DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering: Masterstudium i Samfunnssikkerhet	Vår semesteret, 2023 Åpen / ~~Konfidensiell~~
Forfatter: Viktoria Malena Eik & Katarina Svendsen	
Fagansvarlig ved UiS: Ole Andreas Engen Veileder: Kenneth Arne Pettersen Gould	
Tittel på oppgaven: ISO/IEC 27001 sin innvirkning på digital sikkerhetskultur Engelsk tittel: The impact of ISO/IEC 27001 on cyber security culture	
Studiepoeng: 30	
Emneord: ISO/IEC 27001, standardisering, standardiseringsprosess, digital sikkerhetskultur, ledelsens involvering og forpliktelse, standardens fleksibilitet, økt sikkerhet, sikkerhetsopplæring, sikkerhetsstyring	Sidetall: 69 + vedlegg/annet: 28 Stavanger, 18. juni. 2023

ISO/IEC 27001 sin innvirkning på digitale sikkerhetskultur

Hvordan kan implementering av ISO/IEC 27001 påvirke og potensielt styrke den digitale sikkerhetskulturen i virksomheter?

Masteroppgave i Samfunnssikkerhet

Vår 2023

Viktoria Malena Eik & Katarina Svendsen

Det teknisk- naturvitenskapelige fakultet,

ved Universitetet i Stavanger

Forord

Når denne masteroppgaven leveres, har vi fullført to fantastiske og kunnskapsrike år med mastergrad i samfunnssikkerhet ved Universitetet i Stavanger. Vi vil med det sende en stor takk til våre forelesere, som har vært til stor hjelp, vist engasjement og støtte oss gjennom denne reisen. Uten våre kjære familie, venner, kjæreste og medstudenter hadde ikke dette studieløpet og masteroppgaven vært mulig. Dere har oppmuntret og støttet oss gjennom oppturer og nedturer i denne innholdsrike perioden.

Vi vil uttrykke vår takknemlighet til veileder Kenneth Arne Pettersen Gould, som har vært til stor hjelp. Samtidig som vi ønsker å sende ut en spesiell takk til vår portåpner Siv Una Hagen, som rådført oss med gode innspill og råd gjennom masteroppgave prosessen. Videre ønsker vi å takke våre informanter som har bidratt til vår studie, vi hadde ikke klart dette uten dere. Til slutt sender vi ut en ekstra takk til Angelica Ræge-Svendsen, Odin S. Rørvik og Iselin C. W. Walther som har brukt mye tid til å hjelpe oss med korrekturlesing av oppgaven.

God lesing!

Sammendrag

Denne masteroppgaven utforsker hvordan implementering av ISO/IEC 27001 kan påvirke og potensielt styrke den digitale sikkerhetskulturen i virksomheter. Studien understreker at ISO/IEC 27001 presenterer ingen direkte kobling til den digitale sikkerhetskulturen, men vil ha en indirekte innflytelse. Det benyttes et eksplorativt forskningsdesign, med en kvalitativ studie med abduktiv forskningslogikk. Data ble samlet inn gjennom litteratursøk og semistrukturerte dybdeintervjuer.

Målet for studien er å utforske hvordan man kan styrke virksomhetenes robusthet, når det menneskelige aspektet står for en av de største sårbarhetene. Likevel bemerkes det at ISO/IEC 27001 ikke tar hensyn til det menneskelige aspektet. Ved at det eksisterer lite forskning på samspillet mellom ISO/IEC 27001 og digital sikkerhetskultur, er det derfor interessant å undersøke menneskeaspektet i Standarden for å identifisere hvordan det kan påvirke den digitale sikkerhetskulturen. Gjennom tematisk analyse ble det identifisert fire hovedfunn: ledelsens involvering og forpliktelse, Standardens fleksibilitet, økt sikkerhet og sikkerhetsopplæring.

Funnene viser til viktigheten av Standardens fleksibilitet, da den er i stand til å tilpasse virksomhetenes egne kontekster, som vil ha en videre innflytelse på den digitale sikkerhetskulturen. Effekten av Standardens fleksibilitet på den digitale sikkerhetskulturen er avgjørende etter hvilke beslutninger ledelsessystemet tar når ISO/IEC 27001 implementeres. Samtidig må de negative aspektene av Standardens fleksibilitet diskuteres, ettersom ledelsen kan neglisjere fleksibiliteten. Det kan påvirke virksomhetens sikkerhet, og således ha negativ effekt på ansattes bevissthet. Ansattes engasjement, forpliktelse og deltakelse er avgjørende for den digitale sikkerhetskulturen. Dette har en tett kobling til opplæring, som også er en sentral del av standardiseringsprosessen. Ved kunnskapsheving og tilrettelegging innen informasjonssikkerhet skapes det et fundament som frembringer økende sikkerhet. For å oppnå den ønskede innvirkningen på den digitale sikkerhetskulturen, må ledelsen være bevisst på kvaliteten av opplæringen som tilbys, og den kontinuerlige forbedringen. Resultatene peker også på hvordan Standarden kan fostre en overdreven følelse av sikkerhet, noe som kan skape en falsk trygghetsfølelse som videre kan resultere i at ansatte blir uforsiktige.

Abstract

This master thesis explores how ISO/IEC 27001 can serve as a tool to strengthen the cyber security culture. This study emphasises that ISO/IEC 27001 does not have a direct, but rather an indirect influence on the culture of the organizational cyber security. Especially, as the ISO/IEC 27001 neglect the human aspects. This study uses a qualitative method using an exploratory research design with an abductive research logic. The data was collected though in-depth interviews and literature studies.

The aim of this study is to investigate strategies to enhance organizational resilience, specifically focusing on the human aspects that influence cyber vulnerabilities Due to the limited pre-existing research on the interaction between cyber security culture and ISO/IEC 27001, it is intriguing to investigate how the human component of the ISO/IEC 27001 affects the organization culture. Though the thematic analysis, we discovered four key findings: management involvement and commitment, standards flexibility, increased security, and security training.

The findings underscore the crucial role of standard flexibility, emphasizing its importance in enabling adaptation to an organization's unique context, which can significantly impact its cybersecurity culture. The influence of this flexibility on cybersecurity culture plays a role in the decision-making process when implementing ISO/IEC 27001. However, it's equally important to consider the potential drawbacks of standard flexibility. If mishandled by management, it may unintentionally neglect flexibility, impacting the organization's overall security and employee awareness.

Employees' commitment and active participation play a crucial role in fostering a robust cybersecurity culture, and these factors are closely linked to comprehensive training and management's involvement, a vital element of the standardization process. Elevating awareness and delivering security-related training lays the groundwork for enhanced security measures. However, for this training to significantly impact the cybersecurity culture, management must prioritize the quality of the content and encourage ongoing improvement. The results also indicate that the standard can create an exaggerated sense of security, which may lead to a false sense of confidence and potential carelessness among employees.

Innholdsfortegnelse

Figuroversikt

Tabelloversikt

Begrepsordliste

5S2IS	Five stages to information security
Digdir	Digitaliseringsdirektoratet
DNV	Det Norske Veritas
IEC	The International Electrotechnical Commission
IKT	Informasjons- og kommunikasjonsteknologi
ISO	The International Organization for Standardization
IT	Informasjonsteknologi
ITU	International Telecommunication Union
KIT	Konfidensialitet, integritet og tilgjengelighet
NorSIS	Norsk senter for informasjonssikring
NSM	Nasjonal sikkerhetsmyndighet
PUKK	Planlegge - Utføre - Kontrollere – Korrigere
RSCM	Reciprocal Safety Culture Model
WSC	World Standards Cooperation
WTO	World Trade Organization

1 Innledning

Den digitale utviklingen har resultert i økende sårbarheter for virksomheter og samfunnet. Dermed er det ekstra viktig å bygge seg så robust som mulig for å unngå uønskede hendelser. Parallelt med denne utviklingen har interessen økt for sammenhengen mellom kultur, sårbarhet og sikkerhet i virksomheter (Westrum, 1993; Guldenmund, 2000; Antonsen, 2009; Kringen, 2009; Engen et al. 2016, s. 156). Den økte interessen har satt et lys på den digitale sikkerhetskulturen. Digital sikkerhetskultur består av felles holdninger, normer, verdier, handlinger og kunnskap for å kunne delta trygt i et digitalt samfunn. Den digitale sikkerhetskulturen kan medføre at samfunnet i sin helhet, virksomheter og enkeltpersoner kan bli mer robuste mot digitale trusler. Dette øker tilliten til de digitale tjenestene, som bidrar til å dra mer nytte av fordelene ved digitaliseringen (NorSIS, 2019, s. 7). En rapport fra NorSIS fra 2017 påpeker at digital sikkerhetskultur er et komplekst område, og det er flere mekanismer som kan påvirke den (NorSIS, 2017, s. 11).

Nasjonal sikkerhetsmyndighet (NSM) nevner det å ha god forebyggende sikkerhet vil si at virksomhetene har kunnskap om hvilke verdier som må beskyttes. Virksomhetene må kunne avdekke sine egne sårbarheter og iverksette tiltak for å kunne oppdage dem, basert på en helhetlig risikovurdering. Dette må gjøres utover de tiltakene som regelverket stiller (NSM, 2021, s. 37). Mennesker vil alltid være kilden til noen av de største sårbarhetene, selv om det er uvitende eller vitenene som tilrettelegger for at det kan forekomme datainnbrudd (NSM, 2021, s. 25). Dermed er det viktig med økt sikkerhetsbevissthet og god digital sikkerhetskultur. NSM poengterer videre at det bør bygges en «verktøykasse» som skal beskytte virksomheten, der en del av verktøyet bør ta for seg de menneskelige og organisatoriske aspektene. Ledelsen bør danne et grunnlag med rutiner og IKT-politikk for å kunne regulere IKT-systemer og dens informasjon. Derunder må det skapes mekanismer for å kunne utarbeide strategier for ivaretakelse av informasjonssikkerheten, som blant annet risikovurderinger, lover og retningslinjer, god sikkerhetskultur, brukerveiledninger og mer (NOU, 2015, s. 36).

I kontekst av digital sikkerhetskultur kan standardisering anses som en mekanisme for å igangsette prosesser for ledelsessystemer. Det finnes flere ulike forståelser av begrepet standard. I dette forskningsprosjektet bruker vi en blanding av ISO og Engen et al. sin definisjon: standard blir definert som et dokument som gir retningslinjer, formelle ikke-rettslige

normer/regler eller egenskaper for aktiviteter eller resultater utarbeidet av ISO (Standard Norge, 2006; Engen et al., 2021, s. 48-49). Standarder blir brukt som instrument for planlegging og kontroll, som kan påvirke utviklingen av økonomien, organisering og det daglige liv. Ikke minst kan de bidra til samarbeid og koordinering av virksomheter og verdikjeder på ulike nivåer (Engen et al., 2021). ISO-Standardens effekt kan beskytte virksomheten ved å innføre ledelsessystemer som vil redusere risiko og ivareta virksomhetens omdømme og verdier. Ved fokus på virksomhetenes digitale sikkerhetskultur, vil det være aktuelt å sette fokus på en ISO-standard som tar for seg styringssystem for informasjonssikkerhet, som ISO/IEC 27001. ISO/IEC 27001 sin hensikt er å etablere, implementere, drifte, overvåke, vedlikeholde og forbedre virksomhetens informasjonssikkerhetsstyringssystem. Standarden gir retningslinjer for å kunne identifisere og håndtere informasjonssikkerhetsrisikoer, samt et rammeverk for kontinuerlig forbedring av informasjonssikkerhetspraksis (Standard Norge, u.å.). Likevel understrekes en bemerkelsesverdig mangel. Standarden tar ikke eksplisitt for seg menneskelig atferd og organisasjonskultur, to kritiske faktorer som ofte er kilder til betydelige sårbarheter i virksomheters informasjonssikkerhet. Dette utelukker en viktig dimensjon av sikkerhetsstyring, gitt at menneskelig feil og kulturelle trekk kan være avgjørende for organisasjonens generelle sikkerhetsstatus.

1.1 Tidligere forskning

I en tidligere litteraturstudie av ISO/IEC 27001 ble det observert at 48 prosent av studiene viser at motivasjon var årsaken til at virksomheter standardiserte seg (Heras-Saizarbitoria & Boiral, 2013; Sartor et al., 2016; Culot et al., 2021, s. 82). Ifølge Culot et al. (2021) kan motivasjonen deles i funksjonalistisk og institusjonalistisk motivasjon. Funksjonalistisk er når organisasjonen antar at Standarden vil forbedre dokumentasjon og prosesser. Dette tilsier at virksomheter som har en funksjonalistisk motivasjon bak implementering av Standarden, inkluderer at de også har en forventning til et bedre informasjonssikkerhetssystem. Forventingene stammer fra Standardens omfang, Standardens fokus på kontinuerlig forbedring, og ved implementering av Standarden vil de tilegne seg kunnskap og ferdighet. En annen forventing innen funksjonalistisk motivasjon inkluderer en mer effektiv informasjonsstyring (Culot et al. 2021, s. 82).

Med institusjonalistisk motivasjon for å være standardisert, ser virksomheten på ISO/IEC 27001 som et verktøy for å stille bedre mot eksterne interessenter (Culot et al. 2021, s. 82). Et gjentakende tilfelle er at virksomheter anskaffer ISO standardisering som et kundekrav eller innflytelse fra andre virksomheter eller statlige organer. Dette innebærer at virksomheten forventer å få et bedre omdømme ut av standardiseringen, og ikke minst utstråle pålitelighet til andre virksomheter, kunder og potensielle partnere (Culot et al.. 2021, s. 83). Ku et al. (2009) vektlegger at virksomheter med institusjonalistisk motivasjon velger å standardisere seg innen ISO/IEC 27001 for å vise kundene deres villighet til å jobbe mer proaktivt. Begge former for motivasjon kan ha en indirekte innflytelse på den digitale sikkerhetskulturen.

Litteraturstudien utrykker at 68 prosent av tidligere forskning tar for seg fordeler og ulemper som kan fremkomme ved implementeringen av ISO/IEC 27001. 50 prosent av studiene om ISO/IEC 27001 indikerer at implementering av Standarden bør ses opp mot konteksten virksomheten opererer i, med tanke på motivasjonen, implementeringen og resultater. Studien tar opp ulike meninger om effektive verktøy og metoder, som er angitt i ISO/IEC 27001. Noen påpeker at det gir mye fleksibilitet (Smith el al., 2010), mens andre studier betegner det som en potensiell ulempe i implementeringsprosessen (Lomas, 2010; Rezaei el al., 2014; Culot et al., 2021, s. 84). Det oppsummeres kort at kravene oppleves som for formelle og omfattende. Et eksempel som kommer frem fra Bounagui et al. (2019) er at ISO/IEC 27001 veileder om hva som bør gjøres, men virksomheten er selv ansvarlige for å finne ut av «hvordan» en skal nå disse målene. Med manglende presise metodiske indikasjoner, kan det medføre at virksomheten får lavere nøyaktighet i risikoanalysen og ressursvurderinger, spesielt når ansvaret blir overlatt til individuelle eksperter (Ku el al., 2009; Liao & Chueh, 2012; Culot et al., s. 84).

Litteraturen peker på den manglende veiledningen som fremheves at det er mulige gjensidige avhengigheter mellom organisasjonen og omverden / ytre miljø. Flere mislykkes ved implementering, grunnet en ustrukturert tilnærming for hvordan ressursene skal håndteres. Eksempelvis IT-infrastruktur og tjenester delt mellom lokale enheter i virksomheten (Smith et al., 2010; Stewart, 2018; Culot et al., 2021, s. 86). En annen utfordring er at ISO/IEC 27001 ikke gir tilstrekkelig veiledning om de kulturelle og psykologiske dimensjoner, for å sikre ansattes etterlevelse (Van Wessel et al., 2011; Culot et al., 2021, s. 86). Topa og Karyda (2019) fremhever at det er kun begrensede indikasjoner når det kommer til vurdering av individuelle verdier og vaner, f.eks. personvernhensyn og virksomhetsstyrings holdninger (Topa & Karyda,

2019). Det kan understrekes at denne holdningen til informasjonssikkerheten vil ha tilstedeværelsen av kulturelle forskjeller (Asai & Hakizabera, 2010; Culot et al., 2021, s. 86).

Det andre hovedpoenget som legges frem i artikkelen er hvordan virksomheten strukturerer prosjektstyring. Culot et al. (2021) viser til en tidligere studie som tydeliggjør viktigheten for nødvendig kompetanse om IT, juss og organisasjon, for kunne å utvikle en veldefinert koordineringsmekanisme. Forskningen konkluderer med at prosjektteam og gjennomføringsfaser kan har ulike tilnærminger (Culot et al., 2021, s. 86). Forskingen anerkjenner at det krever lederens godkjenning for å kunne opparbeide et vellykket styringssystem, likevel antyder flere forskningsartikler at det ofte er IT-avdelingen som utarbeider ISO/IEC 27001 standardiseringen alene (Van Wessel., 2011; Akowuah et al., 2013). Videre påpeker Stewart (2018) at informasjonssikkerhetsledere blir sjeldent inkludert i ledergruppen. Ved at ledergruppen samtidig viser minimal bevissthet for standardiseringen for informasjonssikkerhetsstyringssystemet, vil det ofte resultere i lavere budsjett prioriteringer (Everett, 2011; Culot et al. 2021, s. 86). Disse nevnte tilfellene medfører ofte at virksomheter leier inn ekstern støtte som konsulenter for å kunne potensielt forbedre implementeringen av ISO/IEC 27001 (Dionysiou, 2011; Hoy & Foley, 2015; Annarelli et al., 2020). Dette kan påføre virksomheten en ulempe, ettersom det vil hemme organisasjonslæring og potensielt føre til mislykket implementering når virksomheten utfører det resterende arbeidet selv (Ku et al., 2009; Gillies, 2011; Culot et al., 2021, s. 86). Likevel er forskere enig om at oppnåelse av ISO/IEC 27001 standardisering vil kreve betydelig ressurser, som arbeidstid og økonomi (Gillies, 2011; Van Wessel et al., 2011, Culot et al. 2021).

Tidligere forskning fremlegger flere vesentlige aspekter knyttet til implementering av ISO/IEC 27001-Standarden. Motivasjon, enten det er funksjonalistisk eller institusjonalistisk, har betydelig innflytelse på en virksomhetens beslutning om å benytte seg av standardisering. Likevel har implementeringsprosessen diverse utfordringer: Blant annet kan Standardens iboende fleksibilitet og mangel på konkrete metodiske indikasjoner føre til usikkerhet og varierende grad av presisjon i risikoanalyse og ressursvurdering. Videre peker forskningen på at Standarden kan være utilstrekkelig med hensyn på virksomhetens interaksjoner med det ytre miljø, og hvordan kulturelle og psykologiske dimensjoner bør tas i betraktning for å sikre etterlevelse. Dette gir inntrykk av at den reelle implementeringen av ISO/IEC 27001 kan være mer kompleks og krevende enn hva som kan antas ut fra Standardens veiledning. Når det kommer til prosjektstyring og ressursallokering, er det flere virksomheter som overlater

standardiseringsprosessen til IT-avdelingen. Dette kan potensielt føre til underprioritering av nødvendige ressurser, noe som kan være et hinder for en vellykket implementering.

Disse funnene gir en indikasjon på at det kan eksistere et avvik mellom det ISO/IEC 27001-standarden foreskriver, og det faktiske arbeidet med å implementere og vedlikeholde Standarden i praksis. Dette avviket, og hvordan det påvirker den digitale sikkerhetskulturen i virksomheter, vil gi grunnlaget for problemstillingen presentert i neste kapittel.

1.2 Problemstilling

Gjennom den voksende oppmerksomheten rundt informasjonssikkerhet og systemrisiko i organisasjoner, har den digitale sikkerhetskulturen blitt mer betydelig. Digdir fremhever at styrking av informasjonssikkerheten kan blant annet oppnås ved å begrense menneskelige feil gjennom kulturell og kompetansebasert utvikling (Digdir, u.å. a). Kultur er en samling dynamiske tankemønstre som oppstår i samspill med andre mennesker i en virksomhet og hvordan den påvirker samhandlinger som blir utført i omverdenen (Einarsen, Martinsen, & Skogstad, 2017, s. 406).

Litteraturgjennomgangen avdekket mange metoder for å forbedre digital sikkerhetskultur, men det er fortsatt behov for å utforske nye tilnærminger for å styrke den. I forstudien til dette forskningsprosjektet dukket det opp diskusjoner rundt ISO og dens potensielle innvirkning på informasjonssikkerhet i virksomheter. Dette vekket interessen for å undersøke hvordan implementeringen av ISO/IEC 27001 kan bidra til å forbedre den digitale sikkerhetskulturen, noe som har resultert i forskningsprosjektets hovedproblemstilling:

Hvordan kan implementering av ISO/IEC 27001 påvirke og potensielt styrke den digitale sikkerhetskulturen i virksomheter?

Selv om ISO/IEC 27001 ikke direkte nevner sikkerhetskultur eller digital sikkerhetskultur, kan implementeringen av det ha en indirekte påvirkning på virksomhetens digitale sikkerhetskultur. Sikkerhetskultur er verdiene som deles av ansatte i en virksomhet og påvirker tanker og forventninger til sikkerhet (NSM, 2020).

Valget av denne problemstillingen var drevet av flere faktorer, blant annet informasjonssikkerhetens økte relevans og aktualitet. Samtidig ved å undersøke om ISO/IEC 27001 kan brukes for å styrke digital sikkerhetskultur, kan vi styrke virksomhetens robusthet mot menneskelige feil, som er en stor sårbarhet innen digital sikkerhet. Det er et kunnskapshull når det gjelder hvordan ISO/IEC 27001 påvirker den digitale sikkerhetskulturen. Ved å utforske dette emnet, kan vi bidra til å utvide forståelsen og kunnskapen om samspillet mellom digital sikkerhetskultur og denne standarden.

1.2.1 Forskningsspørsmål

I dette forskningsprosjektet vil det i første omgang kartlegges ved bruk av teorier om hvordan en kan endre en digital sikkerhetskultur. Gjennom datainnsamlingen blir det presentert i avsluttende drøfting hvordan en forbedrer en digital sikkerhetskultur ved hjelp av nøkkelfaktorer fra standardiseringen. Det første forskningsspørsmålet lyder derfor som følger:

1. Hvordan endrer man den digitale sikkerhetskulturen i virksomheter?

Andre del av problemstillingen åpner for en dypere studie av hvilke faktorer i standardiseringsprosessen som kan ha en innvirkning på virksomheten. Ved bruk av datainnsamling og litteraturgjennomgang belyses nøkkelfaktorer fra standardiseringsprosessen som vil ha en innvirkning på den digitale sikkerhetskulturen. Dette har bidratt til utviklingen av det andre forskningsspørsmålet:

2. Hvilke faktorer fra standardiseringsprosessen til ISO/IEC 27001 kan ha en innvirkning på virksomhetens digitale sikkerhetskultur?

1.3 Formål

Gjennom problemstillingen ønsker vi å utforske hvordan implementeringen og kontinuerlig etterlevelse av ISO/IEC 27001 kan påvirke virksomhetens ansattes holdninger, atferd og praksis knyttet til informasjonssikkerhet. Vi ønsker å identifisere og analysere nøkkelfaktorer for implementering av Standarden i en virksomhet for å fremme en robust og sterk digital sikkerhetskultur. Det endelige målet ved prosjektet er å gi en forståelse for forholdet implementering av ISO/IEC 27001 vil ha på virksomhetens digitale sikkerhetskultur. Funnene fra dette prosjektet kan være av stor verdi for virksomheter, da de vil kunne gi en dypere innsikt og forståelse av ISO/IEC 27001 som et effektivt verktøy. Det er hittil utført relativt lite forskning på dette området. Likevel er det aktuelt å se hvordan en eksplorerende forskning kan fremme hvilke nytteverdier som vil bistå virksomheter i å systematisk beskytte og håndtere den digitale sikkerheten.

1.4 Forutsetninger og avgrensing

Forskningsprosjektets problemstilling står overfor et komplekst tema, derfor er det nødvendig å sette avgrensinger. Problemstillingen og forskningsspørsmål er utviklet med hensikt til å kunne begrense oppgaven. Forskningsprosjektet sitt fokus er å se på hvordan ISO/IEC 27001 kan ha innvirkning på den digitale sikkerhetskulturen. ISO/IEC 27001 blir referert til som ISO/IEC 27001 eller Standard/Standarden i forskningsprosjektet. Her må det presiseres at ingen virksomhet vil ha lik digital sikkerhetskultur. Enhver kultur i en virksomhet vil være unik, grunnet hvert individ og daglige interaksjoner er ulike. Konteksten vil derfor ha en innvirkning på sluttresultatet til forskningsprosjektet. Dermed kan man påstå at ulike kulturer, mer konkret digital sikkerhetskultur, kan ha noen elementer som er like, som holdninger, verdier og normer.

Gjennom dette prosjektet vil begrepet "informasjonssikkerhet" bli hovedsakelig benyttet. Dette skyldes ikke kun det faktumet at ISO/IEC 27001 bruker begrepet informasjonssikkerhet. Det er flere begreper som kan brukes i terminologien rundt informasjonssikkerhet, som for eksempel, IT-sikkerhet, datasikkerhet, digital sikkerhet og cybersikkerhet. Alle disse begrepene kan ha ulik betydning, dessuten ser vi at betydningen av informasjonssikkerhet hovedsakelig overlapper med de andre begrepene (Jøsang, 2021, s. 14). Begrepet informasjonssikkerhet dreies om å kunne håndtere risiko relatert til virksomhetens informasjonsverdier og behandling av personopplysninger. Dette kan komme i flere ulike former og kan overføres digitalt, ikke minst formidles muntlig (Digdir, u.å. b). Det vil i tillegg ikke gås inn i detaljer om ISO/IEC

27001 ulike krav, grunnet mulig brudd på opphavsretten til ISO/IEC. Dermed vil informasjonen holde seg til litteratursøk og intervjudata ved fremstilling av innholdet i Standarden.

I dette prosjektet har vi et utvalg av ansatte i ulike virksomheter. Valg av virksomheter til dette prosjektet er basert på virksomheter som driver med informasjonssikkerhet, rådgivning ved standardisering og/eller informasjonssikkerhet. Noen av disse virksomhetene leverer nettbaserte tjenester til sine kunder. Ved dette utvalget vil derfor informasjonssikkerhet være en innlysende tematikk å ha søkelys på. På grunn av begrenset tid og oppgavens omfang, vil det ikke være mulig å gå i dybden på alle relevante aktiviteter. Forskningsprosjektet besluttet å foreta et kvalitativ eksplorerende design med dybdeintervjuer av nøkkelpersoner i ulike virksomheter. Formålet med eksplorerende design er for å kunne utforske de ulike forhold og fenomener som er mindre kjent (Johannesen el al., 2016).

1.5 Utforming av oppgaven

Oppgaven sin oppbygningsstruktur vil bestå av syv kapitler og vedlegg. Følgende vil være utgangspunktet for oppbygning av oppgaven.

Kapittel 1 Innledning — Innledning vil kaste lys på oppgavens problemstilling og forskningsspørsmålene, som går ut fra hvordan implementeringen av ISO/IEC 27001 kan påvirke og potensielt styrke den digitale sikkerhetskulturen. Kapittelet vil ta for seg sentrale begrep, tidligere studier, forutsetning og avgrensing for oppgaven.

Kapittel 2 Kontekst — Kontekst kapittelet vil presenterer de kontekstuelle forholdene relatert til ISO, standardiseringsprosessen og ISO/IEC 27001.

Kapittel 3 Teori — I kapittel 3 dannes det teoretiske rammeverket for oppgaven med digital sikkerhetskultur, endring av sikkerhetskultur, standardisering og kontinuerlig forbedring som grunnlag. På hver sin måte setter de lys på problemstillingen.

Kapittel 4 Metode — I metode kapitlet blir det redegjort for de metodiske valgene for oppgaven. For å forstå hvordan ISO/IEC 27001 kan fungere som et virkemiddel, vil teorien om digitale sikkerhet være en komponent i oppgavens teoretiske rammeverk. Metoden for datainnsamling falt på en eksplorativ kvalitativ datainnsamling med utførelse av ti dybdeintervjuer.

Kapittel 5 Empiri og analyse — I dette kapitelet blir analysen av datainnsamlingen fremlagt, der formålet er å formidle fortolkninger, sitater og hovedfunn fra informantene. Gjennom analysen vil det generere grunnlaget for besvarelse av forskningsspørsmålene.

Kapittel 6 Drøfting og diskusjon	Etter presentasjon av sentrale funn, vil vi i kapittel 6 foreta kritisk analyse og drøftet opp empiriske funn mot det teoretiske rammeverket for å kunne besvare oppgavens problemstilling. Eventuelt avdekke avvik fra det teoretiske rammeverket. Drøftingen vil sorteres og struktureres etter forskningsspørsmålene, der forskningsspørsmål to vil diskuteres først. Dernest vil diskusjonen av forskningsspørsmål én fungere som avsluttende drøfting.
Kapittel 7 Konklusjoner og anbefalinger til videre forskning	Det avsluttende kapittel konkludere de sentrale funnene, i tillegg til å svare på problemstillingen og dens implikasjoner. Det avsluttes med anbefalinger for videre forskning.

2 Kontekst

I dette kapitelet blir konteksten bak samspillet mellom ISO/IEC 27001 presentert. Konteksten til forskningen innebærer ISO og ISO/IEC Standardens bakgrunn.

2.1 International Organization for Standardization (ISO)

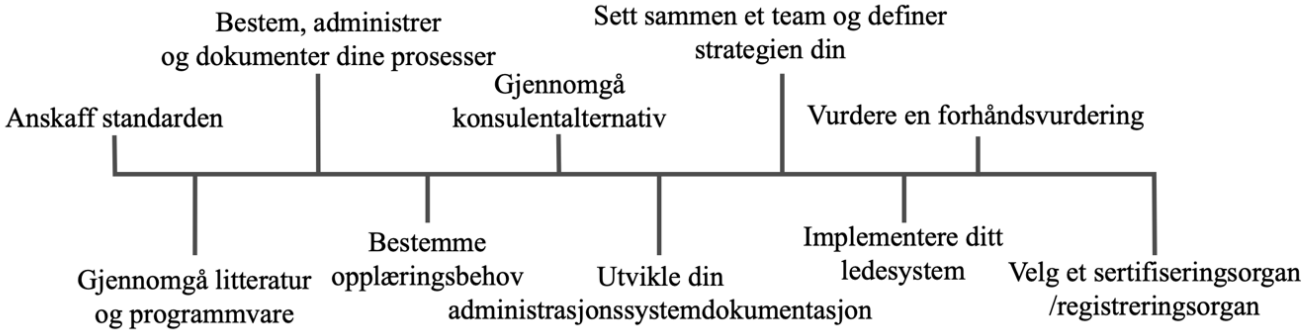
International Organization for Standardization (ISO) har utgitt 24673 ulike standarder, som dekker nesten alle aspektene innen styring, teknologi og produksjon (ISO, u.å, a). Det er en uavhengig, ikke-statlig organisasjon med 167 medlemsland, hvor Standard Norge er det norske medlemmet av ISO (Holtebekk, 2021). Ifølge ISO (2019) vil det å sikre stratifikasjonen for standarder hjelpe virksomheten å blant annet oppnå kompatibilitet mellom tjenester og produkter, for å sikre at de fungerer godt sammen. Standardene spiller også en stor rolle for å identifisere sikkerhetsproblemer og ønsker å fremme trygg og sikker praksis. I tillegg ønsker de å bidra til å fremme deling av ideer, god sikkerhetspraksis og teknologiske kunnskap, for å styrke forbedring på ulike felt (ISO, 2019, s. 4). ISO har som mål for virksomheter å bli mer konkurransedyktig innenfor det globale markedet, gjennom å tilby produkter og tjenester som lever opp til den internasjonale standarden. Virksomheter skal kunne enklere tre inn i nye markeder og styrke kvaliteten, sikkerhet og kompatibiliteten til produktene og tilbudene deres. Ved dette ønsker ISO å øke omsetning og redusere kostnader (ISO, 2019, s. 8).

ISO samarbeider med over 700 organisasjoner, deriblant International Electrotechnical Commission (IEC), International Telecommunication Union (ITU) og World Trade Organization (WTO) (ISO, u.å.b). IEC er en internasjonal, ikke-statlig organisasjon som skaper tekniske standarder innen elektrofag (Hofstad, 2022). Ofte står ISO og IEC sammen før en standard, som f.eks. ISO/IEC 27001. Dette er fordi Standarden ble utviklet i samarbeid mellom de to organisasjonene (Hofstad, 2022). ITU er et overordnet internasjonalt organ for utviklingen av kommunikasjonsteknologi (Delphin, Johnsen & Myren, 2021). I 2001 samarbeidet ISO, IEC og ITU om å danne World Standards Cooperation (WSC), for å styrke standard systemet i organisasjonene (ISO, u.å, b). Noen av de mest populære standardene til ISO er ISO 9001 (kvalitetstyringssystemer) og ISO 14001 (miljøstyringssystemer). Det er til sammen over én million virksomheter og organisasjoner fordelt på over 170 land som er sertifisert innen ISO 9001. ISO 9001 er en standard som forbedrer kvaliteten på produktene og tjenestene til

virksomheten, slik at de oppfyller forventningene til kundene (ISO, u.å, c). Mens det er mer enn 300 000 virksomheter som er sertifisert innen ISO 14001 fordelt på 171 land. ISO 14001 setter krav til styringssystemers innvirkning på miljøet, og gir et rammeverk for et effektivt miljøstyringssystem (ISO, u.å.d).

2.2 Standardiseringsprosess

Når man skal standardisere seg i ISO/IEC-27001 innebærer det at man leser nøye gjennom Standardens ordlyd, samtidig som man må gjøre seg oppmerksom på eventuelle revisjoner. Manglene kontroll på offisielle revisjon kan føre til at man risikerer å miste sertifiseringen (Calder & Van, 2009, s. 7). Ifølge DNV, inneholder selve standardiseringsprosessen ti generelle trinn til å bli sertifisert. Standardiseringsprosessen blir illustrert i Figur 1. Veien til sertifisering (DNV, u.å.).



Figur 1. Veien til sertifisering

For å begynne prosessen med sertifisering må man først tilegne seg en kopi av Standarden og forsøke å forstå kravene. Dette vil dermed bidra til avgjøring om sertifisering av ISO/IEC-27001 Standarden er relevant for virksomheten. Dernest bør det søkes i tilgjengelig og relevant informasjon som er utviklet for å bistå ved å skape en forståelse og implementere Standarden. Det eksisterer også retningslinjer som kan veilede virksomheten i implementeringen av Standarden. Deretter er det viktig å etablere et dedikert team som sammen skal utvikle og implementere systemet (DNV, u.å.). Seniorledelse bør være involvert i beslutningen, da de ofte har hovedansvar for å angi forretningsstrategien som skal støttes av administrasjonssystemet. Teamet som skal holdes ansvarlige for implementeringen vil trenge opplæring for å kunne implementere og opprettholde administrasjonssystemet. Det finnes ulike opplæringsmuligheter som kurs, workshops og seminarer. Dersom det ønskes hjelp fra uavhengige konsulenter, vil de

kunne tilby råd om en strategi for implementeringsprosessen. Et grunnleggende trinn er å frembringe dokumentasjonen for administrasjonssystemet. Beslutt en egnet plattform for dokumentasjonen, slik at den støtter tilstrekkelig administrasjon og kommunikasjon. Dokumentasjonen skal angi retningslinjer og aktiviteter i virksomheten i samsvar med kravene i Standarden (DNV, u.å.).

Deretter må det angis og dokumenteres de nødvendige prosessene i administrasjonssystemet, de skal være i samsvar med retningslinjer, mål og strategi. Disse prosessene skal avdekke områder som produkt- og servicerealisering, kundetilfredshet og administrasjonsprosesser. Når administrasjonssystemet er utviklet, må det implementeres. Kommunikasjon og opplæring spiller en avgjørende rolle i denne fasen. Virksomheten vil praktisere i samsvar med de eksisterende prosessene og kvalifikasjonene for å dokumentere og illustrere effektiviteten til administrasjonssystemet. Før man trer i gang den akkrediterte sertifiseringsprosessen, kan det være lurt å utføre en forhåndsvurdering av administrasjonssystemet. Dette hjelper virksomheter med å identifisere eventuelle avvik eller sårbarheter som kan rettes opp før sertifiseringen. I det siste steget velges et sertifiseringsorgan eller registreringsorgan som vil validere og godkjenne administrasjonssystemet. Dette forholdet vil eksistere over tid, da sertifiseringen må opprettholdes over en tidsperiode på 3 år. Kontinuerlig forbedring er nødvendig (DNV, u.å.).

2.3 ISO/IEC 27001 - Ledelsessystemer for informasjonssikkerhet

ISO/IEC 27001 er en internasjonal standard som setter krav til styringssystemer i henhold til informasjonssikkerhet (Anttila, 2012, s. 1). Informasjonssikkerhet inngår i styring og ledelse av et hvert foretak. Samtidig er det en rekke ulike aspekter av informasjonssikkerhet som krever særskilte kompetanser, noe som gjør at informasjonssikkerhet er et eget område innen styring og ledelse.

Standard kan forklares som en teknisk spesifikasjon eller av andre typer dokumenter som er tilgjengelig for offentligheten, og som er utarbeidet i samarbeid ved eller godkjenning av alle interessentene som berøres av den. Standardene blir basert på teknologi, vitenskap og erfaring (Anttila, 2012, s. 1). ISO/IEC 27001 er et rammeverk som identifiserer og vurderer risikoer ved virksomhetens informasjon, samtidig som den implementerer kontroller for å redusere risikoene (Brenner, 2007, s. 26). Standarden inkluderer også ivaretakelse av krav til lover, forskrifter og retningslinjer for krisehåndtering. Målet til ISO/IEC 27001 er å fremme virksomheters evne til

å beskytte virksomhetens verdifulle informasjonsressurser, i tillegg til å sikre virksomheten sin fremtidig drift (Brenner, 2007, s. 26).

Hver ISO-standard består av flere kapitler ved ulike krav: Kapittel én, to og tre handler om er introduksjon, normativ referanse og definisjoner og vilkår. Kapittel fire setter grunnlaget for rammeverket til ISO Standarden og virksomheten som skal sertifiseres. Kapittel fem omhandler ledelse og deres engasjement til å lede virksomheten til bedre sikkerhet. Kapittel seks handler om å sette planer for hvilke handlinger som skal utføres for å håndtere risikoene. Det inkluderer også å sette kriterium for akseptabel risiko, identifisere risiko, analysere risiko og evaluere risikoen. Kapittel syv tar for seg krav om ressurser, kompetanse og kommunikasjon i virksomheten. Mens kapittel åtte tar for seg operasjonell planlegging og kontroll, tar kapittel ni for seg evaluering av prestasjon. Til slutt handler kapittel ti om kontinuerlig forbedring (Standard Norge, 2023). Standarden vil kunne bidra til å respondere på sikkerhetstrusler som oppstår under utvikling, i tillegg til å redusere kostnader og utgifter på unødvendig forsvarsteknologi (ISO, u.å, e).

Virksomheter som tar i bruk ISO/IEC 27001 kan oppnå en rekke fordeler, inkludert beskyttelse av sensitiv og personlig informasjon som oppbevares både i papirformat og digitalt (BSI, 2019; ISO, u.å, e). Standarden krever også implementering av et rammeverk som samler og beskytter all informasjon på et sted. ISO/IEC 27001 har som mål å beskytte dataens konfidensialitet, integritet og tilgjengelighet (KIT) ved å styrke resiliensen til virksomheten mot cyberangrep, andre teknologiske trusler og andre typer risiko, samtidig sikre beskyttelse på organisasjonsnivå (ISO, u.å, e). Ivaretakelse av KIT kan bidra med å oppfylle informasjonssikkerhetsmålene og verdier. ISO/IEC 27001 definerer konfidensialitet som egenskapen for at informasjon ikke blir tilgjengelig eller vist til uautoriserte individer, entiteter eller prosesser (ISO, 2016; Jøsang, 2021, s. 22). Fokuset på de uautoriserte i kontekst av konfidensialitet, vil være på å kunne opprettholde konfidensialiteten for prosedyrer, praksis, policyer og sikkerhetskultur for å unngå uønskede hendelser som dataangrep eller lekkasje av sensitiv informasjon (Jøsang, 2021). Integritet er evnen til å opprettholde dataressursene sin korrekthet og kompletthet (ISO, 2016; Jøsang, 2021, s. 22). Tilgjengelighet er egenskapen til at informasjonsressurser, data og tjenester er tilgjengelige og anvendbare når en autorisert entitet ber om dem (ISO, 2016; Jøsang, 2021).

3 Teori

I dette kapittelet presenteres oppgavens teoretiske rammeverk som bidrar til å skape en grunnleggende kunnskapsbasis for samspillet mellom ISO/IEC 27001 og digital sikkerhetskultur. Innledningsvis legges det frem en oversikt av begreper forskningsprosjektet tar for seg, der det redegjøres av begrepet digital sikkerhetskultur. Videre legges det frem teorier om standardisering innen informasjonssikkerhet og risiko, og hvordan organisasjoner kan endre, oppbygge og forbedre sikkerhetskultur gjennom standardiseringsprosesser. Til slutt presenteres metode for kontinuerlig forbedring sammen med kvalitetsstyringssystemet PUKK og 5S2IS. Gjennom PUKK og 5S2IS kan organisasjonen systematisk identifisere og håndtere sikkerhetsrisikoer, og kontinuerlig forbedre sin digitale sikkerhetskultur og -praksis. Sammenfattende danner teorikapittelet grunnlaget for oppgavens datagrunnlagsanalyse og diskusjon.

3.1 Digital sikkerhetskultur

Kultur er et omfattende begrep, som brukes i flere forskjellige sammenhenger med ytterlige betydninger. Kultur er et sett med felles delte kognisjoner, også kjent som tankemønstre. Disse tankemønstrene utvikles i samspill av medlemmene i en organisasjon og det vil uttrykke hvordan medlemmene gjør ting i organisasjonen (Einarsen et al., 2017, s. 406). Det finnes ingen entydig definisjon av begrepet organisasjonskultur. Einarsen et al. (2017) definerer begrepet som et sett av felles verdier, normer og virkelighetsoppfatninger som utvikles i en organisasjon når medlemmer samhandler med hverandre og omgivelsene. Dette kommer til uttrykk i medlemmers handlinger og holdninger på jobben (Bang, 2011; Einarsen el al., 2017, s. 406). Definisjonen peker på at kulturen er dynamisk og viser rom til samhandling med omgivelsene og med hverandre (Einarsen el al., 2017). Kort oppsummert kan man forklare begrepet med å si «... måten vi gjør ting her».

Norsk senter for informasjonssikring (2020), NorSIS, definerer digital sikkerhetskultur som de felles verdier, holdninger, normer, kunnskaper og handlinger som bidrar til å avverge fra å bli rammet av digitale trusler. Her er de sosiale normene formet av menneskers atferd i ulike situasjoner. Dette kan forstås som at normer tjener som en veileder for gruppen, eller et sett med regler som styrer hvordan man utfører ulike handlinger. Det vil hjelpe menneskene i kulturen til å kunne få forståelse for hva som er rett eller galt, eller trygt og utrygt. Dette kan

medføre at menneskene i kulturen kan finne et felleskap (Malmedal, 2020, s.11). NorSIS forklarer videre at digital sikkerhetskultur består av følgende områder (Malmedal, 2020, s.11):

- Holdninger til digitalisering og digital sikkerhet
- Tillit og risikooppfattelse
- Synet på styring og kontroll
- Sikkerhetsatferd
- Kunnskap, læring og interesse

Det fremstilles en annen definisjon utarbeidet av Digdir, hvor den har fokus på digital sikkerhetskultur fra et organisatorisk aspekt. Sikkerhetskultur tilhører organisasjonskulturen i virksomheter, og omhandler hvilke elementer som bestemmer hvordan enkelte håndterer systemer og informasjon. Som et resultat av dette danner virksomhetene sikkerhetskultur gjennom kollektive oppfatninger, som kan ha fordeler og ulemper for virksomhetens informasjonssikkerhet.

Kultur og menneskelige faktorer kan ha en avgjørende betydning for informasjonssikkerhet og den digitale sikkerhetskulturen. Ansatte i virksomheter kan selv bli en trussel aktør mot sin egen virksomhet, ettersom ansatte også kan representer sårbarheter som kan utnyttes av eksterne trussel aktører for å kunne angripe virksomheten. Kevin Mitnick (2002) er en kjent ekspert innen sosial manipulering. Mitnick forklarer at den største trusselen mot sikkerheten i en virksomhet er ikke et datavirus, dårlig installert brannmur eller "upatchet" sårbarhet i et program, men det er de ansatte. Han forteller at det er utfra erfaring lettere å manipulere mennesker enn teknologien, spesielt når virksomheter har en tendens til å overse de menneskelige faktorer. Sosial manipulering kan foregå gjennom flere kanaler, der man kan skille mellom tekno-sosial manipulering og fysisk sosial manipulering (Mitnick, 2002; Jøsang, 2021, s. 230). Derfor bør virksomheter ha ekstra søkelys på digital sikkerhetskultur, slik at de kan forebygge og forhindre at farer og trusler forekommer (Jøsang, 2021).

For å opparbeide en god digital sikkerhetskultur må virksomheten motivere sine ansatte til å opptre på en måte som ivaretar sikkerheten. Ifølge Nasjonal Sikkerhetsmyndighet innebærer det å skape og ivareta gode rutiner ved rapportering om feil, avvik og sårbarheter. Det innebærer også å opprette en forståelse og aksept for viktigheten til rutinene og hvorfor disse rutinene eksisterer. Virksomheter som ønsker å opparbeide en tilbakemeldingskultur, må kunne legge til rette for belønninger ved positiv sikkerhetsatferd (NSM, 2020). Virksomheten må samtidig

motivere sine ansatte til å ekspandere sin personlige kompetanse innen sikkerhet på arbeidsplassen. De bør også holde kurs jevnlig innenfor emne sikkerhet, om blant annet sikkerhetsutfordringer på arbeidsplassen (NSM, 2020).

En optimal sikkerhetskultur er drivkraften til en virksomhet som ønsker å oppnå maksimal resiliens (Reason, 1998, s. 298). Dette er et mål som er vanskelig å oppnå, men Reason mener fremdeles at det er et mål vært å streve etter. Reason viser til utfordringen i virksomheter med få antall ulykker, hvor Weick (1991) beskriver sikkerhet som en “dynamic non-event". Som vil si at sikkerhet er usynlig i den forstand at et sikkert utfall avviker ikke fra forventningene, og dermed tiltrekker ikke noe oppmerksomhet. De ansatte ser derfor ingen konsekvens av handlingen, og forventer at dersom de fortsetter å handle slik vil «ingenting» fortsette å skje. Noe Reason påpeker er villendene, ettersom det krever en rekke dynamiske inputs for å skape et stabilt utfall (Reason, 1998, s. 294). Reason mener derfor at når ulykker oppstår sjeldent må man opprette et informertsikkerhets system, for å opprettholde en god sikkerhetsforståelse i virksomheten. Et slikt system vil samle inn data, analysere og informere om ulykker og nesten ulykker, samtidig som systemet vil jobbe proaktivt for å finne avvik og feil ved å gjennomføre regelmessige kontroller. Reason omtaler dette for en informert kultur. I en slik kultur vil lederen av systemet ha kunnskap om det menneskelige, teknologiske, organisatoriske og arbeidsmiljøets nåværende tilstand som tilsier systemets sikkerhetstilstand (Reason, 1998, s. 294). For å opparbeide en god sikkerhetskultur må man dermed ha en informert kultur.

Reason har identifisert fire karakteristikker for hva som vil utgjør en informerende kultur: rapporterende kultur, rettferdig kultur, fleksibel kultur og lærende kultur (Reason, 1997). Disse fire karakteristikkene kan bidra til videre utvikle systemet, samtidig som å oppnå gode resultat i sikkerhetsarbeidet. Gjennom dette blir fokuset på helhetlige sikkerhetstenking innen sikkerhetskulturen i virksomheten, fremfor på hver enkelt person (Hudson el al., 2002). Denne teorien kan gi et innsyn på hva som kan skape en sterkere sikkerhetskultur, og ikke minst kan fremme forståelse og motivasjon. I denne studien vil vi kun utdype om lærende kultur, til tross for at rapporterende-, rettferdig- og fleksibel kultur er aktuelle for forskningen, har vi besluttet å kun benytte én av kulturene for å avgrense studien.

Reason fremhever at en kultur oppnår lærende kultur når systemet er fungerende og etableres gjennom å observere, reflektere, skape og gjennomføre (Reason, 1997). Organisasjonen tar imot kunnskap som anvendes målrettet til læring og utbedring for å forandre adferd. I denne

kulturen oppfordres de ansatte til å lære å ha fokus på kontinuerlig forbedring. Her må det også sette fokus på å kunne bevare kunnskapen, erfaring og evnen til å overføre den til senere bruk. I den lærende kulturen er det akseptabelt å eksperimentere og prøve nye tilnærminger for å kunne oppnå bedre kvalitet og sikkerhet (Hudson el al., 2002).

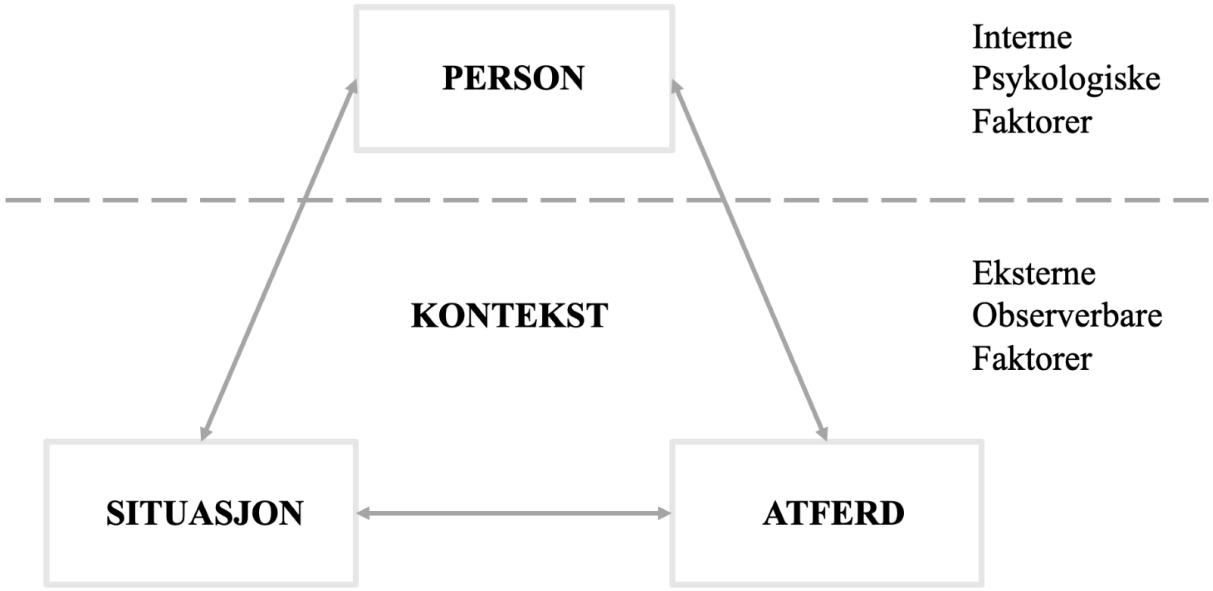
3.1.1 Sikkerhetskultur og sikkerhetsklima

Guldenmund (2000) skiller mellom sikkerhetskultur og sikkerhetsklima. Sikkerhetsklima betegner holdningene de ansatte har til sikkerhet i en virksomhet, mens sikkerhetskultur er det som ligger til grunn for holdningene (Guldenmund, 2000, s. 222). Det vil med andre ord si at sikkerhetsklima er et overordnet konsept av sikkerhetskulturen i en virksomhet. Guldenmund tar for seg ni definisjoner av sikkerhetsklima (se vedlegg 5). Hvor syv av ni definisjoner tar for seg sikkerhetsklima som ansattes persepsjon av sikkerhet på arbeidsplassen. Persepsjon er menneskers oppfattelse av sanseinntrykk. Det er en kompleks prosess, som består av en stimulering av en eller flere sanser, samt vår tolkning av stimuleringen (Svartdal, 2023).

Definisjonene (refererer til vedlegg 5) av sikkerhetskultur handler hovedsakelig om holdninger, dernest forståelser, karakteristikker og verdier (Guldenmund, 2000, s. 229). Guldenmund konkluderer med at skille mellom sikkerhetskultur og sikkerhetsklima er uklart (Guldenmund, 2000, s. 247), som har resultert i at flere bruker de om hverandre, sammen med begrepet sikkerhetsstyring (Fang & Wu, 2013, s. 138). Ettersom flere definerer sikkerhetsklima som persepsjon, foreslår Fang og Wu at sikkerhetsklima kan brukes for å måle sikkerhetskulturen. Ved å bruke en sikkerhetsklimaundersøkelse, kan man få innsikt inn i karakteristikkene og aspektene av sikkerhetskulturen i virksomheten (Fang & Wu, 2013, s. 139). For å skape en forståelse for sikkerhetskultur, kan det ofte være lurt å bruke en modell for å demonstrere begrepets funksjon. En sikkerhetskulturmodell søker å beskrive hvordan sikkerhetskultur antas å være integrert i virksomhetens praksiser og sikkerhetsstyring (Choudhry et al, 2007, s. 999). Flere teoretikere bruker Banduras Reciprocal Determinism som grunnlag ved utvikling av en sikkerhetskulturmodell.

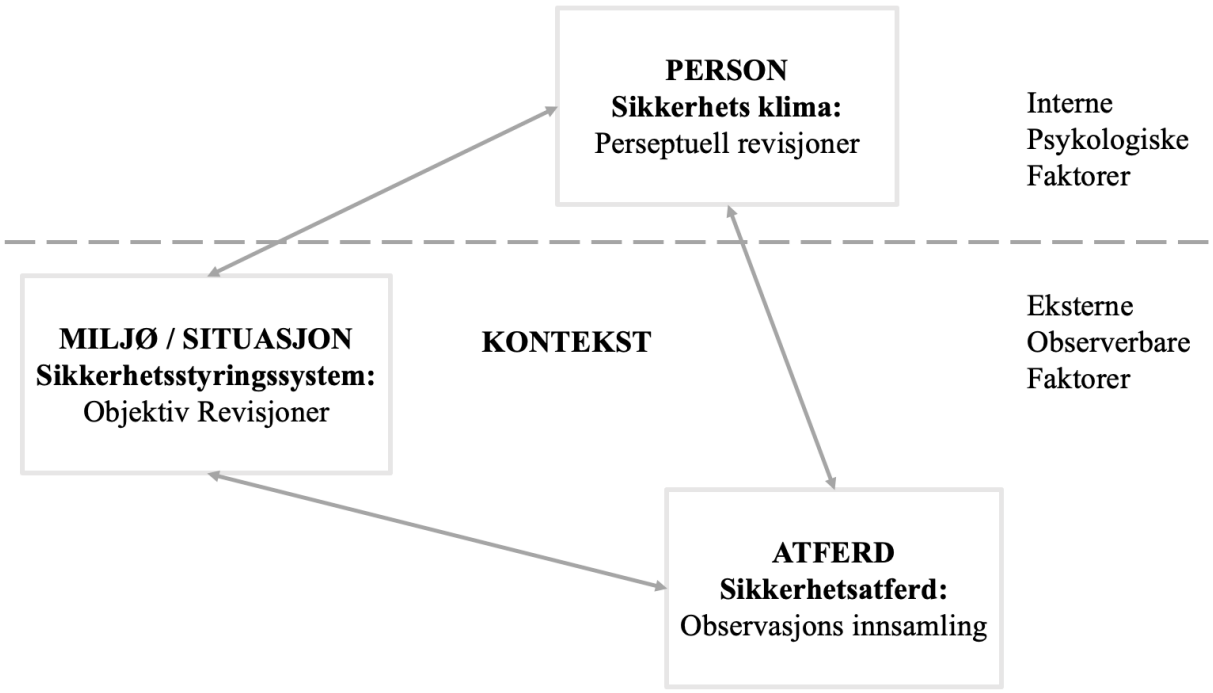
Banduras Reciprocal Determinism modell, også kalt Social Learning Theory, forklarer hvordan mennesker lærer av å observere hvordan andre mennesker oppfører seg. Eksempelvis, kan en ansatt tilpasse atferden sin etter å ha observert andre ansatte. Atferden vil videre bli endret og tilpasset gjennom selvkorrigerende vurderinger som baseres på informasjonen som samles fra

tilbakemeldinger. Som et resultat øker selveffektiviteten til den ansatte (Bandura, 1977; Cooper, 2000, s. 119). Figur 2. demonstrerer en oversatt versjon av Model of Reciprocal Determinism av Bandura 1977.



Figur 2. Model of Reciprocal Determinism

Figur 2 består av en triade av individers atferd, psykologiske faktorer og situasjonsfaktorer innen miljø, som påvirker hverandre og er gjensidig avhengig av hverandre (Fang og Wu, 2013, s. 140). Blant faktorene finner man en prosess som består av handling og reaksjon, der faktorenes påvirkning verken kan påvirke hverandre samtidig eller har nødvendigvis like sterk påvirkningsevne (Fang & Wu, 2013, s. 140). Det tar derfor tid før årsaksfaktoren utøver sine ringvirkninger og den gjensidige påvirkningen blir aktivert. Denne gjensidige innflytelsen betyr, med andre ord, at mennesker er både produsenter og produkter av miljøet de omgås i (Cooper, 2000, s. 119). Situasjoner er dermed like mye individets funksjon, som individets atferd er en funksjon av situasjonen (Bower, 1973; Cooper, 2000, s. 119).



Figur 3. Reciprocal Safety Culture Model

Denne forståelsen av hvordan mennesker forholder seg til sikkerhetskultur var grunnlaget for Coopers arbeid med å utvikle en sikkerhetskulturmodell. Figur 3 viser en oversatt versjon av Coopers (2000) Reciprocal Safety Culture Model (RSCM). Modellen plasserer sikkerhetsklimaet i samme "boks" som person. Dette er grunnet en sikkerhetsklimaundersøkelse vurderer interne psykologiske faktorer, som oppfatninger og holdninger. Sikkerhetsstyringssystemer bruker sjekklister som atferdsmessige sikkerhetstiltak for å vurdere sikkerhetsrelatert atferd. På den annen side brukes kontroller og revisjoner i sikkerhetsstyringssystemer for å vurdere situasjonsrelaterte faktorer (Cooper, 2000, s. 120-121). Det blir derfor mulig å måle sikkerhetskultur på ulike organisasjonsnivåer, fordi hver komponent i sikkerhetskulturen kan måles enten i kombinasjon eller separat. Noe som har vært vanskelig til nå (Cooper, 2000, s. 121). Dette gjør det mulig å bygge et felles rammeverk for sikkerhetskultur. Det er spesielt viktig for virksomheter som samarbeider tett med underleverandører fordi individer fra forskjellige virksomheter kan ha felles oppfatninger om sikkerhet (Cooper, 2000, s. 121).

Innledningsvis redegjorde vi for digital sikkerhetskulturs relevans i dagens samfunn. Dagens samfunn er avhengig av teknologi, og dermed ekstra utsatt for teknologiske trusler. Gjennom

digital sikkerhetskultur teori presenterte vi teoriens relevans og hvordan opparbeide en god digital sikkerhetskultur som kan bidra til å skape en robust sikkerhet i virksomheten. Som man ser, er denne teorien svært sentral for å skape et kunnskapsgrunnlag og teoretisk fundament for å se på hvordan ISO/IEC 27001 kan fungere som et hjelpemiddel for å stryke den digitale sikkerhetskulturen. Dermed blir neste steg å redegjøre for standardisering, som utgjør en del av den nødvendige grunnleggende kunnskapen for forskningsprosjektets tema.

3.2 Standardisering innen informasjonssikkerhet og risiko

Det finnes ulike forståelser av begrepet standard, men det mangles en omforent definisjon av begrepet (Engen et al., 2021, s. 48). Standard er blant annet regler som klassifiserer aktører eller objekter, definerer kvaliteten på produktet, produksjonsprosessen og handelen, viser til retningslinjer for institusjonell og organisatorisk atferd, samtidig som den setter krav til utarbeidelse av dokumentasjon og planlegging (Olsen et al., 2019, s. 5). I tillegg kan standarder og normer være avgjørende faktorer til å definere og veilede regjeringer og internasjonalt samarbeid, da de bidrar til å redusere transaksjonskostnader. Standarder er et viktig verktøy for å sikre kvalitet og pålitelighet i ulike typer aktiviteter. De kan omfatte alt fra målemetoder og kvalitetsstyringsstandarder til jobbkrav og samarbeidsprosedyrer (Olsen el al., 2019). Engen et al. (2021) definerer standardisering som allment aksepterte normer/regler som en mer avgrenset forståelse av begrepet (s. 48).

Normer er regler tilknyttet forventet atferd (Tjora, 2022), og kan deles inn i to typer: formelle normer og uformelle normer (Engen et al., 2021, s. 48). Uformelle normer er uskrevne regler, som er mer rettet mot ønsket, akseptabel og uønsket atferd. De innebærer forskjellig oppfatninger om hva forventet atferd er. Dette kan være normer som tilsier hvordan ting blir håndtert i de ulike organisasjonskulturene (Engen et al., 2021, s. 49). Formelle normer er ofte nedskrevne regler. De kjennetegnes ofte som "besluttet" gjennom en fungerende praksis, dermed kodifisert og nedskrevet (Engen et al., 2021, s. 49). Det eksisterer to forskjellige formelle normer. Vi har rettslige normer/regler som er lovregler som medfølger sanksjoner, og ikke-rettslige normer/regler som ikke er lovregler. Eksempler på ikke-rettslige normer/regler er retningslinjer, allment aksepterte standarder, faglige normer og tekniske standarder (som blant annet ISO/IEC 27001) som er utviklet gjennom ekspert- og profesjonssystemer (Engen et al., 2021, s. 49). Et relevant eksempel her er ISO. ISO definerer standard som et dokument utarbeidet av en anerkjent organisasjon, som gir retningslinjer, regler eller kjennetegn for

aktiviteter eller resultater, og er opprettet for felles og kontinuerlig bruk. Dokumentet er utviklet gjennom konsensus og vedtatt av organisasjonen for å sikre optimal orden i en bestemt sammenheng (Standard Norge, 2006; Engen et al., 2021, s. 49). Forståelsen av begrepene i dette prosjektet er: Standard blir definerte som et dokument som gir retningslinjer, formelle ikke-rettslige normer/regler eller egenskaper for aktiviteter eller resultater utarbeidet av ISO (Standard Norge, 2006; Engen et al., 2021, s. 48-49).

Det er flere grunner til at risikostyring har blitt standardisert. Blant annet handler risiko om fremtiden, noe som er umulig å nøyaktig forutse. Gjennom beregninger og logisk argumentering kan standarder skape en viss følelse av sikkerhet for fremtiden (Engen et al., 2021, s. 50). Det finnes flere definisjoner på begrepet risiko. Risiko er kjent for mange som et produkt av sannsynlighet og konsekvens (Engen el al. 2021, s. 92). Derimot bør man ta inn flere faktorer og innfallsvinkler, usikkerhet, den tilhørende kunnskapsstyrke, og kompleksitet, for å kunne tydeliggjøre risikodefinisjonen. Risiko kan bli opplevd og forstått ulikt med tanke på enkeltindivider, grupper, organisasjoner og institusjoner. I tillegg til å bygge broen mellom en teknisk-rasjonell forståelse og en samfunnsmessig forståelse av risikobegrepet (Engen el al. 2021, s. 93). Aven og Renn (2010) definere risiko som usikkerheten om alvorligheten av hendelser og konsekvenser eller resultater av en aktivitet som mennesker verdsetter (Engen el al. 2021, s. 93). Denne definisjonen ivaretar det kognitive, sosiale og de kulturelle dimensjonene av risikobegrepet, med et spesielt søkelys på det menneske verdsetter.

Risiko er ofte en konsekvens av flere faktorer og prosesser som oppstår uventet og kommer sammen på måter som ikke forventes. I slike situasjoner er det behov for et felles språk for å kunne forstå og å håndtere situasjonen. Standardisering av språk har gjort dette mulig (Engen et al., 2021, s. 51). Standardisering kommer derimot ikke foruten negative effekter. Standard og standardiseringens negative sider er at det kan være svært politisk og bli brukt som politiske virkemidler for å oppnå et mål, noe som grunner i standardens bidrag til koordinering og samarbeid mellom mennesker, organisasjoner og land. Dermed kan de fungere som både verktøy for kontroll og retningslinjer for akseptabel og etisk atferd (Olsen el al., 2019, s. 5). Standarder setter også krav som er til fordel for noen aktører og avverger fra andre, samtidig som standarder kan brukes som syndebukker dersom noe går galt (Olsen el al., 2019, s. 5). Standarder kan ikke straffes og er dermed en måte for enkeltmennesker og organisasjoner å unngå skyld og straff på. På denne måten fungerer standarder som makt uten ansvar. En negativ virkning av standard som politisk motivert er at arbeidsstandarden er knyttet til en maktaktør,

da den bør være vilkårlig. Dess mer vilkårlig standarden er – dess mer usynlig og nøytral fremstår den (Olsen el al., 2019, s. 5). Jore (2020) utrykker at standardisering av risikostyring kan føre til en overdreven følelse av sikkerhet (Engen et al., 2021, s. 51), dermed har aktørene som utarbeider standarder satt seg i en svært mektig posisjon (Büthe & Mattli, 2011; Engen et al., 2021, s. 51).

Det er et økende antall av standarder som blir grunnlaget for informasjonssikkerhet. Det finnes flere standarder som overlapper hverandre når det kommer til regulering av implementering av styringssystem for informasjonssikkerhet. Dermed kan man strukturere det systematiske arbeider for å generelt forbedre kvaliteten på informasjonssikkerhet og de risikoreduserende tiltak (NOU, 2015; Olsen, Juhl, Lindøe & Engen, 2020, s. 173).

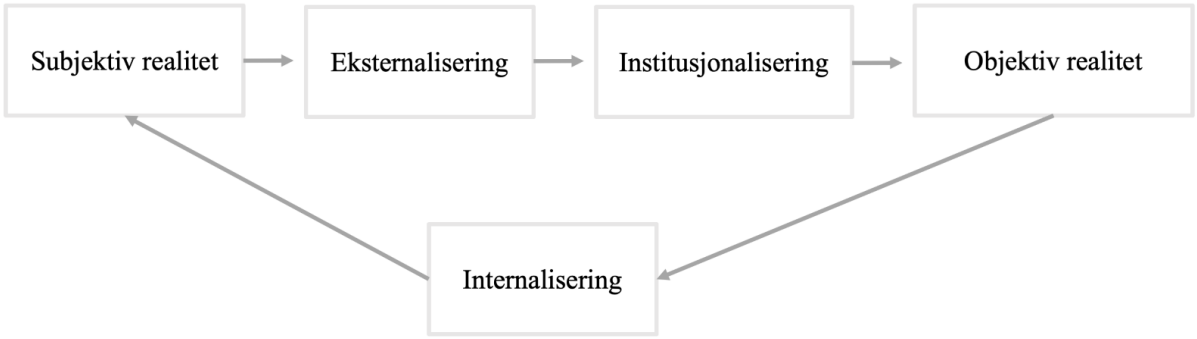
Det krever å ha en forståelse av nødvendigheten til å måtte tilpasse og justere standardene til en spesifikk bransje eller til en konkret kontekst. Hvis det erkjennes at standarder har mulighet for meningsskaping og tolkning, kan de internasjonale og globale standardene være en mulighet til å dele ekspertråd og god praksis for å øke informasjonssikkerheten (R. Skotnes i Olsen et al., 2020, s. 178). Det kan tenkes at den beste praksisen ikke er å følge oppskrifter preskriptivt for implementering av policyer, men som ideer om implementering (Niemimaa og Niemimaa, 2017). Det er imidlertid også viktig å huske at formelle systemer, som bruker standarder, må støttes av deres uformelle systemer, som bevissthet, tillit, forpliktelse og engasjement, for å kunne være effektive (R. Skotnes i Olsen et al., 2020, s. 178).

Denne teorien viser sammenhengen mellom formelle systemer (standarder) og uformelle systemer. De uformelle systemene trekker frem menneskeaspektet, som har lignede elementer til digital sikkerhetskultur, som innebærer tillit, kunnskap / bevissthet og interesse / engasjement. Dermed kan teorien brukes til å demonstrere en kobling mellom standard og digital sikkerhetskultur. For å kunne styrke en digital sikkerhetskultur ved bruk av standard som hjelpemiddel, må man forstå hvordan kulturer er oppbygde og endret. Dette leder oss til neste teori som tar for seg hvordan man endrer en sikkerhetskultur.

3.3 Hvordan endre en sikkerhetskultur

3.3.1 Oppbygningen av sikkerhetskultur

For å kunne se på hvordan sikkerhetskulturer kan endres eller forbedres, må vi forstå hvordan kulturer oppstår. Antonsen (2009) mener kultur kontinuerlig skapes gjennom daglig interaksjoner mellom medlemmer av et samfunn (s. 42). Ifølge Berger og Luckmann (1966) skaper sosiale interaksjoner mønster for atferd gjennom en prosess. De mener den sosiale virkeligheten er både subjektiv og objektiv. Det vil si at den sosiale virkeligheten er både et produkt av mennesker, samtidig som den sosiale virkeligheten eksisterte på et vis før hvert enkelt medlem av samfunnet eller organisasjoner. Det vil med andre ord si at den sosiale virkeligheten oppfattes som at den ikke er et produkt av mennesker, men oppstår under menneskelig interaksjoner og atferd over tid (Antonsen, 2009, s. 42).



Figur 4. Perspektiv på sosiale konstruksjon av virkeligheten

Figur 4 presentere en oversatt utgave av Berger og Luckmann sin modell (1966), som beskriver den sosiale konstruksjonen av virkeligheten. Modellen fungerer som et rammeverk for å forstå hvordan kulturer er skapt, omskapt og endret, og består av tre steg: eksternalisering, institusjonalisering, og internalisering. Antonsen forstår eksternalisering som måten individer anfører deres forståelse eller tolkning av verden inn i verden gjennom handlinger og uttalelser. Gjennom denne prosessen åpner det for tolkninger til andre individer, slik at de kan skape forventinger til hvilken atferd andre vil ha i fremtiden. Disse forventningene skaper grunnlaget for vanemessige handlinger, som er mønster som går igjen i samhandling og interaksjoner (Antonsen, 2009, s. 43). Disse vanemessige handlingene vil med tid bli det som føles som riktig å gjøre for de involverte aktørene, eller som de eneste alternativene for handling. Denne prosessen kalles institusjonalisering, der de sosiale mønstrene får et liv på egenhånd. Under denne prosessen blir de sosiale mønstrene objektivert, som betyr at de blir en del av en objektiv

realitet som omringer dem (Antonsen, 2009, s. 43). Gjennom denne prosessen havner den objektive sosiale realiteten tilbake i individers bevissthet, som påvirker hvordan individer ser verden. Da individer begynner å se verden gjennom de sosiale mønstrene og tilegner seg felles normer og verdier kalles det internalisering (Antonsen, 2009, s. 43).

Likevel bidrar ikke alle aktørers innflytelse på kulturen like mye til å forme den. Keesing (1987, 1994) argumenter for at påvirkningen makt og ideologi har på kultur blir ofte oversett (Antonsen, 2009, s. 43). Prosessen som danner kulturer, er en dynamisk kontinuerlig syklus som vil innebære konstant tolkning og endringer i eksisterende mønstre (Antonsen, 2009, s. 43). Dette perspektivet på hvordan kultur produseres antyder at ettersom kultur skapes, omskapes og endres gjennom daglig interaksjoner og ikke gjennom strategisk beslutningstaking, er kultur ustyrlig og uforutsigbar. Dermed er det ikke lett for en leder å endre kulturer. Det er på den andre siden noen forhold man kan endre; vekstforholdene. Å endre vekstforholdene til kulturen kan føre til kulturendringer, men igjen blir endringene uforutsigbare (Antonsen, 2009, s. 43).

Nielsen (2014) argumenter for at man kan skape kulturendringer ved å se på sikkerhetsklima. Sikkerhetsklima omhandler, som nevnt tidligere, delte persepsjoner innen virksomheten, blant annet om prosedyrer og praksis, både på et formelt og uformelt nivå (Reichers & Schneider, 1990; Nielsen, 2014, s. 8). Han går videre til å argumentere at til tross for at skille mellom sikkerhetskultur og sikkerhetsklima er uklart, er kultur mer abstrakt og stabilt enn klima som er lettere å manipulere (Guldenmund, 2000; Nielsen, 2014, s. 8). Schein (2004) hevder at organisasjonsklima er et uttrykk for den underliggende organisasjonskulturen. Ledere kan derfor bruke organisasjonsklima til å se på det dypere nivå innen kulturen i virksomheten (Nielsen, 2014, s. 8). Dov Zohar (2000) foreslår en annen vinkling på sikkerhetsklima. Sikkerhetsklima dannes gjennom arbeiderenes oppfatning av prioriteringen innenfor sikkerhetsmålene opp imot effektivitetsmålene under tilsyn eller oppfølging (Nielsen, 2014, s. 8). Denne forståelsen av sikkerhetsklima skaper en kobling mellom kulturen og klimaet, ettersom praksis under tilsyn styres av lederes grunnleggende antakelser (kultur) og brukes som retningslinjer for de ansattes handlinger etter hvordan de blir oppfattet (klima) (Nielsen, 2014, s. 8). Nielsen går videre til å påpeke at ikke all praksis under tilsyn er direkte koblet sammen med de grunnleggende antakelsene (kultur), ettersom det finnes flere andre faktorer som kan påvirke tilsynet. Likevel argumenterer Nielsen for at sikkerhetsklima og kultur ikke er avhengig av ett tilsyn ved praksis, men heller mønsteret av prioriteringer som oppstår av flere tilsyn over

tid. Dermed er kontinuerlig og vedvarende endringer i tilsyn med praksis nødvendig for å endre sikkerhetsklimaet og kulturen. Denne tilnærmingen er lederbasert, ettersom endringene kommer fra tilsyn fra ledere (Nielsen, 2014, s. 8).

Nielsen går videre til å argumentere for at endringer i kulturen eller klimaet ikke er en enkel lineær ovenfra-ned prosess, ettersom det innebærer uforutsigbare komplekse sosiale prosesser. Nielsen mener at ved bruk av en kompleks adaptiv systemteori (eller kompleks tilpasningssystemteori) skaper en betydelig forståelse av organisasjonsendringer (Nielsen, 2014, s. 8). Han argumenterer videre for at innen kompleks adaptiv systemteori er interaksjoner hovedkomponenten for endringer i kulturen, og endringene ligger i organisasjonen som en helhet og ikke hos et spesifikt individ. Samtidig som endringens natur er uforutsigbar og ukontrollerbar, ser teorien på selvorganisering som senter i endringsprosessen (Nielsen, 2014, s. 8). Selvorganisering er en prosess der organisering oppstår som et resultat av lokale interaksjoner blant elementene i et uordnet system (Koubatis & Schönberger, 2005). Dermed har ikke lederne av virksomheten full kontroll over endringsprosessen, og kan derfor heller ikke forutse endringene som vil følge. Som et resultat kan ikke endringen oppstå fra ovenfra-ned prosess, men heller oppstå gjennom de daglige interaksjonene i virksomheten. Ledere kan fremdeles påvirke endringene gjennom å styre interaksjonene (Nielsen, 2014, s. 8). Gjennom å kombinere teoriene om organisasjons kultur, sikkerhetsklima og komplekse adaptivt system teori kan man endre kulturen gjennom endring av mønstrene i interaksjonen innad i virksomheten (Nielsen, 2014, s. 8). Det er samtidig andre former ved endring eller forbedring av sikkerhetskulturen.

3.3.2 Forbedring av sikkerhetskultur

Det finnes ulike tilnærminger til hvordan en kan forbedre sikkerhetskulturen. Cooper (2001) hevder at det er flere faktorer som påvirker forbedringen av sikkerhetskulturen, som blant annet ledernes dedikasjon og involvering til å forbedre sikkerhetskulturen. Effektivt lederskap fra øverste ledelse er en nøkkelfaktor i en god sikkerhetskultur, ettersom deres involvering avgjør hvordan arbeiderene forstår og handler rundt sikkerhet. Involvering av hverandre, kan medføre en dynamisk forventning til tillit, ettersom at man ønsker å prestere for å kunne gi et ønsket resultat. Til tross for de mulige risikoene, kan den gjensidige tilliten bidra til å fremme en økende del for kunnskapsheving og engasjement, som er avgjørende for innovasjon (Svare,

Gausdal & Möllering, 2019). Det er viktig å poengtere at det ikke kun er teknologien som skal representere den største delen av de sikkerhetsmessige utfordringer, men menneskene rundt (Sjølstad, Høie, & Daler, 2010, s. 37).

Cooper går videre til å uttrykke hvordan sikkerhetsstyring ofte ikke er et tema som engasjerer mange toppledere og andre ledere (Cooper, 2001, s. 30). De to viktigste faktorene for et godt og effektivt lederskap er en atferd som er både omsorgsfull og kontrollerende. Omsorgsfull atferd innebærer å passe på de ansattes velvære, hjelpe de ansatte ved ulike behov, og etablere et godt forhold til de ansatte, etablere en god toveiskommunikasjon da lederen skal forklare noe og være tilgjengelig. Mens kontrollerende atferd innebærer å fastsette mål, passe på at ytelsesstandarder blir opprettholdt, klargjøre de ansattes jobbroller, forventninger og ansvar, samt med å motivere sine ansatte til å følge prosedyrer og regler (Cooper, 2001, s. 31).

En annen viktig faktor for bedring av sikkerhetskultur er ansattes involvering eller ansattes holdning til sikkerhet. Cooper uttrykker at det ofte er dårlig sikkerhetsholdninger som leder til ulykker. Videre argumenter han for at selv om disse ulykkene oppstår grunnet dårlig sikkerhetsholdninger, stammer flertallet av ulykkene av dypt integrert utrygg atferd blant de ansatte. Dersom man bruker formaliserte sikkerhetsatferd initiativer kan man arbeide med denne utfordringen, gjennom å opparbeide en sikkerhetsatferd som jobber proaktivt for å sette fokus på en god sikkerhetsatferd. Cooper vektlegger at en stor mengde forskning viser til at ved å gjennomføre sikkerhetsatferd initiativer vil nesten alltid resultere i en positiv endring i sikkerhetsytelse og sikkerhetsholdninger (Cooper, 2001, s. 225).

Ledelsen må med andre ord jobbe aktivt for å få sine ansatte til å legge i så mye innsats som mulig få å opparbeide en proaktiv sikkerhetskultur. Det er to typer tilnærming for å klare å vinne de ansattes støtte og entusiasme: passiv og aktiv. Den aktive tilnærmingen innebærer å skape innsats gjennom å delegere ansvar for den daglige sikkerheten til de ansatte. Cooper går videre ved å poengtere at denne tilnærmingen ofte har vært et vellykket bidrag for å utvikle en proaktiv sikkerhetskultur (Cooper, 2001, s. 178). Den passive tilnærmingen gir de ansatte en generell oppfordring til å tenke og handle trygt, og inkluderer sikkerhetstrening. Denne tilnærmingen har, på den andre siden, ofte en begrenset suksess for å opparbeide en proaktiv sikkerhetskultur (Cooper, 2001, s. 178). Som leder oss til neste viktige faktor for å opparbeide en god sikkerhetskultur: Sikkerhetstrening og læring om sikkerhet. Det finnes ulike fremgangsmåter for å lære sine ansatte om sikkerhet, blant annet gjennom sikkerhets

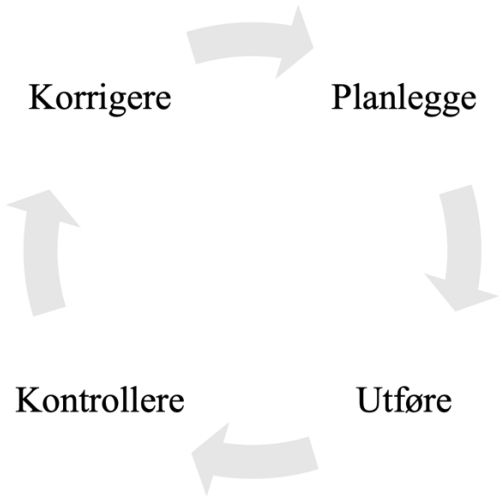
propagander og sikkerhetstrening. Sikkerhets propagander omhandler ofte å skremme sine ansatte til å ta sikkerheten på alvor, eksempelvis "On one end of this CABLE is a 240 volt mains supply, on the other is a DEAD MAN" (Cooper, 2001, s. 178). Slike propagander har ikke hatt den forventet effekten som folk ofte tror. Forskning viser at noen av propagandaene har oppnådd endringer i holdningene og skape frykt på kort sikt, men lite suksess ved å endre atferden (Cooper, 2001, s. 178). Sikkerhetstrening er den mest vanlige formen for å endre ansattes sikkerhetsatferd og holdning. Ifølge Cooper viser forskning at trening er en av de viktigste bidragene som fører til at selskaper kan gå fra høy til lav ulykkes frekvens. Samtidig som det også finnes forskning som viser til at sikkerhetstrening ikke medfører varige endring hos ansattes sikkerhetsatferd og holdninger (Cooper, 2001, s. 182).

Da Cooper har en ledelse baser tilnærming til endring/forbedring av sikkerhetskultur har Antonsen en antropologisk tilnærming. Antonsen mener at da forskere ikke tar for seg den antropologiske tilnærmingen utelukker de flere begrensninger, som er iboende i et mer sosialt konstruktivistisk kultursyn (Antonsen, 2009, s. 103). Ettersom Antonsen definerer kultur som at den dannes i de daglige interaksjonene, og blir konstant endret og utvikles gjennom sosiale interaksjoner, mener han derfor at det ikke finnes en "one-size-fits-all" tilnærming til kultur. Samtidig mener han at sikkerhetskultur og organisasjonskultur ikke blir endret av strategisk beslutningstaking, og er derfor vanskelig for ledelsen å endre, men man kan som nevnt tidligere endre "vekstforholdene" til kulturen (Antonsen, 2009).

I denne teorien blir det presenter ulike perspektiver for endring og forbedring av sikkerhetskultur. Noen teorier er ledelse basert, mens noen ser tar for seg kulturendringer som skapes av samfunnet som en helhet. Denne teorien skaper et godt kunnskapsgrunnlag for analyse av empirien til forskningsspørsmål 1, samtidig som den skaper en grunnleggende forståelse for hvordan ISO/IEC kan ha en innvirkning på digital sikkerhetskultur. Ettersom kultur endres og skapes gjennom daglige interaksjoner, trengs det å jobbe kontinuerlig for å skape en positiv endring. Som leder oss til neste teori, kontinuerlig forbedring, der det presenteres to ulike verktøy for kontinuerlig forbedring.

3.4 Kontinuerlig forbedring

Kulturendringer er en av flere hovedutfordringer som virksomhetene må overkomme. Dersom en virksomhet klarer å håndtere kulturendringene vil virksomheten ha en høyere sannsynlighet for å få en suksessfull standardisering, og være mer egnet for innovasjon (Culot et al., 2021, s. 90). Gillies (2011) tar for seg hvordan «Five stages to information security» (5S2IS) og fire trinns kvalitets forbedringsmetoden PUKK (Planlegge - Utføre - Kontrollere – Korrigere) som kan brukes i ISO/IEC 27001 sitt kap. 10 om kontinuerlig forbedring (s. 371).



Figur 5. PUKK hjulet

PUKK blir illustrert i figur 5, som er et kvalitetsstyringssystem og en kontinuerlig forbedringsmetode for organisasjoner i ulike bransjer (Isniah, Hardi Purba, & Debora, 2020). Metoden begynner med planleggingsfasen, der det skal identifiseres et problem "Hva har skjedd?", deretter analyserer problemet "Hvordan oppsto problemet? Hvilke virkninger har etterfulgt?". Ved at disse faktorene har blitt besvart, lages det en plan for hvordan en skal gå videre. Neste steg er utførelse, der virksomheten implementerer endringen i henhold til planen. Videre skal implementeringen kontrolleres. Det skal gjennomgå test, analysere resultatene og identifisere læringspunkter. "Hva ble resultatet? Gikk planen som forventet? Hvilke effekter fikk implementeringen?". I korrigeringsfasen vil det foretas handlinger basert på de tidligere læringspunkter. Hvis endringen var vellykket, kan virksomheten innføre lærdommen de fikk fra prosessen og iverksette det i en større skala i organisasjonen. Dette kan innebære å lage en standardisert plan for å løse problemet om det oppstår igjen. Hvis endringen mislykkes, må det

gjennomgås hele prosessen på ny, men med en annen plan (Johnson, 2002). Ved å implementere, uten å korrigere og kontrollere, kan det bidra til tap av ressurser og uønsket hendelser. Dermed er det viktig å eliminere det mulige tapet som kan forekomme, ved å foreta korrigeringer (Madan, Jagtap & Teil, 2014). Ved at prosessen gjentas flere ganger, vil det være i stand til å identifisere nye løsninger og forbedringer (Madan et al., 2014).

5S2IS er en kombinasjon av PUKK og Capability Maturity Model (Gilles, 2011, s. 373), samtidig som den bygger på det grunnleggende fundamentet til ISO/IEC 27001 (Humphrey, 1989). 5S2IS tar utgangspunkt i de fire stegene i PUKK, og blitt videre utviklet til fem steg for en kontinuerlig forbedringsprosess (Gilles, 2011, s. 373). Steg én: lag en plan, steg to: lag en protokoll basert på planen, steg tre: mål organisasjonens ytelse basert på protokollen, steg fire: bruk målene fra trinn tre til å forbedre ytelse og minimere avvik, og til slutt omhandler steg fem: om å innarbeide kontinuerlig forbedringsprosessen i virksomheten (Gilles, 2011, s. 374).

Gillies fremhever at systematisk bruk av 5S2IS eller PUKK vil det hjelpe virksomheter med å utvikle og forbedre informasjonssikkerhetens kvalitet. Det blir poengtert hvordan tredje trinn måler organisasjonens progresjon og ytelse i henhold til Standardens retningslinjer fra trinn 2. Det vektlegges viktigheten med å overvåke organisasjonen i overgangen mellom trinnene, spesielt når organisasjonen går fra strategisk forpliktelse til implementering av ISO/IEC 27001. Denne overgangen er forbundet med å ha en betydelig endring på organisasjonskulturen. Forutsatt at den overgangen krever en betydelig akseptering og følelse av eierskap fra ansatte på tvers av organisasjonen (Gillies, 2011, s. 374).

Den kontinuerlige forbedringsprosessen som kommer ved bruk av PUKK, vil kunne bidra til å sjekke de små effektene som kan forekomme av systemet, deretter går det dypere på større og mer spesifikke forbedringer. Implementereringen av PUKK som et kvalitetsstyringssystem kan resultere i å kunne løse problemer ved å forbedre en prosess eller et system i en organisasjon, samt å øke produktivitet (Isniah et al., 2020). Denne metoden iverksettes ofte for å kunne forbedre virksomheten sikkerhetskulturer.

Kontinuerlig forbedring er en sentral del av Standarden, som inneholder et kapittel dedikert til krav om kontinuerlig forbedring. Dermed viser denne teorien til nødvendigheten ved bruk av kontinuerlig forbedring i standardiseringsprosessen. Den utgjør derfor en sentral del i samspillet

mellom ISO/IEC 27001 og digital sikkerhetskultur, da den kan brukes som et forbedringsverktøy for den digitale sikkerhetskulturen. Neste steg i forskningsprosjektet er redegjøring av den metodiske fremgangsmåten som har blitt disponert.

Ut fra denne teorien ser man at kontinuerlig forbedring er en sentral og nødvendig del av implementeringen og etterlevelsen av ISO/IEC 27001. Samtidig som man ser i steg tre av 5S2IS at kontinuerlig forbedringsverktøyet kan påvirke kulturen i virksomheten. Dermed blir dette et sentralt verktøy for hvordan ISO/IEC 27001 kan påvirke digital sikkerhetskultur. Gjennom teori kapittelet som en helhet, har vi presentert fire teorier som bidra til å skape et kunnskapsgrunnlag for prosjektets videre forskning. Neste steg i forskningen er redegjøring for det metodiske valget for data innsamling, som skal videre brukes opp mot teoriene presentert i dette kapittelet.

4 Metode

I dette kapittelet vil den metodiske fremgangsmåten for vårt forskningsdesign og den logiske tilnærming bli forklart og begrunnet. Dette kapitlet vil ta for seg prosessene ved fremgangsmetoden, rekruttering av informanter, datainnsamling, transkribering, datareduksjon og analyseprosess. Utfordringer og endringer vil også bli diskutert, samt prosjektets reliabilitet og validitet.

4.1 Eksplorerende forskningsdesign

Dette forskningsprosjektet vil ta for seg eksplorative forskningsdesign, som vil si at det vil utforske et emne der det er mangel på eksisterende forskning og problemstillingen kan bli uklar (Grenness, 1997). Den eksplorerende problemstillingen har som formål å formidle det en vet lite om (Jacobsen, 2000), og etter vår oppfatning og litteratursøk finnes det lite forskning om hvordan standardisering av ISO/IEC 27001 kan påvirke og potensiell styrke virksomhetenes digitale sikkerhetskultur. Utformingen av masteroppgavens problemstilling og forskningsspørsmål har blitt endret flere ganger. Med eksplorerende problemstilling får en mer detaljert innsikt i hva fenomenet egentlig består av. Fenomenet vil bli konkretisert for å kunne få en bedre forståelse av hva en ønsker å fastsette de aktuelle variabler og tilføre innhold (verdier) til variablene (Jacobsen, 2015, s. 80). I begynnelsen av forskningsprosjektet var det ikke en klar hypotese på hva som skulle forskes på. Desto mer kunnskap og innsikt vi fikk fra forskningen og datainnsamling, ble problemstillingen og hypotesen tydeligere for å kunne avdekke ny kunnskap om fenomenet (Lysgaard, 1967; Jacobsen, 2015, s. 79-80).

Formålet med eksplorerende design er å kunne utforske nærmere et tema som forskeren i utgangspunktet vet lite om før oppstart (Silkoset, Olsson & Gripsrud, 2021). Dette forskningsprosjektet bruker dybdeintervjuer for å utforske detaljene av problemstillingen. Ved undersøkelse av problemstillingen blir det utført en kvalitativ tilnærming av ansatte ved ulike virksomheter. De utvalgte informantene representerer forskjellige fagområder, som dekker tematikken til forskningsprosjektet, som blant annet innen standardisering, ISO, informasjonssikkerhet, ISO/IEC 27001 og sikkerhetskultur. Formålet ved forskningen er i

første omgang å skape en forståelse av det belyste fenomenet, ISO/IEC 27001, sin mulige innvirkning på den digitale sikkerhetskulturen (Silkoset et al., 2021, s. 69).

En kvalitativ studie innebærer innsamling og analyse av data som vanligvis uttrykkes gjennom tekst, der innsamling av data fra dybdeintervjuene kan oppleves som ustrukturert (Grønmo, 2016). Formålet ved bruk av kvalitativ metode er å oppnå kunnskap som går i dybden på fenomenet, for så å skape en helhetlig forståelse (Grønmo, 2016). Innenfor den kvalitative metoden brukes det en abduktiv forskningslogikk til forskningen. En abduktiv forskningslogikk forsøker å skape en forståelse av et fenomen, fremfor en begrunnelse (Blaikie & Priest, 2019, s. 99). Ved bruk av en abduktiv forskningslogikk vil dette forskningsprosjektet få en økt innsikt om teoriene om standardisering og digitale sikkerhetskultur, som videre åpner for å trekke inn nye vinklinger fra de semistrukturerte dybdeintervjuene. Med informantenes besvarelser om Standardens virkning på virksomheten, fikk vi mulighet til å trekke inn faktorene som kunne endre fenomenet.

4.2 Forskningsprosess

I begynnelsen av forskningsprosjektet har det blitt brukt OpenAI sin ChatGPT for idemyldring rundt vår problemstilling, for å kunne få en økt innsikt. Ved bruken av ChatGPT ønskes det å se hva algoritmene tilnærmer seg til vår tematikk, og se på hvilke vinklinger og teorier som kan bli aktuelle å bruke. Dette kan gi oss en mulighet for å finne relevante teorier som vi nødvendigvis ikke hadde funnet ved søk gjennom Google Scholar eller andre søkemotorer. Derimot tar vi hensyn og påpeker til at ChatGPT ikke alltid henviser til pålitelige kilder, og dermed har vi vært kritiske. Ved bruk av relevante innhold produsert fra ChatGPT, har det blitt utført en grundig gjennomgang og kontrollsjekk om informasjonen stemmer med den ordinære kilden.

Informasjonen har samtidig blitt innhentet gjennom ulike former for data. De fleste av artikkelen som teorien baseres på har blitt funnet gjennom søkemotorene som Google Scholar, Oria og Researchgate. Begrunnelsen for bruk av disse søkemotorene er ikke kun for å finne relevant litteratur, men som også gir oss mulighet til å se hvilke forfattere står bak litteraturen og hvor mange som har siterte artikkelen. Den åpner dermed for mulighet til å sjekke hvor pålitelig kilden er.

4.3 Forskningsforløp

Forskningsprosjektets utforming startet i november 2022, og inneholdt på det tidspunktet en helt annen vinkling. Den daværende vinklingen omhandler bevisstgjøring om digital sikkerhet i transnasjonale selskaper, senere ble den spisset til sikkerhetskultur. Til slutt falt det på den nåværende problemstillingen om samspillet mellom ISO/IEC 27001 og digital sikkerhetskultur. Problemstillingen startet veldig generell uten noen konkret tilnærming til hvilken ISO-standard og sikkerhetskultur, deretter avgrenset vi det til ISO/IEC 27001 og digital sikkerhetskultur. Grunnen for at den ble avgrenset til en mer dagsaktuell tilnærming, frem for den "tradisjonelle" sikkerhetskulturen, som har en personsikkerhet og personskade fokus. Deretter ble det naturlig sette søkelys på en ISO-standard som tar for seg styringssystem for informasjonssikkerhet. I motsetning til ISO 45001 - Ledelsessystemer for arbeidsmiljø, som er mer rettet mot HMS.

Underveis i utformingen av forskningsprosjektet har vi vært i kontakt med et firma, som har fungert som en portåpner og ekstern rådgiver. Disse har bidratt til å gi oss et innsyn inn i hvordan en ISO-standard fungerer, gitt råd ved utforming av problemstilling og tematikk, og bidratt i å finne aktuelle informanter. Det er ønskelig å presiseres at vi hadde seks veiledninger med vår tildelte veileder, der vinklingen på oppgaven ble tilpasset rådene. Dermed har utformingen av oppgaven vært i konstant utvikling.

4.4 Datainnsamling

4.4.1 Kvalitativt intervjuer

Gjennomførelsen av datainnsamling er basert på semistrukturerte dybdeintervju med hjelp av en intervjuguide. For å oppnå formålet med kvalitativt dybdeintervju, vil det være mest hensiktsmessig å bruke en fenomenologisk tilnærmingsmetode. Fenomenologi fokuserer på hvordan sosiale fenomener forstås og oppleves, noe som gir en god forståelsesramme for datainnsamlingen for forskningsprosjektet (Krumsvik, 2013, s.62; Tjora, 2012). Fenomenologi vil hjelpe dette forskningsprosjektet til å se hva som bygger på de menneskelige erfaringene og kan dermed gi innsikt i intervjuobjektenes meninger og opplevelser av ulike fenomener rundt standardisering og digital sikkerhetskultur (Brinkmann & Kvale, 2015). Semistrukturerte dybdeintervjuer ga det oss muligheten til å få detaljert informasjon om informantenes oppfatninger, holdninger og opplevelser. Dette kan føre til en dypere forståelse av fenomenet som studeres.

Til vårt formål, har vi valgt å benytte semistrukturerte intervjuer ved hjelp av en intervjuguide som tar for seg spesifikke temaer (Brinkmann & Kvale, 2015, s. 46). Intervjuguiden ligger i vedlegg 1. Vi startet hvert intervju ved å forsøke å forstå informantens kunnskap og erfarings historikk. Ved å stille spørsmålet "Kan du fortelle litt om deg selv?" åpner det opp for at informanten selv velger hva hen synes er viktig å fremheve. Vi har i tillegg syntes det har vært viktig å forstå informantene sitt forhold og oppfatning av digital sikkerhet og ISO/IEC 27001. Det var fremstilt ulike forståelse og definisjoner blant informantene. Ved å få høre informantene sin egen definisjon av tematikken, åpnet det for at forskerne vurderte validiteten og reliabiliteten av datainnsamlingen.

Gjennom de semistrukturerte dybdeintervjuet har vi innhentet informasjon og beskrivelser fra informantene sin oppfatning på de utvalgte tematikkene, med særlig fokus på deres meninger og oppfatninger av fenomenene. Det har blitt utført justeringer på noen av spørsmålene i intervjuguiden etter hvem informanten er, i hensikt for å tilpasse informantens fagfelt og kunnskap. Intervjuguiden legger opp spørsmålene slik at de er åpne, noe som gir informantene mulighet til å utdype seg som de ønsker (Tjora, 2012, s.104 - 105).

4.4.2 Valg av informanter

Utvalget av informantene i dette forskningsprosjektet er samlet gjennom en strategisk utvelgelse. Strategisk utvelgelse innebærer å ta hensyn til ulike faktorer, som for eksempel tilgjengelighet av data, ressurser og tid. Der vi tilegnet oss informasjon på ulike virksomheter som kunne utale seg om ISO, ISO/IEC 27001, digital sikkerhetskultur, informasjonssikkerhet og/eller standardiseringsprosesser. Det ble brukt en kriteriebasert utvelgelse av informanter med snøballmetoden. Kriteriebasert utvelgelse baserer seg på at informanter velges ved at de oppfyller spesielle krav (Johannessen el al., 2016, s. 120). Kravene for dette forskningsprosjektet er at informantene skal oppfylle kriteriet (1) eller (2), eller begge. Kriteriet (1) er at informanten har kjennskap til informasjonssikkerhet og ISO/IEC 27001. Kriteriet (2) er at informanten har kjennskap til standarder og standardiseringsprosesser. Med snøball metoden ble informantene rekruttert ved at forskerne forhøret seg med personer som vet mye om temaet som skal forskes på. Deretter kan de anbefale hvem vi bør ta kontakt med videre (Johannessen el al., 2016, s. 119). Dette ble gjort med å ta kontakt med nettverk på LinkedIn og bekjente i fagmiljøet.

Gjennom grundig forarbeid har vi vært i stand til å velge ut de ideelle informanter for å besvare problemstillingen. Etter en strategisk og strukturert utvelgelsesprosess, fikk vi 10 informanter (se tabell 1). Prosjektet hadde et mål og ønske om å få flere informanter til datainnsamlingen. Det ble sendt ut flere henvendelser til aktuelle informanter, men enkelte personer og virksomheter besvarte ikke våre henvendelser. De aktuelle informantene som svarte at de ikke kunne delta, begrunnet dette med manglende tid samt skepsis til å delta i forskingsprosjektet grunnet bedriftssikkerhet. Utvalget av informanter til dette forskningsprosjekter er ikke nødvendigvis fullverdig representativt, men vil likevel bidra til økt kunnskap om ISO/IEC 27001 som et virkemiddel for å styrke den digitale sikkerhetskulturen.

Til tross for et lavere utvalg av informanter enn først tiltenk, er det likevel et bredt utvalg innenfor tematikken. Dette er til tross for at informantene som ble valgt for å delta i forskningsprosjektet ikke representere hele populasjonen, likevel ønskes det å påpeke at studiens formål er å undersøke hvordan virksomheters digitale sikkerhetskultur kan bli påvirket.

Informant	Arbeidsstilling
Informant 1	Seniorrådgiver HMS & kvalitet
Informant 2	IT-Direktør
Informant 3	Rådgiver HMS & kvalitet
Informant 4	CISO
Informant 5	Seniorrådgiver HMS & kvalitet
Informant 6	Juridisk rådgiver
Informant 7	Seniorrådgiver HMS & kvalitet
Informant 8	Revisjonsleder
Informant 9	Cyber security manager
Informant 10	Daglig leder

Tabell 1. Oversikt over informanter

4.4.3 Utførelse av intervjuene

Intervjuene ble utført i april og mai 2023 og med en varighet på ca. 30 – 60 min. Alle intervjuene tok plass det digitale samtaleverktøyet, Teams, ettersom flere av informantene er bosatt i andre deler av Norge og det var et alternativ som er fleksibelt i forhold til oppgavens tidsbegrensning.

Intervjuene ble utført likt slik at det ikke var en faktor som kunne skape ulikheter i data innsamlingen. Begge forskerne var til stede under alle intervjuene og det ble avklart på forhånd hvem som skulle intervjue informanten og hvem som skulle observere. Intervjuene ble gjennomført med lite nettverksproblemer. To av intervjuene ble utsatt for små korte forstyrrelser, men det ga ikke noen tydelige endringer eller påvirkning på informantenes besvarelse. Intervjuene ble tatt opp med lydopptak, dette ble gjennomført med at informantene fikk denne opplysningen ved første henvisning, i informasjonsskrivet og samtykkeerklæringen, samt muntlig i begynnelsen av intervjuene. Intervjuene ble tatt opp med en iPhone med Nettskjema-diktafon appen. Opptakene ble direkte lastet opp og sikret lagring på Nettskjema, som er i tråd med personvernretningslinjene. I forskningsprosjektets oppstart ble prosjektskissen sendt til Sikt for godkjennelse for å kunne behandle personopplysninger, som behandling av personstemmer. I begynnelsen og slutten av intervjuene ble det også oppklart til informantene, at de har rettigheter til å trekke informasjonen dersom de skulle ønsket det. Kun en av informantene oppga noe informasjon som hen ikke ønsket at skulle inkluderes i prosjektet, og dette ble dermed ikke transkribert av forskerne.

4.5 Datareduksjon og datanalyse

Intervjuene ble utført i april og mai 2023 og med en varighet på ca. 30 – 60 min. Alle intervjuene tok plass det digitale samtaleverktøyet, Teams, ettersom flere av informantene er bosatt i andre deler av Norge og det var et alternativ som er fleksibelt i forhold til oppgavens tidsbegrensning. Intervjuene ble utført likt slik at det ikke var en faktor som kunne skape ulikheter i data innsamlingen. Begge forskerne var til stede under alle intervjuene og det ble avklart på forhånd hvem som skulle intervjue informanten og hvem som skulle observere. Intervjuene ble gjennomført med lite nettverksproblemer. To av intervjuene ble utsatt for små korte forstyrrelser, men det ga ikke noen tydelige endringer eller påvirkning på informantenes besvarelse. Intervjuene ble tatt opp med lydopptak, dette ble gjennomført med at informantene fikk denne opplysningen ved første henvisning, i informasjonsskrivet og samtykkeerklæringen, samt muntlig i begynnelsen av intervjuene. Intervjuene ble tatt opp med en iPhone med Nettskjema-diktafon appen. Opptakene ble direkte lastet opp og sikret lagring på Nettskjema, som er i tråd med personvernretningslinjene. I forskningsprosjektets oppstart ble prosjektskissen sendt til Sikt for godkjennelse for å kunne behandle personopplysninger, som behandling av personstemmer. I begynnelsen og slutten av intervjuene ble det også oppklart til informantene, at de har rettigheter til å trekke informasjonen dersom de skulle ønsket det. Kun

en av informantene oppga noe informasjon som hen ikke ønsket at skulle inkluderes i prosjektet, og dette ble dermed ikke transkribert av forskerne.

4.5.1 Analyse og tolkning

Etter transkriberingen ble datamaterialet kodet, bearbeidet og analysert. Først ble transkriberingen lest gjennom på nytt, slik at vi fikk en oversikt og ideer for arbeidet videre. I den neste fasen av behandling av datamaterialet, gikk vi gjennom besvarelsene, refleksjonene og skildringene fra lydopptakene. Deretter ble de utvalgte tekstene fra transkriberingen kodet ved å finne meningsbærende enheter som var relevante for problemstillingen (Johannessen et al., 2015, s. 174). Forskerne jobbet hver for seg i denne fasen, der man individuelt markerte og organiserte datamaterialet i ulike farget markeringstusjer. Hver meningsbærende enhet fikk sin egen farge, samt med en kommentar med stikkord, temaer eller ideer for det videre arbeidet i analysen. Et eksempel på dette blir illustrert i tabell 2.

Illustrerende utsagn (Naturlig enhet)	Meningsbærende enhet (Deskriptiv koding)	Overordnet tema (Tolkende koding)
«Du må ha en leder som har kompetanse og vet hva han snakker om. Det begynner alltid der. (...) Har du en leder som ikke bryr seg så vil det smitte over på alle i organisasjonen. (…). Den største utfordringen er jo alltid ledelsen.»	Ledelse bør være til stede for å fremme kompetansen, da dette kan ha en overførende effekt på de ansatte.	Endring av digital sikkerhetskultur
«De ansatte blir mer bevisste. Det handler om å forstå risikoer og det handler om å rette seg etter rutiner som skal på plass. Så når det blir en vane, så blir det en kultur. Tenker det vil medføre endringer i kulturen, siden du er nødt til å etablere nye vaner.»	Bevissthet rundt sikkerhet og risikoer skaper forståelse, som videre kan skape vaner og endringer i kulturen.	
«De må ikke bare henge seg opp i policys og rutiner og gamle måter å gjøre det på. De må henge med på hva teknologisk utvikling og hva er det teknologiske trusselbilde som også endrer seg hele tiden.»	Ytre forhold kan påvirke og utvikle de interne forhold i virksomheten.	

Tabell 2. Eksempel på koding benyttet i analysen.

Etter koding, bearbeidet vi empirien ved å sortere, kategorisere, og klargjøre for analysen. I dette forskningsprosjektet benyttet vi oss av en tematisk analyse for bearbeiding av datamaterialet. Tematisk analyse er anbefalt å bruke da den anses som fleksibel og lett anvendelig for nye forskere (Braun & Clark, 2006). Valg av denne metoden begrunnes med at den er enkel og nyttig å bruke for å kunne se helheten og sammenhenger i materialet. Neste fase ble utført i fellesskap, der vi diskuterte og trakk ut relevante tekster fra empirien. De markerte utsagnene med kommentarer ble samlet i et eget dokument, sortert etter farge. I analysedokumentet analyserte vi temaene etter felles mønstre, avvik, sammenhenger og fellestrekk. På denne måten kan man oppdage viktige funn og sammenhenger i materialet, for å kunne besvare forskningsspørsmålene. Vi ønsker å understreke at ved analysering av datamaterialet formulerte vi spørsmålet på en slik måte at de åpnet for at informantene selv kunne velge hva de ønsket å fortelle. Dermed oppstår det et mulig avvik i statistikken, da formulering som "80 prosent av informantene nevnte …", betyr det imidlertid ikke at de resterende 20 prosentene var uenig, kun at dette var et element som ikke kom opp i samtalen. Det er også viktig å bemerke at sitatene i analyse kapittelet blir fremhevet med innrykk, slik at det skal være en tydelig forskjell mellom sitat og analyse.

Ut fra analysedokumentet utformet vi tankekart for hver meningsbærende enhet, for å systematisere kodene til overordnet temaer (Braun & Clark, 2006). Dette skapte en oversikt av kodene, som hjalp med å kunne se sammenhengene. Samtidig kunne man se kodene som ikke lenger var relevante. Ved bruk av koding kom vi frem til to hovedtemaer; (1); Endring av digital sikkerhetskultur (2); Innvirkende faktorer fra standardiseringsprosessen på den digitale sikkerhetskulturen. Etter systematiseringen av tankekartene, ble temaene og faktorene sett opp mot relevante teorier. Ved å se analysen opp mot relevant teori fikk vi en oversikt over de mest relevante teoriene for vårt prosjekt.

4.6 Kvalitetskriterier

4.6.1 Reliabilitet

Reliabilitet er knyttet til forskningsprosjektets pålitelighet og krever nøyaktige målinger for å kunne identifisere eventuelle feilmarginer (Dalland, 2020, s. 43), i tillegg kreves det at forskningen er etterprøvbar. Påliteligheten er et grunnleggende element for kvaliteten av datamaterialet i dette forskningsprosjektet. Den metodiske fordelen ved bruk av semistrukturert dybdeintervju er at den åpner for en mulighet til å tilpasse intervjuguiden etter informantens

kunnskap. Likevel har undersøkelsesopplegget en grunnleggende base i intervjuguiden, som gir samsvar fra gjentatte datainnsamlinger mellom datasettene (Grønmo, 2016, s. 240-241). Redegjøring for hvordan dette prosjektet har samlet inn data og hvilke feilkilder som kan påvirke resultatet, gir mulighet for at leseren selv kan vurdere påliteligheten i dette prosjektet (Dalland, 2020).

Datainnsamling innen kvalitativ forskning er ofte ustrukturert, samtidig kan kunnskapen man innhenter være verdiladet og kontekstavhengig. Derfor vil de forskningsmessige kravene til studiens funn om reproduksjonsbarhet være lite hensiktsmessige, fordi det er lite sannsynlig at en annen forsker kan oppnå de eksakt samme resultatene (Johannessen et al, 2021, s. 229). For å forsterke studiens relabilitet har vi vært tydelige med fremgangsmåter, bruk av sitater, og presentert flere teorier samt tidligere forskning for å vise til gyldighet i funnene. Samtidig som vi tydeliggjør positive og negative trekk ved forskningen.

Det kan også være utfordrende å oppfylle kravene til både etterprøvbarhet og anonymitet (Johannessen el al., 2021). Likevel, ved å være transparent i forskningsprosessen kan de medføre at påliteligheten styrkes ved at forskningen kan vurderes trinn for trinn. Dette kan bidra til å øke tilliten til resultatene og gjøre det lettere for andre forskere å evaluere og bygge videre på forskningsfunnene (Thagaard, 2018). Dette tatt i betrakting, har vi vært nøye på at åpenheten ikke går ut over informantenes anonymitet, da de omtales som "informant 1, 2, 3" osv.

4.6.2 Validitet

Validitet ser på relevans, gyldighet og troverdighet. Det er en viktig faktor i forskningen, som angir om det som skal måles i datainnsamlingen er relevant og gyldig for problemstillingen (Dalland, 2020, s. 43). Videre må det sørges for at det er en sammenheng mellom funn, analyse og resultater. Dette kan oppnås gjennom å bruke logiske modeller og adressere motstridende forklaringer (Yin, 2018).

Intern validitet betyr at forskerens vurderinger og beskrivelser stemmer i samsvar med virkeligheten. Under intervjuene ble det utført noen validerende tiltak for å kontrollere mulige feiltolkninger mellom informantens og forskerne beskrivelser (Kvale & Brinkmann, 2018; Yin, 2016). Det ble utført gjennom å stille oppfølgingsspørsmål til det som har blitt nevnt, som for eksempel, "Har du et eksempel på det?", "Hva mener du med det?" eller "Kan du utdype?". En

annen viktig faktor å belyse er at informantenes ulike forforståelse kan påvirke resultatet. Derfor har vi vært kritiske og reflektert over informantenes svar (Maxwell, 2019). Vi ble bevisst på at forskerne hadde en ulik forståelse av tematikken, enn noen av informantene. I de tilfellene valgte vi å holde en objektiv holdning i intervjuene. Et interessant fenomen som kom frem i datainnsamlingen, er informantenes ulike forståelser av begrepet digital sikkerhetskultur. Dermed vil det være hensiktsmessig å ta hensyn til den ulike forståelsen av forskningsprosjektets tema, ettersom informanten har ulike forutsetninger som kunnskap, erfaring og praksis.

Det er også viktig å informere informantene om deres rettigheter til å få innsyn i datamaterialet om det skulle ønskes, samtidig som de har rettigheter til å korrigere eller slettet opplysninger som de ikke ønsker å dele. Derfor har vi anonymisert gjennom hele prosessen, noe som kan medføre at informantene gir åpnere og mer korrekt informasjon. Anvendelse av lydopptak og videre transkribering øker validiteten av databehandlingen, ettersom en kan bekrefte hva informantene har fortalt. Samlet sett kan sikring av gyldighet og troverdighet være en utfordring i forskning. Men ved bruk av metoder som å gi oppfølgingsspørsmål og informere informantene om deres rettigheter, kan man øke sannsynligheten for at resultatene er relevante og nøyaktige (Johannessen el al., 2021, s. 257). Forskningen skal samtidig vise til bekreftbarhet, som vil si at det kreves å være nøytral, upartisk og selvkritsikt til prosjektet gjennomførelse (Johannessen el al., 2021, s. 259). Bekreftbarhet påvirker samtidig gyldigheten fordi den inkludere motstridene funn som etablerer for at forskningsprosjektet ikke søker etter kritikkløse resultater, men samtidig inkluderer relevante og aktuelle funn.

4.6.3 Forskningsetiske vurderinger

I dette forskningsprosjektet er all forskningen underlagt forskningsetiske prinsipper og retningslinjer, spesielt innen den samfunnsvitenskapelige forskningen (Johannessen el al., 2016, s. 83). Målet med etikk er å skape bevissthet om hvordan man bør handle, vurdere handlingen, de som utfører behandlingen og handlingens utfall (Sagdahl, 2023). Det er flere etiske betraktinger som har blitt tatt i bruk i dette kvalitative forskningsprosjektet, og de viktigste punktene som er relevant er krav om samtykke, informering og konfidensialitet.

Vi startet prosessen med å søke til Sikt etter å ha fullført problemstilling, prosjektskissen, intervjuguiden og informasjonsskrivet. Se godkjennings vedlegg 4. Det ønskes å understreke at

valg gjennom hele undersøkelsesprosessen, har blitt tatt i betraktning ut fra etiske prinsipper (Jacobsen, 2015, s. 45). I begynnelsen av dette forskningsstudiet, ble det utarbeidet et informasjonsskriv som har tatt utgangpunkt i en mal fra Sikt (se vedlegg 2). Informasjonsskrivet er grunnleggende forutsetning for at den frivillige deltakeren i forskningsprosjektet skal være informert om sine rettigheter, gevinster og farer som kan medføre ved deltakelse (Jacobsen, 2015, s. 47). Derfor var det viktig for oss at alle informantene hadde lest og returnert samtykkeerklæringen med signatur (vedlegg 3). All empiriske undersøkelse som innebærer behandling av personopplysninger, som for eksempel lydopptak, har blitt meldt til Sikt. I praksis er det ikke nok å kun anonymisere informantene i den endelige oppgaven, derfor har dette vært et fokus gjennom hele forskningsprosjektet fra start til slutt (Jacobsen, 2015, s. 50-51). Dataen fra intervjuene må holdes konfidensielt slik at informantenes integritet blir ivaretatt (Fangen, 2015). For å ivareta konfidensialitetsprinsippet ved transkribering av intervjuopptakene, har ulike utsagn blitt anonymisert underveis. Eksempel på dette er opplysninger om informantenes arbeidsplass har blitt omtalt som «Arbeidsplass» istedenfor virksomhetens navn.

Hensikten ved intervjuene er å få informantenes forståelse, kunnskap og synspunkt rundt digital sikkerhetskultur og standardisering tematikken, for å kunne bruke dette i vår videre forskning. Ivaretakelse av rettighetene til informantenes deltakelse og bidrag har en betydelig rolle for å kunne få frem informantenes budskap. Dermed er det grunnleggende å sikre informantenes anonyme deltakelse ved å informere, samt oppbevare lydopptakene og empirien er lagret som kryptering. Lydopptakene ble slettet etter transkriberingen var ferdig. Når empirien ble behandlet brukte vi en selvkritisk tilnærming til gjennomgang av funnene, som skyldes av at det er nødvendig å skille mellom informantens og forfatterens tolkninger. For å kunne forhindre at et uklart skille oppstår, blir sitater fra informantene gjengitt (Fangen, 2015).

I dette kapitlet har vi påpekt fremgangsmetoden for datainnsamlingen ved undersøkelse av samspillet mellom ISO/IEC 27001 og digital sikkerhetskultur. Det metodiske valget kan kort oppsummeres til en kvalitativ metode, med et eksplorerende forskningsdesign. Der vi bruker semistrukturert dybdeintervju for å samle inn datamateriale om informanters oppfatning om de relevante elementene for forskningen. Samtidig som vi bruker en litteraturgjennomgang av ulike teorier som kan enten støtte eller motbevise dataen fra informantene. I neste kapittel

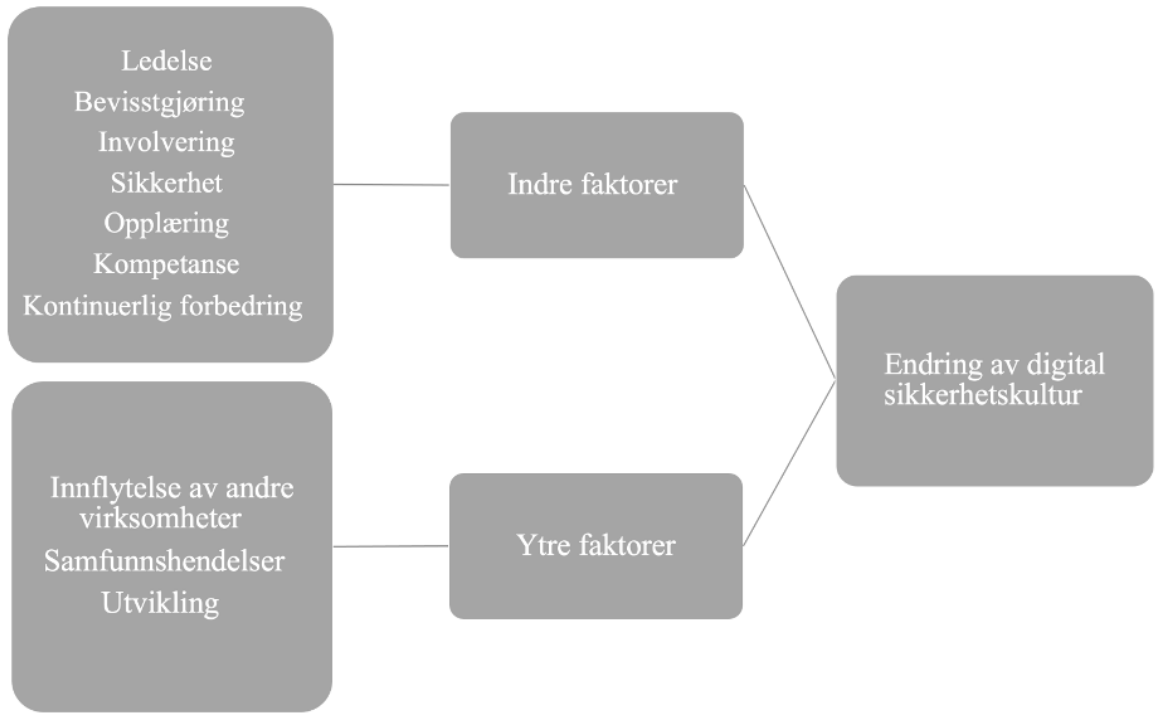
fremlegger vi analysen av datamaterialet fra intervjuene av de ti informantene, og belyser de viktigste elementene som kan bidra til ISO/IEC 27001s innvirkning på digital sikkerhetskultur.

5 Empiri og analyse

I dette kapittelet presenteres datainnsamlingen fra intervjuene, og blir strukturert og sortert etter forskningsspørsmålene. Delkapittel 5.1 tar for seg informantenes bidrag til hvordan skape kulturendring og hvordan forbedre en digital sikkerhetskultur. Delkapittel 5.2 handler om hvordan de innvirkende faktorer fra standardiseringsprosessen vil påvirke den digitale sikkerhetskulturen. Gjennom datafremstillingen vil grunnlaget til besvarelsen av hvordan implementeringen av ISO/IEC 27001 kan påvirke og potensielt styrke den digitale sikkerhetskultur i fremlagt i drøfting.

5.1 Digital sikkerhetskultur endring

Hovedtema én er hvordan man endrer den digitale sikkerhetskulturen i virksomheter. Gjennom analysen kom det frem flere elementer som informantene mente kunne bidra til å skape kulturendringer. Etter kodingen fremkom det flere meningsbærende enheter som ble analysert og kategorisert på tvers. Deretter ble de meningsbærende enhetene sortert inn i to kategorier som falt under hovedtemaet; Endring av digital sikkerhetskultur.



Figur 6. Endring av digital sikkerhetskultur

Figur 6 skaper en oversikt over de forskjellige faktorene som bidrar til kulturendringer i virksomheten som ble funnet under datainnsamlingen. Endringer av digital sikkerhetskultur representerer det overordnete temaet mens indre og ytre faktorer er de overordnede kategoriene som nøkkelfaktorene havner inn under.

5.1.1 Ledelse

Ledelse var et element i digitale sikkerhetskulturendringer som gikk igjen gjentatte ganger under datainnsamlingen. 70 prosent av informantene nevnte viktigheten ved ledelsens involvering og forpliktelse til å arbeide aktivt med forbedring av kulturen og standardiseringsarbeid. Det kreves av ledere å ha engasjement i kulturendrings- og standardiseringsarbeidet for å skape virkninger. "Du må ha en leder som har kompetanse og vet hva han snakker om. Det begynner alltid der. [...] Har du en leder som ikke bryr seg så vil det smitte over på alle i organisasjonen. [...]. Den største utfordringen er jo alltid ledelsen." forteller informant 10. Det kreves av ledere at de har kompetanse og viser interesse ovenfor sikkerhet. De bør lede som eksempel og demonstrere hva de ønsker fra sine ansatte. Ledere må gjøre en innsatts og holde seg selv involvert i kulturen på arbeidsplassen. Dette er til tross for at alle har et felles ansvar for å skape kulturendringer. "Digital sikkerhetskultur er jo at det er et samfunn der alle forstår sin plass og sitt ansvar innenfor sikkerhet" uttrykker informant 4, som jobber aktivt i sin virksomhet for at alle ansatte skal forstå sin rolle i sikkerhetsarbeidet. Likevel er det flere informanter som uttrykker at da de arbeider med standardiserings rådgivning opplever de at ledelsen har dirigert standardiseringsarbeidet til én ansatt, og selv tatt distanse fra standardiseringen. Informant 5 og 10 sine observasjoner påpeker at det ikke alltid er like lett å se spor etter ledelsens innvirkning i standardiseringsprosessen. For å endre dette kreves det at de viser engasjement for arbeidet og tar ansvar for deres innflytelse på kulturen, ifølge informant 10.

Et element som kom fram i analysen var ledelsens innsats i å implementere sikkerhetstiltak for å forbedre sikkerhetskulturen. "En god sikkerhetskultur er der man faktisk har implementert sikkerhetstiltak som beskytter de ansatte, mot disse farene som hele tiden kommer." sier informant 2. Deretter går informanten videre ved å uttrykke hvordan sikkerhetstiltak ikke får noen betydning for kulturen dersom de ikke blir fysisk implementert, "Så det hjelper ikke å ha masse policy og haugevis med Word dokumenter. Det blir ikke noe mer sikkerhet av det. Det det blir sikkerhet av er at du klarer å implementere sikkerhetstiltak". Policyer var et annet ord

som gikk igjen i datainnsamlingen. Både informant 2 og 7 uttrykket at poenget ved å innføre policyer er ikke å skape et stort antall policyer, men å faktisk etterleve dem i arbeidet man utfører. "Det er ikke bare nok å ha en policy som sier slik skal man jobbe, også signere man og tenker ikke mer på den. Men det er jo noe man har med i det daglige." sier informant 7, som utrykker viktigheten ved å arbeide aktivt med policyene. Informant 4 har skrevet en del policyer for virksomheten informanten jobber for, "Etterlevelse er jo noe av det viktigste som finnes, så jeg kan skrive så mange policyer jeg vil [...]. Men hvis ikke disse policyene er etterlevd så er de verdiløse.". Informanten går dermed videre til å forklare hvordan implementering av sikkerhetstiltak er vanskelig, sammen med å skape en forståelse for hvordan og hvorfor ansatte skal utføre tiltakene. "Så når jeg skriver en policy, så prøver jeg å skrive den ikke så langt unna hva vi allerede gjør." sier informant 4, slik at de blir lettere å implementere inn i den daglige rutinen. Imidlertid understreker hen at det er nødvendig å finne en balanse mellom funksjonalitet og sikkerhet. For mye sikkerhet kan koste funksjonaliteten, og for mye funksjonalitet går på bekostning av sikkerheten. Det må gjøres kompromisser, der man kan klare å finne balansen.

Implementering av ISO/IEC 27001 og dens sikkerhetstiltak skaper en effekt på den digitale sikkerhetskulturen som fører til at de ansatte blir mer bevisste på sikkerhet, mener informant 4. Informanten forsetter med å si:

> De ansatte blir mer bevisste. Det handler om å forstå risikoer og det handler om å rette seg etter rutiner som skal på plass. Så når det blir en vane, så blir det en kultur. Tenker det vil medføre endringer i kulturen, siden du er nødt til å etablere nye vaner.

Bevisstgjøringen vil føre til bedre risikoforståelse og større aksept ved implementering av nye rutiner. Som igjen vil kunne føre til kulturendringer. På den andre siden forklarer informanten at effekten av standardiseringen varierer etter den eksisterende digitale sikkerhetskulturen (konteksten), og trenger nødvendigvis ikke å skape store endringer.

5.1.2 Opplæring

Opplæring er en gjentakende tematikk gjennom de fleste intervjuene, der 80 prosent av informantene trekker frem viktigheten. Informantene nevner at ledelsen gjennomfører trening og opplæring til sine ansatte for å kunne kartlegge kompetansen, når det kommer til ansattes

bevissthet, oppfattelse/atferd og kunnskap innad i digital sikkerhet. Innen den digitale sikkerheten er menneskelige feil en av de betydelige årsakene til at det forekommer uønskede hendelser. Informant 7 nevner at menneskelige feil vil forekomme, da mennesker ikke er feilfrie. Ved en slik bevisstgjøring, har 50 prosent av informantene (1, 4, 5, 6 og 9) nevnt at ansatte trenger opplæring, for å kunne opprettholde og/eller forbedre den digitale sikkerhetskulturen. Informantene 1, 2, 4, 5, 6 og 9 (60 prosent) oppgir at nyansatte får opplæring slik at deres ansatte skal kunne ha en god digital sikkerhetsatferd, gjennom digital sikkerhetsopplæring som en del av virksomhetenes onboarding program.

Informant 9 forteller om en positiv tilbakemelding hen fikk fra DNV revisor om virksomhetens digitale sikkerhetsopplæringsprogram for ansatte. Sertifikatet ansatte fikk ved gjennomførelse hadde kun en gyldighet på tre år. Revisoren fortalte hen at det var et godt tiltak for kontinuerlig forbedring, da de fleste virksomheter feiler på kontinuerlig sikkerhetsopplæring av de ansatte ved standardisering av ISO/IEC 27001. Informant 4 som jobber i en annen virksomhet opplyste at de hadde også et lignende oppfølgingsprogram for ansatte i et kontinuerlig løp, og understreket at de ikke tillater noen å ikke gjennomføre programmet.

Informant 2, 4, 5 og 9 nevner også fordelene med å gjennomføre interne kampanjer, som quizer, konkurranser, Awareness training, henge opp plakater i sentrale områder på arbeidsplassen, sende ut phishing-test e-poster. Dette vil bidra til at ansatte blir påminnet om sikkerhetskulturen, sier informant 5. Informant 9 reflekterer også over at interne sikkerhetskampanjer vil øke hvor bevisste ansatte er, og ikke minst når det blir laget med intensjon om å ha det gøy. Ikke kun at kampanjene er seriøse og skremmende.

5.1.3 Kompetanse og kunnskap

Flere informanter hevdet at det er grunnleggende med opplæring for å kunne endre eller styrke den digitale sikkerhetskulturen i virksomheter. Tett koblet med dette nevner 90 prosent av informantene at kompetanse og kunnskap er like viktig. De ni informantene påpeker at dette kreves for å kunne opprettholde og følge med på den raske digitale utviklingen. Informant 10 nevner viktigheten av kompetanse. Samtidig som hen fremhever at for å skape en fungerende sikkerhet internt trenger de ansatte en sikkerhetskompetanse. Ved å opprettholde kompetanse og kunnskap, påstår informant 4, 5, 9 og 10 at det fører til en økt felles forståelse av sikkerhet og persepsjon rundt dette. Derimot påstår informant 3 og 6 at kompetanse og kunnskap vil

kunne medføre flere diskusjoner blant ansatte, som igjen kan føre til en reflekterende god digital sikkerhetskultur.

5.1.4 Informasjonsutveksling

Under kodingen kom det frem at informasjonsutveksling, og det å ha forståelse for hva som skjer i virksomheten, og ikke minst i verden, er viktig. Informant 3 fortalte at informasjonsutveksling er en form for forebygging og ikke minst bevisstgjøring. Informant 3 sier:

> Det er et stort fokus på informasjonsutveksling og hva som skjer. [...]. Det er jo viktig forebygging fordi man vet hvordan en skal forholde seg. Hva jeg kan og ikke kan dele. Hva jeg må gjøre. hva jeg må ikke gjøre. [...]. Det er hvert fall bevisstgjøring, på individnivå og selskapsnivå.

Flere informanter har snakket om viktigheten ved å arbeide sammen når det kommer til å forbedre den digitale sikkerhetskulturen. Informant 9 forteller om hvordan virksomheten bruker awareness training til å skape inkludering og involvering av alle ansatte: "Men det er det å ha god Security awareness, så må alle ansatte forstå og være med på laget. Og det å få dem til å ville ønske å forbedres.". Awareness treningen innebærer ikke at ansatte blir mer bevisste, men man er oppmerksom på risikoer og farer. Informant 3 mener at for å kunne bedre eller endre den digitale sikkerhetskulturen innebærer det at man må være bevisst og oppmerksomme, men også at man arbeider proaktivt, dele erfaringer og kunnskap i et felleskap. Det ligger mye kunnskap i virksomhetene, dermed er det viktig å dele kunnskapen videre og opprette en god læringskultur. Informant 3 avslutter med å påpeke at involvering og inkludering bidrar til å skape en god sikkerhetskultur og en følelse av fellesskap: "Det skal være trygt, alle skal ta en del i dette her og ta et ansvar. Vi er sammen om dette.".

5.1.5 Bevisstgjøring

Bevisstgjøring av ansatte sine holdninger og involvering var et nøkkelbegrep som gikk igjen gjentatte ganger i datainnsamlingen. Åtte av ti informanter nevnte bevisstgjøring som en sentral komponent ved forbedring av digital sikkerhetskultur. Informant 5 forklarer at ved endring av den digitale sikkerhetskulturen: "Det krever en stor grad av bevissthet, og man må slutte å være

så naive. At man forstår truslene før man får de.". Informanten går videre til å forklare viktigheten av bevisstgjøring og risikoforståelse i en god digital sikkerhetskultur.

> Digital sikkerhetskultur er en kultur som er preget av bevissthet og forståelse av farene rundt digitale trusler. Og kjennskap til og vilje til å følge etablerte rutiner. Samt at man er aktive og sier ifra om noe som ikke er bra. Så man er bevisst rundt det og at man har forbedring. Det å ha en kultur som er obs på at man skal bli bedre og bedre, slik man kan øke sikkerheten i virksomheten. Utdyper informant 5.

5.1.6 Kontinuerlig forbedring

Informantene ble bedt om å fortelle oss om hva som kan ha en innvirkning på den digitale sikkerhetskulturen. Kontinuerlig forbedring var et tema alle informantene tok opp. Vi ble oppmerksomme på hvordan informantene selv, og virksomhetene jobber kontinuerlig for å bedre en virksomhets digitale sikkerhetskultur. Informant 1 beskriver kultur og kontinuerlig forbedring slik:

> Sikkerhetskultur? Det er noe du må jobbe med kontinuerlig og ofte. Kultur arbeid, samme om det er digital sikkerhet, HMS eller kvalitet. Det går på at man må være enige om hva som er viktig og hvilket nivå man vil ligge på.

Informant 1 forteller videre at for å kunne jobbe kontinuerlig med den digitale sikkerhetskulturen, er det avhengig av å få alle med på laget, og å holde gode diskusjoner. Kulturbygging er en tung jobb, og krever at alle bidrar med sunne interaksjoner. Informant 1 konkludere med at det er fort gjort å falle ned, men at det tar lang tid å bygge opp når man falt ned på bunn. Informant 10 komme med eksempler hvor "virksomheter ikke bør jobbe med kontinuerlig forbedring kun på onsdager mellom kl. 13:00 – 15:00, men det bør heller flettes inn i den daglige rutinen". Ved å implementere kontinuerlig forbedring systematisk inn i den daglige driften, vil virksomheten sin kultur forbedre seg, og ikke minst yte gode resultater. Informant 7 påpeker videre at hvis man for eksempel har et ledelsessystem for informasjonssikkerhet, og følger prosedyrene der, vil virksomheten ha en forbedring i den digitale sikkerhetskulturen. Men igjen, bevisstgjøring, kommunikasjonen og informasjonen er viktige nøkkelelementer. Det er en kontinuerlig prosess som man kan ikke bare gjøre en gang.

5.1.7 Ytre faktorer

Ekstern påvirkning var også en komponent som kom frem i datainnsamlingen. Informant 3, 6 og 7 snakket om eksterne faktorer som skapet en virkning på den digitale sikkerhetskulturen i virksomheten de arbeidet i. Eksterne faktorer kan for eksempel være innflytelse fra moderselskap, samfunnshendelser og krig. Informant 3 forteller om hvordan moderselskapets gode sikkerhetstiltak og prosedyrer skaper en trygghetsfølelse blant datterselskapets digitale sikkerhetskultur. Informant 5 informerer om at moderselskapet pålegger dem sikkerhetskurs og deler sikkerhetsoppdateringer.

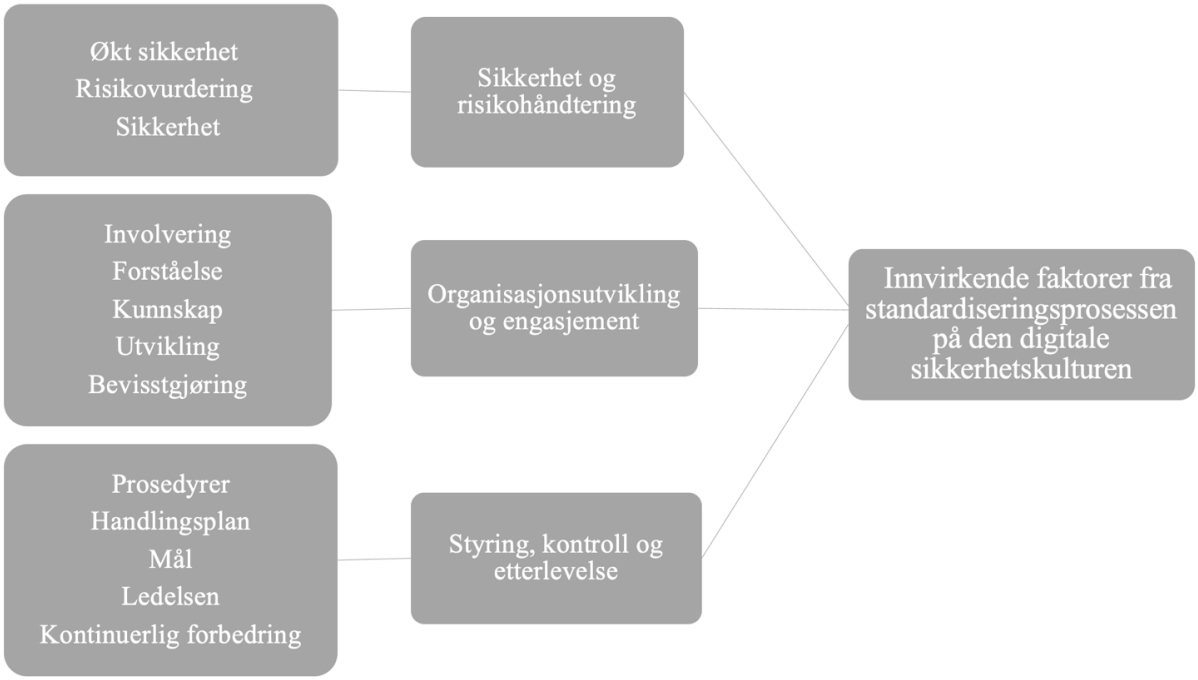
> Vi får jo også mye krav til systematisering og hjelp fra dem. Så de har veldig fokus på det med sikkerhetskultur. Så det har også fått smitteeffekt i virksomheten som er et mindre selskap, men som sakt har vi mange ansatte som jobber med disse tingene, sier informant 6.

Moderselskaper kan frembringe en smitteeffekt over på datterselskaper, noe som kan bidra til å styrke den digitale sikkerhetskulturen. Dermed var det flere informanter som nevnte ekstern innflytelse fra andre selskap som en påvirkning på forbedring av den digitale sikkerhetskulturen. Informant 7 påpekte at forandringer i verden kan gi en innflytelse på ansatte og virksomheten sin bevisstgjøring og tilstand. Når krigen i Ukraina brøt ut i 2022, opplevde informanten en økning i at mennesker tenkte mer på sikkerhet. Videre forteller hen at virksomheten tredde i kraft nye, strengere policyer, spesielt når de også hadde et kontor i Ukraina. Informant 7 informere videre at den digitale sikkerhetskulturen på hen sitt kontor i Norge ble endret på grunn at dette.

Informant 2, 3, 4 og 8 kommer også innpå at den raske teknologiske utviklingen lager preg på endringer i virksomhetens digitale sikkerhetskultur. Virksomheter må ha et forhold til den teknologiske utviklingen, og hendelser som dataangrep rammer virksomheter daglig. Informant 2 fortsetter med: “De må ikke bare henge seg opp i policys og rutiner og gamle måter å gjøre det på. De må henge med på hva teknologisk utvikling og hva er det teknologiske trusselbilde som også endrer seg hele tiden.”. Det blir dermed viktig å følge den teknologiske utviklingen, ettersom den endrer seg fort fra deg om du ikke holde følge. Det blir påpekt av informant 4 at virksomheter som ikke deltar i den digitale utviklingen, vil bli begrenset og vil ikke få noen gevinster. Dette gjelder både på den interne kulturen, men også virksomhetens drift.

5.2 Innvirkende faktorer fra standardiseringsprosessen på den digitale sikkerhetskulturen.

I dette underkapitlet vil vi sette fokus på funn fra datainnsamling som kan knyttes til forskningsspørsmål to. Hvilke faktorer fra standardiseringsprosessen til ISO/IEC 27001 kan ha en innvirkning på virksomhetens digitale sikkerhetskultur? Her blir det fokusert på hvilke faktorer fra selve prosessen av standardiseringen som vil ha en innvirkning på den digitale sikkerhetskulturen.



Figur 7. Innvirkende faktorer fra standardiseringsprosessen på den digitale sikkerhetskulturen

Figur 7 skaper en oversikt over de forskjellige faktorene som har en innvirkning på den digitale sikkerhetskulturen som ble funnet under datainnsamlingen. Innvirkende faktorer fra standardiseringsprosessen på den digitale sikkerhetskulturen representerer det overordnete temaet mens sikkerhet og risikohåndtering, organisasjonsutvikling og engasjement, styring, kontroll og etterlevelse. Disse blir de overordnede kategoriene som nøkkelfaktorene havner inn under.

5.2.1 Sikkerhet og risikohåndtering

Under forskningen så vi på hvilke faktorer fra standardiseringsprosessen til ISO/IEC 27001 som kan ha en innvirkning på virksomhetens digitale sikkerhetskultur. Det kom frem at det var flere komponenter som gikk igjen i intervjuprosessen. 50 prosent av informantene trakk frem økt sikkerhet som en nøkkelfaktor, i form av blant annet risikoreduserende tiltak og informasjonssikkerhet. Informant 1 utdyper om ISO/IEC 27001 sin innflytelse på sikkerheten og hvordan den skaper et høyre sikkerhetsnivå.

> Det er jo overhode ingen tvil at hvis man sertifisere seg i ISO 27001, så er man på et helt annet nivå inne informasjonssikkerhet, enn å ikke være sertifisert. Det er omfattende risikovurderinger i IT infrastruktur, som ligger i bunn av 27001 sertifiseringen. Hvis man ikke gjør en grundig risikovurdering av infrastrukturen, vet man heller ikke hvor risikoen er eller det å kunne miste kontrollen. Fortelle informant 1.

Standardens økning av sikkerhet kommer dermed grunnleggende fra risikovurderingene som blir utført under standardiseringsprosessen. Risikovurderingene kreves å utføres nøye slik at de ikke mister kontrollen over risikoene. Informant 7 forteller om kapittel 6.1 i ISO/IEC 27001, som omhandler å iverksette tiltak for å hindre risiko og identifisere muligheter. Der man bør streve etter å arbeide proaktiv over reaktiv, spesielt når det omhandler å identifisere avvik. Flere informanter forteller hvordan Standardens systematikk bidro i å øke sikkerheten. Informant 5 utdypet hvordan det ble etablert en systematikk og nye sikkerhetsbarrierer som følge av standardiseringsprosessen. Dermed er systematikken, risikobarrierene og andre tiltak for å hindre risiko, nøkkelfaktorer frembragt av prosessen som støtter Standardens innflytelse.

5.2.2 Organisasjonsutvikling og engasjement

Forståelse er et tema som ble nevnt gjentatte ganger, når informantene ble spurt om hvordan en standardisering i en standard kan påvirke en virksomhet. Informantene 1, 4, 5, 6, 8, 9 og 10 (70 prosent av informantene) mener at dersom en virksomhet vil ha en vellykket standardiseringsprosess, er det grunnleggende å ha en intern forståelse, der ledere og ansatte forstår hvorfor det skal iverksettes en ISO-standardiseringsprosess. Informant 1 forteller "Når man jobber seg opp mot en sertifisering, så stilles det krav til organisasjonen, organisasjonens medlemmer og ledelse, at de har en viss forståelse for og vet hvordan en skal gjøre ting".

Ledelsen bør derfor alltid involvere seg i standardiseringsprosessen, samt bør gå frem med å lede veien ved å demonstrere sin forståelse til sine ansatte. Slik kan det skape en medvirkning i hele virksomheten. Det vil kunne medføre at organisasjonen kan stille sterkere og kunne utvikle seg videre.

Det reflekteres av informant 9 om hvordan ISO skal ivareta mange reelle verdier til virksomheten og derfor kan det være en kompleks prosess. Informant 5 forteller at organisasjonen er nødt til å øke forståelsen for Standarden og det tilhørende problemområde. Som følger av dette, er det grunnleggende at involverte har forståelse for hvorfor det gjøres på den metoden, forstå risikoene, forstå sikkerhetstiltakene og rutiner. Det samme forteller informant 4. Hen reflekterer videre at det er utfordrende få alle involverte i standardiseringsprosessen å forstå gevinsten som kan forekomme ved standardisering. Det er en av grunnene flere ansatte kan falle ut av en slik prosess, som dermed kan medføre tap av engasjementet for standardiseringen. Derimot forteller informant 7 at selve standardiseringsprosessen hjelper ansatte med å engasjere seg, men det krever først og fremst at de får en forståelse for hvorfor det er viktig.

Ved at virksomheten vil kunne involvere de ansatte og ha en større deltakelse i standardiseringsprosessen mener både informant 3, 4, 7, 9 og 10 (50 prosent) at det vil skape verdier i form av bevisstgjøring, effektivitet, ivaretakelse og nytte. Informant 3 nevner også begrepet medvirkning, som vil frembringe samhold blant de ansatte: “Det blir mer systematisert og eierforhold, mer oversikt. Man får mer involvering og medvirkning [...]. Det skaper teamarbeid og lagspill. Jeg tenker sertifiseringer gjør at man blir bedre på mange måter.”. Standarden vil medføre flere positive faktorer som teamarbeid og lagspill, involvering og medvirkning. Dermed kan standardiseringsprosessen frembringe faktorer som blant annet forståelse, medvirkning og bevisstgjøring som vil kunne påvirke den digitale sikkerhetskulturen.

Ved at ansatte er involverte i standardiseringsprosessen vil det skape forståelse, dette mener informant 10 er viktig for at det skal være en engasjert holdning for standardiseringen. Uten engasjement vil sertifiseringen ikke ha noe særlig nytte for virksomheten. Senere forteller hen viktigheten med riktig motivasjon ved beslutning om standardisering:

> Hvis motivasjonen er at de bare må ha sertifisering, da blir det bare en kost side for bedriften. Hvis bedriften tenker at vi gjør denne sertifiseringen for at vi skal skape engasjement og for at vi skal bli en bedre bedrift, så blir det en bedre bedrift. Da vil du se det på omsetning og resultat.

Dermed kan motivasjonen bak valget om standardisering påvirke innsatsen og arbeidet som blir gjort under og etter standardiseringsprosessen. Uten deltakelse og involvering av ledelsen eller ansatte, blir ikke fokuset opprettholdt og ikke minst vil det påvirke kulturen. Innpå samme tema utdyper informant 7, om viktigheten ved ledelsens forpliktelse og at de utfører sin del av arbeidet:

> Toppledelsen skal demonstrere sin forpliktelse til systemet. Og sørge for at de har nok ressurser for å jobbe med systemet. Man må involvere alle som eier eller er en del av systemet. Det er ikke kun kvalitetsleder eller en person som skal dra lasset. Må sørges for at ledelsen involverer alle hele veien, for å kunne skape en god kultur. Det å bygge kultur er kjempeviktig uansett hvilket fagområde. Må få med alle involverte er kjempeviktig.

Toppledelsen skal lede veien, og å demonstrere sin forpliktelse er viktige faktorer dersom man ønsker en effekt på den digitale sikkerhetskulturen. Samtidig som involvering av alle parter skal bidra i standardiseringen. Etter systematisering av kodingen, falt noen av sitatene til informantene 1, 3, 4, 7, 8 og 10 (60 prosent) under koden "Utvikling". Under denne koden faller begreper som blant annet; kontinuerlig forbedring, utvikling, forbedringsforslag, styrke intern kunnskap. Disse utnevnelsene kommer frem ved spørsmålet om hvordan standardisering vil påvirke virksomheter. Informant 7 påpeker at Standarden kan bidra til at virksomheter blir mer innovative, ettersom deler av Standarden stiller krav på hvordan man skal håndtere ved oppstart og håndtering av noe nytt. Den kontinuerlige forbedringen vil medføre at virksomheten utvikler seg internt også, sier informant 8. Ved at Standarden legger opp krav for at virksomheten jobber kontinuerlig, vil det stadig arbeides for å oppnå forbedringer. Det vil skape verdi i form av at en utvikler seg bedre kvalitet og sikkerhetspraksiser for å ivareta ansatte og kundene. Informant 4 mener kommunikasjon er viktig. Hen forteller videre at virksomheten vil begrense seg selv hvis de ikke kommunisere ut hva gevinsten kan bli, dermed vil organisasjonen bli svekket i utviklingen. Dette kan videre påvirke den indre motivasjonen til de ansatte.

5.2.3 Ledelse, styring og etterlevelse

Standardisering er lagt opp for at organisasjonen skal løfte seg ved å vedlikeholde rutiner og system på en systematisk måte, sier Informant 5. Det belyses av informant 8 at standardiseringen vil bidra til at organisasjonen skaper et rammeverk, som går veldig metodisk til verks. Rammeverket vil ta for seg definerte målsetninger, organisering og andre systematiske prosesser som finnes i virksomheten. Dette vil videre medføre at ansatte vil forstå hensikten og verdien av standardiseringen. Videre påpeker informant 8 at ISO-standardisering er som å ha et kvalitetsstempel. Informant 6 kan fortelle at det er ikke en enkel sak å bli standardisert, samt å få alle engasjert. Virksomheten må jobbe systematisk og grundig, der involverte ledere og ansatte er nødt til å ha forståelse og bevissthet om prosessene i standardiseringen. Hvis ikke, vil en ikke klarer å bli sertifisert.

Under innsamling av data gikk styring, kontroll og etterlevelse igjen som nøkkelfaktorer. Informant 3 og 4 forteller at Standarden åpner for at virksomheten selv oppretter mål og handlingsplaner. De bestemmer selv hvor ofte de skal ha internrevisjoner, lager sine egne prosedyrer og policyer, men da de er satt *må* de følges til punkt og prikke. Informant 3 utdyper:

> Når man lager mål og handlingsplan, så må man se om ting har fungert eller ikke, og ledelsens gjennomgåelse ser på det som har skjedd. Så er det fokus på internrevisjoner og de skal også være risikobasert. Så alt er lagt opp til å være risikobasert, og Standarden sier ikke at man må gjøre det sånn og sånn. Men de sier at man må selv finne den metoden som passer beste for dem. Så må finne på prosesser og prosedyrer selv. Poenget er ikke at alle prosesser skal være like. Poenget er at man har en kontekst, man har ledelsens gjennomgåelse, ha fokus på driften, det er det som er Standarden, og ikke hvordan man løser det.

I standardiseringsprosessen velger bedrifter selv metoden de vil bruke under standardiseringsprosessen, dette er til tross for at virksomhetene har krav de må følge. På den andre siden åpner Standarden for at de selv skal lage mål og handlingsplaner, og utføre egne internrevisjoner. Dette åpner for at virksomheter kan selv tilpasse Standarden etter

virksomhetens kontekst. Informant 1 forteller hvordan hen har erfart at internrevisjoner sjeldent blir utført dersom det ikke har en sammenheng med en standardiseringsprosess:

> Det jeg har erfart er at det er ingen bedrifter som kommer på selv at de burde kanskje gjøre en internrevisjon for å sjekke om man faktisk følger sine egne prosedyrer kanskje eller ledelsen gjennomgåelse for å lage en policy og mål, på at man skal hele tiden bli bedre. Det er uhyre sjeldent at bedrifter klarer å jobbe med de tingen, uten at de går aktivt inn for en ISO-sertifisering, for å kunne bygge seg opp i henhold til ISO Standardene. De får, etter mitt syn, en god del på plass som de ikke har forutsetning eller mulighet til å få på plass uten å iverksette arbeidet til en ISO-standard.

Dermed varierer utfallet av ISO/IEC-27001 som et hjelpemiddel for å styrke den digitale sikkerhetskulturen, alt etter hvilken metode det velges for utførelse av internrevisjoner, prosedyrer og policyer. Dette faller ofte på ledelsen eller dem som sitter med ansvaret for sikkerhet og/eller standardiseringsprosessen, men det er flere oppgaver enn kun valg av mål, metode og prosedyrer som kan få et påvirkende utfall. Informant 7 utdyper ledelsens rolle i resultatet av standardiseringsprosessen: "Suksesskriterier er at ledelsen er med". Hen går videre ved å fortelle om en tidligere kunde som ble standardisert, hvor det var ingen etterlevelse av lederen. "Det er veldig tragisk. The walk and talk. Det er så viktig at ledelsen formidler budskapet og gevinsten." sier informant 7.

Informant 7 går videre ved å forklare at dersom virksomheten har opprettet prosedyrer, har den da satt egne krav som samsvarer med lovverk eller en standard. Deretter må virksomheten lage en oversikt over hvilke lover, regler og krav de har satt, og dernest demonstrere hvor etterlevelsen er i prosedyrene. Dersom prosedyrene ikke følges, skal det meldes avvik. Disse avvikene må behandles for å finne den grunnleggende årsaken. Samtidig som de må meldes inn, ettersom de kan representere brudd på lovkrav, kundekrav og standardkrav. Dermed bør etterlevelse bli tatt seriøst i standardiseringsprosessen.

I standardiseringsprosesser blir ofte PUKK brukt som et verktøy for implementering av Standarden. Informant 3 forteller at fordelen ved bruk av PUKK er at det er en forbedrings sirkel med hensikt at man starter med noe og avslutter med noe helt annet. Videre forteller hen at det er et verktøy som har vært tidligere i internkontrollforskriften, men heller med "Planlegge, utføre, studere og handle". Poenget er at det endrer prosedyrer og måten man gjør ting på for å

bli enda bedre. I Standarden er det jo ledelsens gjennomgåelse som er viktig del, der man ser prosessene og målene. Ved å bruke denne arbeidsmetodikken som et verktøy, kan ledelsen få en form for kontroll. Informanten avslutter med å utdype om fordelen ved bruk av PUKK:

> Det er bare at tankegangen er der, så vil ting bli bedre. Det skaper en form for å være proaktiv. Man er jo reaktiv når det har skjedd noe, men hvis du er i forbedringsprosessen eller bruker PUKK hjulet i forkant, og bruke det kontinuerlig i alt du gjør så tenker jeg det er veldig nyttig. Man må sette mye arbeid i det, men poenget er at det må være en bevisstgjøring.

Ved å bruke PUKK hjulet kan de ansatte bidra til å skape et kontinuerlig proaktivt arbeid, og dermed kunne bidra til å opprettholde standardisering. PUKK hjulet kan derfor være et nyttig verktøy, som bidrar med å skape en bevisstgjøring.

I dette kapitelet har vi lagt frem analysen av datainnsamlingen fra de semistrukturerte dybde intervjuene. Som en midlertidig oppsummering ser vi at det er flere elementer som kan bidra til å skape kulturendringer, som ledelsen, bevisstgjøring, involvering av ansatte og ledelsen, sikkerhetstiltak, sikkerhetsopplæring og kompetanseheving, kontinuerlig forbedring og ytre faktorer. Samtidig som faktorer fra ISO/IEC 27001 som kan påvirke den digitale sikkerhetskulturen, var økt sikkerhet, ledelsens involvering og engasjement, ledelsens iverksetting av prosedyrer, fremgangsmåte, mål og igjen kontinuering forbedring. I neste kapittel drøftes empirien opp mot den tidligere presenterte teorien, der hovedfaktorer vil blir fremhevet.

6 Drøfting og diskusjon

I dette kapitlet blir den analyserte datainnsamlingen drøftet og diskutert i forhold til teoriene som ble presentert tidligere. Formålet er å besvare forskningsspørsmålene på best mulig måte, som sammen i en helhet besvarer hvordan implementeringen av ISO/IEC kan påvirke og potensielt styrke digital sikkerhetskultur. Drøftingskapittelet deles inn i to hovedkategorier; faktorer fra ISO/IEC 27001 som kan påvirke virksomhetens digitale sikkerhetskultur, og endring av digitale sikkerhetskultur. Den siste hovedkategorien vil bli presentert om som avsluttende drøfting.

6.1 Ledelse, styring og etterlevelse

En av hovedfaktorene fra funnene er at Standarden er fleksibel i valg av standardiseringsmetode, krav, mål og prosedyrer. 30 prosent av informantene utdypet om Standardens åpenhet for valg av fremgangsmåte, der virksomheten selv bestemmer mål, handlingsplan og hvor ofte de skal ha internrevisjoner. Etter fastsettelse av de nevnte elementene *må* de etterleves. Bounagui et al. (2019) bekrefter dette ved å poengtere at ISO/IEC 27001 fungerer som en veiledning for hva som må gjøres, men det er opp til virksomheten å velge "hvordan" de skal gå frem for å nå målene (Ku et al., 2009; Liao & Chueh, 2012; Culot et al., s. 84). Smith et al. (2010) forteller at Standardens fleksibilitet kan være en ulempe (Lomas, 2010; Rezaei et al., 2014; Culot et al., 2021, s. 84), ettersom det kan skape lavere nøyaktighet i utførelse av risikovurdering og ressursvurdering (Ku et al., 2009; Liao & Chueh, 2012; Culot et al., s. 84). Til tross for dette, kan det tenkes at lavere nøyaktighet kan medføre at ansatte blir mindre bevisst på farene, dermed kan det påvirke virksomhetens sikkerhetskultur.

På den andre siden viser 50 prosent av studiene utført om ISO/IEC 27001 at Standarden må ses opp mot konteksten til virksomheten (Culot et al., 2021, s. 88). Det samme kan argumenteres opp mot virksomhetens egne kontekst, som innebærer at Standarden må ses opp mot blant annet størrelsen på virksomheten, antall ansatte og bransje. Dermed kan man argumentere for at Standardens fleksibilitet eksisterer for å kunne tilpasses alle virksomheters sikkerhetskultur. Antonsen (2009) påpeker at de ikke finnes en "one-size-fits-all" tilnærming til kultur, når kultur er kontekstbasert. Likevel gir Standarden ikke tilstrekkelig veiledning om de kulturelle og psykologiske dimensjoner, som vil kunne sikre ansattes etterlevelse av Standarden (Van Wessel et al., 2011; Culot et al. 2021, s. 86). Dermed mangler det en direkte kobling til det

menneskelige aspektet i Standarden, og har derfor ikke en direkte tilkobling til den digitale sikkerhetskulturen. Likevel understeker Asai og Hakiabera (2010) at det alltid vil være en underliggende individuelle kulturelle forskjeller for holdningen til informasjonssikkerheten, uavhengig om det er en relasjon til standardisering (Culot et al., 2021).

Effekten Standardens nøkkelfaktor, fleksibilitet, har på den digitale sikkerhetskulturen blir derfor avhengig av ledelsens fremgangsmåte for håndtering av systemet, slik som valg av mål, prosedyrer osv. 70 prosent av informantene mente at ledelsens involvering og forpliktelse var faktorer som påvirket Standardens innflytelse på den digitale sikkerhetskulturen. Noe som samsvarer med Cooper (2001) sin teori om effektivt lederskap, der deres involvering er avgjørende for hvordan arbeiderene forstår og handler rundt sikkerhet. Informant 10 utdyper om kravene til ledelsen ved implementering av Standarden. Der det forventes at ledelsen skal ha kompetanse og være involvert. Informanten forteller at det kan skape en smitteeffekt på de ansatte. Kapittel 5 i ISO/IEC 27001 er dedikert til lederskap og forpliktelse. Kapitlet fremhever viktigheten med ledelsens oppgaver og dens forpliktelse for å kunne nå Standardens hensikt, noe som samsvarer med funnene i datainnsamlingen. Dermed blir det presisert i kapittel 5 at det ikke inkluderer en direkte kobling til virksomhetenes sikkerhetskultur, men har en indirekte innflytelse på kulturen. Likevel viser analysen en parallell kobling mellom kap. 5 og funnene fra informantenes påstander, om at lederens forpliktelse er en av de grunnleggende elementene for en god digitale sikkerhetskultur. Informant 7 tar opp tematikken rundt kap. 5., der det legges frem at det må sørges for at ledelsen er involvert, og ikke minst at alle er involverte i systemet, for å kunne skape god sikkerhetskultur. I lik sammenheng forteller informant 4 at alle har et felles ansvar for å skape kulturendringer, da kulturendringer stammer fra de kontinuerlige daglige interaksjoner mellom medlemmene av samfunnet (Antonsen, 2009, s.42).

Dermed ser man at ledelsens forpliktelse og involvering i standardiseringsprosessen og sikkerhetskultur, er en viktig faktor for at Standarden skal ha en innvirkning på den digitale sikkerhetskulturen. Likevel ser man at sikkerhetsstyring ofte ikke er et tema som engasjerer mange toppledere eller andre ledere (Cooper, 2001, s. 30). I likhet med dette kunne flere informanter fortelle at de opplevde flere ganger at ledelsen har dirigert standardiseringsarbeidet til én ansatt, og selv distansert seg fra arbeidet. Dermed ser man at dette er et gjentakende fenomen i sikkerhetsstyring, til tross for at forskning belyser at det krever ledelsens godkjenning for å skapet et suksessfullt styringssystem (Culot et al, 2021). Dersom ledelsen ikke involverer seg i standardiseringsarbeidet og dirigerer arbeidet til en spesifikk person eller avdeling, kan

man vurdere om Standarden ikke har noen effekt på den digitale sikkerhetskulturen. Dette kan skyldes at Standardens fordeler for den digitale sikkerhetskulturen ikke formidlers til resterende ansatte. Samtidig som funnene fra intervjuene viser at ledelsen bør gå fram som eksempel for å kunne skape kulturendringer.

Et annet relevant punkt som kan ha en betydning for Standardens suksesskriterier, er bruk av konsulenter under standardiseringsprosessen. Informant 2 hevdet at dersom man velger å utføre prosessen selv, vil fokus internt øke mer enn om virksomheten bruker eksterne ressurser til å utføre jobben. Videre kan det derfor argumenteres for at det tilegnes mer effekt ut av standardiseringsprosessen dersom man velger å gjøre det selv. Det kan frembringe mer kunnskap om Standarden, samtidig som det blir lettere å sette tydelige og realistiske mål. I likhet med dette viser forskning at bruk av eksterne resurser kan hindre organisatorisk lære og føre til mislykket standardiseringsprosess (Ku et al., 2009; Gillies, 2011). Likevel kan bruk av eksterne resurser være gunstig i form av økonomisk belastning og sparte arbeidstimer. Det kan argumenteres for at dersom virksomheten ønsker å utføre arbeidet selv, kan det få en større gevinst for den digitale sikkerhetskulturen. Ettersom den digitale sikkerhetskulturen tilegner seg mer kunnskap og arbeider tett sammenvevd med Standarden. Derimot trenger ikke eksterne ressurser nødvendigvis hemme virksomheten. Hvis en virksomhet har manglende kunnskap og interne resurser, kan å trekke inn eksterne ressurser hjelpe og styrke virksomhetens kunnskap rundt informasjonssikkerheten. Ved at virksomhetens kunnskap styrkes, vil det kunne øke kollektiv bevissthet, forståelse og holdning rundt den digitale sikkerhetskulturen.

Dermed kan eksterne faktorer skape en innflytelse på den digitale sikkerhetskulturen, noe som 50 prosent av informantene vektla. Da det forekommer endringer eller utvikling i samfunnet kan det utgi en direkte eller indirekte påvirkning på virksomhets sikkerhetskultur. Banduras Social Learning teori, tar for seg hvordan mennesker får innflytelse av miljø og atferd i en spesifikk kontekst med eksterne observerbare faktorer (Cooper, 2000). Disse faktorene kan gjensidig påvirke hverandre, som skaper ringvirkninger som kan utløse endring av holdning, reaksjon og handling (Fang & Wu, 2013). Informant 7 kunne utdype om hvordan forandringene i verden, som dataangrep, pandemi og krig, vil påvirke hvordan mennesker handler rundt sikkerhet. Dermed blir ledelsens reaksjon og tilpasningsdyktighet nødvendige for å håndtere ytrefaktorers påvirkning på virksomhetens drift. Det kan argumenteres for at virksomheters digitale sikkerhetskultur kan få innflytelse av ytrefaktorer som er utenfor virksomheten sin kontroll. Innflytelsen kan oppfattes som negative, da deres effekt kan medfører frivillig eller

ufrivillig endring. Derimot kan det få en positiv utvikling og forbedring i virksomheten. Innvirkningen dette vil ha på den digitale sikkerhetskulturen er endringer på atferd og holdninger til sikkerhet.

Et annet relevant punkt som vil få betydning for standardiseringens suksess, er motivasjon. Informant 10 hevder at motivasjonen bak beslutningen om standardisering vil påvirke innsatsen og arbeidet under og etter standardiseringsprosessen. I samsvar med dette kommer Culot et al. med to ulike former for motivasjon: funksjonalistisk og institusjonalistisk. Hvor virksomhetens funksjonalistiske motivasjon for implementering av Standarden er å få et effektivt og bedre informasjonssikkerhets system. Dermed vil en institusjonalistisk motivasjon til ISO/IEC 27001 være begrunnet med å stille seg bedre mot eksterne interessenter (Culot et al. 2021, s. 82). Virksomheter med denne motivasjonen standardiseres seg for økonomiske årsaker med å anskaffe flere kunder og partnere. Dermed vil motivasjonen for standardiseringen påvirke resultatet, samtidig som den vil påvirke innvirkningen på den digitale sikkerhetskulturen.

6.2 Organisasjonsutvikling og engasjement

80 prosent av informantene trekker frem viktigheten av opplæring. Ifølge flere informanter brukes opplæring og trening for å lære om sikkeratferd, men også for å kunne identifisere bevisstheten, oppfattelse og atferd om den digitale sikkerheten. Noe som samsvarer med standardiseringsprosessen, som fremhever viktigheten av opplæring. Samtidig som tilegning av kunnskap er en sentral del av en digital sikkerhetskultur. NorSIS fremhever at en digital sikkerhetskultur består av felles verdier, holdninger, normer, kunnskaper og handlinger som skal bidra til å avverge virksomheten fra å bli rammet av digitale trusler (Malmedal, 2020, s.11). Som tidligere nevnt, er normer noe som er tilknyttet forventet atferd (Tjora, 2022), og tilsier hvordan ting blir håndtert i organisasjonskulturene (Engen et al., 2021, s. 49). ISO/IEC 27001 kan anses som en form for formell ikke-rettslig norm, som gir retningslinjer (Engen et al., 2021, s. 48-49). Standarden påvirker de organisatoriske normer og atferd til sikkerhet, som vil etablere en felles forståelse for den digitale sikkerhetskulturen. Derimot kan man også sette lys på at den eksisterende digitale sikkerhetskulturen kan påvirke implementering og oppfølgingen av ISO/IEC 27001. Dette vil påpeke viktigheten med balanse mellom de to elementene for å kunne styrke sikkerheten.

Opplæring og tilrettelegging for kunnskapsheving innen sikkerhet kan argumenteres for å være grunnlaget for hvordan virksomheten operere sikkerhetsmessig. Informantene 2, 4, 5 og 9 utdypet hvor essensiell digital sikkerhetsopplæring er for ansatte. En del av sikkerhetsopplæringen innebærer å gjennomføre interne kampanjer for ansatte for å kunne vedlikeholde kunnskapen og ikke minst bevisstheten. Ledelsen kan bygge en sikkerhetskultur som følger med den digitale utviklingen ved å implementere kontinuerlig sikkerhetsprogrammer. Opplæring utgjør derfor en viktig del av ledelsen. Det kan argumenters for at opplæring og kunnskapsheving kan fungere som grunnlaget til vekstforholdene (Antonsen, 2009, s. 43). Antonsen understreker at det er utfordrerne å endre kulturer, ettersom de skapes gjennom daglig interaksjoner, samtidig som kultur er ustyrlig og uforutsigbar (Antonsen, 2009, s. 43).

Dermed kan opplæring om sikkerhet og ISO/IEC 27001 bidra til å skape endring i den digitale sikkerhetskulturen, da det vil øke den interne forståelsen og legge grunnlag for involvering av ansatte. Informant 9 reflekterte over innholdet i opplæringen, da det bør streves etter å skape engasjement. Uformelle systemer, som engasjement, tillit, bevissthet og forpliktelse, kan brukes sammen med formelle systemet, som standarder. Dermed kan Standarden fungere mer effektivt fordi den hjelper til med å dele informasjonen og god praksis for å forbedre informasjonssikkerheten (R. Skotnes i Olsen et al., 2020, s. 178).

På den andre siden kan det argumenteres for at dersom opplæring og kunnskapsheving skal ha en effekt, må de oppfylle visse krav. Ledelsen må være oppmerksom på at kvaliteten på innholdet er i trå med den digitale sikkerhetsutviklingen. Parallelt med dette vektlegger Reason (1997) nødvendigheten med å ha en god lærende kultur. Der det oppfordres til å sette fokus på kvalitet og den kontinuerlige forbedringen (Hudson et al., 2002). Logikken i teorien viser at kontinuerlig forbedring og kvalitet er nødvendig for at opplæring skal ha en effekt på den digitale sikkerhetskulturen.

6.3 Sikkerhet og risikohåndtering

Funnene fra intervjuene viser til at en av hovedfaktorene er hvordan Standarden vil kunne gi økt sikkerhet, som skyldes ISO/IEC 27001 sitt fokus på risikoreduserende tiltak og styrking av informasjonssikkerhetssystemer, dette bekreftes også av 50 prosent av informantene. Funnet

samsvarer med Standardens mål om å fremme virksomhetens evne til å beskytte verdifulle informasjonsressurser, samt å sikre videre drift, og kravet om å utføre risiko reduserende tiltak (Brenner, 2007, s. 26). Imidlertid kan standardisering skape en overdreven følelse av sikkerhet (Engen et al., 2021, s. 51), som kan føre til at mennesker blir uforsiktige. Noen av informantene påpekte at moderselskapets gode sikkerhetstiltak og prosedyrer skaper en trygghetsfølelse blant datterselskapet, når de er pålagt sikkerhetskurs og sikkerhetsoppdateringer. Dette kan gi en falsk trygghetsfølelse, ettersom det ikke er datterselskapets egne sikkerhetstiltak. Hvor mye moderselskapet kan beskytte datterselskapet sitt digitale sikkerhet er noe en bør stille kritisk til.

I sammenheng med at standardisering kan skape en overdreven følelse av sikkerhet, argumenterer Reason for at få antall uønsket hendelser kan i seg selv bli en utfordring. Et sikkert utfall er usynlig, da alt går etter forventing og ikke tiltrekkes oppmerksomhet (Reason, 1998, s. 294). Standarden kan dermed gi en falsk trygghetsfølelse, grunnet da ansatte har mangel på feil vil de fortsette å handle slik med en forventning om at "ingenting" vil fortsette å skje. Reason mener at for å oppnå et sikkert utfall kreves det en rekke dynamiske faktorer og handlinger (Reason, 1998, s. 294). Med andre ord kan de "usynlig sikre utfallene" gi en falsk trygghetsfølelse, ettersom de ansatte kan bli uforsiktige. Mitnick argumenterer for at virksomheter bør ha ekstra fokus på digital sikkerhetskultur, ettersom ansatte er den største trusselen mot sikkerhet, som skyldes at mennesker er letter å manipulere enn teknologi (Jøsang, 2021, s. 230). Sett ut fra teorien til Mitnick bør ISO/IEC ha et stort fokus på det menneskelig aspekter ved utvikling av en standard som skal beskytte virksomhetens informasjonssystem, da samfunnets største utfordring er digitale teknologi (Mitnick, 2002; Jøsang, 2021, s. 230). Spesielt med tanke på at Culots samling av tidligere forskning av ISO/IEC 27001 viser at kulturendringer er en hovedutfordring å overkomme (Culot et al., 2021, s. 90).

Ut fra logikken i teoriene ser man utfordringen ved at standardisering kan gi en falsk trygghetsfølelse, som kan føre til lavere sikkerhet. Det betyr imidlertid ikke at Standarden i seg selv ikke gir en økt sikkerhet, tvert imot viser funnene våre at økt sikkerhet stemmer. Forutsetningen til at teoriene peker på den falske trygghetsfølelse, må ses opp mot menneskeaspektet i virksomhetens kontekst. Dermed kan kvaliteten på arbeide være en faktor som avgjør Standardens effekt på den digitale sikkerhetskulturen.

For at økt sikkerhet skal ha en betydning på den digitale sikkerhetskulturen var det flere komponenter som kom frem i analysen. Komponenter som å øke de ansattes bevissthet og

sikkerhets forståelse. Samtidig som kompetanse og kunnskap, ledelsens styring, opplæring og kontinuerlig forbedring er komponenter som har effekt på hvordan økt sikkerhet kan påvirke digital sikkerhetskultur. Dersom alle parter involveres og bidrar kan det hjelpe med å motarbeide de negative effektene. Alle informantene antydet at menneskeaspektet var en viktig komponent ved Standardens effekt på den digitale sikkerhetskultur. Hvor 80 prosent av informantene mente at bevisstgjøring av involvering og holdning til sikkerhet var en nøkkelfaktor for å kunne forbedre den digitale sikkerhetskulturen. Dette indikerer at økt sikkerhet, som er en av Standardens viktigste komponent, vil ha en innvirkning på kulturen. Det betyr at menneskelige aspekter bør inkluderes i standardiseringsprosessen. Samtidig kan den økte sikkerheten i Standarden også øke bevisstgjøringen og forståelsen hos de involverte i prosessen. Imidlertid fremhever Culot et al. at virksomheter som standardiseres, ofte tildeler standardiseringsarbeidet til IT-avdelingen alene (Van Wessel, 2011; Akowuah et al., 2013). Dette er til tross for ledelsens involvering er spesielt viktig, noe som funnen fra intervjuene støtter opp. Informant 5 og 10 sine observasjoner bekreft Culot sin påstand, gitt at det ikke alltid er like lett å se spor etter ledelsens arbeid under standardiseringsprosessen.

Økt sikkerhet er en av hovedfaktorene fra ISO/IEC 27001 standardiseringsprosessen som kan ha en innvirkning på virksomhetens digitale sikkerhetskultur. Dermed ser man at økt sikkerhet stemmer med både teorien og dataen fra intervjuene, til tross for at den har noen negative virkninger. Ved å inkludere det menneskelige aspektet kan de negative virkningene unngås.

6.4 Avsluttende drøfting

I dette kapitelet blir den avsluttende drøfting fremlagt. Kapitelet tar for seg forskningsspørsmål 1 om kulturendringer, og drøfter opp mot hovedfunnene fra drøftekapitelet presentert ovenfor. Det vil dermed fungere som en avsluttende drøfting, der det forsøkes å svare på om implementeringen av ISO/IEC 27001 kan påvirke og potensielt styrke den digitale sikkerhetskulturen.

Funnene fra analysen viser at det er flere faktorer som bidrar til å endre en kultur, mer spesifikt forbedre en kultur. Faktorer som at Standarden er fleksibel i form av krav, mål, metode osv. vil skape en indirekte påvirkning på kulturen, da det er avhengig av ledelsens valg av fremgangsmåte. Ledelsens påvirkning på kultur er et omtalt emne, hvor noen mener den kan ha en innflytelse, andre mener den har liten. Ifølge Antonsen (2009) skapes kultur kontinuerlig gjennom daglige interaksjoner mellom medlemmer av den aktuelle arbeidsplassen, som viser til at ledelsens involvering i kulturen kan skape en virkning. Dette underbygger funnet fra analysen, som viser at 70 prosent av informanter påpekte viktigheten av ledelsens involvering og forpliktelse ved kulturendringer. Funnet viser samtidig at motivasjonen bak standardiseringen kan påvirke ledelsen innsats og forpliktelse til standardiseringsarbeidet, da det vil påvirke arbeide ved den digitale sikkerhetskulturen. Ettersom den digitale sikkerhetskulturen krever at det arbeides kontinuering for å være i takt med den digitale utviklingen. Noe som støttes av informantenes utsagn, hvor alle (100 prosent) informantene nevnte at kontinuering forbedring var et element som hadde en innvirkning på den digitale sikkerhetskulturen. Samtidig som ISO/IEC 27001 har et eget kapittel (kapittel ti) tilegnet kontinuerlig forbedring. Gilles (2011) utdyper hvordan PUKK og Five stages to Information Security (5S2IS) er verktøy som kan brukes ved den kontinuerlige forbedringen i standardiseringsarbeidet. Gjennom bruk av slike verktøy for kontinuerlig forbedring kan virksomheten resultere i forbedret informasjonssikkerhets kvalitet og en betydelig endring i organisasjonskulturen (Gillies, 2011, s. 374).

På den andre siden forteller Berger og Luckmann sitt perspektiv om hvordan kultur skapes, omskapes og endres gjennom de daglige interaksjonene, og ikke gjennom strategisk beslutningstaking. Noe som skyldes at kultur er ustyrlig og uforutsigbar (Antonsen, 2009, s. 43). Dermed ligger det mer bak ledelsens involvering og forpliktelse til kulturendringer. Det betyr fremdeles ikke at kulturendringer er umulig, kun at de ikke er lette å kontrollere. På den

andre siden kan man endre vekstforholdene til en kultur, men endringene vil fremdeles være uforutsigbare (Antonsen, 2009, s. 43). Likevel ser man at noen former for strategisk beslutningstaking kan ha en indirekte effekt på sikkerhetskultur. Ved at implementeringen av ISO/IEC 27001 krever å utarbeide sikkerhetspolitikk og prosedyrer. Disse kravene vil hjelpe virksomheten til å etablere et rammeverk og retningslinjer for hvordan ledelsen og ansatte skal håndtere informasjonssikkerheten. Dette tiltaket vil indirekte påvirke bevisstheten rundt den digitale sikkerhetskulturen ved å sikre at ansatte får en felles forståelse av sikkerhetskravene og hva som forventes. En annen form for strategisk beslutningstaking som kan ha indirekte effekt på sikkerhetskulturen er, som nevnt tidligere, ansattes sikkerhetsopplæring. Dette vil bidra til å øke den interne forståelsen og engasjement som kreves for ansattes involvering, som igjen vil påvirke den digitale sikkerhetskulturen. På den andre siden har ikke alle individers innflytelse på kulturen en like stor betydning for å skape kulturendringer (Antonsen, 2009, s. 43). Nielsen argumenter gjennom bruk av kompleks adaptiv systemteori, at endringene ligger i organisasjonen som en helhet og ikke hos et spesifikt individ, da interaksjoner er hovedkomponenten for endring i kulturen (Nielsen, 2014, s. 8). Likevel argumenterer Nielsen for at ledere kan fremdeles påvirke endringene gjennom å styre interaksjonene (2014, s. 8), ved å involvere seg på arbeidsplassen.

Dov Zohar (2000) argumenterer for at ledere kan skape endringer i kulturen gjennom tilsynspraksis over tid. Der sikkerhetsklima dannes gjennom arbeiderenes oppfatning av prioriteringen innenfor sikkerhetsmålene opp imot effektivitetsmålene (Nielsen, 2014, s. 8). Noe som styrkes av informant 4, som utdypet viktigheten ved å ha balansen mellom funksjonalitet og sikkerhet. Der for mye sikkerhet kan gå på bekostning av funksjonalitet og omvendt. Dov Zohar sin forståelse viser til en sammenheng mellom sikkerhetskultur og -klima, der tilsynspraksis påvirkes direkte av ledernes grunnleggende antakelser (kultur) som styrer de ansattes handlinger (klima). Logikken i denne teorien argumenterer for at ledere har en direkte innflytelse på kulturen, men krever kontinuerlig og vedvarende endringer i tilsyn ved praksis for å skape endringer i kulturen. Det kan derfor argumenters for at ledelsens involvering i kulturen kan skape virkninger gjennom ulike metoder. Med hensyn til denne teorien kan ledere bruke metoden ved implementering av Standarden, ved at den bidrar til å innarbeide Standardens innhold inn i den daglige rutinen til de ansatte. Samtidig som metoden kan skape grunnlaget for vekstforholdene til kulturen, da ledelsen er involvert og til stede for de daglige interaksjonene. Informant 4 hevder at for å skape en kultur må man ha forståelse for risikoer og kunne tilpasse seg rutiner. Videre argumenterer informanten for at da rutiner blir til vaner, blir

det en kultur. Berger og Luckmann forklarer hvordan man skaper vaner, man skaper forventinger til atferd hos andre individer. Forventingene skaper grunnlaget for vanemessige handlinger, som er mønster som gjentas i interaksjoner og samhandling. Med tid blir disse vanemessige handlingene den naturlige å handle på (Antonsen, 2009, s. 43). Dermed ser man at rutiners roller i kulturendring er sentrale elementer å ta i betrakting, og kan fungere som et grunnlag ved utarbeide vekstforhold til kulturen.

7 Konklusjon

I denne forskningen har vi forsøkt å besvare følgende problemstilling: Hvordan kan implementering av ISO/IEC 27001 påvirke og potensielt styrke den digitale sikkerhetskulturen i virksomheter?

Gjennom et eksplorativt forskningsdesign har vi foretatt en kvalitativ studie, med en abduktiv forskningslogikk. Vi har samlet inn data gjennom litteratursøk og semistrukturert dybde intervjuer for å besvare spørsmålene. Ved analysering av dataen har det blitt gjennomgått en tematisk analyse, for å finne de relevante faktorene som kom frem gjentatte ganger i analysen. Gjennom analysen har vi kommet frem til fire hovedfunn: Ledelsens involvering og forpliktelse, Standardens fleksibilitet, økt sikkerhet og sikkerhetsopplæring. Det må belyses at Standarden inkluderer ingen direkte kobling til sikkerhetskultur, men har en indirekte innflytelse på kulturen.

Hensikten for vår problemstilling har vært å kunne utforske hva som kan forsterke virksomhetens robusthet, når det menneskelige aspektet er den største delen av sårbarheten. Samspillet mellom ISO/IEC 27001 og digital sikkerhetskultur er et emne med lite eksisterende forskning, det er hensiktsmessig å undersøke menneskeaspektet ved Standarden. Ved å ramme inn forståelsen er det funnet flere elementer ved menneskeaspektet som er nødvendig for at Standarden skal få en effekt på den digitale sikkerhetskulturen.

Standardens fleksibilitet kom frem som et hovedfunn da viktigheten ved at standarden kan tilpasses til virksomhetens kontekst er nødvendig. Innvirkende faktorer fra standardiseringsprosessen på den digitale sikkerhetskulturen er avgjørende for hvilke valg ledelsessystemet iverksetter ved implementering av ISO/IEC 27001. Fremdeles er det noen negative sider ved Standardens fleksibilitet som må belyses. Fleksibiliteten kan påvirke bevisstheten til de ansatte ovenfor risikoene, som kan videre få en negativ effekt på sikkerheten og den digitale sikkerhetskulturen. 70 prosent av informantene fremhevet viktigheten ved ledelsens involvering og forpliktelse. Noe som samsvarer på med Cooper (2001) sin teori om effektivt lederskap og kapittel fem i ISO/IEC 27001. Ansatte kan bli påvirket av ledelsen engasjement og forpliktelse, spesielt når kulturendringer skjer i de daglige interaksjonene. Ansattes deltakelse og forpliktelser er midlertidig like viktig for den digitale sikkerhetskulturen.

80 prosent av informantene vektla viktigheten ved opplæring, som er også en elementær del av standardiseringsprosessen. Kunnskapsheving er betydelig del av digital sikkerhetskultur (Malmedal, 2020), som gjør at opplæring og tilrettelegging innen sikkerhet kan fungere som grunnlaget for vekstforholdene (Antonsen, 2009, s. 43). Den interne forståelsen vil øke og legge grunnlaget for involvering av ansatte. På den andre siden må ledelsen være bevisst på kvaliteten av opplæring, slik det kan oppnås ønsket innvirkning på den digitale sikkerhetskulturen. Opplæringen må oppfylle visse krav, samtidig som kontinuerlig forbedring er nødvendig for å skape en god lærende kultur (Hudson et al., 2002). 50 prosent av informantene fremhevde økt sikkerhet som en nøkkelfaktor i Standarden. Funnet samsvarer med Standardens mål og dens risiko reduserende tiltak (Brenner 2007, s. 26). Vi ser også at Standarden kan skape en overdreven følelse av sikkerhet (Engen et al., 2021, s. 51), som kan føre til at mennesker får en falsk trygghetsfølelse og blir uforsiktige. Derfor krever det at virksomheter har ekstra fokus på den digitale sikkerhetskulturen (Jøsang, 2021, s. 230). 80 prosent av informantene understreket betydningen for hvordan øking av ansattes bevissthet og sikkerhetsforståelse kan ha et avgjørende resultat for standardiseringen.

Fleksibiliteten til ISO/IEC 27001 er tett sammenkoblet med ledelsens involvering og forpliktelse, samt avgjørende for å oppnå økt sikkerhet og endring av den digitale sikkerhetskulturen. Sikkerhetsopplæring av ansatte er også viktig for å kunne unngå negative sikkerhetssider. Disse funnene viser at alle fire hovedaspektene påvirker hverandre og er gjensidig avhengige, med ledelsen som et sentralt element. Ledelsens aktive involvering i standardiseringsprosessen er nødvendig for å oppnå effekt på den digitale sikkerhetskulturen ved at kulturendringer ligger i de daglige interaksjonene. Det er viktig å merke seg at Standarden mangler kulturelle og psykologiske dimensjoner som kan sikre ansattes etterlevelse. Det handler om at ledelsen må skape gode vekstforhold for kulturen og involvere de ansatte i standardiseringen.

7.1 Forslag til videre forskning

Etter å ha forsket på samspillet mellom ISO/IEC 27001 og digital sikkerhetskultur, har kunnskapshullet for dette fenomenet blitt tydeliggjort. Det menneskelige aspektet i ISO/IEC 27001 har en manglende tilstedeværelse, til tross for at det er en avgjørende del av sikkerhetsstyring. Forskningen belyser at innflytelsen standarder, som ISO/IEC 27001, har en indirekte virkning på virksomheters digitale sikkerhetskultur.

Det vil være aktuelt å utforske videre betydningen av de psykologiske og kulturelle aspektene i implementeringen av ISO/IEC 27001. Ytterligere forskning kan undersøke hvordan individuelle psykologiske faktorer påvirker etterlevelsen av Standarden. Det hadde vært interessant å gjennomføre måling av effektiviteten til ISO/IEC 27001 gjennom å utvikle et måleinstrument. Der målingen vil vurdere effekten på de menneskelige psykologiske tilnærminger til digital sikkerhet før og etter implementering av. Dette er et begivenhetsrik emne som anses relevant og aktuell for videre belysning.

8 Litteraturliste

Akowuah, F., Yuan, X., Xu, J. & Wang, H. (2013). A survey of security standards applicable to health information systems. *International Journal of Information Security and Privacy,* Vol. 7 No. 4, pp. 22-36.

Annarelli, A., Nonino, F. & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers and Industrial Engineering*, Vol. 149, 106829.

Antonsen, S. (2009). *Safety culture: theory, method, and improvement*. Ashgate.

Anttila, J., Jussila, K., Kajava, J. & Kamaja, I. (2012). Integrating ISO 27001 and other managerial discipline standards with processes of management in organizations. Availability, Reliability and Security (ARES). *Seventh International Conference* on*: IEEE, s. 1-13.* 10.1109/ARES.2012.93

Asai, T. & Hakizabera, A.U. (2010). Human-related problems of information security in East African cross-cultural environments. *Information Management and Computer Security,* Vol. 18 No. 5, pp. 328-338.

Aven, T. & Renn, O., (2010). *Risk management and governance. concepts, guidelines and applications*. Springer.

Bandura, A. (1977). *Social Learning Theory.* Prentice-Hall.

Bang, H. (2011). *Organisasjonskultur* (4. utg.). Universitetsforlaget

Berends, J.J. (1996). *On the Measurement of Safety Culture* (Unpublished graduation report). Eindhoven University of Technology.

Berger, P. L., & Luckmann, T. (1966). *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Anchor Books.

Blaikie, N., & Priest, J. (2019). *Designing social research: The logic of anticipation*. John Wiley & Sons.

Bounagui, Y., Mezrioui, A. and Hafiddi, H. (2019). Toward a unified framework for Cloud Computing governance: an approach for evaluating and integrating IT management and governance models. *Computer Standards and Interfaces*, Vol. 62, pp. 98-118.

Bowers, K. S. (1973). Situationism in psychology: an analysis and a critique. *Psychological review,* 80(5), 307.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology,* 3(2), 77-101. http://dx.doi.org/10.1191/1478088706qp063oa

Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk management,* 54(1), s. 24. https://www.yumpu.com/en/document/view/2304214/iso-27001-risk-management-and-compliance

Brinkmann, S. & Kvale, S. (2015). *Det kvalitative forskningsintervju* (T. M. Anderssen & J. Rygge, Trans. 3. utg., 2. oppl. (red.) Gyldendal akademisk.

Brown, R.L., Holmes, H. (1986). The use of a factor-analytic procedure for assessing the validity of an employee safety climate model. *Accident Analysis and Prevention* 18 (6), 455-470.

BSI. (u.å.). *ISO/IEC 27001- Information security managment (ISMS)*. https://www.bsigroup.com/en-GB/iso-27001-information-security/

Büthe, T. & Mattli, W. (2011). *The new global rulers: the privatization of regulation in the world economy.* Princeton University Press.

Cabrera, D.D., Isla, R., Vilela, L.D. (1997). An evaluation of safety climate in ground handling activities. Soekkha, H.M. (red.), *Aviation Safety, Proceedings of the IASC-97 International Aviation Safety Conference*, Netherlands, 27-29 August, pp. 255-268.

Choudhry, R. M., Fang, D. & Mohamed, S. (2007). The nature of safety culture: A survey of the state-of-the-art. *Safety Science*, *45*(10), 993-1012. https://doi.org/https://doi.org/10.1016/j.ssci.2006.09.003

Cooper, D. (2000). Towards a model of safety culture. *Safety Science*, *36*(2), 111-136. DOI:10.1016/S0925-7535(00)00035-7

Cooper, D. (2001). Improving Safety Culture: A Practical Guide. *Researchgate*. https://www.researchgate.net/publication/284371696_Improving_Safety_Culture_A_Practical_Guide

Cooper, D., (1994). Validation of a Safety Climate Measure. *Paper presented at the British Psychological Society, Annual Occupational Psychology Conference*.

Cox, S., Cox, T., 1991. *The structure of employee attitudes to safety: a European example. Work and Stress* 5 (2), 93-106, DOI: 10.1080/02678379108257007

Coyle, I.R., Sleeman, S.D., Adams, N., (1995). *Safety climate.* Journal of Safety Research 26 (4), 247-254.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal.,* 33(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202

Dalland, O. (2020). *Metode og oppgaveskriving*. (Utg. 7). Gyldendal Norsk Forlag As.

DeDobbeleer, N., Béland, F. (1991). A safety climate measure for construction sites. *Journal of Safety Research* 22, 97-103.

Delphin, I. L. A., Johnsen, R., Myren, S. K. (2021, 06.06). *Den internasjonale teleunion*. Store Norske Leksikon. https://snl.no/Den_internasjonale_teleunion

Digdir (u.å. a). *Om sikkerhetstiltak.* https://www.digdir.no/informasjonssikkerhet/om-sikkerhetstiltak/3042#8_dokumentasjon_av_sikkerhetstiltak_

Digdir. (2021). *Veileder i kompetanse- og kulturutvikling innen digitalsikkerhet.* https://www.digdir.no/informasjonssikkerhet/veileder-i-kompetanse-ogkulturutvikling-innen-digital-sikkerhet/2141

Digdir. (u.å. b). *Informasjonssikkerhet – en forutsetning for å nå virksomhetens mål.* https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-en-forutsetning-na-virksomhetens-mal/1123

Dionysiou, I. (2011). An investigation on compliance with ISO 27001 in Cypriot private and public organisations. *International Journal of Services and Standards*, Vol. 7 Nos 3-4, pp. 197-234.

DNV. (u.å.). *Sertifiseringsprosessen*. https://www.dnv.no/assurance/systemsertifisering/the-road-to-certification.html

Einarsen, S., Martinsen, Ø. L., & Skogstad, A (red.) (2017). *Organisasjon og ledelse*. Gyldendal Akademisk

Engen, O. A., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E., Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet*. Cappelen Damm Akademisk.

Engen, O.A., Gould, K. A.P., Kruke, B.I., Lindøe, P., Olsen, K. H. & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet.* (2. utg.). Cappelen Damm Akademisk.

Everett, C. (2011). Is ISO 27001 worth it? *Computer Fraud and Security*, Vol. 2011 No. 1, pp. 5-7.

Fang, D. & Wu, H. (2013). Development of a Safety Culture Interaction (SCI) model for construction projects. *Safety Science*, *57*, 138-149. https://doi.org/https://doi.org/10.1016/j.ssci.2013.02.003

Fangen, K. (2015, 17. juni). *Kvalitativ metode.* https://www.forskningsetikk.no/ressurser/fbib/metoder/kvalitativ-metode/.

Geller, E.S., (1994). Ten principles for achieving a Total Safety Culture. *Professional Safety September* 18- 24.

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000*, The TQM Journal*, Vol. 23 No. 4, pp. 367-376.

Glennon, D.P., (1982a). Measuring organisational safety climate. *Australian Safety News* January/February 23-28.

Glennon, D.P., (1982b). Safety climate in organisations. *Proceedings of the 19th Annual Conference of the Ergonomics Society of Australia and New Zealand*, 17-31.

Grenness, T. (1997). *Innføring i vitenskapsteori og metode.* (Utg. 1). Tano Aschehoug

Grønmo, S. (2016). *Samfunnsvitenskapelige metoder* (Utg. 2). Fagbokforlaget.

Guldenmund, F. W. (2000). The nature of safety culture: a review of theory and research. *Safety Science*, *34*(1), 215-257. https://doi.org/https://doi.org/10.1016/S0925-7535(00)00014-X

Heras-Saizarbitoria, I. & Boiral, O. (2013). ISO 9001 and ISO 14001: towards a research agenda on management system standards. *International Journal of Management Reviews,* Vol. 15 No. 1, pp. 47-65.

Ho, L.H., Hsu, M.T. & Yen, T.M. (2015). Identifying core control items of information security management and improvement strategies by applying fuzzy DEMATEL. *Information and Computer Security*, Vol. 23 No. 2, pp. 161-177.

Hofstad, K. (2022, 10.01). *International Electrotechnical Commission*. Store Norske Leksikon. https://snl.no/International_Electrotechnical_Commission

Holtebekk, T. (2021, 27.06). *ISO*. Store Norske Leksikon. https://snl.no/ISO

Hoy, Z. & Foley, A. (2015). A structured approach to integrating audits to create organizational efficiencies: ISO 9001 and ISO 27001 audits. *Total Quality Management and Business Excellence,* Vol. 26 Nos 5-6, pp. 690-702.

Hudson, P., D, P. & G.C., v. d. G. (2002). *The Hearts and Minds Program: Understanding HSE Culture.* https://www.researchgate.net/profile/Patrick_Hudson/publication/281236503_SPE73938/data/55dc3f2408aed6a199ac8d82/SPE73938.pdf

Humphrey, W.S. (1987). Characterising the software process: a maturity framework. *Software Engineering Institute,* CMU/SEI-87-TR-11, DTIC Number ADA182895.

International Safety Advisory Group (1991). Safety Culture (Safety Series No. 75-INSAG-4). *International Atomic Energy Agency*

Isniah, S., Hardi Purba, H., & Debora, F. (2020). Plan do check action (PDCA) method: literature review and research issues. *Jurnal Sistem Dan Manajemen Industri*, 4(1), 72–81. https://doi.org/10.30656/jsmi.v4i1.2186

ISO. (2016). *ISO/IEC 27001. Information security management systems*. https://www.iso.org/isoiec-27001-information-security.html.

ISO. (2019). *ISO in brief.* https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf

ISO. (u.å. a). *About us*. https://www.iso.org/about-us.html

ISO. (u.å.b). *Structure and governance*. https://www.iso.org/structure.html

ISO. (u.å.c). *ISO 9001 and related standards. Quality management*. https://www.iso.org/iso-9001-quality-management.html

ISO. (u.å.d). *ISO 14001 and related standards. Environmental management.* https://www.iso.org/iso-14001-environmental-management.html

ISO. (u.å.e). *ISO/IEC 27001 and related standards. Information security management.* https://www.iso.org/isoiec-27001-information-security.html

Jacobsen, D. I. (2000). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode.* Høyskoleforlaget.

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode. (*Utg. 3). Høyskoleforlaget.

Johannessen, A., Christiansen, E., & Stensaker, I. G. (2021). *Forskningsmetode for økonomisk-administrative fag* (4. utg.). Fagbokforlaget.

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode*. (utg. 5) Abstrakt forlag.

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2021). *Introduksjon til samfunnsvitenskapelig metode*. (utg. 6) Abstrakt forlag.

Johnson, C. N. (2002). The Benefits of PDCA, use this cycle for continual process improvement. *American Society for Quality,* Vol. 35. Iss 5. https://www.proquest.com/openview/6fb24b731a9c0c8bafd90096fd751e76/1?pq-origsite=gscholar&cbl=34671

Jore, S.H. (2020). Standardization of terrorism risk analysis: A means or an obstacle to achieving security? I Olsen, O. E., Juhl, K., Lindøe & Engen, O.A. (red.) *Standardization and Risk Governance: A Multi-Disciplinary Approach.* Routledge.

Jøsang, A. (2021). *Informasjonssikkerhet. Teori og praksis*. Universitetsforlaget.

Keesing, R. M. (1987). Anthropology as Interpretive Quest. *Current Anthropology*, 28, 161-176

Keesing, R. M. (1994). Theories of Culture Revisited. Borofsky. R. (red.) *Assessing Cultural Anthropology*. McGraw-Hill.

Koubatis A. & Schönberger, J. Y. (2005). Risk management of complex critical systems. *Int. J. Critical Infrastructures*, Vol. 1, Nos. 2/3, pp.195–215

Koubatis, A., & Schonberger, J. Y. (2005). Risk management of complex critical systems. *International journal of critical infrastructures*, 1(2-3), 195-215.

Kringen, J. (2015). *Culture and control. Regulation of risk in the Norwegian petroleum industry*. Doktorgradsavhandling. Universitates i Oslo.

Krumsvik, R. J. (2013). *Innføring i forskningsdesign og kvalitativ metode. Kompendium.* Fagbokforlaget Vigmostad & Bjørke AS.

Ku, C., Chang, Y. & Yen, D.C. (2009). National information security policy and its implementation: a case study in Taiwan. *Telecommunications Policy*, Vol. 33 No. 7, pp. 371-384.

Kvale, S., & Brinkmann, S. (2018). *Doing interviews*. 1-208.

Lee, T.R., (1996). Perceptions, attitudes and behaviour: the vital elements of a safety culture. *Health and Safety* October, 1-15.

Li, Y. & Guldenmund, F. W. (2018). Safety management systems: A broad overview of the literature. *Safety Science*, *103*, 94-123. https://doi.org/https://doi.org/10.1016/j.ssci.2017.11.016

Liao, K.H. & Chueh, H.E. (2012). An evaluation model of information security management of medical staff. *International Journal of Innovative Computing,* Information and Control, Vol. 8 No. 11, pp. 7865-7873.

Lomas, E. (2010). Information governance: information security and access within a UK context. *Records Management Journal,* Vol. 20 No. 2, pp. 182-198.

Lutness, J., (1987). Measuring up: assessing safety with climate surveys. *Occupational Health and Safety* 56, 20-26.

Lysgaard, S. (1967). *Arbeiderkollektivet*. Pax Forlag

Madan, M., Jagtap, P. & Teil, S. (2014). Warranty System Productivity Improvement. *Warranty Claims Reduction*, 54–65. https://doi.org/10.1201/b17122-11

Malmedal, B. (2020). NORDMENN OG DIGITAL SIKKERHETSKULTUR 2020 - Kommentar til årets befolkningsundersøkelse. *NorSIS*. https://norsis.no/content/uploads/2022/05/Nordmenn-og-digital-sikkerhetskultur-2020-web-1.pdf

Maxwell, J. (2009). Designing a Qualitative Study. *The 123 SAGE handbook of Applied Social Reserch Methods.* Brickman, & D. Rog, (red.) Sage.

Mitnick, K. (2002, 14. oktober). How to hack people. *BBC news*. http://news.bbc.co.uk/2/hi/technology/2320121.stm

Nasjonal Sikkerhetsmyndighet (2021). *Risiko 2021 – helhetlig sikring mot sammensatte trusler*. https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/det-digitale-risikobildet/

Nasjonal sikkerhetsmyndighet (2020. 01.09). *Grunnprinsipper for personellsikkerhet*. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/opprettholde-og-oppdage/skape-en-god-sikkerhetskultur/

Nettvett (2021). *Digital sikkerhetskultur.* https://nettvett.no/digitalsikkerhetskultur/

Nielsen, K. J. (2014). Improving safety culture through the health and safety organization: A case study. *Journal of Safety Research*, *48*, 7-17. https://doi.org/https://doi.org/10.1016/j.jsr.2013.10.003

Niemimaa, E. & Niemimaa, M. (2017*).* Information systems security policy implementation in practice: From best practices to situated practices*.* *European Journal of Information Systems*, 26(1), pp. 1–20

Niskanen, T. (1994). Safety climate in the road administration. *Safety Science* 17, 237-255.

NOU (2015). Digital sårbarhet – sikkert samfunn – Beskytte enkelt mennesker og samfunn i en digitalisert verden. *Norsk Offentlig Utredning.* https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

Olsen, O. E., Juhl, K., Lindøe & Engen, O.A (2019). *Standardization and Risk Governance: A Multi-Disciplinary Approach* (1. utg.). Taylor & Francis. https://doi.org/10.4324/9780429290817

Ostrom, L., Wilhelmsen, C., & Kaplan, B., (1993). Assessing safety culture. *Nuclear Safety* 34 (2), 163-172.

Pidgeon, N.F. (1991). Safety culture and risk management in organizations. *Journal of Cross-Cultural Psychology* 22 (1), 129-140.

Reason, J. (1997). *Managing the Risks of Organizational Accidents.* Ashgate.

Reason, J. (1998). Achiving a safe culture: theory and practice. *Work & Stress*, 12:3, 293-306, DOI: 10.1080/02678379808256868

Reichers, A. E., & Schneider, B. (1990). Climate and culture: An evolution of constructs. *Organizational climate and culture*, 1, 5-39.

Rezaei, G., Ansari, M., Memari, A., Zahraee, S.M. & Shaharoun, A.M. (2014). A huiristic method for information scaling in manufacturing organizations., *Jurnal Teknologi,* Vol. 69 No. 3, pp. 87-91.

Safety Research Unit, (1993). *The Contribution of Attitudinal and Management Factors to Risk in the Chemical Industry* (Final Report to the Health and Safety Executive). Psychology Department University of Surrey.

Sagdahl, S. M. (2023, 21. januar). *Etikk*. https://snl.no/etikk.

Sartor, M., Orzes, G., Di Mauro, C., Ebrahimpour, M. & Nassimbeni, G. (2016). The SA8000 social certification standard: literature review and theory-based research agenda. *International Journal of Production Economics,* Vol. 175, pp. 164-181.

Schein, E. H. (1994). *Organisasjonskultur og ledelse, er kulturendring mulig?* Libro Forlag.

Schein, E. H. (2010). *Organizational culture and leadership* (Vol. 2). John Wiley & Sons.

Silkoset, R., Olsson, U. H & Gripsrud G. (2021). *Metode, dataanalyse og innsikt.* (4. Utg.) Cappelen Damm As

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

Smith, S., Winchester, D., Bunker, D. and Jamieson, R. (2010). Circuits of power: a study of mandated compliance to an information systems security 'de jure' standard in a government organization. *MIS Quarterly,* Vol. 34 No. 3, pp. 463-486.

Standard Norge (u.å.). *Håndtering av personinformasjon* (NS-EN ISO/IEC 27701). https://standard.no/fagomrader/it-sikkerhet-og-personvern/internasjonal-standard-for-handtering-av-personinformasjon-ns-iso-27701/

Standard Norge. (2006). *Standardisering og beslektede aktiviteter — Generelle termer (ISO/IEC Guide 2:2004).* https://online.standard.no/ns-en-45020-2006

Standard Norge. (2023). *Informasjonssikkerhet, cybersikkerhet og personvern – Ledelsessystemer for informasjonssikkerhet – Krav.* (NS-ISO/IEC 27001:2022)

Stewart, A. (2018). A utilitarian re-examination of enterprise-scale information security management. *Information and Computer Security*. Vol. 26 No. 1, pp. 39-57.

Svare, H., Gausdal, A.H., & Möllering, G. (2019). The function of ability, benevolence, and integrity based trust in innovation networks. *Industry and Innovation* 27 (6) 585–604 https://doi.org/10.1080/13662716.2019.1632695

Svartdal, F. (2023). *Persepsjon. Store norske leksikon*. http://snl.no/persepsjon

Thagaard, T. (2018). *Systematikk og innlevelse: en innføring i kvalitativ metode* (5. utg.). Fagbokforlaget.

Tjora, A. (2012). *Kvalitative forskningsmetoder i praksis.* Gyldendal Norsk Forlag AS.

Tjora, A. (2022, 24.01). *Norm*. Store Norske Leksikon. https://snl.no/norm

Topa, I. & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. *Information and Computer Security*, Vol. 27 No. 3, pp. 326-342.

Van Wessel, R., Yang, X. & De Vries, H.J. (2011). Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study. *Technology Analysis and Strategic Management*, Vol. 23 No. 8, pp. 865-879.

Weick, K. E. (1991). *The Social Psychology of Organizing* (2. utg.). McGraw-Hill Education.

Westrum, R. (1993). Culture with requisite imagination, i J.A.Wise, V. Hopkin & P. Stager (red.) *Verification and validation of complex systems. Human factors issues.* Springer.

Williamson, A.M., Feyer, A.-M., Cairns, D., Biancotti, D. (1997). The development of a measure of safety climate: the role of safety perceptions and attitudes. *Safety Science* 25, 15-27.

Yin, R. K. (2018). Case study research and applications: Design and methods (6 utg.). *SAGE*

Zohar, D. (1980). Safety climate in industrial organizations: theoretical and applied implications. *Journal of Applied Psychology* 65 (1), 96-102.

Zohar, D. (2000). A group-level model of Safety Climate: Testing the Effect of Group Climate on Microaccidents in Manufacturing Jobs. *Journal of Applied Psychology*, 85, 585-596.

Zohar, D. (2014). Safety climate: Conceptualization, measurement, and improvement. In B. Schneider & K. M. Barbera (red.) *The Oxford handbook of organizational climate and culture* (pp. 317–334). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199860715.013.0017

9 Vedlegg

Vedlegg 1 – Intervjuguide

Bakgrunn

1. Kan du fortelle oss litt om deg selv?
    a. Hvor lenge har du jobbet i organisasjonen og hva er din funksjon i forhold til sikkerhet?
    b. Hvor lenge har du jobbet i din nåværende stilling?
    c. Fortell kort om din utdanning/akademiske bakgrunn?

Digital sikkerhet

2. Hva betyr digital sikkerhet for deg?
    a. Hvilken innvirkning har digital sikkerhet på ditt arbeid?
    b. Hva synes du det kreves for å styrke den digitale sikkerheten?
    c. Hvordan forholder organisasjonen seg til informasjonssikkerhet, og hvilke implementeringer har blitt iverksatt?
3. Benytter virksomheten et rammeverk eller prosedyrer for håndtering av informasjonssikkerhet?

Sikkerhetskultur og digital sikkerhetskultur

4. Hva er digital sikkerhetskultur?
    a. Hva anser du å være en god sikkerhetskultur?
5. Hvordan vil du beskrive deres digitale sikkerhetskultur?
    a. Hvor stort er fokuset på sikkerhet hos de ansatte?
    b. Hvilke utfordringer er knyttet til sikkerhetskulturen?

Ledelse, sikkerhet og risikooppfattelse

6. Hvor ofte utfører dere risikovurderinger?
7. Hvilke tiltak har dere for å øke bevisstheten om digitalsikkerhet og den tilhørende risiko?
8. Hvordan jobber toppledelse med sikkerhetskultur / digital sikkerhetskultur?-
9. Får dere ansatte noe jevnlig opplæring i digitalsikkerhet?

10. Hvilke tiltak har dere innført for å bidra til en god digital sikkerhetskultur i virksomheten?

Standard spørsmål

11. Hvordan kan sertifisering i standarder kan påvirke virksomheten/organisasjonen?
12. Hvilken nytte kan ISO har i forbindelse med ulike krav som kan stilles av f.eks myndigheter eller kunder.
13. Hvordan kan implementering av standarder / prosedyrer gi noe virking på sikkerhetskulturen?
14. Vil sertifisering av standarder påvirke bevisstheten og kunnskapen til ansatte gjennom hele organisasjonen?
15. Kunne du se for deg noen utfordringer eller begrensinger som kan forekomme ved å bli sertifisert?

ISO - 27001 spørsmål

16. Hva var bakgrunnen til at bedriften valgte å sertifisere seg i ISO-27001?
17. Hvorfor valgte dere ISO 27001 for informasjonssikkerhet?
18. Hvilke verdier ser der i sertifiseringen?
19. Kan du si noe om det var lagt merke til noen endringer i den digitale sikkerhetskulturen etter/under sertifisering av ISO-27001?
    a. Var det mye endringer i sikkerheten før og etter sertifisering?
    b. Synes du sertifiseringen er et godt verktøy for en sikker fremtid? Hvorfor?
20. Hvordan opplevde dere sertifiseringen?
    a. Opplevde dere den som lønnsomt, nyttig og enkelt?
21. Hva gjør dere for å sikre at nyansatte lærer om / forstår viktigheten av sertifiseringen?
22. Hvordan kan sertifisering en bidra til håndtering av potensielle trusler og sårbarheter?
23. Hvordan vil du si sertifisering og de implementere tiltak bidrar til å redusere risikoen?
24. Opplevde dere noen begrensinger eller utfordringer med å sertifiseres i ISO 27001?
25. Hvilke nytte kan ISO har i forbindelse med ulike krav som kan stilles av f.eks myndigheter og kunder? (Still dette om de ikke nevner noe)

Avslutningsvis

26. Helt til slutt, er det noe du har lyst til å si som vi ikke har kommet inn på tidligere?

Vedlegg 2 – Informasjonsskriv

Vil du delta i forskningsprosjektet ” ISO/IEC 27001 sin innvirkning på digitale sikkerhetskultur?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt om ISO/IEC 27001 sin innvirkning på virksomhetenes digitale sikkerhetskultur. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Formålet ved forskningsprosjektet er å undersøke hvordan implementering av ISO/IEC 27001 kan påvirke og potensielt styrke den digitale sikkerhetskulturen i virksomheter. Gjennom problemstillingen ønsker vi å utforske hvordan implementeringen og kontinuerlig etterlevelse av ISO/IEC 27001 kan påvirke virksomhetens ansatte sine holdninger, atferd og praksis knyttet til informasjonssikkerhet. Vi ønsker å identifisere og analysere nøkkelfaktorer for implementering av Standarden i en virksomhet for å fremme en robust og sterk digital sikkerhetskultur. Funnene i dette prosjektet vil være verdifulle for virksomheter, ettersom de søker å forstå virkningen av ISO/IEC 27001 på den digitale sikkerhetskulturen og vil bidrar til å ta informerte beslutninger om implementering av standarder.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Stavanger ved det teknisk- naturvitenskaplige fakultet / Institutt for sikkerhet, økonomi og planlegging er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Utvalget er nøye gjennomtenkt og utpekt etter deres relevans til forskningsprosjektets problemstilling. Våre kriterier for aktuelle intervjukandidater går på ledere eller relevante nøkkelpersoner som har fokus på ISO/IEC 27001, digital sikkerhetskultur og virksomhetens digitale sikkerhet.

Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det at du deltar på et intervju. Metoden for dette forskningsprosjektet er kvalitative metoder, dermed dybdeintervju på rundt 45 - 60 min. Hvis intervjukandidater velger å delta i prosjektet, innebærer det at vi vil samle inn opplysninger ved lydopptak under intervjuet. For å ivareta personvern blir dette videre transkribert og anonymisert, slik at lydopptaket kan bli slettet.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Ved behandling av opplysningene ved dette forskningsprosjektet vil kun studentene Katarina Svendsen og Viktoria Eik, og vår veileder Kenneth Arne Pettersen Gould, med begrenset tilgang, være de eneste som har tilgang på informasjonen.
Tiltakene for sikring av personopplysningene vil alle datamaterialer oppbevares kryptert. Navn og kontaktopplysninger vil bli behandlet og bli erstattet med en kode som lagres i en egen navneliste adskilt fra øvrige data.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes *når oppgaven blir godkjent*, som er tiltenkt å avsluttes 15. juni 2023. Etter prosjektslutt vil datamaterialet med dine personopplysninger anonymiseres. Dette inkludere at personopplysninger, inkludert lydopptak blir anonymiserte.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Stavanger - Institutt for sikkerhet, økonomi og planlegging har Sikt – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- *Katarina Svendsen – katarina.svendsen@gmail.com*
- *Viktoria Eik – Viktoria.eik98@gmail.com*
- Vårt personvernombud: *Rolf Jegervatn - personvernombud@uis.no*

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra Sikt, kan du ta kontakt via:

- Epost: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Med vennlig hilsen,

Viktoria Eik & Katarina Svendsen
Studenter ved Universitetet i Stavanger

Vedlegg 3 - Samtykkeerklæring

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet; *ISO/IEC 27001 sin innvirkning på digitale sikkerhetskultur*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju
- at mine personopplysninger lagres frem til prosjektslutt

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 4 - Godkjenning av Sikt

Vurdering av behandling av personopplysninger

Referansenummer
811376

Vurderingstype
Standard

Dato
25.03.2023

Prosjekttittel
Standardiserings påvirkning for digital sikkerhetskultur

Behandlingsansvarlig institusjon
Universitetet i Stavanger / Det teknisk- naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Prosjektansvarlig
Kenneth Arne Pettersen Gould

Student
Viktoria Malena Eik

Prosjektperiode
02.01.2023 - 15.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 15.06.2023.

Meldeskjema

Kommentar
OM VURDERINGEN
Sikt har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

FØLG DIN INSTITUSJONS RETNINGSLINJER
Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandører som din institusjon har avtale med (f.eks. ved skylagring, nettspørreskjema, videosamtale el.)

Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Se våre nettsider om hvilke endringer du må melde: https://sikt.no/melde-endringar-i-meldeskjema

OPPFØLGING AV PROSJEKTET
Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Vedlegg 5 - Definisjoner av sikkerhetsklima og sikkerhetskultur

Definitions of safety climate and safety culture (Guldenmund, 2000, s. 228-229).

Reference	Definition of safety culture/climate
Zohar (1980)	A summary of molar perceptions that employees share about their work environments (safety climate)
Glennon (1982a,b)	Employees' perceptions of the many characteristics of their organization that have a direct impact upon their behavior to reduce or eliminate danger (safety climate) and, safety climate is a special kind of organizational climate
Brown and Holmes (1986)	A set of perceptions or beliefs held by an individual and/or group about a particular entity (safety climate)
Lutness (1987)	Not explicitly stated (safety climate)
Cox and Cox (1991)	Safety cultures reflect the attitudes, beliefs, perceptions, and values that employees share in relation to safety (safety culture)
Dedobbeleer and Béland (1991)	Molar perceptions people have of their work settings (safety climate)
International Safety Advisory Group (1991)	Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance (safety culture)
Pidgeon (1991)	The set of beliefs, norms, attitudes, roles, and social and technical practices that are concerned with minimising the exposure of employees, managers, customers, and members of the public to conditions considered dangerous or injurious (safety culture)
Ostrom et al. (1993)	The concept that the organisation's beliefs and attitudes, manifested in actions, policies, and procedures, affect its safety performance (safety culture)
Safety Research Unit (1993)	Not explicitly stated (safety climate)
Cooper and Philips (1994)	Safety climate is concerned with the shared perceptions and beliefs that workers hold regarding safety in their workplace (safety climate)

Geller (1994)	In a total safety culture (TSC), everyone feels responsible for safety and pursues it on a daily basis (safety culture)
Niskanen (1994)	Safety climate refers to a set of attributes that can be perceived about particular work organisations and which may be induced by the policies and practices that those organisations impose upon their workers and supervisors (safety climate)
Coyle et al. (1995)	The objective measurement of attitudes and perceptions toward occupational health and safety issues (safety climate)
Berends (1996)	The collective mental programming towards safety of a group of organisation members (safety culture)
Lee (1996)	The safety culture of an organisation is the product of individual and group values, attitudes, perceptions, competencies, and patterns of behaviour that determine the commitment to, and the style and proficiency of, and organisation's health and safety management (safety culture)
Cabrera et al. (1997)	The shared perceptions of organisational members about their work environment and, more precisely, about their organisational safety policies (safety climate)
Williamson et al. (1997)	Safety climate is a summary concept describing the safety ethic in an organisation or workplace which is reflected in employees' beliefs about safety (safety climate)