på å gjøre en litteraturanalyse av eksisterende metoder for å måle sikkerhetskultur og dernest velge en av disse for gjennomføring på NTNU. Gruppen blir delaktige i å sette omfang på oppgaven og skal selv styre gjennomføringen av målingen. Gruppen skal analysere resultatene og basert på disse, foreslå tiltak for å øke informasjonssikkerhetskulturen.

Denne oppgaven har derfor 3 hovedområder:

1. Gjennomgang og analyse av beste praksis innenfor Sikkerhetskultur.
2. Velge rammeverk og gjennomføre en måling på NTNU.
3. Foreslå tiltak til å bedre sikkerhetskulturen på NTNU.

Egnede metoder for å gjennomføre oppgaven er litteraturanalyse i forarbeidet og case studie hvor oppdragsgiver bistår med å sette scope. Gruppen gjennomfører case studien i henhold til beste praksis, gjerne ved hjelp av kvalitative verktøy, slik som intervjuer, spørreundersøkelser og analyse.

Studentgruppen vil gjennom prosjektet få erfaring på:

- Kvalitative undersøkelser og innsamling av data.
- Økt forståelse for metodikk og gjennomføring innenfor informasjonssikkerhetskultur
- Økt forståelse for risikovurderinger.
- Økt forståelse for sikkerhetsarbeid og dynamikk i store organisasjoner.
- Dataanalyse.
- Innsikt i sikkerhetsutfordringer.

Oppgaven passer bra for en gruppe på 2-3 personer med faglig vekt på informasjonssikkerhetsstyring. Forståelse for statistikk (analyse av intervju og spørreundersøkelser) er en fordel og interesse for organisatoriske utfordringer i sikkerhetsarbeid er nødvendig.

B Skript for å hente epost adresser for IT-avdelingen fra NTNU nettside

```
#!/usr/bin/env python
# coding=utf-8
# requirements
from selenium import webdriver
from selenium.webdriver.firefox.options import Options
from selenium.webdriver.common.keys import Keys
from bs4 import BeautifulSoup
import re
import os
import argparse

"""
Funtions
"""
#write to file if the email is unique
def wtf(adr):
    with open(outfile, "r+") as file:
        for line in file:
            if adr in line:
               break
        else: # not found, we are at the eof
            file.write(adr) # append missing data
            file.write("\n")

# get all the emails from the section
def parseSection(url):
    driver.get(url)
    sectionhtml = BeautifulSoup(driver.page_source, 'lxml')
    #get all the email addresses from the page
    for i in sectionhtml.find_all("span", {"class":"email"}):
        wtf(str(i.get_text()).strip())

"""
MAIN
"""
# parse arguments from user
parser = argparse.ArgumentParser(description='Hent epost for alle som jobber i en avdeling')
parser.add_argument('-u','--url', type=str, help='url til avdelingen"', required=True)
parser.add_argument('-o','--outFile', type=str, help='Filen som skal skrives til', required=True)
args = parser.parse_args()

# get the arguments in variables
url = args.url
outfile = args.outFile
open(outfile, 'a').close()

# dont display the browser...
options = Options()
options.headless = True

# create new firefox session with options
driver = webdriver.Firefox(firefox_options=options)
driver.implicitly_wait(10)

#get all the section-urls
driver.get(url)
soup = BeautifulSoup(driver.page_source, 'lxml')
outerdivelement = soup.find('div', {"class":"innholdstekst"})

#loop all the sections
for i in outerdivelement.find_all('li'):
    parseSection(i.find(href=True)["href"])

#get the email addresses from the "frontpage"
parseSection(url)

#exit quietly
driver.quit()
```

C Visual Basic macro for arbeidsbok i excel

EksportTilSelectSurvey - 1

```
'Export selected rows
Sub export()
Application.ScreenUpdating = False
' Different worksheets
Dim mainSheet As Worksheet ' Hovedarket med statements og slikt
Dim dimensionsSheet As Worksheet ' Ark med dimensjoner
Dim questionTypeSheet As Worksheet ' Ark med spËrsmëlstype
Dim exportSheet As Worksheet ' Arket som lages med eksporterte statements

Set mainSheet = ActiveWorkbook.Sheets("statements")
Set dimensionsSheet = ActiveWorkbook.Sheets("Dimensions")
Set questionTypeSheet = ActiveWorkbook.Sheets("QuestionType")

mainSheet.Activate

' Gë gjennom hver rad der kolonne med export er satt til sann
Dim eksportKolonne As String 'Eksport Status'
Dim engelskKolonne As String 'English kolonne med pëstander
Dim norskKolonne As String ' Norsk kolonne med pëstander
Dim komponentKolonne As String ' Komponent kolonne med komponent
Dim questionTypeKolonne As String ' SpËrsmëls type kolonne med typer

Dim eksportRange As Range ' Range med eksport status
Dim engCol As Long 'kolonna med engelsk
Dim norCol As Long ' Kolonna med norsk
Dim komponentCol As Long ' Kolonna med komponent
Dim questionCol As Long ' Kolonna med spËrsmël

' Sett verdien til kolonne teksten
eksportKolonne = "EksportStatus"
engelskKolonne = "English"
norskKolonne = "Norsk"
komponentKolonne = "Komponent"
questionTypeKolonne = "SpËrsmëls type"

' Finner kolonna identifisert med eksportKolonne og velger alle radene
Set eksportRange = Cells.Find(eksportKolonne, LookIn:=xlValues, LookAt:=xlWhole).EntireColumn.Speci
alCells(xlCellTypeConstants).Offset(1).SpecialCells(xlCellTypeConstants)

' Setter kolonne nummeret til variabel.
engCol = Cells.Find(engelskKolonne, LookIn:=xlValues, LookAt:=xlWhole).Column
norCol = Cells.Find(norskKolonne, LookIn:=xlValues, LookAt:=xlWhole).Column
komponentCol = Cells.Find(komponentKolonne, LookIn:=xlValues, LookAt:=xlWhole).Column
questionCol = Cells.Find(questionTypeKolonne, LookIn:=xlValues, LookAt:=xlWhole).Column

' Looper gjennom hver rad
For Each rad In eksportRange.Cells

    ' Hvis checkbox er merket
    If rad = True Then
      ' Bruk raden til ë hente engelsk og norsk spËrsmël og konfigurasjon
      Dim rowN As Long
      Dim eng As Variant
      Dim nor As Variant
      Dim komponent As Variant
      Dim questionType As Variant
      Dim questionTypeId As Integer
      Dim qtLookup As Range
      rowN = rad.Row

      eng = Cells(RowIndex:=rowN, ColumnIndex:=engCol) ' Finner engelsk pëstand
      nor = Cells(RowIndex:=rowN, ColumnIndex:=norCol) ' Finner norsk pëstand
      komponent = Cells(RowIndex:=rowN, ColumnIndex:=komponentCol) ' Finner komponent
      questionType = Cells(RowIndex:=rowN, ColumnIndex:=questionCol) ' Finner spËrsmëltype teksten
      ' Finn id til questionType, the id must be used by SelectSurvey

      With questionTypeSheet ' Finn id til spËrsmëlstype i annet ark
        Set qtLookup = .Cells.Find(questionType, LookIn:=xlValues, LookAt:=xlWhole)
        questionTypeId = .Cells(RowIndex:=qtLookup.Cells.Row, ColumnIndex:=(qtLookup.Cells.Column -
 1))
        'Debug.Print questionTypeId
      End With

      Set exportSheet = CreateSheetExport()
      Dim RetVal As Variant
      RetVal = WriteTypeThree(exportSheet, 1, nor, "d", "d", True, komponent)
```

```
      ' Gë gjennom hver rad og eksportere det til eksport-ark
      '


      'MsgBox rowN & ", " & engCol & ": " & nor & ", Komponent: " & komponent
      'Dim rowN = sjekkboks.
        'For rad = 1 To Rows.Count
            'If Cells(rad, 1).Top = chkbx.Top Then

                'Dim eng As Variant
                'Dim nor As Variant
                'eng = Worksheets("statements").Range("A" & rad).Value
                'nor = Worksheets("statements").Range("B" & rad).Value
                'MsgBox eng & vbNewLine & nor

                'With Worksheet("eksportTilSelectSurveyNOR")
                'newRow = .Range("A" & Rows.Count).End(xlUp).Row + 1
                'Exit For
            'End If
        'Next rad
    End If
Next
Application.ScreenUpdating = True
End Sub

Private Function CreateSheetExport() As Worksheet
    Dim sheetName As String
    With ThisWorkbook
        sheetName = "Exported" & (.Sheets.Count)
        .Sheets.Add(After:=.Sheets(.Sheets.Count)).Name = sheetName
        Set CreateSheetExport = .Sheets(sheetName)
    End With
End Function

' Skriver type 3 spËrsmël til export arket
Private Function WriteTypeThree(ByVal toSheet As Worksheet, ByVal pageNumber As Integer, ByVal qTex
t As String, ByVal qAlias As String, ByVal qSubText As String, ByVal requiredYN As String, ByVal th
reeSixtyQCategory As String)
    With toSheet
        newRow = .Range("A" & Rows.Count).End(xlUp).Row + 1 ' neste rad tall
        .Cells(RowIndex:=newRow, ColumnIndex:=1).Value = 3 ' skriv type spËrsmël
        .Cells(RowIndex:=newRow, ColumnIndex:=2).Value = pageNumber ' Sidetallet
        .Cells(RowIndex:=newRow, ColumnIndex:=3).Value = qText ' SpËrsmëlet
        .Cells(RowIndex:=newRow, ColumnIndex:=4).Value = qAlias ' Alias for spËrsmëlet
        .Cells(RowIndex:=newRow, ColumnIndex:=5).Value = qSubText ' sub tekst for spËrsmëlet
        .Cells(RowIndex:=newRow, ColumnIndex:=6).Value = requiredYN ' Pëkrevd
        .Cells(RowIndex:=newRow, ColumnIndex:=7).Value = threeSixtyQCategory ' Kategori/komponent
        .Cells(RowIndex:=newRow, ColumnIndex:=3).Value = ""
        .Cells(RowIndex:=newRow, ColumnIndex:=3).Value = ""
    End With
End Function
```

D Intervju av Roar Thon

Erfaringer med andre kjente rammeverk?
Norsis og Kai Roer sitt rammeverk er to ytterpunkter. Spørreundersøkelser, som feks NorSIS tilbyr gir som regel mer informasjon om kunnskap enn reell adferd. Det er noe som må tas høyde for når undersøkelser vurderes. Mens med feks. Kai Roer sitt rammeverk så får man et større innblikk fordi man bruker data fra hendelser og spørreundersøkelser som en kombinasjon. Før Kai Roer begynte med firmaet sitt som han har nå så hadde han et open source rammeverk.

Kultur og organisasjonskultur er et litt uklart begrep. Hva legger du I det?
Sidestiller sikkerhetskultur og organisasjonskultur. Skal ikke ha et styringssystem for sikkerhet, men et som inkluderer sikkerhet. Få sikkerhet inn i den grunnleggende driften fra starten av.

Når det gjelder sikkerhetskultur. Vil du si at den har forandret seg over tid ?
Det er et relativt nytt begrep. Før var det større fokus på fysisk sikkerhet og dokumentsikkerhet. Etterhvert som teknologien ble mer tilgjengelig
I August 2012 publiserte 22. Juli kommisjonen sin rapport, og den tar i bruk begrepet sikkerhetskultur på en helt annen måte og gjør at begrepet i seg selv blir mer utbredt. Dette var mye på grunn av kritikk til den offentlige kulturen. Var en vekker for mange bedrifter.
Statoil Rapporten fra Inas menas (år?) var også en knusende dom av kulturen,som gikk ut på at ingen forstår at de som enkeltpersoner har et bidrag å komme med i sikkerheten.
Sikkerhetskulturen er der uansett, alle har en form for organisasjonskulturen.

Vil begrepet sikkerhetskultur få en annen betydning avhengig av størrelsen på bedriften?
I en stor bedrift kan man få subkulturer, mens i mindre organisasjoner på feks 20 personer så får man personer som avviker fra det normale. Det vil finnes forskjeller i kultur og tilnærming til sikkerhet. Forskjeller mellom jagerflypiloter og transport i forsvaret. For jagerflypiloten så er sikkerhet viktig men for transport kan det bli litt mer abstrakt.

Hva kjennetegner bedrifter som har god sikkerhetskultur ?
Åpenhet, delingskultur, godt arbeidsmiljø. Viktig at alle de ansatte trives og er stolte av jobben sin og ikke at det er kritikk og negativitet hele tiden.

En ekstrem men optimal tilnærming er forsvarets spesialenheter, hvor man hele tiden korrigerer hverandre og det er et felles mål om å være best.

Hva kan være viktige faktorer / indikatorer som et rammeverk burde ta med?
F Eks. Hva er viktig å tenke på når man gjennomfører en måling.
Kai roer sitt rammeverk er en kombinasjon av en kvalitativ og kvantitativ tilnærming.
Det må velges ut ifra hvilken organisasjon man er. Faktorer man kan se på er kanskje. "føler du at du får nok informasjon om sikkerhet?", "vet du om hva virksomheten utsettes for til daglig?", "Forstår du hva konsekvensene er dersom sikkerheten kompromitteres?" Dette kan være fine tilnærminger i tillegg til de "tradisjonelle" spørsmålene

De fleste er stolte av arbeidsplassen og merkevaren sin. Det er viktig å prøve å få de ansatte i organisasjonen med på å ha en felles tilnærming til å forebygge hendelser.

Har NSM et rammeverk / metode for kartlegging av informasjonssikkerhet som anbefales til bedrifter?
Nei. Det kan føre til at mange bare tar det rammeverket og bruker det uten at det spesialiseres til virksomhetens behov.

Er det noen forskjell på å måle sikkerhetskultur i små avdelinger kontra store?
Stor bedrifter kan ha ulike subkulturer eller forskjellige tilnærmingsmåter, ved at ulike avdelinger har et annet forhold til sikkerhet. I små bedrifter kan det være lettere å måle hva gjennomsnitts kulturen faktisk er. Det kan være naturlig at ulike avdelinger har ulik tilnærming til sikkerhetskultur og ikke alltid at den "beste" avdelingen har den riktige sikkerhetskulturen.

Hva tenker du er en passende lengde på en spørreundersøkelse?
Har man en lengre undersøkelse så er det færre som gjennomfører. Har man et tema som interesserer så passer det bra med en lengre undersøkelse, og de vil ha større motivasjon for å være med på å bidra. Det vil være forskjellig å spørre sikkerhetsavdelingen kontra HR for eksempel.

Ang. Demografi på spørreundersøkelser, er det nødvendig å se på f eks. Kjønn?
Ja. fordi kjønn har en stor betydning. For eksempel så kan menn være litt mer risikovillige og "tar en sjans", mens kvinner er litt mindre risikovillige og tvilende til egne kunnskaper. Interessante opplysninger fra Kai Roer sine publikasjoner. Uansett så er identifisering en viktig faktor. De som scorer best på sikkerhetskultur har ofte en god balanse mellom kjønnene fordi man balanserer ut sterke og svake sider.

Hvordan ser du på å bruke faste spørsmål fra år til år. Vil de ansatte kjenne igjen spørsmålene?
Nei, ikke dersom man har det årlig. Viktig at dersom man måler på sikt at man har noen faste spørsmål. Da kan man måle forandringen på noen spesifikke spørsmål.

Hva er ditt syn på kvalitativ og kvantitativ analyse av resultatene fra en spørreundersøkelse?
Som sagt så er kunnskap ikke det samme som atferd og en spørreundersøkelse vil ta tak i den ansattes kunnskap. Viktig at man er kritisk til tallene og spør seg selv om hvorfor man fikk det resultatet man fikk. Etter undersøkelsen kan man for eksempel spørre avdelingssjefene om de kjenner seg igjen i tallene. Få igang en diskusjon med avdelingen basert på tallene fra undersøkelsen.

Kan man endre sikkerhetskulturen bare med litt opplæring eller noen foredrag?
Kunnskap endrer sjeldent adferd. For å endre kulturen må man vite hvordan kulturen er og hva man ønsker at den skal være. Samt en plan på hvordan man skal komme dit man vil. Det er en kontinuerlig prosess. Som sagt så er det å skape diskusjon et tiltak i seg selv.

En annen viktig ting er å prøve å se på hvorfor tiltaket er der? Er det nødvendig eller er det noe man alltid har gjort tidligere uten at det har noe konkret effekt.

Å kartlegge både gode og negative hendelser kan brukes til å påpeke enkeltområder for forbedring eller skryt.

Generelt sett, er det noen tiltak som du mener passer best eller har en god effekt?
Kommer ikke bort ifra å tilføye de ansatte kunnskap. Virkemidler for å formidle dette er viktig å se på. Men man må passe på at virkemidlene ikke blir for store slik at det ikke overskygger budskapet eller kunnskapen bak. Det er ikke nødvendigvis sikkerhetssjefen som skal formidle dette budskapet. Andre profesjoner som vet hvordan man kan motivere og begeistre bør være med på ansvaret.

Tror du at en aksept for masserapportering i en bedrift kan føre til bedre sikkerhetskultur?
Ja. Bedre med for mye enn for lite rapportering.

Tar det lang tid å forbedre en organisasjonskultur?
Vil ikke si noe spesifikt om hvor lang tid det tar. Det er en kontinuerlig prosess.
Man må måle hvor man er, for å finne forbedringsområder. Bruke formidlings virkemidler over tid i tillegg til målinger underveis slik at man kan se hvordan man ligger ann.

Har du noen generelle tips eller ideer som kan være viktig å se på ved vår oppgave?
I akademia så er forståelsen av deling en utfordring. Man må prøve å identifisere hva som er sikre områder og hva man kan dele.

E Intervju av Bjarte Malmedal

Intervju Bjarte Malmedal 12.02.2019

Hvilke rammeverk kjenner du til? Har Norsis noe vi kan benytte?

Se NorSIS rapport 2015 2016, gir det teoretiske grunnlaget for kultur undersøkelse. Spørsmål som ble stilt står der.

Tilpasninger: Beskrevet i rapport 2017 2018. Gjengitt i rapporten. Omfattende litteraturstudiet. Mange som snakker om sikkerhetskultur, det de gjør kartlegger adferd. Forskjell på kultur og adferd. Eksempel adferd: Sjekke om ansatte trykker på lenker. Sikkerhetskultur kunnskap, holdninger, måler trykker på lenker.

Forsket på holdninger og meninger. Bredt perspektiv.

Skille kultur og adferd. Egen metode. Brukt 50 virksomheter. 20 000 besvarelser, 70 000 utsendte.

Opplyse: digital sikkerhetskultur tilnærme seg det deskriptivt, måling=kartlegging. Kultur skal ikke rangeres ift. Ikke bedre enn noen andre. Forutsetninger spiller inn. Hvordan den er. Men forsiktig med å si noe om forskjellen. Forskjellige behov. Deskriptivt mener NorSIS er bra. Nasjonalt perspektiv kan være forskjellig fra bedrift.

Andre metoder: normativ tilnærming. Tallverdier, noen gir tall for sammenligningsgrunnlag. Ikke godt for NorSIS.

Man må snakke om kultur med samme perspektiv. Holdninger rettet mot mål.

Spørreundersøkelse, intervju, etc. På alle ansatte eller ledelse. Ulike tilnærminger?

Kommer an på hva man ønsker. Hva ønsker man? Ønsker å vite hva ledelsen ønsker. En kombinasjon er viktig. Fra ledelsen kan man få målene for hva som ønsker det skal være. Gap analyse mellom ledelse og ansatte.

For evt. Spørreundersøkelse. Hvordan formulere spørsmål?

Tok norsis et halvt år og komme fram til sine spørsmål. Kjørte pilottester med folk. For å komme fram til riktige spørsmål.

Når Norsis gjør undersøkelser bruker de 25 spørsmål til alle. Endres ikke. I tillegg 5 spørsmål organisasjonen kan lage selv. Da får man tilpasning og felles base med data. For å at man skal kunne sammenligne med andre virksomheter. Men ikke nødvendigvis heldig å sammenligne med andre. Eks. Forsvaret og politi har forskjellige grunnlag og mål. Kan bruke norsis rammeverk. Godt analysegrunnlag. Alle de dataene er tilgjenglig.

Viktig å tenke på ved vårt use case?

Ofte få personer som svarer. Signifakt og usikkerhet i svar. Fjerne tilfeldigheter og finne kjernen.

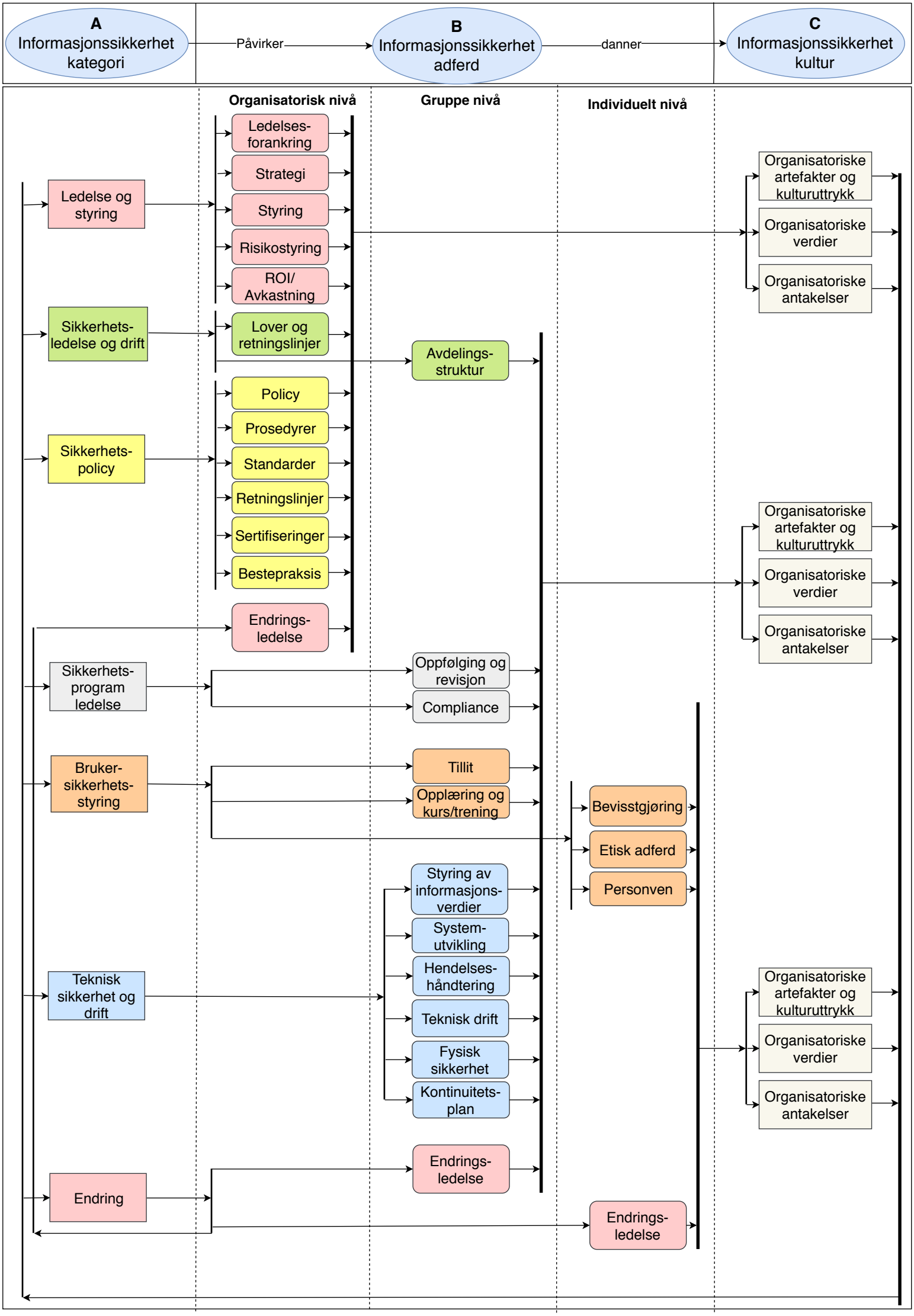
Du kan bruke hvilket som helst rammeverk..men hva betyr det. Må dekke prosessen i etterkant. Må finne ut av hva ledelsen ønsker. Hvilke typer holdninger ønsker ledelsen. Kart fra ledelsen fra hva de ønsker. Hva er bakgrunnen for svarene. Setter inn tiltak på. Planlagt før man starter.

Basere spørsmål på hva?

Erfaring: Sikkerhetspolicy er ofte ikke en policy, utgått policy. Kan være vanskelig å finne en god policy som er up to date. Dybdeintervju med sikkerhetsansvarlig for å finne ut dagens ståsted.

Får ferske føringer. Forankring og forventing. Når funnene kommer tilbake, det sikkerhetsansvarlig sa om «opplæring» kanskje ikke stemte. Lage plan. Tiltak, finansiering.

F Information Security Framework


A
Informasjonssikkerhet kategori
Påvirker
B
Informasjonssikkerhet adferd
danner
C
Informasjonssikkerhet kultur
Organisatorisk nivå
Gruppe nivå
Individuelt nivå
Ledelses-forankring
Strategi
Styring
Risikostyring
ROI/ Avkastning
Ledelse og styring
Sikkerhets-ledelse og drift
Lover og retningslinjer
Avdelings-struktur
Policy
Prosedyrer
Standarder
Retningslinjer
Sertifiseringer
Bestepraksis
Sikkerhets-policy
Endrings-ledelse
Organisatoriske artefakter og kulturuttrykk
Organisatoriske verdier
Organisatoriske antakelser
Sikkerhets-program ledelse
Oppfølging og revisjon
Compliance
Bruker-sikkerhets-styring
Tillit
Opplæring og kurs/trening
Bevisstgjøring
Etisk adferd
Personven
Styring av informasjons-verdier
System-utvikling
Hendelses-håndtering
Teknisk drift
Fysisk sikkerhet
Kontinuitets-plan
Teknisk sikkerhet og drift
Endring
Endrings-ledelse
Endrings-ledelse

G Rammeverk og evalueringsverktøy for informasjonssikkerhet kultur

Rammeverk og evalueringsverktøy for informasjonssikkerhetskultur

Basert på Information Security Culture Assessment – ISCULA – Da Veiga

Type dokument	Rammeverk
Forvaltes av	
Godkjent av	
Klassifisering	Åpen
Gjelder fra	
Gjelder til	
Unntatt offentligheten	Nei

1. Formål

Formålet med arbeidet med informasjonssikkerhetskultur er å ivareta og sikre informasjonsverdier hos NTNU. Spesifikt for en måling av informasjonssikkerhetskultur er målet å identifisere spesifikke områder hvor arbeidet med informasjonssikkerhet kan vedlikeholdes og forbedres. Målingen skal redusere kostnad, ressurser og tid brukt på å oppnå et akseptabelt nivå for informasjonssikkerhetskultur, og vil også bidra til vise hvor man kan legge ressursene for høyest effekt.

2. Hvem kan bruke rammeverket

Rammeverket er tiltenkt brukt i avdelinger hos NTNU.

3. Styrende dokument

Retningslinje for arbeid med sikkerhetskultur og opplæring innen informasjonssikkerhet.

Rammeverket

1. Utvikling

Rammeverket er et resultat av en bacheloroppgave i regi av Gaute Wangen avdeling for sikkerhet hos NTNU. Bacheloroppgaven sine deltagere er Joakim Nereng Ellestad, Anders Gustad, Espen Skuggerud og Magnus Lien Lilja. Rammeverket presentert her er utviklet ut fra forskning utført av Adéle da Veiga og veileder Prof. J.H.P. Eloff i forbindelse med doktoroppgaven (Cultivating and assessing information security culture) i informasjonsteknologi hos University of Pretoria september 2008. Forskningen finnes i sin helhet (link). Rammeverket presentert her er en norsk oversettelse, med tilpasninger for NTNU.

Forslag til gjennomføring for måling av informasjonssikkerhetskultur

Det finnes flere metoder for hvordan man kan gjennomføre undersøkelser. ISCULA[1] (Figur 6.1) illustrerer en stegvis prosess bestående av fem steg for gjennomføring ved måling av informasjonssikkerhet. ISCULA fungerer som en prosessbasert veileder for gjennomføring. Prosessen bidrar til planlegging, tildeling av roller, kvalitetssikring av data og identifisere handlingsplaner ved sikkerhetskulturundersøkelsen.

Steg 1: Forberedelse og planlegging for måling av informasjonssikkerhetskultur

Første steg for gjennomføring av en undersøkelse er planlegging. Under presenteres syv steg for gjennomføring.

Steg 1.1 Involvere interessenter

Prosjektet må få støtte av interessenter og godkjennes av ledelse. Det er viktig å identifisere de riktige interessentene da et slikt prosjekt ofte krever samarbeid på tvers av ansvarsområder hvor resultater benyttes på tvers av interessenter og avdelinger som legger grunnlaget (input) for videre arbeid[2].

Steg 1.2 Utvikle ett verktøy for måling av informasjonssikkerhetskultur

Spørreundersøkelsen som benyttes for vurdering og måling må imøtekomme de objektive målene som er satt innledende i grunnlaget. Dette krever at spørsmålene effektivt kan identifisere kulturen innad organisasjonen. Det vil si at spørsmålene som benyttes er generiske eller forhåndsutviklet for å passe inn organisasjonens miljø. Dette kan oppnås ved å gjennomføre *workshops* med interessentene. For å unngå at spørsmålene kun adresserer teknologiske aspekter er det viktig å inkludere forretningsmessig deltakelse; dette gjør spørreundersøkelsens ordlyd og terminologi forståelig uavhengig av målgruppens individer og deres roller. Eksempelvis må målgruppen kunne kjenne seg igjen i stillingstittel som blir brukt i undersøkelsen.

En spørreundersøkelse inneholder ofte demografiske spørsmål for å forstå sammensetningen av menneskene i målgruppen, og for å kunne segmentere data i analysen. De demografiske spørsmålene bør derfor være tilpasset målgruppen. Generelt vil disse spørsmålene dekke forretningsområder, geografiske og ansettelsesforhold som hvor lenge den ansatte har jobbet i nåværende stilling og stillingsbeskrivelse/tittel.

Demografiske data som har blitt benyttet i undersøkelser tidligere har vært seksjonstilhørighet. Andre data som kan være aktuelle er alder, ansettelsesforhold, ansiennitet i nåværende stilling eller antall tidligere arbeidsforhold.

---

[1] Information Security Culture Assessment

[2] https://innsida.ntnu.no/documents/10157/2550717837/Retningslinje+for+arbeid+med+sikkerhetskultur+og+oppl%C3%A6ring.pdf/ee78e950-d96b-492d-b36b-b376d925603f

Hvis det ikke eksisterer en spørreundersøkelse fra før av må innledende arbeid gjennomføres for å avdekke bakgrunn for måling. For eksempel, hvilke komponenter skal vurderes ved måling av informasjonssikkerhetskultur? Kapittel 4 i ISCF[3] kan benyttes for å identifisere de ulike komponentene av informasjonssikkerhetskulturen og deretter utvikle påstander/spørsmål som kan benyttes i undersøkelsen.

Intervju- og diskusjonsrunder kan også benyttes som grunnlag for utviklingen av spørsmål ved å identifisere områder av interesse skreddersydd for organisasjonen/avdeling. Eksempelvis, *ledere tror ikke ansatte vet hvor finne policyer som gjelder de* eller *ansatte har ingen motivasjon for å delta på seminarer som tiltak for å øke virksomhetens informasjonssikkerhet*. De initiale spørsmålene og påstandene kan bygge på disse identifiserte komponentene og problemer som ble avdekket ved intervju/diskusjonsforum.

Når det videre refereres og snakkes om påstander og spørsmål menes påstandene/spørsmålene brukt i informasjonssikkerhetskultur-undersøkelsen. De allerede eksisterende spørsmålene kan vike fra problemområdet som er avdekket etter intervju eller diskusjon med de involverte. Det er derfor viktig ikke å blande spørsmålene for å ikke ødelegge det statistiske grunnlaget som de eksisterende spørsmålene gir. Nye spørsmål som inkluderes i undersøkelsen kan skilles ut i en egen seksjon.

Steg 1.3 Validering av undersøkelsen

For å sikre statistisk validitet er det viktig at spørsmålene adresserer de målene som ble satt som bakgrunn for prosjektet. Validitet bidrar også til pålitelige og stabile resultater over tid.

Spørsmålene må derfor tilspisses organisasjonens og ansattes oppfatning av sikkerhetskultur. Spørsmålene må fokusere på hva som utgjør informasjonssikkerhet i organisasjonen og brukerens oppfatning av denne sikkerheten.

For NTNU innebærer dette at spørsmålene har grunnlag i komponentene vist i figur 1(referer til komponenter grafikk). Hvis eksisterende spørsmål ønskes å inkorporeres i ISCULA må de valideres ved å gi spørsmålene grunnlag i en av komponentene. Spørsmålet bør kunne knyttes til en komponent for at det skal kunne benyttes i undersøkelsen. Det må da valideres om hvert område/komponent er tilstrekkelig dekket. Hver komponent må være dekket med en påstand eller spørsmål i undersøkelsen for å sørge for at resultatet fra undersøkelsen er gyldig og kan bli brukt som grunnlag. Dette gjelder da ved tilføying av nye spørsmål til undersøkelsen.

Neste seksjon vil gå gjennom prinsippene som må ligge til grunn for utvikling av påstander og spørsmål til undersøkelsen. Disse vil bidra til at spørreundersøkelsens terminologi adresserer korrekt målgruppe og at den er forståelig for denne gruppen, og at undersøkelsens spørsmål vil gi pålitelig data.

a. Kortfattethet og klarhet

Formuleringen på påstandene må være tydelig, kortfattet og direkte. En påstand burde være formulert slik: «NTNU har dokumentert politikk for informasjonssikkerhet», fremfor «Organisasjonen har informasjonssikkerhetskrav som jeg må etterkomme og som er dokumentert i en policy hvor

[3] information security culture framework

informasjonssikkerhet er sett på som viktig», da dette ikke bare er en lengre påstand, men kan også virke utydelig.

b. Vokabularet til respondenten og fagterminologi

Det må tas hensyn til respondentens vokabular ved formulering av påstander og spørsmål. Ordene må ikke være for vanskelige å forstå eller involvere kompliserte problemer eller kreve spesialisert kunnskap. For eksempel er «Business continuity-planen forklarer hva hver person skal gjøre i tilfelle en hendelse» bedre fremfor: «Organisasjonen har en business continuity plan som inkluderer prosedyrer for IT avdelingen for å sikre dokumenter og it utstyr.»

Det er en stor del terminologi som er spesifikke for informasjonssikkerhet og teknologi, som generelt sett ansatte ikke nødvendigvis kjenner til. Terminologi som trussel, informasjonsverdier, business continuity plan, informasjonssikkerhetshendelse eller begrepet best practice må være definert på forhånd i undersøkelsen for ikke å skape forvirring eller feiltolkning av påstander og spørsmål. Det kan være aktuelt å ta med eksempler i enkelte påstander og spørsmål, for å tydeliggjøre hva man ønsker spørre om. Det er viktig at eksemplene er gjenkjennelig for leseren, dvs. at eksemplene må formes og valideres for hver gang undersøkelsen brukes i ulike avdelinger, slik at begrepene er tilpasset målgruppen.

c. Korte setninger og ingen sjargong

Korte setninger gjør undersøkelsen raskere å få unnagjort og lager en positiv driv for respondenten. Formuleringer som bruker uttrykk som bare er kjent fra informasjonssikkerhet-miljøet kan være forvirrende for andre ansatte under andre avdelinger.

d. Ett konsept eller problem

Påstander/spørsmål burde bare måle ett konsept eller problem. Spørsmålene må valideres for å ikke inneholde flere påstander enn ett. Spørsmål som kan ha mer enn en mening må også bli unngått.

e. Klare skiller mellom svaralternativer

Der det tilbys svaralternativer må alternativene være klart skilt. Det må ikke forekomme overlapping i hverandre eller at de mener det samme.

For eksempel er dette et eksempel på uheldige svaralternativer:

«Jeg er informert om informasjonssikkerhets krav gjennom epost …(velg et svaralternativ)»

1. En gang i måneden
2. En eller flere ganger i måneden
3. To eller tre ganger i måneden
4. Tre eller flere ganger i måneden

Her overlapper alternativ 2 og 3 hverandre og respondenten kan bli usikker på hva som skal velges. Resultatet kan bli påvirket ettersom alternativ 2 kan bli sett på som negativt og alternativ 3 som positivt. Alternativene burde heller formuleres som følgende for å slippe overlapping:

1. Ingen ganger
2. En eller to ganger i måneden
3. Tre til fire ganger i måneden
4. Fem eller flere ganger i måneden

f. Utforming av undersøkelsen

Utformingen på undersøkelsen må være visuelt attraktiv og godt presentert, ettersom dette kan gjøre svarprosenten betydelig bedre. Følgende steg burde vurderes ved utforming av undersøkelsen:

- En formell begrunnelse for gjennomføringen av undersøkelsen med signering av ledelse. Jo høyere forankring, jo bedre.
- Beskrivelse av konfidensialiteten til undersøkelsen og hvordan ansattes anonymitet ivaretas. Ansatte kan vegre seg for å delta om de tror svar kan spores tilbake til dem.
- Tiden det tar å fullføre undersøkelsen bør ikke overstige 10 minutter. Det er viktig at det er en balanse i antall spørsmål og hvor lang tid det vil ta for en respondent å gjennomføre undersøkelsen, da man med for lang gjennomført tid risikerer at respondenten gir opp underveis og man får ikke den dataen man ønsker. Samtidig ønsker man nok spørsmål til å adressere flest mulige kategorier. Det anbefales at man velger antall spørsmål ut ifra hvor mange spørsmål man antar respondenten rekker gå gjennom på den anbefalte tiden, sett bort i fra den demografiske dataen.

Tabell 1 Validering av eksisterende spørsmål

Komponent kategori	Komponent	Spørsmål fra eksisterende undersøkelse	Tilstrekkelig	Foreslått påstander ved informasjonssikkerhets kultur
Ledelse og administrasjon	Ledelses-forankring	Jeg mener det er viktig å implementere informasjonssikkerhet i organisasjonen.	Nei	Rektoratet ved NTNU poengterer viktigheten ved å beskytte konfidensiell informasjon.
	Strategi	NTNU har en plan og strategi for informasjonssikkerhet	Nei	Jeg mener det er nødvendig med beskyttelse av informasjon for måloppnåelsen til NTNU. Jeg mener NTNU gir tilstrekkelig oppmerksomhet til informasjonssikkerhet. Informasjonssikkerhetsmekanismer implementert hos NTNU støtter NTNUs måloppnåelse.

Steg 1.4 Kunnskapsspørsmål

Formålet med seksjonen i undersøkelsen som omhandler kunnskap er å måle spesifikk kunnskap eller adferd hos ansatte i avdelingen. Disse påstandene kan være utformet av avdelingsleder eller leder for seksjon for digital sikkerhet. Påstandene ønsker å adressere hvor mye kunnskap ansatte har angående informasjonssikkerhet. For eksempel kan det tenkes at man har dårlig informasjonssikkerhetskultur

som igjen skyldes mangelfull opplæring. Påstander kan også avdekke eventuelle bekymringer om informasjonssikkerhet, som for eksempel sprik mellom hva ledelsen forventer hva de ansatte skal kunne, og hva de ansatte faktisk vet.

Steg 1.5 Demografiske opplysninger

De demografiske spørsmålene er med for å segmentere data, lage teorier og knytte sammenhenger mellom demografiske data.

De demografiske data som er anbefalt å ha med er alder, seksjon, avdeling, ansettelsesforhold, ansiennitet i nåværende stilling, antall tidligere ansettelsesforhold eller hvilken utdannelse respondenten har.

Det må ved tolkning av besvarelsen tas hensyn til at dersom forholdet mellom demografiske data og antall besvarelser ikke er optimal kan ikke den demografiske dataen brukes i tolkningen. Tommelfingerregelen er at det skal være like mange besvarelser per oppdeling som antall spørsmål i undersøkelsen. Det betyr i prinsippet at ved små avdelinger vil det være hensiktsmessig å fjerne en del av den demografiske dataen, da det ikke kommer til å foreligge et resultat som kan brukes. Det må tas en vurdering på hvilke demografiske data som er nødvendige, da det kan anses som like kostnadseffektivt å utføre eventuelle tiltak etter målingen på en hel avdeling, i isteden for å sette tiltak basert på segregerte grupper.

Steg 1.6 Utvalgsstørrelse

Antall spørsmål i undersøkelsen må være representativt i forhold til antall ansatte undersøkelsen går ut til i avdelingen. Ved NTNU, sees det på som ideelt å sende ut undersøkelsen til alle ansatte i en avdeling og bruke demografiske data for å skille resultat innad i avdelingen. Det er et krav at undersøkelsen ikke varer noe mer enn 8-10 minutter, ideelt sett ønskes undersøkelsen å vare mellom 6-8 minutter (ref. Randi, HR og HMS avdeling). Det må derfor undersøkes på forhånd hvor lang tid undersøkelsen tar. Det er estimert at rundt 30-40 spørsmål vil holde seg innen dette kravet. I tillegg til tidskravet er det viktig at svarprosenten er god nok for tolkning av resultatet. Dette er for å sørge at dataen man henter inn er representativt. Det ønskes da høyest mulig andel respondenter i avdelingen undersøkelsen går ut til. En tommelfingerregel er at det burde være like mange besvarelser per oppdeling som antall spørsmål i undersøkelsen. Gruppen som utsteder undersøkelsen må drøfte i forkant av utstedelsen og gjøre seg enig om hva som er godt nok statistisk grunnlag for tolkning av data. Det kan også hende ved segregering av innhentet data i etterkant av undersøkelsen at man er nødt til å tilpasse og forandre segmentering, hvis man finner ut at man ikke har nok data til at det er representativt å segmentere inn i ønskede kategorier.

Steg 1.7 Utføring av pilotundersøkelse

Før spørsmålene kan sendes ut til målgruppen må spørsmålene testes på et mindre antall ansatte. Dette gir de ansvarlige for undersøkelsen muligheten for å forutse reaksjonen til den endelige målgruppen og kan deretter revidere spørsmålene og bruke eventuelle tilbakemeldinger. Disse pilot-testene bidrar til at mangfoldet i målgruppen er representert, ved små begreps- og terminologi-justeringer som sørger for at alle ansatte forstår spørsmålene stilt på lik måte.

Steg 1.8 Valg av passende målingsverktøy

Prosessen for distribusjon, gjennomføring og datainnsamling av spørreundersøkelsen må etableres. Det finnes flere måter for samling av data, eksempelvis papirbasert versjon, utstedelse via e-mail, intranett-løsninger eller intervjuer.

Det finnes ulike verktøy som kan benyttes, men det er viktig å velge ut ifra hva som passer organisasjonen og anses som mest kostnadseffektivt. Select Survey er et eksempel av digitale verktøy for spørreundersøkelser.

Steg 2 Administrasjon rundt undersøkelsen

Administrasjon av undersøkelsen er prosessen knyttet til distribusjon til målgruppen og hvordan undersøkelsen samles for analyse. Denne prosessen deles inn i tre følgende steg.

Steg 2.1 Informer om undersøkelsen

Formidling av formålet for undersøkelsen til de ansatte er viktig, da dette sørger for økt deltakelse og kvalitet av data. Det kan sendes ut et varsel til målgruppen om at det vil bli gjennomført en spørreundersøkelse der objektivet forklares. Det finnes også andre alternativer for å formidle undersøkelsen, eksempelvis som plakater eller ved bruk av insentiver. Det er viktig at informere deltakere om at de ikke kan identifiseres ut ifra svarene i undersøkelsen, da dette også kan bidra til økt kvalitet og korrekt data.

Steg 2.2 Publiser undersøkelsen

Undersøkelsen sendes ut gjennom det medium og kanal valgfritt for organisasjonen. Dette kan være papirbaserte og elektroniske undersøkelser, enten sendt på e-mail eller **gjennomføres** på organisasjonens intranett. Obs, benyttes Internett er det viktig at tilgangen er regulert.

Steg 2.3 Oppfølging av svar

Respons og svar må oppfølges slik at man sørger for statistisk representativ data av de enkelte biografiske områdene dataen vil bli segmentert på, eksempelvis de ulike stillingene ansatte har og avdelinger. Det finnes flere statistiske metoder som kan benytter for å avgjøre størrelsen av “sample size”. For eksempel kan trender benyttes i samspill med fokusgrupper for å verifisere data, i tilfelle utilstrekkelig respons og svar.

Steg 3: Evaluering av undersøkelsen

Data fra undersøkelsen blir analysert med bruk av statistiske metoder. Hvilke statiske metoder som blir brukt skal bli avklart i planleggingsfasen. Statistiske metoder kan også brukes for å validere spørreundersøkelsen.

Steg 3 .1 Analysere

Følgende statistiske metoder kan benyttes for å identifisere hvilke elementer det skal fokuseres på for å forbedre sikkerhetskulturen:

- Frekvensdistribusjon
- Aritmetisk gjennomsnitt
- Standardavvik
- T-test
- Variansanalyse
- *Cut-off*

Steg 3.2: Validere undersøkelsen

Undersøkelsen kan valideres gjennom å utføre en statistisk analyse. Målet med analysen er å forbedre undersøkelsen til senere bruk og gi økt statistisk gyldig resultat.

Se den engelske utgaven for gjennomføring av validering.

Steg 3.3: Pålitelighet

Se den engelske utgaven for gjennomføring av pålitelighet.

Steg 4: Dokumentasjon og tilbakemelding

Funn og resultater fra undersøkelsen oppsummeres i en rapport. Det anbefales lage to rapporter, én for ledelsen og én for ansatte som deltok i undersøkelsen.

Steg 4.1: Utarbeide en rapport for måling av sikkerhetskultur

Rapporten kan bli delt inn i seks deler: executive summary, bakgrunnen for undersøkelsen, metodikk, resultater, tolkning av resultater og anbefalinger. Executive summary er spesielt viktig fordi det fremhever den praktiske betydningen av funnene som er av største interesse for organisasjonen. Det bør inneholde følgende punkter:

- Hva ble gjort?
- Hvordan ble det gjort?
- Når var det gjort?
- Hvem og hvor mange respondenter var involvert?
- Hva ble funnet i undersøkelsen?
- Hva er konsekvensene av funnene i undersøkelsen?
- Hva anbefales videre?

Funnene fra undersøkelsen kan fremlegges til ledelsen som en presentasjon, eller på organisasjonens intranett. Det anbefales bruk av visuelle hjelpemidler for å fremme budskapet.

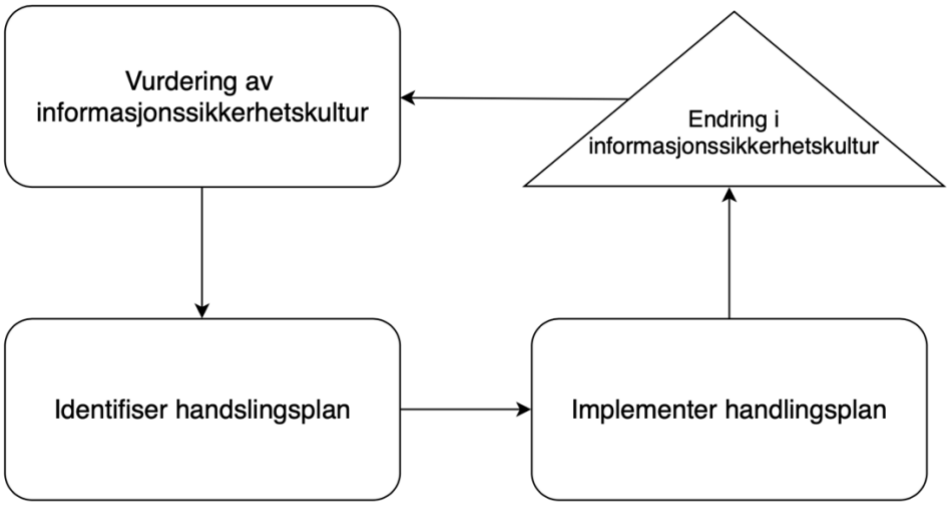
Steg 5: Utføre handlingsplan

Etter utført undersøkelse er det viktig å gå videre med handlingsplanene. Man finner ofte motstand ved å gjennomføre endringer, men det er svært viktig å utføre de handlingene som kan forbedre kulturen. Underveis i undersøkelsen er det viktig at alle involverte parter (steg 1.1) holdes oppdatert med utviklingen og at det fortsatt kommer positiv engasjement fra ledelsen. Man kan for eksempel gjennomføre en workshop der involverte parter møtes og funnene/resultatet fra undersøkelsen presenteres og handlingsplaner blir gitt til de som skal gjennomføre det.

Steg 5.1: Informasjonssikkerhet bevissthetskampanje

En måte å adressere funnene av undersøkelsen er å lage en bevissthetskampanje. En slik kampanje kan hjelpe med å bygge en god kultur og få riktige verdier opp på agendaen. Figur 1: 'Syklus for endringer ved informasjonssikkerhetskultur viser stegene som kan brukes for å adressere funnene.

Prosessen starter med en undersøkelse på informasjonssikkerhetskultur, der resultatet vil være handlingsplaner for spesifikke områder man ønsker adressere. For eksempel kan en handlingsplan være å informere eller kommunisere sikkerhetskonsepter til ansatte, forklare retningslinjer for sikkerhet eller gi bevisstgjøre for ansvaret gjeldende sikkerhet i organisasjonen. Handlingsplaner skal samles og være enkelt å slå opp i. Handlingsplaner blir gitt til individer for gjennomførelse og man må også bestemmer tidsfrister. Når handlingsplanene iverksettes må man også følge disse opp for å se om handlingsplanene fungerer. Over tid vil endringer oppstå ettersom ansattes bevissthet og forståelse for informasjonssikkerhet forbedres. Etterhvert ser man også endringer i kulturen; da er det viktig å utføre en senere undersøkelse for å se om endringene er positivt forbedret og om handlingsplanene var vellykkede. Man kan da sammenligne den første og den andre undersøkelsen for å få innsikt i utviklingen. Deretter kan man utarbeide nye handlingsplaner eller forbedre disse, og syklusen fortsetter.



Figur 1: 'Syklus for endringer ved informasjonssikkerhetskultur'

H Litteraturanalyse

Litteraturanalyse av rammeverk for måling av informasjonssikkerhetkultur

Joakim Ellestad, Anders Gustad, Magnus Lien Lilja, Espen Skuggerud

Litteraturanalysen er en rapport som tar for seg prosessen fra innhenting av rammeverk til diskusjon og sammenlikning av rammeverkene. Rapporten starter med en initiell vurdering opp i mot noen grunnleggende krav til rammeverkene. Disse kravene tar for seg blandt annet alderen og kredibiliteten til rammeverkene. Målet er å filtrere bort rammeverk som ikke er verdt å bruke tid på i en grundig analyse. Til den initielle vurderingen startet vi med syv rammeverk, hvorav tre av de passerte alle kravene og ble med videre til en dyptgående analyse. Sammenlikningsgrunnlaget i dypdykket er blandt annet diskusjon av hvilke egenskaper et rammeverk burde inneholde. Det legges spesielt vekt på ulike tilnærminger til måling og hvilke indikatorer som burde måles basert på analyse av ulike kilder. Disse egenskapene blir diskutert opp i mot hvert av de tre rammeverkene som kom videre fra den initielle vurderingen. Rapporten avsluttes med en diskusjon rundt styrker og svakheter hos de forskjellige rammeverkene.

Innhold

Figurer

Tabeller

1 Innledning

Denne rapporten er en analyse av eksisterende rammeverk innenfor prosessen med måling av sikkerhetskultur. Analysen gir en metodisk tilnærming for å sammenligne og veie opp rammeverk mot hverandre i forhold til gitte egenskaper og krav. I kapittel 2 settes de initielle kravene til rammeverkene. Disse kravene sørger for at rammeverket er opp til en viss standard, og vil utelukke de rammeverk som tydelig ikke er faglig dekkende. Videre gjøres deretter en grovanalyse for å se hvilke rammeverk som skal taes med videre til vurdering. Kapittel 3 prøver å fremme bestepraksis og tar med erfaringer fra eksperter innenfor området. Kapittelen tar for seg hvordan man måler, hvordan utføres målingen, hva skal man måle.
Videre, i kapittel 4, utvikles en kravspesifikasjon som gir føringen for hva oppdragsgiver ønsker seg. Dypdykket i kapittel 5 er en vurdering av de rammeverkene, som ble resultatet fra den initielle vurderinga, opp mot bestepraksis og kravspesifikasjonen. Kapittelet skal legge til rette for en diskusjon av rammeverkene og gi grunnlag for en utvelgelse.

2 Initiell vurdering

Dette kapittelet starter med noen initielle krav for rammeverket som helt grunnleggende settes som grovfilter. Grovanalysen vil gjennom hvert rammeverk drøfte de forskjellige rammeverkene opp mot de initielle kravene, og luke ut de som ikke støtter kravene.

2.1 Initielle krav for rammeverk

Ved det første steget i prosessen i å finne rammeverk for måling av sikkerhetskultur som kan benyttes for NTNU, så settes initielle krav. Initielle krav settes som en grovfiltrering for å luke ut rammeverk som ikke er verdt å gjøre dypdykk på. Krav på følgende punktliste sees på som essensielle da disse vil sørge for at rammeverkene er tilstrekkelig oppdatert, innehar tilstrekkelig kredibilitet og annerkjennelse og ikke bryter med sentrale reglement og politikk satt ved NTNU.

- Rammeverket/rapporten er et resultat av forskning fra anerkjente forskere i informasjonssikkerhetsmiljøet, eller har opphav i bedrifter som har godt renomé.
- Rammeverket/rapporten kan ikke være eldre enn 15 år.
- Rammeverket/rapporten har en logisk god struktur.
- Rammeverket/rapporten skal benytte refereranser og kilder.
- Rammeverkets utbytte må være under eierskap av NTNU.

Ved det første kravet vi ønsker å se på er kredibilitet. Om det gjøres funn ved at rapporten er støttet eller har sponsor, vil vi nevne dette. Man har også hatt i baktanken om resultatene brukt i rammeverkene er representative, og gjort en teoretisk triangulering ved å se på om teorien brukt er overenstemmende med annen teori. Kravet om alder er gitt med tanke på utviklingshastigheten på temaene relatert til IT og teknologi. Teknologi og IT er i stadig utvikling, og det er en felles observasjon at det har vært en kraftig økning i utvikling og framgang de siste årene. Likevel sees det på som interessant å se på noe eldre litteratur da det inkluderer sosiale aspekter, for eksempel organisasjonskultur, og teorien bak dette kan være like relevant i dag. Ved at rapporten følger en god struktur øker kredibilitet. Det anses som naturlig at en rapport følger en viss standard i forhold til vitenskapelig forskning, ved for eksempel at rapporten har en tydelig metode og teori slik at etterprøvbarhet er mulig. Ved referanser og kilder ønsker vi validitet. Vi ønsker at det finnes god forankring ved utsagn i en rapport, dette også for å sikre at premisser og utsagn er sanne. Til slutt settes det et krav om at informasjon og data som hentes ut av undersøkelsen ikke kan deles med tredjeparter. Dette kravet settes i henhold til NTNUs forpliktelser. Det vil si at informasjon ikke kan deles med tredjeparter eller andre enn eier av informasjon, i henhold til “Sentrale lover og forskrifter” på informasjonssikkerhetsområdet under NTNU’s Politikk for informasjonssikkerhet [3].

2.2 Grovanalyse

Grovanalysen vil ta for seg hver rapport ved innledende å vise en tabell med navnet på rapporten, forfatter, eventuelle medvirkende, hvem eller hvilke organisasjon som har publisert rapporten, når den er publisert, og hvilke bedrifter eller organisasjoner rapporten og rammeverket eventuelt har blitt utført på. Rammeverkene skal vurderes opp imot kravene, som er definert i seksjon 2.1. Vi tar også med andre mangler ved rammeverkene som ikke er definert i kravene. Ut i fra dette blir det bestemt om rammeverkene er verdt å bruke tid på i en dyptgående analyse.

2.2.1 SjekkIT

Navn	Informasjonssikerhet – atdferd, holdninger og kultur
Forfatter	Yngve Nordby, Christian Waale Hansen
Publisert	NTNU(ROSS)
Publikasjonsår	2005
Brukt av	NSM, Telenor, Rikstrygdeverket og Statens forvaltningstjeneste

Tabell 1: Rammeverk: SjekkIT - informasjon

Rapporten SjekkIT er skrevet i tilknytting til prosjektet *Informasjonssikkeret, Adferd, holdnigner og kultur*. SjekkIT fokuserer på et gjennomgående tema om å rette fokus mot menneskelige og organisatoriske faktorer i relasjon med sikkerhetsarbeid. Rapporten legger fram to bruksområder for *SjekkIT*. Én statistisk tilnærming for utbedring av sikkerhet knyttet opp i mot temaet og én hvor spørsmål kan brukes til å lede en gruppeprosess for bevisstgjøring og trening vedrørende sikkerhetskultur. Rapporten er et samarbeid og videreføring av et tidligere prosjekt mellom NTNU og NSM, gjennomført 2002-03. Arbeidet er utført ved Institutt for industriell økonomi og ledelse(IØT) og HMS med professor Jan Hovden som veileder. Noen sentrale siteringer og referanser er for eksempel, *Hearts and Minds* [4] og *Informasjonssikkerhet og innsideproblematikk* [5]. Rammeverket bygger på Scheins trenivåmodell av kultur [6].
Spørsmålskjemaet består av 30 grunnspørsmål og en tilleggspakke på 34 spørsmål med ulike temaer basert på hvilke målgruppe man ønsker å adresse. Temaene som adresseres er kunnskap og holdning, adferd, policy og ledelse, og revisjon. Man ønsker unngå 'Ja' og 'Nei' spørsmål og benytter derfor likert-skala[1]. Videre sier rapporten at hvis rammeverket brukes som et diagnoseverktøy må det være en kvantitativ tilnærming[2] med mange respondenter. Rapporten presenterer tre metoder for innehenting av data: webbasert spørrundersøkelse, papirbasert spørreundersøkelse og intervjuer. Rapporten fremstår som lettlest og har en veldig god struktur som gjør at det er lett å slå opp på ønskede steder. Rammeverket er 14 år gammelt og er på grensen til å ikke overholde alderskravet vi har satt. Totalt sett fremstår innholdet som troverdig. Rapporten viser til kilder og sentral teori i arbeidet med sikkerhetskultur. SjekkIT anses som tilstrekklig for videre vurdering etter kravene vi stiller i den initielle vurderingen.

2.2.2 The Security Culture Framework

Security Culture Framework kalles *Et åpent rammeverk for å bygge og vedlikeholde sikkerhetskultur i enhver organisasjon* [3]. Rammeverket er utarbeidet av Kai Roer, og det kan anses som nyere publikasjon da det er publisert i 2015. Roer har utgitt bøker og rapporter, holdt konferanser på sikkerhet og ledelse, og fått pris for sitt bidrag til å fremme sikker bruk av nettskytjenester av Cloud Security Alliance Norge. Selve dokumentet som omhandler rammeverket tar først for seg en mål-template, der man setter de initielle

[1] https://snl.no/Likert-skala - (01.04.2019)
[2] https://snl.no/kvantitativ - (01.04.2019)
[3] https://securityculturefreamework.net

Navn	The Security Culture Framework
Forfatter	Kai Roer
Publisert	Security Culture Framework Forum
Publikasjonsår	2015
Brukt av	N/A

Tabell 2: Rammeverk: The Security Culture Framework - informasjon

målte metrikker man ønsker adressere og sette tiltak på, og deretter ett SMART-basert[4] mål som du ønsker treffe. En annen mal/template tar for seg roller og rollers ansvar, som enkelt forklarer hvem som gjennomfører de forskjellige programmene som skal gjøres for å nå de SMART-baserte målene. Templaten "Audience Analysis" forteller hvordan identifisere forskjellige avdelingers mål. Dette for å lage aktiviteter som passer avdelingen best for å kunne oppnå målene, som gjøres gjennom en siste template som omhandler aktiviteter. Selve dokumentet til rammeverket sier lite om hvordan man skal gå frem for å bruke rammeverket. Det framstår som å følge en viss prosess, men det kan virke som om det er utelatt en større del av forklaringen rundt hvert steg i prosessen, som igjen gjør det vanskelig å gjennomføre stegene. Rapporten kan anses som tilstrekkelig da det referes til anerkjente personer på fagfeltet og brukes kjente publikasjoner for drøfting og argumentasjon. Dog anses det som vanskelig å se hvilke aktører som har benyttet seg av rammeverket. Ved gjennomgang av Security Culture Report 2018[7] ønskes det se på hvilke aktører som det er utført målinger på, men det gis ingen konkrete navn, bare hvilke sektorer som er målt. Aggregering av innhentet data er ikke omtalt i rammeverket, det er der CLTRe toolkit kommer inn i bildet. CLTRe toolkit er en SaaS for måling, vurdering og forbedring av kulturen [5].
Det finnes lite dokumentasjon om CLTRe-verktøyet, og det finnes ingen konkret forklaring i hvordan måling og vurdering gjøres i selve softwaren/SaaS løsningen. Ved konsultasjon med Roer, forfatter av Security Culture Framework, blir det forklart at softwaren vil gjøre selve målingen, men ulempen her er at softwaren selv ikke er fritt tilgjengelig. Ved eventuell kjøp av tjenesten vil man miste konfidensialitet ovenfor informasjon da dette deles utenfor eierskap med en tredjepart. Siden utbyttet vil deles med en tredjepart, støtter ikke bruk av Security Culture Framework de inititielle kravene om at utbytte ikke kan deles utenfor eierskap ved NTNU, og tas derfor ut av videre vurdering.

2.2.3 Understanding And Measuring Information Security Culture

Navn	Understanding An Measuring Information Security Culture
Forfatter	Mohammed Alnatheer, Taizan Chan, karen Nelson
Publisert	Pan, S & Cao, T (Eds.) Proceedings of the 16th Pacific Asia Conference on Information Systems (PACIS), 11 - 15 July, 2012, Vietnam
Publikasjonsår	2012
Brukt av	N/A

Tabell 3: Rammeverk: Understanding An Measuring Information Security Culture - informasjon

Rapporten sin abstrakt innleder med å si at hensiken er å utvikle et mål for måling av informasjonssikkerhet. Fordi rapporten er skrevet for en tidsskrift, som har forskere som målgruppe er det naturlig at rapporten har språk deretter, som gjør rapporten noe tunglest, men godt detaljert. Rapporten er skrevet av tre forskere fra Universitet for Teknologi i Australia. Alnatheer er tilknyttet institutt for informasjonssikkerhet, mens Chan og Nelson er tilnyttet fakultetet for forskning og ingeniørvitenskap. Rapporten ble

[4] S.M.A.R.T - Specific, Measurable, Achievable, Relevant, Time-Oriented
[5] https://get.clt.re/the-cltre-toolkit/

publisert i PACIS[6] som i følge Wikipedia er et anerkjent forum for forskere, industri og beslutningstakere for å utveksle forskningresultater og ideer om vedtak av ledende informasjonsteknologi og praksis. Chan har på Google Scholar[7] 2725 siteringer, mens de to andre ikke har har profil der. På researchgate har Nelson[8] 63 forsknings artikler, mens Alnatheer[9] har seks. Inntrykket er tilstrekkelig og gir god kredibilitet til videre arbeid med rapporten deres.

2.2.4 Cultivating and Assessing Information Security Culture

Navn	Cultivating and Assessing Information Security Culture
Forfatter	Adéle da Veiga, Jan Eloff
Publisert	(phd thesis)
Publikasjonsår	2008
Brukt av	N/A

Tabell 4: Rammeverk: A framework and assessment instrument for information security culture - informasjon

Dette rammeverket er en publikasjon som handler om å dyrke en informasjonssikkerhetskultur i en organisasjon, i tillegg til å illustrere hvordan man bruker den. Rammeverket er et resultat av Da Veiga sin forskning mot sin PhD grad hos University of Pretoria med Eloff som veileder. Eloff har en PdD i computer science. Da Veiga har pr. 08.02.19 blitt sitert i 1023 publikasjoner, mens Eloff har blitt sitert i 5165 utgivelser. Det gir god kredibilitet til forfatterne av rapporten. Rapporten presenterer tydlige steg for å ta i bruk rammeverket. Rapporten beskriver også en meget detaljert prosess for valg av teori bak rammeverket. Den tar utgangspunkt i Robbins [1] trenivå modell for organisasjonskultur kobinert med Schein [6] og har konkludert i 43 spørsmål for å kartlegge sikkerhetskultur. Basert på den initielle vurderingen regnes dette rammeverket som aktuelt for å ta med til videre vurdering.

2.2.5 Analyzing Information Security Culture

Navn	Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture
Forfatter	Thomas Schlienger, Stephanie Teufel
Publisert	14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.
Publikasjonsår	2003
Brukt av	Privat bank(Sveits) [2]

Tabell 5: Rammeverk: Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture - informasjon

Rapporten fra Schlienger og Teufel gir et innblikk i deres foreslåtte og testede metode for analyse av informasjonssikkerhetkultur. Teufel har på Google Scholar 1227 siteringer per 13.02.19 [10]. Schlienger er ikke oppført der, men har 228 siteringer på Researchgate [11]. Rapporten er ifølge Scholar sitert 107 ganger [12]. Dette viser at deres bidrag i

[6] https://en.wikipedia.org/wiki/Pacific_Asia_Conference_on_Information_Systems - 09.02.2019
[7] https://scholar.google.no/citations?user=HOuqDCIAAAAJ&hl=en&oi=sra - 09.02.2019
[8] https://www.researchgate.net/profile/Karen_Nelson20 - 09.02.2019
[9] https://www.researchgate.net/profile/Mohammed_Alnatheer - 09.02.2019
[10] https://scholar.google.no/citations?user=5L5ZJ-4AAAAJ&hl=en&oi=sra - 13.02.2019
[11] https://www.researchgate.net/profile/Thomas_Schlienger - 13.02.2019
[12] https://scholar.google.no/scholar?oi=bibs&hl=en&cites=4641101311271267346&as_sdt=5 - 13.02.2019

feltet har blitt brukt i annen forskning og artikler, dette gir grunnlag nok for å kunne stole på rapporten. Rapporten har god argumentasjon og kildebruk noe som gjør den svært attraktiv å arbeide videre med. Rapporten kan synes å være noe tynn når det kommer til detaljer rundt selve rammeverket og gjennomførelse. En rapport fra samme forskere er Schlienger and Teufel [2], den bygger videre på denne forskingen samt rammeverket [8]. Rapporten Schlienger and Teufel [2] viser rammeverket brukt i Sveitsiske Orange og konkluderer med at rammeverket oppnåde målene. Praktisk sett blir det vanskelig å bruke dette rammeverket da detaljer rundt det er spredd på to forskningsrapporter. Rapportene gir heller ingen direkte føringer og innebærer at vi må selv hente ut hvordan rammeverket fungerer i praksis. Dette kan resultere i feil bruk av rammeverket og kan gjøre resultat fra målingen ugyldig. Vi vil ikke arbeide direkte videre med denne, men det kan være nødvendig å bruke noe av dens teori.

2.2.6 Information security culture: A Behaviour Compliance Conceptual Framework

Navn	Information security culture: A Behaviour Compliance Conceptual Framework
Forfatter	Salahuddin Alfawaz, Karen Nelson & Kavoos Mohannak
Publisert	8th Australiasaian Information Security Conference (AISC) Brisbane Australia
Publikasjonsår	2010
Brukt av	N/A

Tabell 6: Rammeverk: Information security culture: A Behaviour Compliance Conceptual Framework - informasjon

Rapporten forklarer kompleksiteten av informasjonssikkerhet og hvordan dette arbeidet ikke ansees som komplett uten forståelse av menneskelige faktorene som adferd og holdninger. Spesifikt forklares det at ansatte som utøver kriminelle handlinger er rasjonelle med enten interne eller eksterne faktorer. Rammeverket baseres på Fishbein & Ajzens *Theory of Reasoned Action* som sier at individes handlinger og adferd er bestemt av individets intensjoner for dette [9].

Theory of Planned Behavior er en utvidelse av denne som korte trekk sier at hvor lett en prosess kan gjennomføres påvirker i stor grad ansattes adferd til denne [10]. Det er gjennomgående i rapporten at Security Awareness Training, forståelse for hvordan organisatoriske policyer og retningslinjer påvirker er avgjørende for hvor sårbar en prosess er og oppfattes av ansatte. Rapporten sier at *Fishbein* og *Ajzen* ikke knytter sikkerhetsarbeidet mot kultur, noe som denne rapporten ønsker å oppnå.

Videre forteller rapporten viktigheten av å kunne klassifisere individer inn i lovlige og ikke lovlige-handlinger ut i fra karekeristikka. Dette formålet er todelt. Den første delen omhandler å kategorisere et fenomen som "ikke-lovlige handlingerbidrar til å kunne systematisk identifisere og addressere disse handlingene. Den andre er at en slik klassifisering bidrar til at en organisasjon kan prioritere tiltak og innsats.

Rammeverket benytter videre studiet gjennomført av Petersons and Smiths model av nasjonal kultur som teorigrunnlag [11][12].

Når det gjelder forfatterene av rammeverket så har ingen av de bruker på Google scholar, men de har profiler på semantic scholar [13]. Det er en nettside som hjelper forskere å finne relevante publikasjoner med god kvalitet. Der har Salahuddin Alfawaz to publikasjoner med 69 siteringer, hvorav alle siteringene er fra dette rammeverket. Semantic scholar har en metode å kartlegge i hvor stor grad det har vært siteringer med høy

[13] https://www.semanticscholar.org/ - (10.04.2019)

påvirkning fra pulbikasjonen. Dette blir bestemt blant annet med machine learning [14]. Her har Karen Nelson 70 siteringer med høy påvirkning, som er et betydelig antall. Den siste forfatteren Kavoos Mohannak, har fem publikasjoner med fire siteringer med høy påvirkning. Samlet sett så har forfatterne liten kredibilitet.

Rammeverket har gode eksempler for å beskrive bakgrunnsteorien til rammeverket, men selve prosessen til rammeverket er lite dokumentert. Dette gjør at rammeverket er vanskelig å bruke og hovedgrunnen til at det ikke blir med i videre vurdering.

2.2.7 A comprehensive human factor framework for information security in organizations

Navn	A comprehensive human factor framework for information security in organizations
Forfatter	Areej Alhogail, Abdurrahman Mirza & Saad Haj Bakry
Publisert	Journal of Theoretical and Applied Information Technology
Publikasjonsår	2015
Brukt av	N/A

Tabell 7: Rammeverk: A comprehensive human factor framework for information security in organizations - informasjon

Rapporten sier at sikkerhetsarbeid ikke er komplett uten identifisering av menneskelige faktorer.Forfatter Areej Alhogail med 171 siteringer[15] og Saad Haj med Bakry 754[16], hennholdvis 8 og 7 for denne rapporten. Dette gir forfatterne noe kredibilitet. Rapporten bygger på Schneier [13],Da Veiga and Eloff [14] og Martins et al. [15] felles konklusjon om at menneskelig adferd er det det svakeste leddet i sikkerhetskjeden. Rapporten legger fram en model som addreserer de menneskelige faktorer som spiller inn og kan påvirke ansattes adferd innad i en organisasjon. Rapporten presenterer videre en måling av hvor godt mottatt dette rammeverket er. Denne målingen sier ingenting om hvem som har har vært med i undersøkelsen. Rapporten presenterer problemområdet svært teoretisk som viser kompleksiteten av temaet, men ingenting konkret om hvordan det skal løses i praksis og gjennomføres. Rapporten bygger på teori som er annerkjent, med sterke siteringer. Det som gjør at dette rammeverket ikke blir med til videre vurdering er at rapporten sier lite om prosessen rundt gjennomføring av målingen.

[14] https://www.semanticscholar.org/faq#influential-citations - (10.04.2019)

[15] https://scholar.google.com/citations?user=t7RwEfAAAAAJ&hl=en

[16] https://scholar.google.com/citations?hl=en&user=qXlxNWIAAAAJ&view_op=list_works&sortby=pubdate

3 Drøfting av egenskaper

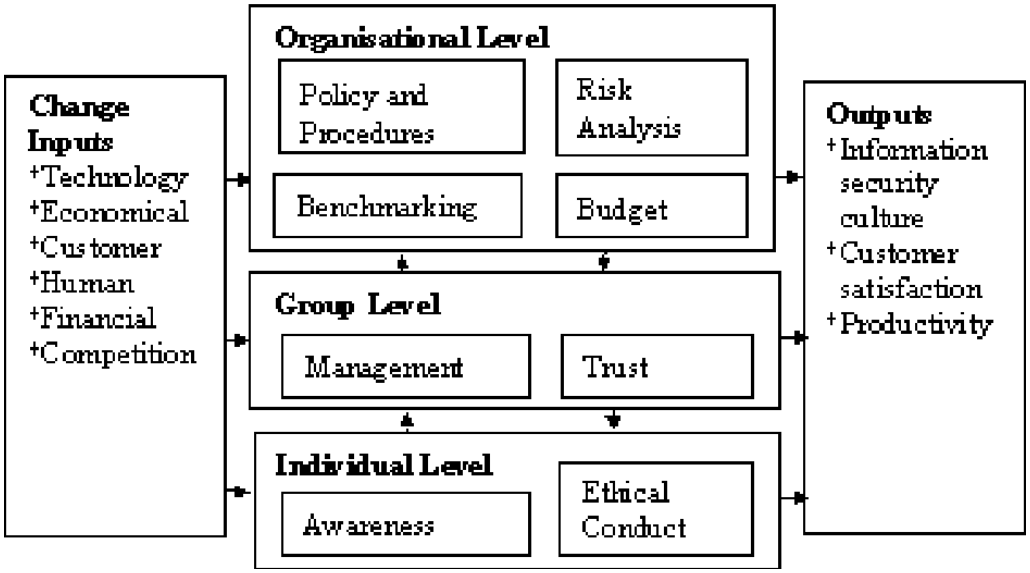
Det følger ingen suksesshistorie sammen med rammeverkene og det er dermed svært vanskelig å avgjøre om rammeverkets tilnærming til måling av sikkerhetskultur er god. Det blir da viktig å trekke fram litteratur som kan argumentere for metoder og tilnærminger som kan fremme eller trekke ned rammeverkene. Naturligvis blir det viktig å holde høy kvalitet på litteraturen for å få stor kredibilitet til deres konklusjoner. I dette kapitlet forsøker vi å dekke flere viktige temeaer som går igjen i rammeverkene og presenterer erfaringer og meninger fra ekspertene Bjarte Malmedal (NORSIS) og Roar Thon (NSM).

3.1 Hva skal måles

Et viktig element i utføringen av en måling er å ha gode indikatorer. Man bruker indikatorer for å angi eller beskrive forhold som er for kompliserte eller for kostbare å måle direkte [16]. Rammeverk kan ha egne indikatorer for sikkerhetskultur og det vil være viktig å velge de indikatorene som vil være best for NTNU.
Norsis [17] har basert sine indikatorer på de initielle forskningsspørsmålene. Indikatorene puttes sammen i en elektronisk spørreundersøkelse som skal gi et godt datagrunnlag for å besvare forsnkingsspørsmålene. Norsis påpeker viktigheten med å skille mellom adferdsel, f.eks. om en ansatt klikker på phising linker eller deler sine passord kontra deres sett med hodninger, verdier og følelser angående et spesifikt emne. Norsis konkluderte med åtte punkter som cyber sikkerhet består av; *collectivism, governance and control, trust, risk perception, techno-optimism and digitalization, competence, interest, behavior*
Schlienger and Teufel [2] har i sin forskning standardisert en spørreundersøkelse basert på en organisasatorisk adferdsmodell som deler adferd i tre deler; artefakter, felles verdier og grunnleggende antagelser og oppfatninger. Schlienger og Teufel mener for å kunne måle de verdiene med nagativ sosial reaksjoner må man skille mellom offisielle og sanne verdier. Spørsmålene ble formet utifra målet som settes, som i undersøkelsen var basert på sikkerhetsspolycien, intervju med CISO og en audit. Et eksempel spørsmål er vist i figur 2.
En annen modell er Robbins [1] trenivåmodell for organisasjonskultur, som deler kultur på tre nivåer: individuell, gruppe og organisatorisk nivå. Modellen brukes blant annet av Vroom and Solms [18] og Martins and Elofe [19], modellen er vist i figur 1
Deriverte spørsmål fra policy kan være uheldig å bruke da sikkerhetspolycier ofte er utdaterte og policien ikke nødvendigvis er en god policy D. Bjarte foreslår å heller benytte sikkerhetsansvarlig for å finne dagens ståsted.

Roer and Petrič [20, s. 16] ser også viktigheten av å måle de sanne verdiene og har utviklet sin modell med syv dimensjoner for å måle kultur: attitude, cognition, behavior, communication, norms, responsebility, compliance.

Det ser ut til å være god enighet at det må streves etter å måle de sanne verdiene og ansattes verdier og holdninger angående spesifikke emner. I utførelsen av dette er ulike modeller brukt. I litteraturen er modellen i figur 1 brukt mest. Det påpekes av [17, s. 29] at målingen må prøve å si noe om hva folk gjør eller vil håndtere en situasjon, ikke hvordan de tidligere har handlet. Det er også enighet i at målingen og modellen må utformes av føringer som sikkerhetspolicy eller fra sikkerhetsansvarlig.



Figur 1: [1] trenivåmodell for organisasjonskultur

***Table 2.* Example question**

2	The computer and electronic communications systems should be used for Orange's business activities only.			
	a) Personally I think, this is	True	False	I don't know
	b) Orange regards this as	True	False	I don't know
	c) If I were responsible, I would regard this as	True	False	I don't know

Figur 2: Eksempel spørsmål fra [2]

3.2 Tilnærming til måling

Det er to metoder for tilnærming til måling av sikkerhetskultur - kvalitativ og kvantitativ måling. Den kvantitative metoden handler, som tidligere nevnt i teorikapitlet, om kvantifiserbar informasjon, som for eksempel antall, frekvens og tid. Kvalitativ metode omhandler en skriftlig deskriptiv fremstilling av metrikker.

Vi ønsker å gjøre en undersøkelse på hvilke metoder og tilnærminger som blir brukt av forskjellige rammeverk og rapporter og hvorfor de forskjellige metodene er valgt. Dette for få en forståelse over en muligens anbefalt fremgangsmåte, og som også vil være en faktor til hvilke egenskaper et rammeverk burde inneholde.

Tool Supported Management of Information Security Culture bruker verktøy, eller software som aggregerer data, ser svakheter under en baseline og gir forslag til tiltak. Schlienger og Teufel mener at ved bruk av spørreundersøkelse burde man benytte verktøy for utdeling av undersøkelsen og aggregering av innsamlet data da det er mer tidseffektivt, og man trenger mindre resurser for å gjennomføre prosessen [2, 21]. De benytter seg av et standardisert spørreskjema basert på organisatorisk atferd som kategoriseres på organisasjon, grupper og individer, med spørsmål relatert til forskjellige områder som atferd og kommunikasjon og andre faktorer relevant innen organisatorisk kultur [2]. Siden organisasjoner og bedrifter er forskjellige ble det også rådet å implementere tilleggspørsmål eller forandre på spørreskjemaet, for å tilfredsstille forskjellige organisasjoner og bedrifters krav med tanke på deres forskjellige mål og målsetninger [2, chap. 4].

Martin og Eloff benyttet seg av spørreskjema i 'INFORMATION SECURITY CULTURE', som tok for seg spørsmål for å dekke sikkerhetsbevissthet på individuelt nivå, ledelse og tillit på gruppenivå, og policy og prosedyrer på et organisatorisk nivå. Disse for å få en indikasjon på sikkerhetskulturen på de nevnte punktene [22]. For å analysere den innsamlede dataen ble det brukt software for analyse og visuell fremvisning i form av en pre-etablert baseline og grafer som viste forbedringen eller forverringen av de målte faktorene.

Yngve Nordby og Christian Waale Hansen ved 'Informasjonssikkerhet atferd, holdninger og kultur' argumenterer at man ønsker mest mulig respondender som overhodet mulig når man ønsker samle inn data, for å få et bedre statistisk grunnlag [23, p.38]. Et større statistisk materiale gir bedre grunnlag for subjektiv hypotesetesting. De har tre metoder for innsamling av data; spørreundersøkelse, enten papirbasert eller web-basert, og intervjuer. Det forklares at at en web-basert undersøkelse vil være en god framgangsmetode om man ønsker nå større deler av en organisasjon og få ett mer helhetlig bilde av sikkerhetskulturen. Dette kan også sees som en ulempe ved at nyansene fra en avdeling til en annen falmer. Det gir også potensielt større ærlighet ved svar da man kan anomyisere svarene, men dette kan også gå begge veier [24]. En av fordelene ved å gjennomføre en slik undersøkelse ved spørsmål, er at man ønsker å få deltakerne til å reflektere over de gitte spørsmålene, får å få de til å tenke over ønsket atferd. Ved ett intervju gir det mulighet til utdyping av spørsmål og dermed gi økt bevissthet på forankring ved spørsmål og ønsket atferd [25]. Intervjurunder er ressurskrevende og gir et mindre statistisk grunnlag over samme tidsperiode man gjør undersøkelsen. Som nevnt mister man deltakere anonymitet, og svar gitt reflekterer ikke nødvendigvis da faktisk avgjørelser som gjøres i praksis [25, 24].

Flere større aktører har gjennomført kvalitative anayser av sikkerhetskultur. NORSIS [1] har i 2016, 2017 og 2018 gjennomført en undersøkelse hos forskjellige bedrifter og organisasjoner i Norge[2]. Disse ble gjennomført og målt ved kvalitativ analyse, der man benyttet standardiserte spørsmål, som gav tallbaserte svar med gjennomsnittsmåling som standardmål [26]. Ved å gjennomføre denne årlige målingen, kan man basert på gjennomsnittsmålingene som ble gjort, se hvorvidt det er en forbedring eller forverring på

[1] https://norsis.no
[2] https://norsis.no/nordmenn-og-digital-sikkerhetskultur-2018/

forskjellige målinger.

European Network and Information Security Agency (ENISA) sier i 'How to raise information security awareness'[27] at ved større selskaper ønsker man gjennomføre kvantitativ undersøkelse ved spørreskjema da dette skaper større statistisk grunnlag. Basert på budsjetter, hva en bedrift eller organisasjon arbeider med og størrelsen på organisasjonen, kunne det argumenteres for kvalitativ undersøkelse ved intervju, om det finnes hensiktsmessig. [27]

Ved bruk av spørreskjemaer er spørsmål gjerne fordelt på nivåer i forhold til organisasjonshierarki, da man ønsker på hvorvidt det er forskjeller på de nedre og øvre delene av hierarkiet [24]. Spørsmål lages og formuleres på en måte som avdekker individuelle holdninger, kunnskap om policyer og hvilke avgjørelser man tar i praksis.

For å sikre seg at innhentet informasjon er representativt på ett større basis, går det som en tommelfingerregel å ha minst fem ganger så mange svar i forhold til antall spørsmål i undersøkelsen. Dette for å sikre seg at informasjonen innhentet er representativt på ett større basis [14, 28].

Det diskuteres også hvorvidt menneskelige faktorer som påvirker sikkerhet kan måles kvalitativt. Alsaker (2004) mener Kufås og Mølmann (2003) ved utvikling av SjekkIT, at det er en svakhet rundt det å sette enkle spørsmål til respondender da de kan beskrive situasjoner feilaktig ved å fremstille en situasjon som annerledes enn faktum. Alsaker mener at det burde vurderes å benytte kvalitative metoder på grunn av dette. Samtidig påpekes det at målingsmetoden også burde være enkel og lite tidkrevende, dersom man ser behov for å gjøre periodvise målinger for best mulig oppfølging av endringer [29].

Ved en gjennomgang av undersøkelser og rapporter gjort på sikkerhetskultur gjennom årene, har undersøkelsene som går som de mest vellykkede og suksessfulle benyttet kvantitative målinger.

> "Quantitative research methods such as conducting surveys and the validation of frameworks and questionnaires have been deployed with great success in the information security discipline (Schlienger and Teufel, 2005; Straub et al., 2004; Straub, 1990; Workman et al., in press; Siponen et al., 2007; Woon et al., 2005)." [14, p. 71]

Ettersom de fleste studiene som tilsies som vellykkede har benyttet seg av kvantitative undersøkelser, så er det ikke forhåndsbestemt at sluttvurderingen vil benytte seg av kvantitativ undersøkelse. Punktene fra denne drøftingen taes med videre ved dypdykket som gjennomføres på rammeverkene som er i tråd med de intielle satte kravene under kapittel to.

4 Kravspesifikasjon

For å legge til rette for et godt sammenlikningsgrunnlag mellom rammeverkene, kreves det at vi har tatt høyde for eksterne krav, retningslinjer og regelverk på forhånd. Dette vil i tillegg til å sørge for at valgt rammeverk forholder seg til gjeldene anordninger også legge til rette for at rammeverket vi presenterer kan bli brukt aktivt innad i organisasjonen for å kartlegge sikkerhetskultur. I dette kapittelet presenteres det eksterne rammer og ønsker for hva et rammeverk skal oppnå og forholde seg til.

4.1 Krav fra oppdragsgiver

1. Rammeverket skal være lett å forstå for personale som ikke har erfaring fra denne typen kartlegginger fra før.
   Det er ikke et krav at en person uten noen kunnskap om cyber og informasjons-ikkerhetskultur skal kunne utføre målingen. Her menes det at rammeverket skal være entydig og lett å forstå for personer med noe IT relevant utdannelse. For å unngå at dette blir en subjektiv mening for den enkelte, skal vi se på i hvor stor grad rammeverket som vurdres forklarer begreper.
2. Fremgangsmetoden for målingen skal være tydelig.
   Her skal det vurderes i hvor stor grad av usikkerhet som foreligger rundt hva som er prosessen for gjennomføring av en måling med bruk av det aktuelle rammeverket. Målet er at fremgangsmåten skal være så tydelig forklart som mulig.
3. Ønskelig med kvalitativ tolkning av resultatet.
4. Lett å tolke resultat og komme med relevante tiltak.
5. Foreslå tiltak basert på alle faktorer resultatet av målingen resulterer i.
   Med dette menes det at rammeverket vi kommer frem til skal ha en tiltakspakke som henger sammen med styrker og svakheter som analysen av målingen fører til. I de avdelingene hvor kartleggingen blir gjennomført er det ikke sikkert at alle har de samme styrkene og svakhentene når det gjelder sikkerhetskultur. Derfor er det viktig og komme med forslag til tiltak på alle elementene som er resultatet av målingen, og ikke bare svakhetene etter den første målingen vi gjennomfører.

4.2 Lovpålagte retningslinjer

1. Anonymisering av resultat og måling. Det skal ikke foretas en granskning av enkeltpersoner, men være en helhetlig måling på avdelingsbasis. For å sørge for at dette blir ivaretatt skal en eventuell spørreundersøkelse være anonym i tillegg til å ikke inkludere for mange demografiske opplysninger, slik at man indirekte kan identifisere enkeltpersoner. [1]
2. Undersøkelsen skal ha klare rammer for hvilke opplysninger som er relevante å samle inn [1].

[1] https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/personvern-pa-arbeidsplassen/?id=1333 - 15.02.2019

5 Dypdykk

Dette kapittelet går dypere inn i hvert av rammeverkene som passerete den initielle vurderingen i kapittel 2. Her diskuteres hvor bra rammeverkene passer opp i mot kravene i kapittel 4. Det skal også vurderes hvor bra rammeverkene passer opp imot egenskaper diskutert i kapittel 3. Denne diskusjonen skal legge grunnlaget for å velge ut et passende rammeverk senere i litteraturanalysen. Dette kapittelet skal også diskutere og legge frem sterke sider ved hvert rammeverk. Det er ikke sikkert at vi ender opp med ett rammeverk som passer alle kravene og egenskapene vi ønsker. En vurdering av rammeverkets sterke sider skal gi oss et godt grunnlag for å tilpasse rammeverkene til et som passer for vårt scenario.

5.1 SjekkIT

5.1.1 Oppbygning

Hovedmålet med dette rammeverket er å tilby ett konkret verktøy som kan brukes for å måle en virksomhets sikkerhetskultur. Hovedsakelig er rammeverket bygd opp av en innledende del med ulike perspektiver på sikkerhetskultur, en teoridel og fremgangsmåte for utvikling etterfulgt av en gjennomgang av de konkrete bruksområdene til rammeverket. Målsetningene varier basert på bruksområdet til rammeverket, men det er i all hovedsak laget for å nå bredt ut til alle typer virksomheter. Prosjektet ble startet på bakgrunn av at NTNU og NSM ønsket å rette fokus mot sikkerhetskultur-relaterte problemstillinger. SjekkIT bygger på et tidligere samarbeid mellom NTNU og NSM hvor det ble utviklet et verktøy for å kartlegge holdninger, adferd og kultur i forbindelse med informasjonssikkerhet [5]. Dette var igjen en rapport som baserte seg på et verktøy som heter "*Hearts and minds*" [4]. Shell tok i bruk dette rammeverket allerede i 1986 og beskrier en markant positiv effekt frem til 2001. SjekkIT er bygget videre på punkter som Kufås og Møllmann mente kunne forbedres [5]. Disse punktene har dannet grunnlaget for utviklingen av sjekkIT og blir konkretisert videre i rammeverket. Senere ble disse punktene utbedret og presentert på et arbeidsseminar der hvor oppdragsgivere, brukere, fageksperter og potensielt nye brukere var til stede. Hovedinnspillene herfra ble tatt med videre i utviklingsprosessen. Verktøyet sjekkIT baserer seg i stor grad på Schein trenivåmodell av kultur [6] og har spesielt fokus på de to øverse nivåene. Rammeverket har to konkrete bruksområder, med forskjellige målsetninger.

1. **Diagnoseverktøy** Her er målsetingen å måle tilstanden til virksomhenten i tillegg til å avdekke sterke og svake sider. Dette skal ligge til grunn for målrettede tiltak. Denne prosessen starter med en kvantiativ datainnsamlingsmetode, etterfulgt av en statistisk analyse av resultatene.
2. **Forbedringsverktøy** Den andre metoden brukes for å bygge sikkerhetskultur. Det gjøres ved å arrangere en workshop/søkekonferanse. Datainnsamlingen foregår på samme måte, men flere parter deltar for å analysere resultatet og komme med forbedringer og tiltak som kan bedre sikkerhetskulturen. Her er målsetningen å gi grunnlag for diskusjon rundt sikkerheten og problemområder.

5.1.2 Indikatorer

Indikatorene som ligger til grunn for spørsmålene brukt i SjekkIT er: kunnskap og holdning, atferd, policy og ledelse, revisjon. De fire indikatorene er utviklet gjennom et arbeidsseminar med eksperter på området. Indikatorene er noe likt det NORSIS [17] har

konkludert med er kjernene i sikkerhetskultur er. Blandt annet kan kunnskap, holdning og adferd relateres til det NORSIS sier om *competence* og *behavior*. Slik som Schlienger and Teufel [2], Vroom and Solms [18] og Martins and Elofe [19] har også SjekkIT brukt Scheins trenivåmodell for kultur. SjekkIT har fokus på de øverste delene av modellen, de forsøker ikke å avdekke de underliggende verdiene, men fokuserer på rutiner og adferd(det synlige). De antar dermed at endring av rutiner og adferd kan påvirke holdninger og dermed også påvirke organisasjonsspesifikke verdier slik at de på sikt ligger til grunn for atferden.

5.1.3 Tilnærming til måling

SjekkIT har utviklet spørsmål for å avdekke sikkerhetskulturen. Svaralternativene på hvert spørsmål er delt i fem deler, som kan overføres til en likert skala fra en til fem. Tre av svaralternativene har tekst som beskriver hva det nivået er. Skalaen gir ikke indikasjon på at fem er mer rett enn en og deltaker på dermed lese alle alternativene før besvarelse gis.
SjekkIT gjennomføres som en statistisk/kvantitativ undersøkelse [23, s. 36]. Rammeverket påpeker at man må være forsiktige og ikke dra bastante slutninger dersom man har en ensidig kvantitativ tilnærming. Det ble konkludert med i kapittelet om måling 3.2 at kvantitative undersøkelser er mest utbredt og kanskje mest suksessfullt også. Dette trygger SjekkIT sin bruk av denne tilnærmingen.

Om SjekkIT brukes for å bygge sikkerhetskultur med bruk av workshop/søkekonferanse blir resultatet fra målingen tolket kvalitativt av deltagerne. Tolkningen ligger til grunn for utarbeidelse av forbedringsområder og tiltak.

5.1.4 Kravspesifikasjon

I Listen under beskrives det hvordan sjekkIT stiller seg opp imot krav fra 4.1. **Krav fra oppdragsgiver**

- 1. SjekkIT har gode oppdelinger og forklarer godt utførelsen begreper og teorier.
- 2. SjekkIT viser klare fremgangsmetoder og bruksområder for gjennomføring.
- 3. SjekkIT presenterer to fremgangsmetoder for rammeverket. Tolkningsmetoden avhenger av hvilken fremgangsmetode man velger.
- 4. SjekkIT kategoriserer spørsmålene slik at det er muligheter for å analysere resultatet og knytte det opp mot en indikator. Ut i fra denne indikatoren er det muligheter for å finne relevante tiltak spesifike for kategorien. SjekkIT spesifiserer ingen prosess for dette
- 5. SjekkIT har ingen tiltak direkte knyttet opp mot kategoriene eller spørsmålene i dem. Om SJekkIT brukes for å bygge sikkerhetskultur vil tiltak og forbedringer utarbeides med deltagerne i workshop/søkekonferansen.

Lovpålagte krav

- 1. SjekkIT samler inn flere demografiske data som i enkelte tilfeller der det er stor ulikehet i demografien kan være med på å peke ut enkeltpersoner. F.eks. er alder, kjønn, ansettelsesforhold og antall år i virksomheten med på å peke ut enkeltpersoner og responsen fra noen av gruppene skiller seg ut.
- 2. SjekkIT sier ingenting om bakgrunnen for demografiske data, men de benyttes for å kunne gi målrettede tiltak og forbedringsprosesser mot enkeltgrupper i organisasjonen.

5.1.5 Styrker

I listen under presenteres det styrker ved sjekkIT.

- SjekkIT er en forbedret utgave fra et tidligere arbeid.

- SjekkIT er utviklet i sammarbeid med NTNU, NSM og SINTEF
- Veldig godt dokumentert og lett å forstå

5.1.6 Svakheter

I listen under presenteres det svakheter ved sjekkIT.

- Favner ikke alle typer ledelsesperspektiver: har fokus på byråkratiske ledelsesstrukturer [23, s. 9]
- SjekkIT synes å konkludere for mye i svaralternativene
- Sier lite om analyse av innsamlede data

5.2 Understanding And Measuring Information Security Culture

5.2.1 Oppbygning

Målet med dette rammeverket er å utvikle en måling av informasjonssikkerhetskultur. Forfatterne hadde en foregående litteraturanalyse som kom frem til at det mangler et skille mellom faktorer som er med på å danne sikkerhetskultur og faktorer som påvirker sikkerhetskultur. Forskjellen mellom disse faktorene går igjen som en hovedtilnærming gjennom hele rapporten. I deres definisjon av sikkerhetskultur bruker de en kombinasjon av definisjoner fra flere rammeverk. De trekker frem at sikkerhetskultur er en subkultur som støtter tekniske sikkerhetstiltak, og at det er viktig med god sikkerhetskultur som en naturlig del av den daglige arbeidsaktiviteten. De trekker spesielt frem at ingen av definisjonene fra litteraturanalysen sier noe om hva som danner og påvirker sikkerhetskulturen. I utformingen av spørreundersøkelsen bruker de en 5 nivå likert-skala fra svært uenig til svært enig. Uformingen av denne er basert på tidligere forskning for å sørge for validitet. Det er lagt stor vekt på spørreundersøkelsens gyldighet. Det ble brukt et ekspertpanel for å vurdere spørsmålene, etter metodikk fra [30]. Avslutningsvis presenterer rapporten funnene fra spørreundersøkeksen, og en forklaring på hvordan de har tolket dataene statistisk.

5.2.2 Indikatorer

Basert på åtte intervjuer fra åtte forskjellige organisasjoner, samt på bakgrunn av eksisterende litteratur kom de frem til indikatorer som er med på å danne og påvirke sikkerhetskulturen. Her ble hovedsakelig informasjonssikkerhetsledere og eksperter intervjuet fra alle typer organsiasjoner. Både privat og offentlig sektor, med organisasjonsstørrelse fra 100 - 3100 ansatte og ulike typer industri. Det er vanskelig å avgjøre om disse indikatorene er bedre egnet for NTNU enn andre. Indikatorene er *Top Management Involvement In information Security*, *Information Security Policy Enforcements*, *Information Security Training*, *Information Security Awereness*, *Information Security Ownership*. Indikatorene er ulikt det som tidligere er nevnt i seksjonen om hva som skal måles 3.1. Indikatorene fokuserer mye på retningslinjer, policy og mangler indikatorer for selve kulturen. Spørsmålene derivert fra indikatorene prøver i stor grad å avdekke svakheter ved sikkerheten og hvordan praksisen rundt informasjonssikkerheten er. Indikatorene måler ikke de sanne verdiene til ansatte noe som er nevnt i seksjon 3.1 at er en viktig del.

5.2.3 Tilnærming til måling

Utførelse av målingen er basert på en kvantitativ tilnærming lik andre 3.2. Undersøkelsen bearbeides med en statisktisk analyse. Det ble brukt en kvantitativ tilnærming ved utarbeiding av indikatorer, men dette har lite å si når selve undersøkelsen analyseres kvalitativt.

5.2.4 Kravspesifikasjon

Under beskrives det hvordan rammeverket stiller seg opp mot krav fra kravspesifikasjonen 4.1.

Krav fra oppdragsgiver

- 1. Rapporten forklarer i liten grad begreper som ikke er innlysende at leseren skal kunne. Spesielt i Kapittel 5 *Model testing*, som handler om validering, brukes det mange statistiske uttrykk som ikke er evidente. Denne publikasjonen var originalt publisert til en konferanse for forskere, 'PACIS' [1]. Da er det naturlig at målgruppen allerede innehar en form for relevant bakgrunnskunnskap. Basert på dette virker det som om rapporten fremlegges på en måte hvor det regnes med at leseren allerede innhar en viss kompetanse om emnet.
- 2. Rammeverket gir ikke en god fremgangsmåte for hvordan det kan brukes. Det foreligger ingen klare retningslinjer som tar for seg forbredelse til tolkning av data.
- 3. Rammeverket utfører en kvantitativ måling og tolkning av resultatet.
- 4. Dette rammeverket presenterer ikke en tiltakspakke for resultatene av målingen. Målet med dette rammeverket var å måle informasjonssikkerhetskulturen. Tiltak blir derfor utenfor dette rammeverkets omfang.
- 5. Rammeverket har ingen tiltak eller forbedringsprosesser som kan iverksettes.

Lovpålagte krav

- 1. Rammeverket sier ingenting spesifikt om hvilke demografiske data som skal samles inn. Fra statistikk fra undersøkelsen kan det forstås at organisasjonstype, organisasjonstørrelse, deltaker sin alder og type industri ble samlet inn.
- 2. Rammeverket gir et godt grunnlag for hvilke spørsmål som brukes/er utformet og deres relevans.

5.2.5 Styrker

Avdelingsstørrelsen og type arbeidsområde for avdelingene på NTNU varierer mye. Det er derfor viktig å ta høyde for dette i rammeverket. I forskningen som denne rapporten bygger på har de stor variasjon i demografien, og da spesielt antall ansatte, type sektor og industri. Dette er svært positivt med rammeverket og gjør det bedre egnet for bruk på NTNU. Sørsmålene i rammeverket har også konkrete kilder i fra hvor de er hentet.

5.2.6 Svakheter

En stor svakhet ved rammeverket er at det er vanskelig å forstå bruken av det. Siden det er tenkt at rammeverket skal kunne bli brukt senere for måling av sikkerhetskultur på NTNU, så er det viktig at det er enkelt å bruke for å sette igang en kartleggning. En annenn negativ side er at vi oppfatter spørsmålene som veldig ledene. Med dette menes det at det er lett å forstå hva som er det riktigesvaret på spørsmålet. Dette kan føre til at respondentene velger det som er riktig svar istendenfor det som er dens reele oppfatning.

5.3 Cultivating and Assessing Information Security Culture

5.3.1 Oppbygning

Hovedformålet med dette rammeverket er fremme og forbedre sikkerhetskulturen hos en organisasjon, og illustrere på hvilke måter man kan gjøre dette. *Cultivating and Assessing Information Security Culture* starter med å introdusere viktigheten med god sikkerhetskultur da en viss sum av tapte fortjenester skyldes interne hendelser utført av ansatte, både utilsiktede og tilsiktede. Det påpekes at man bør addressere tiltak som tar for seg flere kontroller som fremmer god atferd, og ikke bare addresserer det tekniske; derav

[1] https://aisel.aisnet.org/pacis/ - 19.02.2019

skape en god sikkerhetsbevisst kultur. Man ser på alle komponenter, både tekniske, prosedyriske og menneskelig atferd og holdninger. Det forklares at organisatorisk kultur og organisatorisk atferd er grunnleggende for sikkerskultur, og de følger Scheins trenivåmodell basert på individell-, gruppe- og organisatorisk nivå [6].

Det diskuteres nyere forskning og studier, der det tas eksempler fra kjente studier og ved hvilke styrker og mangler de har. Eksempelvis nevnes det hvordan nåværende forskning gjerne foreslår tiltak som går på bevisstgjøring og opplæring av sikkerhet for ansatte, men at det ikke fokuseres på faktisk atferd og holdninger. Hovedsaklig poengteres det at forskning og studier mangler å integrere organisatorisk kultur og atferd med informasjonssikkerhet, for å kultivere en forandring på Scheins trenivåmodell.

Det gjøres en teoretisk forklaring av organisatorisk kultur og dens sammenheng med sikkerhetskultur. Samtidig brukes komponententer fra Scheins trenivåmodell, der man forklarer hvordan disse påvirker hverandre og til hvilken grad. Det forklares hvordan organisatorisk struktur varierer fra en organisasjon til en annen, i forhold til organisasjonens grad av sentralisering og formalitet på "hvordan ting er gjort innad organisasjonen", og derav forholde seg til dette når man addresserer sikkerhetskulturen en organisasjon for å gjøre korrekte tiltak med sikkerhet og brukervennlighet i balanse. Det adresseres til forskjellige studier tidligere gjort av eksperter angående hvorfor adressere sikkerhetskultur og hvorfor temaet er viktig, der det går igjen at dårlig kultur kan resultere i økomiske tap, tap av omdømme eller lignende.

Det sees på forskjellige studier og undersøkelser gjort av ulike eksperter som anses som fremtredende innen fagfeltet ved hvordan disse definerer ulike begreper og hva disse legger vekt på i målingen av sikkerhetskultur. De mest essensielle punktene angående hva som er viktig å måle taes med videre, validitetstestes og benyttes som ankerpunkt i spørreundersøkelsen som blir utviklet i rammeverket. Det sørges for at grunnleggende begreper er tydeliggjort før man taes i gjennom prosessen for utvikling av rammeverket.

Komponenter i en organisasjon, eksempelvis policy eller bevisstgjøring av sikkerhet for ansatte, blir valgt ut i fra kjente kilder som tar for seg informasjonssikkerhet, ala ISO-standard, ISF [2] og flere. Hver komponent forklares med hvordan påvirkning disse har på kultur, og er nødvendig i rammeverket.

Ett eget kapittel definerer rammeverket som skal brukes. Det gir en stegvis forklaring av hvordan komponenter påvirker atferd, som igjen utvikler sikkerhetskulturen innad en organisasjon. Neste kapittel fokuserer på prosessen for å vurdere sikkerhetskultur. Prosessen presenteres stegvis og forklarer involveringen av interessenter, validering av komponenterer som bør analyseres og pålitelighetstesting av disse komponentene. Det gjøres en vurdering av positive og negative sider ved forskjellige undersøkelsesmetoder, og vises til tidligere kjente eksperters undersøkelser og resultater av disse. Det forklares hvordan språkformulering burde gjøres i forhold til respondenters bakgrunn i organisasjonen eller bedriften, og stegvis hvordan utvikle analysen, hvordan formidle den, hvordan samle og analysere innhentet informasjon. Det vises også hvordan gjenomføring av pålitelighet- og validieringstester i forhold til å se hvorvidt innhentet data er representativt og danner ett korrekt bilde på kulturen, og også hvordan dette burde drøftes innad i organisasjonen, om ansatte og ledelesen kjenner seg igjen i statistikken. Det illustreres også tiltak og hvordan man gjør disse, basert på de svakeste punktene man adresserer innad organisasjonen. Hele prosessen vil omtales som ISCULA (Vedlegg C) som forklarer hvert steg i prosessen fra planlegging av måling til sluttrapportskriving og innføring av tiltak.

5.3.2 Indikatorer

Sikkerhetskultur blir blant annet definert her som hvordan ting er gjøres innad en organisasjon for å beskytte den informasjon de innhar, og at kulturen baseres på organisatorisk

[2] https://www.securityforum.org

kultur. Bedring av kulturen menes å gjøres gjennom å øke bevisstheten på ansattes interaksjon med sikkerhetskontroller, og at disse kontrollene adresser alle typer kontroller - ikke bare tekniske. Rammeverket adresserer tekniske, prosedyriske og menneskelig atferd som komponenter innad informasjonssikkerhet, som påvirker sikkerhetsatferd og deretter utvikler sikkerhetskultur.

Det uttrykkes at organisatorisk kultur har stor påvirkning på en organisasjons prestasjoner, og at atferd kan utvikles og sees på tre nivåer; individuell-, gruppe-, og organisatorisk nivå [1].Det vises i en oversikt hvordan sikkerhetskomponententer påvirker atferd i forhold til informasjonssikkerhet på de tre nivåene, og hvordan disse over tid utvikler kulturen og hvordan ting er gjort innad en organisasjon, som igjen kan sees på artefakter, normer og verdier og grunnleggende antakelser, da Scheins modell.

Ved å fusjonere *Robbins* og *Shein* identifiseres syv kategorier som hver inneholder forskjellige komponenter, som kan klassifiseres på organisatorisk, gruppe eller individuellt nivå i forhold til påvirkining til atferd. Disse igjen reflekteres i Scheins modell på artefakter, verdier og grunnleggende antakelser. Ved klassifisering kan man måle spesifikt opp i mot den enkelte komponent, og derav målrettet addressere tiltak opp i mot komponenten. Figuren [Fig.5.3 14, p. 97] viser de hvordan forskjellige sikkerhetskomponentene påvirker atferd på de strukturelle nivåene, og dermed fører til kulturell utvikling som igjen kan sees på Scheins-modellen.

5.3.3 Tilnærming til måling

Det benyttes syv kategorier, med spørsmål knyttet til underkategorier som eksempelvis går spesifikt på risk management eller policies. Disse kategoriene er analysert i rapporten, og også ved tidligere undersøkelser for pålitelighet og validitering. Det vises ved målinger av eksperter og bruk av Chronbachs alpha for pålitelighetstester av komponentene, og det gis uttrykk for at komponentene er gode for å kunne adressere sikkerhetskultur.

Spørsmålene er formulert som påstander, der man svarer på en skala fra én til fem, der én indikerer sterk uenighet til påstanden, og fem indikerer sterk enighet. En subkategori stiller tre påstander som gir en påstand gitt i uttrykk av hva som er kandidatens tanke om påstanden, hva kandidaten tror organisasjonens fellestanke er om påstanden, og en tredje påstand som gir en påstand om beste løsning.

Det refereres til en undersøkelse der SurveyTracker [3] er brukt for utdeling av spørreundersøkelsen og innsamlingen av data. Det vises til at ved statistisk analyse behøves minst fem ganger antall respondenter i forhold til antall spørsmål i undersøkelsen. Det fremvises ingen statistisk analyse av noe innhentet data, ei heller noen forklaring på hvordan dette skal eller burde gjøres, som sees på som en mangel i rapporten.

5.3.4 Kravspesifikasjon

I listen nedenfor beskrives det hvordan rammeverket stiller seg opp imot krav gitt i kapittel 4. **Krav fra oppdragsgiver**

1. Rapporten gir gode forklaringer på nødvendige begreper og indikatorer som blir benyttet.
2. Rammeverket gir gode retningslinjer for bruken av rammeverket.
3. Rammeverket gir gode retningslinjer for kvantitativ statistisk analyse. Rammeverket støtter ikke bruken av kvalitative metoder [31, kap. 7, s. 160]. Rammeverket gir forslag til bruk av fokuse grupper for å bekrefte resultat hvor et statistisk representabelt svar ikke ble oppnådd.
4. Rammeverket har eksempler for å tolke resultatet og viser til tiltak som kan iverskettes.
5. Rammeverket gir ingen konkret tiltakspakke for resultatet av målingen.

[3] http://surveytrackersoftware.com

Lovpålagte krav

1. Rapporten forteller ikke noe om demografi eller anonymitet ved spørreundersøkelser som kan negativt identifisere enkeltpersoner og bryter derfor ikke med Norsk personvern 1
2. Rammeverket har retningslinjer for hvilke demografiske data den samler inn og hvordan de brukes i analysen.

5.3.5 Styrker

- NTNU benytter og identifiserer organisasjonskultur i dag med den samme teorien og tilnærming som rammeverket diskuterer[4]
- Fusjonering av *Schein*[14] og *Robbins* teori[1] presenterer syv komponenter som gir et godt overblikk om hvordan Informasjonssikkerhet påvirker adferd som igjen kultivereres inn i en organisasjonskultur.
- Rammeverket benytter kvantitativ tilnærming for måling. Det er generel enighet for denne metoden uavhengig av forfattere innad miljøet [24, 32]

Rammeverket inneholder en god forklaring på fremgangsmåten; prosessen for hvem å involvere, hvordan utforme spørreundersøkelsen, inkludert utdeling og analyse av data, og til slutt implementere og utføre tiltak. Teoridelen er godt forklarende, og det er med andre ord ikke nødvendig med dyp bakgrunnsforståelse til temaet for å få god nytte av sikkerhetsvurderingen. Det gies eksempler på kvalitative tolkninger av den statistiske analysen, og gjør det lett å forstå hvordan man skal implementere løsninger og tiltak til undersøkede påstander som får svakt resultat. Motpoler i den målte statistikken settes opp i mot hverandre på en visuell måte slik at man lett ser hvilke påstander som stiller svakt og derfor kan addressere spesifikke sub-komponenter og arbeide på tiltak til disse. Helhetlig stiller rammeverket sterkt på krav fra oppdragsgiver og utfører de fleste punkter i henhold til bestepraksis når det gjelder utføring av vurdering av sikkerhetskultur.

5.3.6 Svakheter

- Det kan drøftes og konkluderes som en svakhet av enkelte eksperter da man ikke benytter seg av noe kvalitativ undersøkelse, men det drøftes i rapporten og gies gode grunner til at kvantitativ måte er bedre løsning og har flere positive sider sammenlignet med kvantitativ undersøkelse. Eksempelvis er statistisk robusthet, nøyere måling av data og forandring av kultur over tid, og faktum at det er mindre tidkrevende og derfor også en mer kosteffektiv løsning [14, p.105].
- Det gies ikke en spesifikk tiltakspakke, men dette sees ikke på som en stor svakhet i seg selv da rapporten forklarer hvordan adressere de svakeste påstandene som blir funnet i undersøkelsen og gir eksempler på hvordan tiltak kan settes på disse. Det gies altså spillerom for resultatanalyse, og rom for drøfting mellom ledelsen angående eventuelle tiltak som bør settes inn for forbedring.

Det er drøftet om kvalitativ undersøkelse er nødvendig for analyse av sikkerhetskultur, men det sees ikke på som grunnleggende etter studier av tidligere undersøkelser og ekspertuttalelser med betydning for emnet. Det kunne ønskes en tiltakspakke for enkelhets skyld, der det er gitt spesifikke tiltak basert på komponenterer man adresserer seg svak på, men dette er etter omfattende studier ikke typisk i rammeverk, da det avhengir av type organisasjon eller bedrift. Det er vanskelig å spesifikt adressere generelle tiltak som skal kunne dekke alle og enhvers behov, dessuten omfattende å legge ved; det konkluderes som tilstrekkelig å gjøre en intern drøfting av statistikk, internt hos ledelsen og utvikle tiltak basert på signifikans, risiko og andre faktorer som er ønsket påvirket ved å sikkerhetskulturvurderingen.

[4] https://innsida.ntnu.no/wiki/-/wiki/Norsk/Organisasjonskultur+-+for+ledere

5.4 Oppsummering og Diskusjon

I denne seksjonen sammenliknes rammeverkene fra dypdykket (se kapittel 5). Det sees på de ulike rammeverkenes sterke og svake sider i tillegg til å se hvordan de stiller seg opp imot krav fra kravspesifikasjonen (se kapittel 4). I denne seksjonen blir navnene til rammerkene forkortet til fordel for økt lesbarhet. Forkortelsene som blir brukt er som følger:

- **SjekkIT** - Informasjonssikkerhet: atferd, holdninger og kultur
- **UMISC** - Understanding and measuring information security culture
- **ISCF** - Cultivating and Assessing Information Security Culture

Krav	**SjekkIT**	**UMISC**	**ISCF**
Inget krav om forkunnskaper før gjennomføring	X		X
Tydelig fremgangsmetode	X	~	X
Benytter kvalitativ tolknings metode	~		
Lett å tolke data og å foreslå tiltak	X	X	X
Tiltak basert på resultat av undersøkelse			
Anonymisert resultat og måling			
Klarhet i hvilke opplysninger som er relevant å lagre	X		~

Tabell 8: Oppsummering av krav for rammeverkene

Tabellen oppsummerer vår gjennomgang av utvalgte rammeverk. Som tabellen beskriver, så finnes det i dag ikke ett rammeverk som oppfyller alle våre krav. Dette har direkte årsak med at rammeverk i seg selv er definert ulikt og derav ulik målsetninger for hva rammeverkene skal oppnå.

Disse kravene gir oss bare en liten pekepin på hvordan rammeverkene stiller seg opp mot hverandre ut i fra noen av kravene vi har satt. Det at et rammeverk ikke oppfyller et krav betyr ikke at det blir utelukket. Flere av kravene er noe rammeverket eller rapporten ikke sier noe om spesifikt, men kan tilpasses i etterkant. Dette gjelder for eksempel "*Anonymisert resultat og måling*". Her kan man lett tilpasse kravet i etterkant ved å gjennomføre målingen på en tilfredstillende måte, selv om rammeverket ikke sier noe om dette.

SjekkIT og ISCF oppfyller de samme kravene ut ifra kravspesifikasjonene. De har begge en gjennomgående tydeling og lett forståelig prosess. UMISC har en noe mer utydlig prosess og er relativt tunglest dersom man har lite forkunnskaper i cyber. Ingen av rammeverkene sier noe om tiltak eller hvordan man kan tolke resultatene for å lage relevante tiltak. Dette kommer også an på målsetningen til rammeverkene. Man er ikke nødt til å gjennomføre en måling for å komme med tiltak og derfor dette ofte to separate prosesser.

Når det gjelder tolkningsmetoden for resultatet av målingen som rammeverkene beskriver benyttes det stort sett en kvantitativ tilnærming. SjekkIT presenterer to bruksområder ved rammeverket: *diagnoseverkøy* og *forbedringsverktøy*. Dersom man velger å bruke sjekkIT som et diagnoseverkøy får man en kvantitativ tilnærming til resultatene hvor man bruker gjennomsnitt. Velger man å bruke sjekkIT som et forbedringsvertøy, får man en mer kvalitativ tolkning av resultatene ved at man skaper diskusjon rundt tallene fra målingen. ISCF og UMISC presenterer rene kvantitative tolkninger. Dette kan gjøres til en litt mer kvalitativ prosess ved at man er kristiske til resultatene fra målingen og bruker de som et diskusjonsgrunnlag innad i avdelingen.

Det er en utfordring å kombinere rammeverkene. Dersom man tar de alle de sterke sidene fra hvert rammeverk og setter de sammen til et rammeverk er det fare for at rammeverkene mister hensikten. Som et ytterpunkt kan man si at hele rammeverket, med all teorien rundt, ender opp i en spørreundersøkelse. Dersom man forandrer på hele eller deler av undersøkelsen ved at man kombinerer med spørsmål fra et annet

rammeverk vil man kunne stå i fare for å miste deler av teorien og dokumentasjonen bak spørsmålene.

Bibliografi

[1] Stephen P. Robbins. *Organizational Behavior*. Prentice Hall, 2001. ISBN 9780130184191. URL https://books.google.no/books?id=fEPUIjNddhUC.

[2] Thomas Schlienger and Stephanie Teufel. Tool supported management of information security culture. In *IFIP International Information Security Conference*, pages 65–77. Springer, 2005.

[3] NTNU. Politikk for informasjonssikkerhet. 2018. URL https://innsida.ntnu.no/wiki/-/wiki/Norsk/Politikk+for+informasjonssikkerhet.

[4] Patrick Hudson. The hearts and minds project. 01 2004. URL https://www.researchgate.net/publication/281236607_The_Hearts_and_Minds_Project.

[5] Ivar Kufås and Roy Are Mølmann. Informasjonssikkerhet og innsideproblematikk, 2003.

[6] Edgar H Schein. *Organizational culture.*, volume 45. American Psychological Association, 1990.

[7] CLTRe AS. Security culture report 2018, measure to improve, 2014. URL https://get.clt.re/security-culture-report-2018/.

[8] Thomas Schlienger and Stephanie Teufel. Information security culture: From analysis to change. *South African Computer Journal*, 31:46–52, 2003.

[9] Martin Fishbein and Icek Ajzen. Belief, attitude, intention, and behavior: An introduction to theory and research. 1977.

[10] Icek Ajzen. From intentions to actions: A theory of planned behavior. In *Action control*, pages 11–39. Springer, 1985.

[11] Kathryn Parsons, Agata McCormac, Marcus Butavicius, and Lael Ferguson. Human factors and information security: individual, culture and security environment. 2010. en tldr hva det dreier seg om.

[12] Edward E Smith and Douglas L Medin. *Categories and concepts*, volume 9. Harvard University Press Cambridge, MA, 1981.

[13] Bruce Schneier. *Secrets and lies: digital security in a networked world*. John Wiley & Sons, 2011.

[14] Adéle Da Veiga and Jan Hp Eloff. A framework and assessment instrument for information security culture. *Computers & Security*, 29(2):196–207, 2010. URL https://www.sciencedirect.com/science/article/pii/S0167404809000923.

[15] N Martins, A Da Veiga, and Jan HP Eloff. Information security culture-validation of an assessment instrument. *Southern African Business Review*, 11(1):147–166, 2007.

[16] Dahlum. Sirianne. Indikator, 2014. URL https://snl.no/indikator. Accessed 17.02.2019.

[17] Hanne Eggen Røislien Bjarte Malmedal. The norwegian cyber security culture. 2016. URL https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf.

[18] Cheryl Vroom and Rossouw von Solms. Towards information security behavioural compliance. *Computers Security*, 23(3):191 – 198, 2004. ISSN 0167-4048. doi: https://doi.org/10.1016/j.cose.2004.01.012. URL http://www.sciencedirect.com/science/article/pii/S016740480400032X.

[19] Adéle Martins and Jan Elofe. Information security culture. In *Security in the information society*, pages 203–214. Springer, 2002.

[20] Kai Roer and Dr. Gregor Petrič. To measure security culture: A scientific approach. Report, 2018.

[21] P Hättenschwiler and A Gachet. Skriptum in decision support systems theory i. *University of Fribourg*, 2003.

[22] JAN ELOFF A. MARTINS. Information security culture, part five: Social and ethical aspects of information security. page 208, 2002. URL https://link.springer.com/content/pdf/10.1007%2F978-0-387-35586-3_16.pdf.

[23] Yngve Nordby. *Informasjonssikkerhet : atferd, holdninger og kultur*, volume 200504 of *ROSS (NTNU) (trykt utg.)*. NTNU, Institutt for produksjons- og kvalitetsteknikk, Trondheim, 2005. ISBN 8277062222. en tldr hva det dreier seg om.

[24] T. Schlienger and S. Teufel. Analyzing information security culture: increased trust by an appropriate information security culture. In *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*, pages 405–409. ISBN 1529-4188. doi: 10.1109/DEXA.2003.1232055. URL https://ieeexplore.ieee.org/ielx5/8719/27592/01232055.pdf?tp=&arnumber=1232055&isnumber=27592.

[25] Stig O Johnsen, C Hansen, M Line, Yngve Nordby, ELIOT Rich, and Ying Qian. Checkit–a program to measure and improve information security and safety culture. *International Journal of Performability Engineering*, 3(1):174–186, 2007.

[26] Hanne Eggen Røislien Bjarte Malmedal. Nordmenn og digital sikkerhetskultur. 2018. URL https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf.

[27] ENISA. The new users' guide: How to raise information security awareness. page xx, 2010. URL https://www.enisa.europa.eu.

[28] Adele Da Veiga, Nico Martins, and Jan HP Eloff. Information security culture-validation of an assessment instrument. *Southern African Business Review*, 11(1): 147–166, 2007.

[29] Magnus Alsaker. Indikatorer for informasjonssikkerhet. 2004. URL https://sh.ehelse.no/hkode/arkiv/Delte%20dokumenter/KITH/upload/1177/R08-04IndikatorerInformasjonssikkerhet.pdf.

[30] Gary C Moore and Izak Benbasat. Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information systems research*, 2(3):192–222, 1991.

[31] Adéle da Veiga. *Cultivating and Assessing Information Security Culture*. Thesis, 2008.

[32] Salahuddin Alfawaz, Karen Nelson, and Kavoos Mohannak. Information security culture - a behaviour compliance conceptual framework. pages 47–55, 2010. URL https://dl.acm.org/citation.cfm?id=1862275.

A Oppg. 38. Sikkerhetskultur ved NTNU

Oppdragsgiver

Oppdragsgiver: IIK, Seksjon for Digital Sikkerhet, NTNU
Kontaktperson: Gaute Wangen
Adresse: NTNU i Gjøvik, Kontor A128
Telefon: 9070883
Epost: gaute.wangen@ntnu.no

Sikkerhetskultur ved NTNU

NTNU Seksjon for Digital Sikkerhet arbeider kontinuerlig med innføring av styringssystem for informasjonssikkerhet. En sentral del av dette er arbeid med sikkerhetskultur. Som en offentlig og akademisk institusjon er balansen mellom tilstrekkelig frihet og åpenhet versus krav til sikkerhet i cyber et utfordrende mål. En gjennomgang av informasjonssikkerhetskulturen dreier seg i hovedsak om å kartlegge hvilke svakheter og styrker som finnes internt. En konsekvens av dårlig sikkerhetskultur kan gå utover bedriften i forskjellige former, blant annet økonomiske tap og dårlig omdømme. Dette kan igjen være med på å utsette de eventuelle konkurransefortrinn bedriften har i forhold til markedet.

Oppgaven

Formålet med denne oppgaven er å gjøre en måling av sikkerhetskultur på NTNU. Oppgaven går ut på å gjøre en litteraturanalyse av eksisterende metoder for å måle sikkerhetskultur og dernest velge en av disse for gjennomføring på NTNU. Gruppen blir delaktige i å sette omfang på oppgaven og skal selv styre gjennomføringen av målingen. Gruppen skal analysere resultatene og basert på disse, foreslå tiltak for å øke informasjonssikkerhetskulturen.

Denne oppgaven har derfor 3 hovedområder:

1. Gjennomgang og analyse av beste praksis innenfor Sikkerhetskultur.
2. Velge rammeverk og gjennomføre en måling på NTNU.
3. Foreslå tiltak til å bedre sikkerhetskulturen på NTNU.

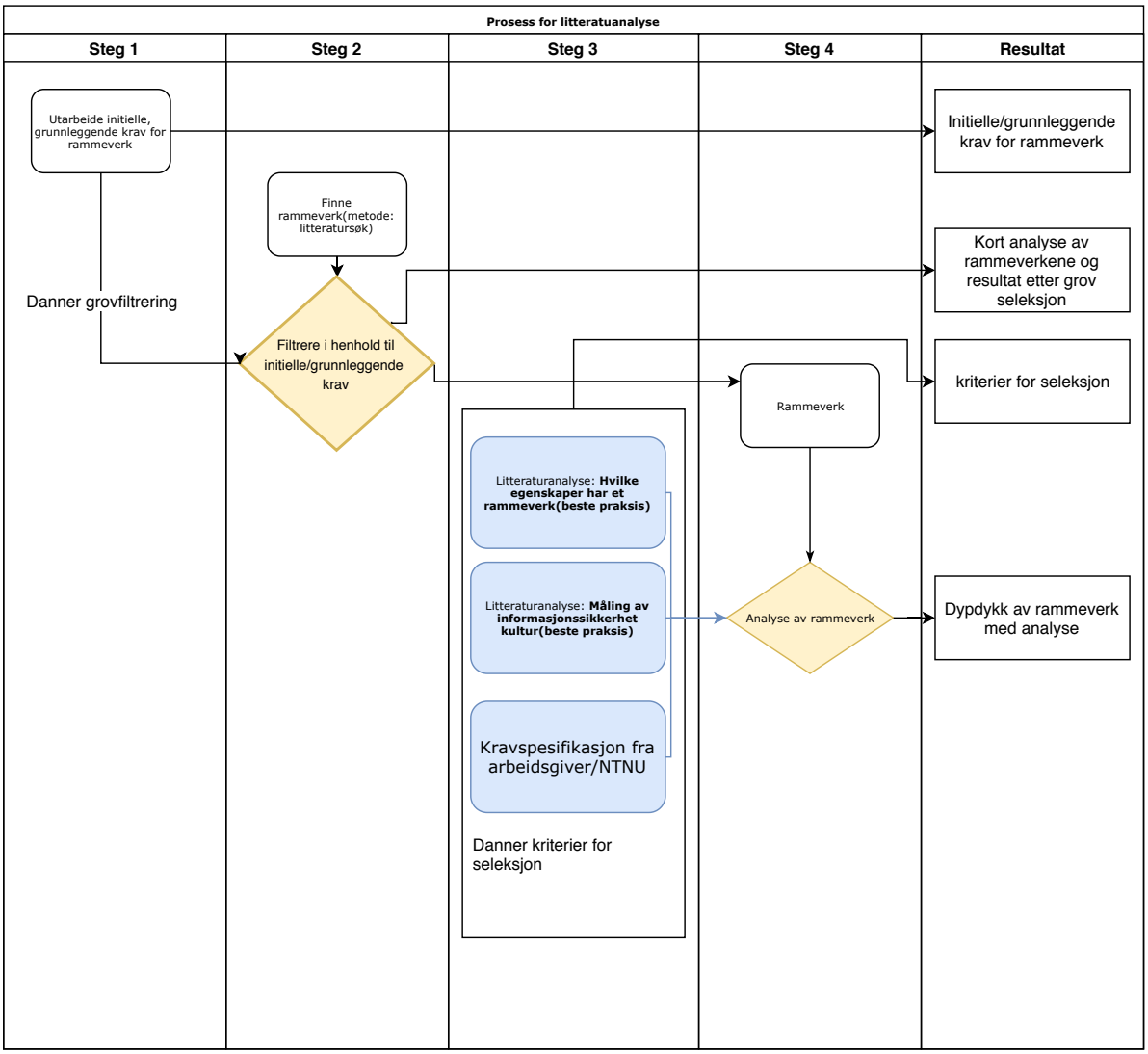
Egnede metoder for å gjennomføre oppgaven er litteraturanalyse i forarbeidet og case studie hvor oppdragsgiver bistår med å sette scope. Gruppen gjennomfører case studien i henhold til beste praksis, gjerne ved hjelp av kvalitative verktøy, slik som intervjuer, spørreundersøkelser og analyse.

Studentgruppen vil gjennom prosjektet få erfaring på:

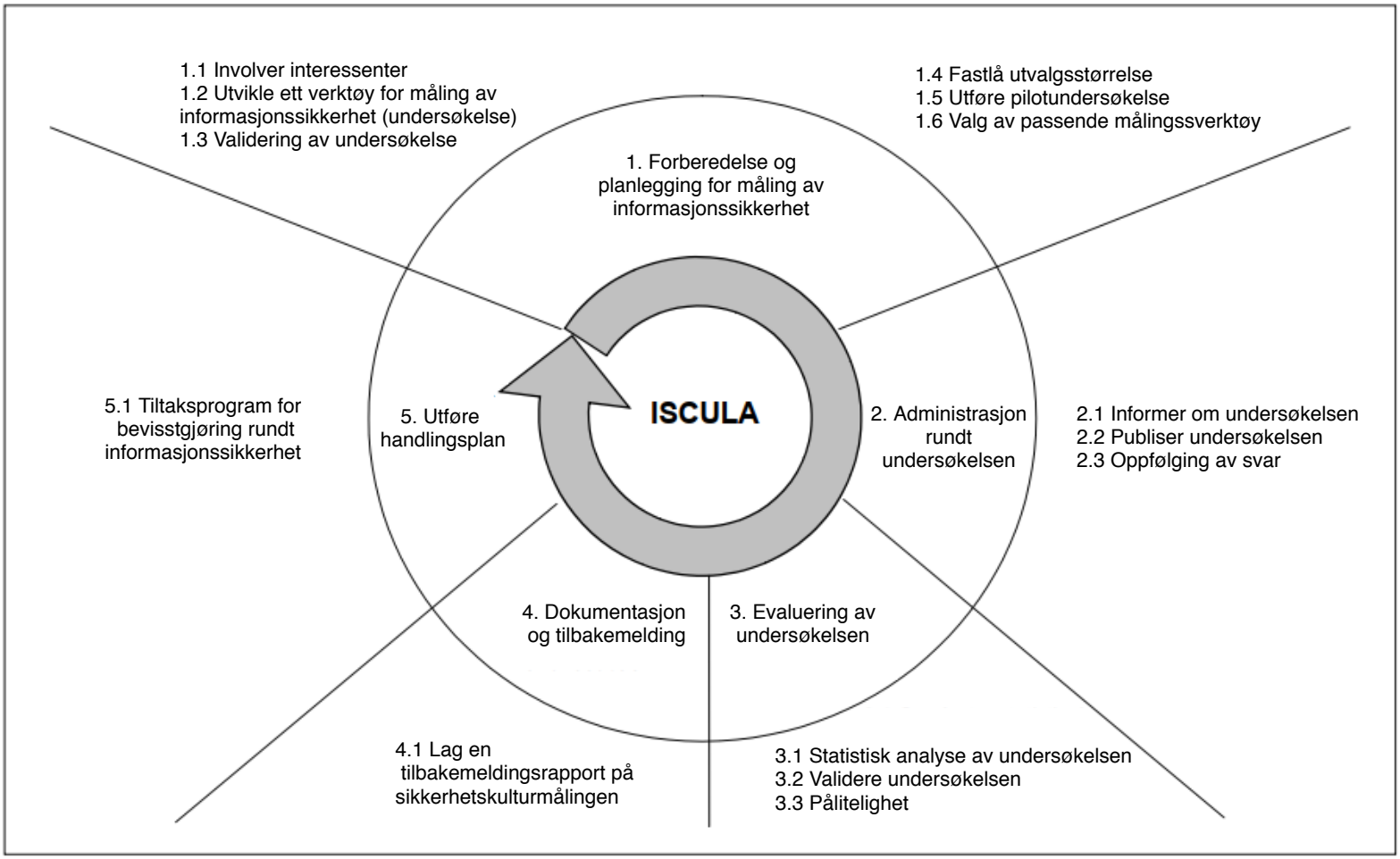
- Kvalitative undersøkelser og innsamling av data.
- Økt forståelse for metodikk og gjennomføring innenfor informasjonssikkerhetskultur
- Økt forståelse for risikovurderinger.
- Økt forståelse for sikkerhetsarbeid og dynamikk i store organisasjoner.
- Dataanalyse.
- Innsikt i sikkerhetsutfordringer.

Oppgaven passer bra for en gruppe på 2-3 personer med faglig vekt på informasjonssikkerhetsstyring. Forståelse for statistikk (analyse av intervju og spørreundersøkelser) er en fordel og interesse for organisatoriske utfordringer i sikkerhetsarbeid er nødvendig.

B Grafisk fremstilling av litteraturanalyse


Prosess for litteratuanalyse
Steg 1
Steg 2
Steg 3
Steg 4
Resultat
Utarbeide initielle, grunnleggende krav for rammeverk
Finne rammeverk(metode: litteratursøk)
Danner grovfiltrering
Filtrere i henhold til initielle/grunnleggende krav
Litteraturanalyse: Hvilke egenskaper har et rammeverk(beste praksis)
Litteraturanalyse: Måling av informasjonssikkerhet kultur(beste praksis)
Kravspesifikasjon fra arbeidsgiver/NTNU
Danner kriterier for seleksjon
Rammeverk
Analyse av rammeverk
Initielle/grunnleggende krav for rammeverk
Kort analyse av rammeverkene og resultat etter grov seleksjon
kriterier for seleksjon
Dypdykk av rammeverk med analyse

C ISCULA-modell


1.1 Involver interessenter
1.2 Utvikle ett verktøy for måling av informasjonssikkerhet (undersøkelse)
1.3 Validering av undersøkelse
1. Forberedelse og planlegging for måling av informasjonssikkerhet
1.4 Fastlå utvalgsstørrelse
1.5 Utføre pilotundersøkelse
1.6 Valg av passende målingssverktøy
5.1 Tiltaksprogram for bevisstgjøring rundt informasjonssikkerhet
5. Utføre handlingsplan
ISCULA
2. Administrasjon rundt undersøkelsen
2.1 Informer om undersøkelsen
2.2 Publiser undersøkelsen
2.3 Oppfølging av svar
4. Dokumentasjon og tilbakemelding
3. Evaluering av undersøkelsen
4.1 Lag en tilbakemeldingsrapport på sikkerhetskulturmålingen
3.1 Statistisk analyse av undersøkelsen
3.2 Validere undersøkelsen
3.3 Pålitelighet

D Intervju med Bjarte Malmedal

Intervju Bjarte Malmedal 12.02.2019

Hvilke rammeverk kjenner du til? Har Norsis noe vi kan benytte?

Se NorSIS rapport 2015 2016, gir det teoretiske grunnlaget for kultur undersøkelse. Spørsmål som ble stilt står der.

Tilpasninger: Beskrevet i rapport 2017 2018. Gjengitt i rapporten. Omfattende litteraturstudiet. Mange som snakker om sikkerhetskultur, det de gjør kartlegger adferd. Forskjell på kultur og adferd. Eksempel adferd: Sjekke om ansatte trykker på lenker. Sikkerhetskultur kunnskap, holdninger, måler trykker på lenker.

Forsket på holdninger og meninger. Bredt perspektiv.

Skille kultur og adferd. Egen metode. Brukt 50 virksomheter. 20 000 besvarelser, 70 000 utsendte.

Opplyse: digital sikkerhetskultur tilnærme seg det deskriptivt, måling=kartlegging. Kultur skal ikke rangeres ift. Ikke bedre enn noen andre. Forutsetninger spiller inn. Hvordan den er. Men forsiktig med å si noe om forskjellen. Forskjellige behov. Deskriptivt mener NorSIS er bra. Nasjonalt perspektiv kan være forskjellig fra bedrift.

Andre metoder: normativ tilnærming. Tallverdier, noen gir tall for sammenligningsgrunnlag. Ikke godt for NorSIS.

Man må snakke om kultur med samme perspektiv. Holdninger rettet mot mål.

Spørreundersøkelse, intervju, etc. På alle ansatte eller ledelse. Ulike tilnærminger?

Kommer an på hva man ønsker. Hva ønsker man? Ønsker å vite hva ledelsen ønsker. En kombinasjon er viktig. Fra ledelsen kan man få målene for hva som ønsker det skal være. Gap analyse mellom ledelse og ansatte.

For evt. Spørreundersøkelse. Hvordan formulere spørsmål?

Tok norsis et halvt år og komme fram til sine spørsmål. Kjørte pilottester med folk. For å komme fram til riktige spørsmål.

Når Norsis gjør undersøkelser bruker de 25 spørsmål til alle. Endres ikke. I tillegg 5 spørsmål organisasjonen kan lage selv. Da får man tilpasning og felles base med data. For å at man skal kunne sammenligne med andre virksomheter. Men ikke nødvendigvis heldig å sammenligne med andre. Eks. Forsvaret og politi har forskjellige grunnlag og mål. Kan bruke norsis rammeverk. Godt analysegrunnlag. Alle de dataene er tilgjenglig.

Viktig å tenke på ved vårt use case?

Ofte få personer som svarer. Signifakt og usikkerhet i svar. Fjerne tilfeldigheter og finne kjernen.

Du kan bruke hvilket som helst rammeverk..men hva betyr det. Må dekke prosessen i etterkant. Må finne ut av hva ledelsen ønsker. Hvilke typer holdninger ønsker ledelsen. Kart fra ledelsen fra hva de ønsker. Hva er bakgrunnen for svarene. Setter inn tiltak på. Planlagt før man starter.

Basere spørsmål på hva?

Erfaring: Sikkerhetspolicy er ofte ikke en policy, utgått policy. Kan være vanskelig å finne en god policy som er up to date. Dybdeintervju med sikkerhetsansvarlig for å finne ut dagens ståsted.

Får ferske føringer. Forankring og forventing. Når funnene kommer tilbake, det sikkerhetsansvarlig sa om «opplæring» kanskje ikke stemte. Lage plan. Tiltak, finansiering.

I Undersøkelsen som den fremstod for respondentene

Måling av informasjonssikkerhetskultur

Formål

Arbeidet med informasjonssikkerhetskultur er stadfestet i NTNU sine retningslinjer for arbeid med sikkerhetskultur og opplæring. Formålet er å gjøre lederlinjen bedre rustet til å ha oversikt og kontroll over egne informasjonsverdier, og medarbeidere bedre i stand til å ivareta informasjonssikkerheten i sine arbeidsprosesser og kommunikasjonsflyt.

Undersøkelsen er et samarbeid mellom seksjon for digital sikkerhet og HR- og HMS-avdelingen med en bachelorgruppe på IT-Drift og Informasjonssikkerhet på Gjøvik.

Resultatene fra undersøkelsen vil bidra til å gi et bedre overblikk over den nåværende sikkerhetskulturen og hjelpe i utviklingen av et rammeverk for måling av informasjonssikkerhetskultur på NTNU.

Oppbygning

Undersøkelsen starter på neste side med to demografiske spørsmål. Det er totalt 36 spørsmål fordelt på side 3 til 6.
Undersøkelsen tar maksimalt 10 minutter å gjennomføre.

Svarene vil bli behandlet anonymt.

Begrepsforklaring

Her er noen viktige begreper vi bruker i undersøkelsen:

- **Informasjonsverdier**:
  - Deles inn i to kategorier: *Primærverdier* handler om hva vi gjør og hvordan, og informasjonen vi benytter (forretningsprosesser og aktiviteter, informasjon). *Sekundærverdier* handler om de verktøyene vi bruker og kompetansen hos de som bruker verktøyene. (Hardware, software, nettverk, ansatte, lokasjoner, organisasjonsstrukturer).

- **Fortrolig informasjon:**
  - Fortrolig eller strengt fortrolig klassifisert informasjon.

- **Politikk for informasjonssikkerhet:**
  - Her menes selve dokumentet "Politikk for informasjonssikkerhet" som er underlagt IKT-reglementet.

Demografi

1. Hvilken seksjon hører du til?*

- Digital sikkerhet
- IT-brukerstøtte
- IT-drift
- IT-forvaltning
- IT-strategi og -styring
- IT-utvikling
- Campus-IT Gjøvik
- Campus-IT Ålesund
- Annet? Skriv her

2. Jeg har lest politikk for informasjonssikkerhet*

○ Ja ○ Nei ○ Vet ikke

3. Jeg vet hvor jeg kan lese politikk for informasjonssikkerhet*

○ Yes ○ No

4. Jeg forstår innholdet gitt i politikk for informasjonssikkerhet.*

○ Yes ○ No

5. Jeg vet hva informasjonssikkerhet omhandler.*

○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

6. Jeg vet risikoene ved å åpne e-post fra ukjente sendere, spesielt hvis den inneholder vedlegg.*

○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

7. Jeg låser for det meste datamaskinen min når jeg forlater den.*

○ Yes ○ No

8. Jeg mottar meldinger om informasjonssikkerhet helst i følgende kanaler. Du kan velge étt eller flere alternativ.*

For eksempel endringer i rutiner og håndtering av informasjonsverdier eller viktige hendelser

☐ Plakater
☐ E-post
☐ Diskusjonsgrupper
☐ Presentasjoner
☐ SMS
☐ Web basert opplæring
☐ Info - skjermer
☐ Promoterende varer (merchandise)
☐ Videoer
☐ Annet? Skriv her

9. Jeg får nok informasjon om sikkerhet?*

○ Yes ○ No

10. Jeg vet hvilke ansvar jeg har angående informasjonssikkerhet.*

○ Yes ○ No

11. Jeg mottar tilstrekkelig opplæring og trening i verktøyene jeg bruker daglig.*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

12. Informasjonssikkerhet er viktig i min avdeling for beskyttelse av informasjonssverdier.*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

13. Ansatte i min avdeling mener informasjonssikkerhet er viktig.*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

14. Jeg er klar over aspektene relatert til informasjonssikkerhet i jobben min (f.eks. Hvilke informasjonsverdier jeg jobber med som klassifiseres som fortrolig eller ved endring av passord).*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

15. Jeg aksepterer at det er mitt ansvar å beskytte informasjonsverdier.*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

16. Det er klare retningslinjer for hvordan beskytte brukere sin fortrolige informasjon (studenter, ansatte).*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

17. Endringer i avdelingen for å beskytte informasjonsverdier er positivt akseptert (f.eks. bruke passord for håndholdte enheter som nettbrett eller innføring av to-faktor autentisering for datamaskin og applikasjoner).*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

18. Min leder har informasjonssikkerhet på møteagendaen/dagsorden.*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

19. Ledelsen oppfatter informasjonssikkerhet som viktig.*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

20. Jeg mener det er nødvendig med informasjonssikkerhet for måloppnåelsen til NTNU.*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

21. Jeg mener NTNU gir tilstrekkelig oppmerksomhet til informasjonssikkerhet.*
    ○ Svært uenig ○ Uenig ○ Noe uenig ○ Noe enig ○ Enig ○ Svært enig

22. Jeg mener NTNU forplikter seg til informasjonssikkerhet.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

23. Det er viktig å forstå trusler og sårbarheter som eksponerer informasjonsverdiene i arbeidsmiljøet mitt for risiko.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

24. Ledelsen sørger for at jeg etterlever IKT-reglementet.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

25. Ansatte i min avdeling forholder seg til IKT-reglementet.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

26. Jeg bør holdes ansvarlig for handlingene mine hvis jeg ikke overholder IKT-reglementet.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

27. Jeg mener retningslinjer som berører mitt daglige arbeid er tilstrekkelig.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

28. Jeg mener retningslinje for sikker utvikling brukes ved innføring eller utvikling av systemer.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

29. Jeg opplever at det er aksept for å melde avvik på informasjonssikkerhet i seksjonen jeg jobber i.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

30. Jeg bruker private applikasjoner for å utføre arbeid relatert til jobben min.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

31. I så fall, hvilke tre private applikasjoner anser du som de viktigste i ditt daglige arbeid?

32. Jeg kjenner til arbeidsprosessene ved andre fakulteter i NTNU.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

33. Jeg klassifiserer informasjonen jeg jobber med.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

34. I seksjonen jeg jobber i har vi oversikt over hvilke informasjonsverdier vi behandler.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

35. Seksjonen jeg jobber i implementerer risikoreduserende tiltak.*

Svært uenig | Uenig | Noe uenig | Noe enig | Enig | Svært enig

36. Lederen min er opptatt av at vi kan lære og forbedre oss av de avvik som meldes inn.*

Svært uenig | Uenig | Noe Uenig | Noe enig | Enig | Svært enig

37. Tilbakemeldinger

J Møtereferat med veileder

Informasjon

Dette dokumentet er en samling av referater fra gruppemøter:

Formatet på datoene er DDMMMÅÅ

(for eksempel *22JAN19)*

16JAN19

Grupperegler:

- Inspirert fra frode sine forslag til grupperegler
- Startpunkt for møtet --> jobbe til hele agendaen er ferdig
- Definere hva som er oppmøtetidspunktet
- Lese agendaen før møtet
- Leder som passer på at ikke møtet sklir ut
- Løse problemet dersom ikke arbeidsoppgavene blir utført
    - Klarer man ikke deadlinene som er satt, bør man kommunisere det i god tid
- Handlinger ved gjentatte regelbrudd:
    - 3 stegs prosess som beskrevet i forprosjektplanen
- Kildehenvisninger er en kontinuerlig prosess

Problemstilling

- Hva er status for sikkerhetskultur på NTNU i dag
- Målsetting for gruppen:
    - Utvikle måling av sikkerhetskultur som kan brukes om igjen
- Hvorfor forbedre sikkerhetskulturen:

Diverse:

- Lage egen spørsmålsliste
- Alle burde følge litt med på andre sitt arbeid, og vite hva alle jobber med
- Litteraturundersøkelse:
    - Tittel
    - Link
    - Sammendrag
        - Hva man har fått ut av det man har lest
- Definering av oppgaven til å vite hva det omhandler
- Prøve å få noen rapporter fra hendelser som sier at informasjonssikkherhetskulturen må forbedres
- Prøve å bli ferdig med prosjektplanen til fredag kl. 1600
    - Kan evt. Få revurdert den innen fristen (1. Februar)

18JAN19

Scope / problemområdet / problemavgrensning

- Ikke begrense oss til en grafisk lokasjon
- Omfang på målingen:

Sende mail med spørsmål om effektmål til Gaute

- Fikk svar som blir lastet opp til Sharepoint

Lage effektmål

- Målbart bedret sikkerhetskultur
- Finne ut av hvordan den nåværende situasjonen er på NTNU når det gjelder sikkerhetskultur

Utforme rammeverk for måling:

- Sammenlikne rammeverk basert på krav vi har:
    - Lage en tabell for sammenlikning

- Krav NTNU har til rammeverk?
    - Representativt bilde/måling
    - Behandling av data
    - ISO har krav til nye rammeverk som skal innføres?
- Krav fra oppdragsgiver
    - Kvalitativt

Risikovurdering

- Felles beslutningsgrunnlag fører til bedre vurderingsevne på analysen
- Fastslått sannsynligheter og konsekvenser på eventuelle risikoer som kan utsette prosjektet.

23JAN19

Teorikapittel:

Oversikt over hvordan Latex skal se ut (organisering)

- Flowchart
- Finner litt ut av hvordan struktureringen blir underveis i prosessen, etter hva som er best
    - En fil pr. Kapittel?
    - Bruke innsidas guide for hvordan man skriver en bacheloroppgave
        - Anders tar dette

Litteraturanalyse:

- Hvordan kan vi vite hva vi skal se etter (rammeverk)?
    - Basere det på et teorikapittel?
    - Krav til rammeverk:
        - Hold i organisasjonen
        - Ikke bare tekniske ting
- Føre inn i kilder fortløpende (kilder.bib i latex)
    - Benytter oss av syntax som er skrevet som en "mal" i latex
    - Lage egen tittel
- Spørsmål om sjekkIT:
    - Er det fortsatt aktuelt i dagens samfunn?
        - Kulturen og informasjonsbiten har forandret seg veldig siden 2005

Diverse:

- La Ernst (veileder) få lese-tilgang til Latex
- Spørsmål til veiledningsmøter

Videre arbeid:

- Lese rammeverk:
    - Skrive ned det man selv syntes er nyttig
        - Være litt kritisk når man leser
        - NTNU i bakhodet
- Strukturere oppgaven

25JAN19

Diverse:

- Fordele arbeidsoppgaver i Trello.
- Hvilke rammeverk har vi funnet?

Litteraturanalysen:

- Hvordan vi skal strukturere den?
- Se på hvilke rammeverk som finnes og hvordan de fungerer

- Eget word-dokument på sharepoint
- WBS på analysedelen

Teoridelen:

- Hvor dypt skal vi gå inn i definisjonene?
- Gjøre teoridelen før man starter med litteraturanalysen
- Skrives rett i Latex
- Definisjoner står i trello
- Starte med noen definisjoner så vi har et grunnlag for litteraturanalysen
- Fordele litt oppgaver med å definere begreper

- Ha med et metodikk kapittel som beskriver litt om hvordan vi har gått frem i litteraturanalysen

Scope for målingen:

- Definere sopet etter hvert som vi begynner med målingsbiten av oppgaven

30JAN19

Diverse:

- Kilder
    - Skrive de under på hver side, eller ha de samlet bakerst?

Forberedelser til veiledningsmøte:

- Godkjenne innledningen / andre ting fra forprosjektet
- Få tilbakemelding på startprosessen i bacheloroppgaven
    - Teori
    - Innledningen
- Hva kan veileder hjelp oss med?
- Tilbakemeldinger på forprosjektet

Gjennomgang av hverandres skriving

06FEB19

Forslag til prosessering av litteraturanalyse

- Grovfiltrering
- Krav fra fagfolk om hva som er et bra rammeverk / hva et bra rammeverk skal inneholde
- Andre krav
- Dypdykk
- Utvelgelsesprosess
- Implementasjon av valgt rammeverk

TODO

- Hente inn informasjon fra kontaktene våre om “metrikker”
- Få godkjent forslag til prosess av litteraturanalysen
- Finne et dokument der hvor det er gjennomført en måling av informasjonssikkerhetskultur
- Er det muligheter for å tilpasse rammeverket på egenthånd, dersom det ikke er noen som passer?

Lage “standardmail” for kontakt med personer

08FEB19

Gjennomgang av møtet med Veileder og Gaute

Fordele oppgaver –> grovfiltrering

13FEB19

Diskusjon av intervju med Bjarte fra NorSIS

Finne konkrete krav til rammeverk

Enighet om å flytte alt av litteraturanalysen over til sharelatex (overleaf)

Skrive ut alle rammeverkene. Prøve å finne en strukturert måte å gå gjennom rammeverkene på

Strukturere latex-doumentet 'litteraturanalyse'

15FEB19

Rammeverk:

- Ta med noen spørsmål fra sikkerhetssjefen, med ting som er aktuelt nå på NTNU

Litteraturanalysen:

- Ta med flere initiele krav, slik at flere blir filtrert ut tidlig i prosessen
- Ta med "sensitiv data" og tredjeparter som et eget krav i grovanalysen

Ferdig med til og med krav før rammeverk til Søndag

20FEB19

Stadfestet intervju med Roar Thon

Diskusjon rundt rammeverk så langt og planen videre

- Trenger en tydeligere definisjon om hva et rammeverk er / hva vi legger i det.

Planlegge videre arbeid og tidsfrister

Bestemte å ikke se etter flere rammeverk fra nå av.

Plan om å sende forespørsel til spørreundersøkelse til Gaute så snart vi får svar fra HMS avdelingen

22FEB19

Fikk endelig respons tilbake fra HMS

- Gjennomgang av denne mailen

Sende mail til Gaute ang. Planlegging av spørreundersøkelse

Status på framgang i litteraturanalysen

Hvilke muligheter har vi?

27FEB19

Gjennomgang av dypdykket:

- Sammendrag av hva alle har kommet frem til / funnet ut av hvert sitt område
- Kombinere spørsmål fra flere ulike rammeverk?

Hvordan gå frem på valg av rammeverk biten

- Muligheter
    - Sammenlikne alle rammeverkene mot kravene
    - Må være muligheter for å gjøre forandringer i rammeverket over tid
    - Muligheter for å legge til egne tilpassede spørsmål
        - Ulikt fokus i hver bedrift
- SjekkIT vs ELOFF'en
    - Sammenlikne sterke og svake sider
- Prosessen:

28FEB19 – 15MARS19

Arbeid med dypdykk og utforming av spørreundersøkelsen

16MARS19

Diskusjon rundt de tre leveransene til Gaute.

Spørreundersøkelsen:

- For mange spørsmål:
    - Hvordan luke ut spørsmål på en god måte
    - Skrive ned prosessen for å velge spørsmål til avdelingen
        - Hvor mange spørsmål
        - Se på NTNU sine hjemmesider og mørketalls undersøkelsen
        - Høre med avdelingsleder
- Sende mail til Husemoen evt. Andre?
    - Er det for mye å kreve å ta med Husemoen i prioriteringen av spørsmål i alle avdelingene --> kan føre til at avdelingene ikke utfører målinger fordi det blir for mye byråkrati.
    - Få tilbakemeldinger på komponentene?

17MARS19

Arbeid med å oversette prosessen for gjennomføring av rammeverket til Norsk

- Utfordringer med å oversette prosess for validering av rammeverket og statistiske metoder
    - Tilpasninger

Arbeide med valg av rammeverk i bacheloroppgaven

19MARS19

Gå igjennom tilbakemeldinger på spørsmål fra Gaute.

Se på tiltak til hvert spørsmål

Definere hva "knowledge statements" er for noe i rammeverket

Se på demografiske opplysninger til spørreundersøkelsen

Føre arbeidsoppgaver inn i trello og jobbe selvstendig med de

20MARS19

Select survey:

- Joakim er den eneste med bruker og ønsker å fordele ansvaret
- De andre gruppemedlemmene må lage bruker

Gjennomgang av hvordan vi skal prioritere komponenter

- Random
- Plukke ut det vi har mest lyst på basert på subjektiv vurdering
- Se på mørketallsundersøkelsen og hendelser
    - Nedgang hendelser = kan utelukke de årsakene
- Se på seksjonene i avdelingene og hvilke komponenter som går igjen der

    - Hva kjennetegner IT-avdelingen:
- Sammenlikne spørsmålene med hendelser
- Se på hva Roar Thon og andre eksperter mener
- Kombinasjon
- Alle spørsmål må være relevante for alle i hele avdelingen = sørge for god spredning og lite regresjon.

Finne punkter / TODO's i backloggen

21MARS19

Jobbing med arbeidsoppgaver

Planlegging av veiledningsmøtet i morgen

Fikk tilgang til select-survey og flere retningslinjer

22MARS19

Joakim viser frem regnearket over spørsmål til undersøkelsen

Tilbakemeldinger fra Håkon Alstad

Planlegging av morgendagens workshop

23MARS19

Svar fra Randi:

- Mistolket spørsmålet og må vente litt til på svar
- Fortsetter å jobbe uten tilbakemeldingen fra Randi

Velge ut komponenter

Hvordan skal man velge?

- Velge ut de komponentene som har mest poeng, og se hvor mange spørsmål det blir til sammen.
- De komponentene som har flest poeng burde kanskje også ha flest spørsmål?
- Se på hvilke komponenter som kan passe for hver enkelt seksjon i IT avdelingen:
- De som har fra 2 til og med 3 poeng er med videre + change management i tillegg
- Filtrere ut kunnskapsspørsmål:
    - Går igjennom alle og fjerne / endre de som er irrelevante / uklare
- Ta med noen av Spørsmålene Roar Thon kom med
- Ta med komponentene bevisstgjøring og Etisk adferd i tillegg til de som har mest poeng:
- Bregner tidsbruken pr. Spørsmål i snitt og kom frem til at vi vikk 33 spørsmål, og det tar rundt 8.5 minutter

- Rekkefølge på spørsmålene:
    - Random:
        - Aktivere skallen for hvert spørsmål
        - Roar Thon sa noe om dette
    - Sekvensielt:
        - Kan tenke at spørsmålene er like
    - Alt på en side:
        - Spare noen sekunder
        - Raskere
        - Lettere å gå tilbake å endre svar
    - Flere sider:
        - Omstiller seg litt
        - Liten pause
        - Litt mer fokusert på akkurat den siden du er på
        - Spørre om vi syntes at formatet var bra

Fikk enda et svar fra Randi:

- Skrive hvilke komponenter vi kan hente ut fra mailen fra Randi
    - Risikostyring

24MARS19

Fjerne alle påstandene i undersøkelsen som har opphav i *Industry input*

25MARS19 - 28MARS19

Møter hver dag med klargjøring av spørreundersøkelsen.

Endringer på undersøkelsen for tilbakemeldinger fra Gaute, Randi og «bestemor».

29MARS19

Sendte ut spørreundersøkelsen til alle på IT avdelingen i dag klokken 08:44.

Første «analysene» tyder på at undersøkelsen er godt innenfor 10 minutter.

04APRIL19

Planlegging av videre arbeid

- Ting som skal gjøres før bacheloroppgaven sendes til Ernst:
    - Legge ved litteraturanalysen til bacheloropgaven
- Norsk oversettelse:
    - Se litt på hvordan oversettelsen av spørsmål kan gjøres bedre
- Diverse:
    - Tilbakemeldinger
    - Se over hva vi har skrevet så langt
        - Rette skrivefeil og motsigelser
- Analysen:
    - Vente med analysen til etter påske

Diskusjon av problem i innsamling av grunnlagsdataen

Hva ønsker vi tilbakemeldinger på:

- Trenger ikke se på skrivefeil, men at det er en rød tråd og at strukturen gir mening.
- Hele kapittel 4
- Oppsett av teorikapittel
- Tilbakemelding på kapittel 1 – 9

PÅSKEFERIE

24APRIL19

- Fordele arbeid mtp analyse av statistikk
    - Espen: 1 - 8
    - Joakim: 9 - 16
    - Magnus: 17 - 26
    - Anders: 27 - 36
- Finne ut av hvordan vi bruker SPSS
- Tilbakemelding fra Ernst?

26APRIL19

- Vi trenger kanskje litt flere argumenter for at vi valgte Da Veiga rammeverket i valg av rammeverk?
- Avslutningen: Oppsummering eller konklusjon?
    - Begge?
- Jobbe med kommentarer fra møte og statistikk

01MAI19

Oppdatere Trello

Gå igjennom rapporten å fikse blå TODO punkter

Oppdatere analysen av spørreundersøkelsen for å komme frem til tiltak

Tolkning:

- Dra inn punkter fra innledningen og teoridelen i tolkningen
  - Roar Thon
  - NorSIS rapporter (kapittel som forklarer hva som er viktig i denne typen arbeid → se på gode setninger)
  - Se på hva som er sterke punkter
- Se om vi finner en komponent som er dårligere enn andre

02MAI19

Tolkning av spørsmål

03MAI19

Gjennomgang av tilbakemeldinger fra møte med Ernst

Tolkning/analyse av spørsmål

05MAI19

Utforming av tiltaksplan og gjennomgang av diskusjonspunkter/TODO's i rapporten

10MAI19

Forberedelser til møte med veileder

Gjennomgang av møte med veileder

Fordele arbiedsoppgaver

K Møtereferat fra gruppemøter

K.1 1 februar

Forprosjektet:

Enighet med oppdragsgiver om hva som skal skje

Effektmål:

- Litt mer konkret
- Økt forståelse av sikkerhetskutlur på NTNU
- Vil at andre skal ta i bruk rammeverket og bruke det
- Komme med forslag til effektmål
- Se på mål på policien/politikken til NTNU
  - Vi skal bidra på dette målet
  - Sitere dette i rapporten
- Mål nr. 2 i politikken til NTNU
  - Være med på sikkerhetsarbeidet og være med å bidra til denne måloppnåelsen
  - Referere til "politikk for info ..." -> 7.2.
- Viktig at man definerer spørsmål man vil ha svar på, enten det er mål eller problemstillinger.
  - Hva er essensen i det vi skal svare på

Sende ny utgave av forprosjektet til Ernst

- Systemutviklingsmodell:
  - Teoridel før litteraturanalysen:
    - Det er jo mye samme greia egentlig ...

Diverse:

- Begreper fra ISO27000
- Gjøres på egenhånd innad i avdelinger
- HMS har ansvaret for sikkerhetskultur i NTNU
  - Snakke med henne
- Se på oppgaven til Fernando og Iver T. Johnsen?
  - NTNU bachelor oppgave
- Snakke med NORSIS --> Bjarte ? Malmedal
  - Røslien --> Cyberforsvaret
  - Snakke med de for å høre om sikkerhetskultur
  - Erfaringer
- Fordele oppgaver slike at man får mest mulig igjen for timene
- Flytt utkast til 1. mai istedenfor 12 eller 16. (gjerne ferdig førsteutkast 1. mai, så Ernst ser over oppgave i påsken)
  - Vi har plan om førsteutkast 12 April. Så den er grei

Rammeverk:

- Kriterier for å velge ut rammeverk:

- Er det en prosess
-

Struktur i rapporten:

- Metode
  - Alternative metoder som vi ikke har valgt, argumentasjon, vise litt oversikt over ulike måter å gjøre det på

Spørsmål:

- GAUTE --> Tall fra NTNU for hendelser og rapportering
  - Hvis det finnes rapporter som sier noe om / konkluderer med at hendelsen skjedde på grunn av svikt blant de ansatte / innsidetrusler så kan man si noe om at det er behov for bedre sikkerhetskultur

  Ikke sikkerhetskultur

  Sende en epost på dette til Gaute

  SjekkIT har blitt gjort tidligere

- Hvor dypt skal man gå inn i definisjonene på teoridelen av bacheloroppgavne?
  - Teori vs. definisjon. Hva vil det være sentralt å definere?

  Gi leseren et bilde av hva domene handler om på sentrale begreper i oppgaven

  Ved diskutering så må det ende med en konklusjon

- Hvilke krav har NTNU for innføring eller oppretting av rammeverk?
  - Hvilke krav har NTNU for infosec rammeverk?

  Lett å forstå og generell nok til å bli forstått av andre som ikke har IT – utdannelse

  Gjelder også begrepsbruken i rammeverket / fremgangsmåten

- Skal ha med både en referanseliste og en bibliografi
  - Bibliografi: liste over litteratur

- Referanseliste/litteraturliste: kildehenvisning

  Varierende --> kan skille mellom

  Må gi leseren en mulighet til å oppsøke videre informasjon

  URL / andre ting går i fotnote mens andre “skikkelige” artikkleler går i referanselisten

  Husk å ta med besøkstid

- Skal vi komme inn i prosjektet med hypotesers som presenteres innledende i rapporten

  Forskningsspørsmål

  Rammeverk

  Gjennomføring

  Utarbeiding

- Vi finner mye teori, lite rammeverk. SjekkIT, Security Culture Framework, Eloff Er det godt nok å sammenligne disse tre?
  - Finnes andre rammeverk --> Må ha flere enn tre stykker for å sammenlikne
  - Oppgaven

- Snakke om i hvilken grad det er lurt å inkludere Kai Roer

  Snakke med Kai Roer for å kjøpe inn rammeverk

  Garantert noe som kan Benyttes

  Gaute har trua på dette

K.2 8 februar

Tilbakemelding på prosess av litteraturanalysen:

Grovfiltrering:

- Sjekke kilder fra flere store norske bedrifter:
  - DIFI
  - NorSIS
  - NSM
  - UIO
  - HMS
- Litt mer konkret
  - Årstall

Egenskaper for rammeverk:

- Sjekke om NSM har noe; Thon er veldig på mener Gaute
- Få datagrunnlag fra Gaute, kan gi informasjon på hvordan det ligger an
- Struktur:
  - Vedlegg på rapporten og sammendrag

Kravspesifikasjon fra oppdragsgiver:

- Litt likt med det oppdragsgiver mener?

Dypdykk på rammeverk:

- Grunnlaget til et valg / en vurdering

Er det muligheter for å tilpasse rammeverket på egenhånd, dersom det ikke er noen som passer?

- Kan sy sammen fra flere rammeverk, men husk sitering og argumentasjon

Forslag til forbedringer / endringer av et rammeverk

- TODO:
  - Komme i gang med å finne rammeverk / fremgangsmåte
  - Prøv å se frem i tid for å forutse hva metode for måling kan være
- Sammenlikningsgrunnlag:
  - Finne flere rapporter
- Skille mellom fotnoter og bibliografi
- Ta med når en nettside ble aksessert sist i bibliografien
- Figurer må være godt lesbare

Diverse:

- HMS:
  1. Randi Utstrand
  2. Nina Tranø
- Kommunikasjon
  - Tore Hugubakken --> HMS avdelingen på NTNU
    - Hjelp til kommunikasjons-relaterte ting
- Ta hensyn til type organisasjon
  - NTNU vs. Forsvaret (åpen vs. lukket)

    - Forstå hva man produserer
        - Risiko for kjernevirksomheten
- Spørreundersøkelse, godkjenning muligens 3-4 uker
    - 200 pers, IT-avdelingen? Får mørketall fra fjor av Gaute
    - Via mail, grunnet kontroll
    - Finn ut angående undersøkelse innen kort tid (2 uker), kanskje intervju i Trondheim?

K.3 15 februar

Fremgang:

- Snakke med Bjarte
    - Spørsmål fra NORSIS er ganske "breie"
- Fått svar fra Roar
- Funnet rammeverk:
    - Alder på rammeverk har kanskje ikke så stor betydning
- Klassifisering av rammeverk:
    - Prøve å rette det mot NTNU
- Snakke med Kai Roer:
    - Litt hemmelighetsfullt hva pakken hans består av
    - Kan vi bruke det uten konsulentbistand?
    - I så fall må det utelukkes

Tidsplan fremover:

- Ta kontakt med HMS
    - Prøve å få hun / de "med på laget"
    - Kanskje de / hun har noe forslag eller noen ideer
    - Kanskje ringe? --> purring
    - Få tilbakemeldinger fa de
        - Gjeninnføring av policy osv.
            - Tenkt lite rundt det, og det er lite ressurser
            - Generelt gjort lite rundt sikkerhetskultur
- Forskjeller på rammeverk i forhold til detaljer og hvor dypt de går
    - Spørreundersøkelse:
        - Kombinere fra andre oppgaver
        - Ønske om å ikke ha spørsmål som trekker konklusjoner med en gang
- Få datagrunnlag fra Gaute
- Hva må til for å få planlagt en spørreundersøkelse:
    - Hvor: Bestemme avdeling / fakultet
        - Kanskje HMS har et forslag
            - De har kanskje tanker eller ideer om vår plan --> basert på det så må vi komme med en plan for gjennomføring av spørreundersøkelse
                - Sendes til Gaute i løpet av neste uke
        - Gautes forslag
    - Hva: Måle sikkerhetskultur (Generelt)
    - Når: Tidsrom?
- Forskjellige seksjoner innenfor IT – avdelingen
    - Tenke på demografiske data
        - Tenkte på hvor mye demografi man samler
- Krav til rammeverk:
    - Beholde dataen selv --> kan være mye sensitiv data
    - Kan være såpass "enkelt" at en som har litt peiling kan forstå det, og ikke nødvendigvis en hvilken som helst instituttleder
    - Komme med krav til rammeverk og hvorfor disse er viktig

        - Bør være greit for leseren og lese teksten uten referanser, og fremdeles forstå teksten
- Tidsplan på når vi skal ha funnet rammeverk:
    - 1. Mars
    - Rammeverk skal ha blitt valgt til neste møte

Diverse

- Må ha spørreundersøkelse på WEB
- Ikke bruk ark!
- Tiltakspakke basert på hver av faktorene i spørreundersøkelsen, dersom det er ulike styrker og svakheter fra avdeling til avdeling
    - Se på tiltak som har "tekniske" løsninger også
- Kan ikke finne et rammeverk som passer for alle nivåer i en bedrift, må sikte seg inn på "målet"
    - Forankring i institutt
- Se på forskningsrapporter, men vær kritisk ...
- Har en Ph.d. student som er psykolog dersom vi trenger råd
- Anbefalt antall ord på en bachelor rapport:
    - 70/80 --> 180?
- Ta med mye av dokumentasjon på prosessen, da hvordan man har jobbet er en del av oppgaven..
- Referanser til mail er greit dersom man legger med mailen
    - Evt. Sitater med godkjenning fra eier
- Spørreundersøkelse program:
    - Select survey --> in house program..
- Dele opp gruppa så man kan arbeide i parallell så fort man har mulighet
    - TTT
    - Noen fullfører dypdykk, mens andre jobber med spørreundersøkelsen

Tanker/ideer

- Prøve å lage et rammeverk til slutt som tar for seg hele prosessen?
- Ta styrker fra de forskjellige delene og kombinere de?
    - Kan bli vanskelig å kombinere?

K.4 1 mars

Fremgang:

- Dypdykk ferdig.
- Valg av rammeverk
- Ligger I rute iht. GANTT
- Kontakt med HR/Randi er opprettet. Validering av spørsmål.
- Jobber videre med "ELOFF" Ønsker å få spørsmål.

Tidsplan framover:

- Utarbeide selve rapporten.
- Paralellt med utarbeiding/strukturere spørreundersøkelse og gjøre klart.
- Husemoen blir med videre mtp relevante spørsmål. Samme blir HR. Da Veiga I loopen.
-

Diverse:

- Gaute -> Hvordan ligger du ann med spørreundersøkelsen og denne prosessen? Er det godkjent ? Skal du har førsteutkast?
- Hva om svakheter er avdekket I et rammeverk? Hvordan kan vi presentere forbedringer? Gjør dette valget av rammeverk-eller rammeverket I seg selv ugyldig?

Tilbakemeldiger:

- (Viktig=Kritisk til analyse av svarene ift. Hva vi sier I spørreundersøkelse. Presentasjon kontro tolkning.
- Ernst poengterte at det er meget viktig å være kritisk I analysen av dataen fra spørreundersøkelsen. Hva kan vi egentlig konkuldere osv. Her bør vi benytte hjelp.
- Vi må ha et lite diskusjonsavsnitt som forklarer-setter antakelgser om avdelingen I ht til fordeling, student-t tilnærming etc. Bruk ordene "rimelig og anta"
- Sjekk dypdykk iht. Motsigelser og lesbarhet. Presenter dette til ernst som et utkast for tilbakemeldinger.
-

K.5 8 mars

Tilbakemelding på spørsmål i spørreundersøkelsen:

- Gaute og co. Går igjennom spørsmålene for å sjekke forståelse osv.
- Tidspunkt:
    - Fredag om én uke --> validere spørsmålene (15.02)

Skal man oppdatere spørsmålene med ISO standarder?

Bruke politikk for informasjonssikkerhet på noen av spm.?

- Fikk ikke svar på dette

Framgang:

- Lage kortfattet norsk Version av rammeverket, samt oversette spørsmålene til Norsk.

Kombinere hendelsesdata med spørreundersøkelse

- Se litt på dette
- Bruke det som diskusjonsgrunnlag i etterkant
- Veldig interessert i å kombinere dette
- Sammenlikne resultater med denne?

Diverse spørreundersøkelse:

- Skreddersy spørsmålene til å nå alle avdelingene og ikke
- 85 spørsmål er for mye --> kommer til å miste respondenter
- 10 minutter er “maks”
- Kanskje 50% må droppes
- Trenger en del spørsmål for å dekke alle kategoriene:
- Må prioritere spørsmål

- Forslag: se på hvordan hendelsesbilde er, og prioritere ut ifra dette
- Viktig at man tenker kritisk

Tilbakemeldinger fra Ernst på dypdykket så langt:

- Inntrykk:
    - Referanseuken virker riktig
    - Småting: referanser på riktig side av punktum
    - Vant til at man bare bruker nummer i referanser
    - Går greit å ha det sånn som nå:
- Generelt:
    - Være kritisk når man leser.

- Gjøre det “barnevennlig” for den som leser.
- Ingenting er opplagt for den som leser.
- “guide” leseren.
- Fullstendige setninger.

K.6 14 mars

Validering av spørsmål med Oppdragsgiver

Agenda:

- Sette Gaute litt inn i rammeverket 10min
- 45min gå igjennom spørsmål for å sjekke forståelse og godkjenning
    - Tilpasse spørsmålene til NTNU
        - Å velge ut subkomponenter vi ønsker å angripe
    - Sikre lik forståelse av oversatte spørsmål
    - Validering av spørsmål

- Diverse (5min)
    - Demografi --> ikke ta med for mye

- Utfordringer vi har:
    - Flere spørsmål på en underkategori angriper det samme (x og y akse) på figuren, men kan man fjerne 2/3 og fremdeles ha et grunnlag for vurdering i den kategorien?
    - Adaptere rammeverket til NTNU

Generell tilbakemelding på spørsmål:

Skal alle komponentene spørres til alle personene i organisasjonen?

- Ikke alle komponenter som gjelder for alle avdelingene

Skal vi skille de forskjellige seksjonene i IT – avdelingen?

- Problemer med de demografiske dataene
- Forskjellige synspunkt fra subavdeling
- Å spørre om de forskjellige seksjonene de ansatte tilhører

Definere begreper i starten av undersøkelsen.

Ha en plan bak spørsmålene. Ta høyde for hva svaret betyr og hva det kan brukes til

Tenke igjennom hvilke scenarioer som kan komme til å skje i undersøkelsen

Ta hensyn til premisser/antakelser som ligger til grunn for spørsmålene

K.7 22 mars

Hva skal det skrives metode for? F.eks. når vi velger ut fokusområder for undersøkelsen

Alt mulig, eller bare hovedpunktene?

- Diskutere alternativer til fremgang --> Hovedsakelige ting
- Småting trengs ikke å beskrives i detalj
- noen av punktene være et resultat av valgt metode

Trenger vi en engelsk versjon av undersøkelsen?

- Litt usikker på behovet på IT-avdelingen

Flere av spørsmålene kan få en annen betydning når man skriver de på norsk

- Se an behovet for engelsk versjon
- Mister anonymiteten dersom noen svarer på engelsk
- Burde ta det med

Kan ikke bruke Email list funksjonen i select-survey:

- Var ikke klar over at dette var et krav
- Ønsker å bruke listen for den funksjonaliteten det medfører
- Dersom respondentene vet om at det ikke er anonymt kan det påvirke svarene
- Litt usikkerhet rundt dette
- videresende mail til Gatue

Hypoteser for spørsmålene i undersøkelsen - Hvordan analysere dataene?

- Avdelingen har "egentlig" en bakgrunn for undersøkelsen, men i dette tilfellet er det en generell måling.
- Har ikke rammeverket en hypotese for målingen
- Delmål:
  - Områdene vi ønsker å undersøkelse
    - Finne hypoteser basert på indikatorene?
  - Se på komponentene å finne hva som ligger bak de
  - Finne konkrete eksempler
  - Kort vei fra komponent til en hypotese
  - Viktig at vi får med Randi på undersøkelsen

Status på spørreundersøkelsen

- Gaute: jobber med saken, prøver å få med Randi på laget
- Får forhåpentligvis sendt ut den i dag

Vår status:

- Litt bak Gantt men kan ta oss inn hvis vi får ut undersøkelsen i løpet av neste uke

Korte ned spørreundersøkelsen:

- Ekspertvurderinger
- Hendelser

Diverse:

- Skrive at vi behandler svarene anonymt
- Burde være forsiktige med demografiske opplysninger:
    - Ta det veldig generisk
    - Interessant å se på seksjonene
- Veldig viktig at vi holder 10 minutter slik at vi får mange svar => god oppgave
- Kvalitetssikre spørsmålene for personer som ikke er i IT avdelingen. Er det noe de ikke skjønner?
    - Er dette metodikk?
    - "Syreteste" alle spørsmålene, eller bare de som er relevante?

Tidsperspektiv

- veileder og oppdragsgiver mener at vi ligger greit an

Tilbakemeldinger på litteraturanalysen:

- Måten vi referer på er litt rart/uvant
    - Parentes og tall er vanlig å bruke --> endre alle referansene til å benytte tall.
- Fotnoten i setningen skal plasseres litt forskjellig avhengig av bruken
    - Fotnoten skal rett ved den tingen man ønsker å påpeke
    - Eller bak påstanden man ønsker å "referere" til

K.8 29 mars

Diverse:

Hvor mange respondenter er «bra nok»

- Sende purring mot slutten av neste uke
- Når har man bra nok datagrunnlag:
    - Vurderes fortløpende
    - Litt usikkerhet rundt hvor mange prosent som er representativt
    - Kjører to uker med en purremail, og se hvor mange man får inn
        - Evt. Sende en ny purremail
    - Må avsluttes senest etter påsken / før påsken

Kan begynne å se på hvordan demografien i IT-avdelingen ser ut.

- (Hvordan gruppa i målgruppen ser ut)

Spørsmål:

Individuelt refleksjonsnotat?

- Legges ved rapporten ved innlevering i insperia
- Hvordan man opplever at prosessen har vært
    - Interne konflikter eller liknende
- Tenke litt på dette gjennom hele prosessen

K.9 2 april

Statistikk med Gaute

Diverse:

Analyse av spørreundersøkelse og ikke så mye annet.

Problemstilling:

Problemstilling: Måling av sikkerhetskultur

Forskingsspørsmål:

> Avledet ut ifra forskningsspørsmålene
>
> Spisser formuleringen

Hypotese:

> Ofte så går det ikke an å bevise at det er sant: enten styrke eller svekke
>
> Forsiktig med å påstå at noe er sant

Metode

Velge en forskningsmetode

Finnes mange metoder

Datatyper

Representativitet → finne ut hvordan fordelingen til de som svarer er

Kategoriske:

- Seksjonstilhørighet

Ordinale:

- Subjektive data som for eksempel lav, medium, høy
  - Man ikke regne gjennomsnitt på disse typer data
  - Likert skala er denne typen
- Distribusjon:
  - Range sier noe om distribusjon:
  - Varians: spredning i datasettet
  - Median: midterste verdien etter sortering
  -

Kvantitative variable:

- Kontinuerlige variabler som for eksempel høyde el.

Behandling av data

SPSS

Startes via NTNU sin IP

Output som SPSS og importer i SPSS

Gjøre klar data til analyse i SPSS:

- Gjøre om Likert skala til rang (1-6)
- Label på data i SPSS
- Endre datatype fra stirng til numeric
    - Kan ikke kjøre dataanalyse på dette før dette er ferdig

Grunnlagsdata og feilmargin

Finne ut hvor Representative dataene er

Flere respondenter i populasjonen fører til mindre feilmargin

Sammenlikne innsamlet data med det som er grunnlaget

Konfidensintervall

- Angir feilmargin i dataen
- 95% er «standard» verdi
- Må ha en øvre og nedre grense
- Stor varians: stor spredning i distribusjonen

Feilmargin

- Bruk kalkulator for dette

Deskriptiv

- Beskriver det mest grunnleggende i datasettet
    - Starter med en variabel og beskriver denne
        - Ekstremverdier:
- Beskrive distribusjonen

Bivariate

- Kategorisk + ordinal
- Ja/Nei = ANOVA (signifikans → Tester om en ting har)

Tukey

- Kjører den ikke på Likert skalaen

Korrelasjon:

- Likert skala
- Pearson alpha?

Tilbakemeldingsboks:

- Samle og finne fellesnevnere
- Samle inn i brede kategorier
- Kvantifisere
- Kan fikse på skrivefeil, men det bør noteres

NB:

1. Rapporter ALT på en nøktern måte

K.10 5 april

Diverse:

Bruke diskusjonen for å "samle spørsmålene" i kategorier --> konkludere / diskutere innenfor hvert punkt

Automatisere SPSS gjennomføringen?

prøve å få analysen til å gi mening på hvert spørsmål kan være en utfordring ved automatisering

Tilbakemeldinger på vet ikke svar på Likert skala spørsmål:

Hvordan kan man adressere usikkerheten i svaret / responsen?

se på mørketall, hvordan de har behandlet kritikk:

samler kritikken --> rydder --> adresserer relevante ting

se på spørsmålene evt. korrigere de som er litt

viktig at vi gjør den jobben med å behandle tilbakemeldinger

diskutere de å si hva vi har / har ikke gjort å hvorfor

Kan fjerne alle svarene til de som har svart tullesvar

Fortrolig informasjon i oppgaven --> mest sannsynlig , nei

Sjekke distribusjonen på avdelingene

Må ha 30 fra hver kategori for å kunne si noe om de via statistisk metode

Sende alle del-leveransene samlet til Gaute i slutten av oppgaven

Fikse på spørreundersøkelsen etter tilbakemeldingene:

Spørsmålene i undersøkelsen:

ta de gjerne med på engelsk

avhoppere av undersøkelsen kan fjernes med en gang.

gjør det lettere å analysere resultatene i etterkant. Slipper å rapportere N= for hvert spørsmål, men kan isteden ta det som en helhet for alle spørsmålene .

K.11 26 april

- Spørsmål analyse:
    - Feilmargin og "sample-size"
    - ANOVA--> Hva betyr de forskjellige forkortelsene
        - Tukey funker ikke
        - Hva betyr outputet fra anova analysen?
        - Hva er anova uten signifikans?
    - Kan man teste korrelasjon mellom for eksempel ordinale data og kategoriske data (demografi)
        - Må man ha noen hypoteser for å kunne teste dette?
    - Er det noen deskriptive analyser, som ikke gir mening for ordinale data?
        - Variansen for ordinale data?
            - Sier kanskje ikke så mye, man ser mye ut ifra grafen
    - Generelt:
        - Pass på å ikke ta forhastede konklusjoner
        - Husk på representativitet
    - Refleksjon:
        - Er det noe med spørsmålet som gjorde at mange svarte dette?
        - Hvorfor har vi fått disse svarene
- Neste fredag = forslag til tiltakspakke presenteres for Gaute:
- Tiltakspakke:
    - Foreslå tiltak med pris er lov
    - Vanskelig å si hvor det er forbedringspotensialer
    - Trenger kanskje ikke å ta noen avgjørelse om hva som er dårlig og bra
    - Diskusjon (alt er nyttig informasjon)
    -
- Tilbakemeldinger på rapporten
    - Generelt:
        - Inntrykk av bra jobbing
        - Vanskelig å forstå hva det egentlig handler om
        - Passe på at leseren forstår at det er sikkerhetskultur det handler om
        - "barnevennlig" språk i starten. Slik at leseren, helt grunnleggende ting. Sette de store linjene. Gjør det opplagt i starten.
            -

        - Litt annen formatering ()
        - Tar mye tid å skrive god tekst
    - Teoridel/generelle skrivefeil
        - Bra Vitenskapelig tilsnitt
        - Blir litt faktasetning-basert. (pirking)
        - Knytte sammen setningene litt bedre for å hjelpe leseren
            - Bruk av "dette"
        - Hopper litt mellom temaer
            - Blir litt for mye opp til leseren å tolke ulike ting
            - Fortelle hva som er sammenhengen mellom noen ting
        - Fremstille alt litt mer ryddig for den som leser og ikke kan noe om temaet

        - Introdusere ting litt bedre (for eksempel undersøkelser)
        - Bruk av referanser er litt dårlig enkelte plasser.
        - Litt mangelfull setningsoppbygging
    - Rammeverk seksjonen:
        - Se på det i sammenheng med det foran i teksten
        - "… Trengs en struktur rundt målingen.. "
        - Har mulighet til å si at "med rammeverk mener vi … "
        - Si at vi har kommet frem til at rammeverk er definert forskjellig.
    - Metode:
        - Kortfattet (google scholar)
        - Antar at man vet hva oria er
        - Starte med å definere hvordan vi kan finne ut det vi ønsker å finne ut.
            - For å oppnå …. er det nødvendig med en litteraturanalyse for å se på hva som finnes
                - Introdusere kapittelet / seksjonen bedre

K.12 3 mai

Skal punkter slik som rammer, avgrensninger, tidsmessige rammer, målsetninger osv. med i innledningen?

- Burde kunne lese oppgaven å få et fullverdig bilde av hele prosjektet
- Har skrevet om det i forprosjektet?
    - Kanskje ta med det som er naturlig å ta med?
    - Unødvendig å skrive ting to ganger
    - Avgrensningene gjelder noe som er relevant for resultatet
        - Se på gamle bacheloroppgaver

Fikk til å kjøre tukey-test, men ingen av spørsmålene er i nærheten av godt nok signifikansnivå. Hva gjør vi da?

- Kan si at det ikke er noen grupper som skiller seg ut

Hvor mye skal vi gjøre ut av tiltakene? Kost nytte osv.?

Tiltakspakke kan gjøres på to måter: alle komponenter eller bare svake sider?

Er dette riktig (bilde av tiltak fra Da Veiga rameverket)?

- Gjør vårt beste: tiltaksforslag og vi kan gjerne ta med kostnad osv.
- Se igjennom slides fra ITSM for å se hva vi kan estimere kostnad osv. ut i fra.
- Har vi noe bestepraksis å gå ut ifra når vi lager tiltak?
    - Roar
    - Spill fra DiFi

Hvordan liste opp tiltak? Under seksjon for kategori? Topp 10 dårligste påstander?

Er et riktig at de ansatte skal holdes ansvarlig (individuell basis) ved brudd på IKT-reglementet?

- Avhengig av hvor grovt bruddet er, men generelt sett den ansatte som er ansvarlig

Tilbakemeldinger fra Ernst på resten av rapporten:

- Kapittel 4:
    - Tilbakemelding:
        - Dele opp oppgaven tydeligere mellom litteraturanalyse og valg av rammeverk
        - Flytte noe av egenskaper og krav (4.2) ut i teorikapittelet?
            - Forklare hva fremmede begreper er (eksempler)
        - Vanskelig å finne tråden / sammenhengen i det vi skriver enkelte ganger
        - Knytte det opp mot det i innledningen / teoridelen
        - Innlede med en sammenheng mellom delene og hvorfor noe av teorien henger sammen med det foregående
        - Gjøre det tydligere at hele kapittel 4 er et utdrag av litteraturanalysen
        - Forklare stegene kort hva de stegene vi har delt inn litteraturanalysen inn i når vi introduserer de
        - Initiel vurdering (krav):
            - Si at vi kommer tilbake til kravene senere …
            - Konsekvent i hvordan det skrives opp.

        - Begrunnelse en plass
    - Passe på at man kan knytte kravene sammen på en god måte
    - Benytter kilder og referanser blir litt utydelig
- Konsekvent bruk av «rapporten» / «Rammeverket»
- Litt dårlig begrunnelse på kravet om at rammeverket skal være open source
- Researchgate og scholar

- Initiell vurdering av rammeverkene:
    - Konklusjonen kommer litt tidlig
    - Referanser til alle rammeverkene
    - En liten oppsummering på slutten
- Presentere intervju med personer:
    - Påstand X blir styrket i intervjuet med Y …

- Dypdykket:
    - Starte å si litt generelt om rammeverket. (Før innledning)
        - Målsetningen for rammeverket
    - Struktur: bytte om på målsetning og oppbygning
    - Oppgi akronymer tidligere
    - Pass på riktig bruk av utheving.
        - Uthev det som er viktig
    - Gjøre det opplagt hva som er styrker og svakheter
    - Referansebruk
- Sammenlikning:
    - Gi rammeverkene navn tidligere (akronymer)

Diverse:

- Kan lage en sammenlikning av hvor mange prosent ansatte vi har fått fra hver avdeling.
- Problemstillingen bør være klar og tydelig.
- Småplukk med hvor referansene puttes i setningen

K.13 10 mai

Oppsummering:

- Sideantallet er greit. Men må prøve å unngå å repetere oss sel

Gjennomgang av tiltaksplan med Gaute:

- Rammeverket og vår metode er mitt motstridende.
- Merke komponenter i figuren til rammeverket → presentasjon

- Snakke med Stian Husemoen om komponentene
    - Evt. De andre personer (Gaute og Vebjørn)

Forespørsel fra Gaute

- Sammendrag på fire sider
- Innhold:
    - Hovedfunn
    - Tiltak