NTNU
Kunnskap for en bedre verden

Modell for innføring av et ledelsessystem for informasjonssikkerhet

Bacheloroppgave i Informasjonsbehandling – IINI3011

Simen Sand

Natalia Ravna

Martin Rønning

Innleveringsfrist: 20.05.2019

Norges teknisk-naturvitenskapelige universitet

Institutt for datateknologi og informatikk

Forord

Denne hovedoppgaven er den avsluttende delen av vårt studieprogram Informatikk med spesialisering i informasjonsbehandling. Vår faglige veileder gjennom formuleringen av denne oppgaven var Bjørn Klefstad, og vi ønsker å rette en stor takk til han for tett og god oppfølging gjennom hele prosessen. Videre ønsker vi å vise vår takknemlighet ovenfor de virksomhetene som gikk med på å stille til intervju og gi gode, tydelige og ikke minst ærlige svar på et emne som vil ansees som sensitivt. Innholdet i denne oppgaven står for forfatternes regning.

Tittel	Modell for innføring av et ledelsessystem for informasjonssikkerhet
Dato	20.05.2019
Deltakere	Simen Sand, Natalia Ravna, Martin Rønning
Veileder	Bjørn Klefstad
Oppdragsgiver	NTNU
Nøkkelord	ISMS, GDPR, ISO 27001, ISO 27002, PDCA, Informasjonssikkerhet, Datatilsynet, Difi, NSM, NorSIS
Totalt antall sider	94
Antall vedlegg	3

Sammendrag

Formålet til denne forskningsrapporten er å analysere hvorvidt vår nåværende modell for innføring av et ISMS har blitt foreldet som følge av store fremskritt og endringer innen feltet, hvordan den nye personvernsforordningen (GDPR) har påvirket denne prosessen og hvordan ISO-standardene, spesifikt ISO-27001 og ISO-27002, hjelper bedrifter med arbeidet om å holde seg i tråd med de lover og reguleringer som kreves. For å besvare dette spørsmålet har vi intervjuet to forskjellige virksomheter angående deres arbeid med ISMS, og fått deres syn på hvordan de stiller seg i forhold til den modellen vi presenterte for dem. Vi benytter oss også av teori fra forskjellige aktører i Norge som arbeider innen informasjonssikkerhet, samt teori rundt ISO-standardene og GDPR. Resultatene våre viste at vår modell var gjenkjennbar hos virksomhetene, men at de ikke hadde arbeidet konkret opp mot en slik modell, men at den gjenspeilet hvordan de arbeidet med dette emnet. Det vi også fant ut fra virksomhetene var at implementeringen av GDPR ledet dem til et større fokus rundt denne forordningen for å kunne være presentable fremfor klientene sine. Alle resultatene i denne rapporten leder oss til å kunne konkludere med at ISO-standarden 27001 fortsatt er grunnlaget for beste praksis når det er snakk om implementering av et ISMS. Fra det perspektivet, uttrykker dette studiet den sentrale stillingen ISO-standardene har når man jobber opp imot implementering og kontinuerlig forbedring av et ISMS, og for overholdelse av de lover og forordninger man er nødt til å følge.

Abstract

The purpose of this paper is to analyze whether our current model for implementation of an ISMS has been deprecated following the tremendous advancements within the field, how the new data protection regulation (GDPR) has affected this process and how the ISO-standards, specifically ISO-27001 and ISO-27002, helps businesses achieve compliance with the laws and regulations they are required to follow. To answer this question, we interviewed two separate businesses about their work with ISMS as well as their take on the model that we presented for them. We also incorporate theoretic material from different organizations that work within the security field in Norway, as well as the ISO-standards and the GDPR. Our results showed that the model that was presented to them was familiar in terms of how they work with ISMS, but that it was from a subconscious side and that they did not have a specific model that they had worked against. They also admitted to how the implementation of the GDPR had led to an increased focus on compliance in order to act presentable towards their clients. However, all our results lead us to conclude that the ISO-standard 27001 is the root of best practice in terms of the implementation of an ISMS. From that perspective, this study emphasizes on the importance of the ISO-standards when working towards implementing and continually improving an ISMS, and for the compliance of mandatory laws and regulations.

Begrepsliste og forkortelser

Standard: er en teknisk spesifikasjon som beskriver hvordan ulike objekter skal kunne defineres på en entydig måte, for eksempel mål og vekt, eller som beskriver arbeidsmetoder, for eksempel kvalitetsstyring i en bedrift. Standarder blir vanligvis utviklet og vedlikeholdt av en standardiseringsorganisasjon på nasjonalt, europeisk eller globalt plan (Wikipedia, 2018).

ISO: International Organization for Standardization er en internasjonal standardiseringsorganisasjon som utgir standarder innenfor en rekke områder (Wikipedia, 2018)

IEC: International Electrotechnical Commission er en ideell, ikke-statlig internasjonal standardiseringsorganisasjon som utformer og publiserer internasjonale standarder for alle typer elektrisk, elektronisk og relatert teknologi under samlebetegnelsen «elektroteknologi» (Wikipedia, 2017)

NEK: Norsk Elektroteknisk Komite er det norske medlemsorganet i IEC. NEK er en aktiv, selvstendig og nøytral medlemsorganisasjon som har ansvaret for norsk standardiseringsarbeid innen el- og ekom (NEK, u.d.)

BSI: British Standards Institution er det nasjonale standardorganet i Storbritannia. BSI produserer tekniske standarder på et bredt spekter av produkter og tjenester, og leverer også sertifisering og standardrelaterte tjenester til bedrifter (Wikipedia, 2019).

BS: British Standard er standarder som produseres av BSI.

EN: European Standard er standarder som utvikles av CEN (European Committee for Standardization)

NS: Norsk Standard. Organisasjonen utvikler og forvalter standarder i Norge. Gjennom Standard Online gjør Standard Norge norske, europeiske og internasjonale standarder tilgjengelige og bidrar til at de tas i bruk (Standard Norge, 2019).

PDCA: Plan, Do, Check og Act. Iterative prosesser for gjennomføring av kontroll og kontinuerlig forbedring av prosesser og tjenester.

GDPR: General Data Protection Regulation, en forordning fra EU som regulerer hvordan personopplysninger behandles, samt styrke rettighetene til privatpersoner.

Personopplysninger: Alt av opplysninger som kan bidra til å identifisere enkeltpersoner på bakgrunn av de gitte opplysningene.

Kontrollør: Betegner den kontrollerende delen i et samarbeid om behandling av personopplysninger.

Prosessor: Betegner den parten som behandler/prosesserer personopplysninger.

Data subjekt: Enkeltperson som får sine data samlet inn av kontrollør og prosessor til bearbeiding.

Personvern: Omhandler rettigheten til å ha et privatliv og retten til å bestemme over egne personopplysninger.

NorSIS: Norsk senter for informasjonssikring er en forening som ble stiftet 2. februar 2010, og som er en del av regjeringens helhetlige satsing på informasjonssikkerhet i Norge.

NSM: «Nasjonal sikkerhetsmyndighet er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser.» (Nasjonal Sikkerhetsmyndighet, 2019)

Datatilsynet: et norsk, uavhengig forvaltningsorgan administrativt underordnet Kommunal- og moderniseringsdepartementet, opprettet 1. januar 1980. Datatilsynet er både tilsyn og ombud, og har som oppgave å overvåke overholdelse av personopplysningsloven. (Wikipedia, 2019)

Difi: Direktoratet for IKT og forvaltning er et norsk statlig direktorat opprettet 1. januar 2008, og ligger under Kommunal og moderniseringsdepartementet. Særlig ansvar for digitalisering av offentlig sektor, offentlige anskaffelser og forvaltningsutvikling. Vil endre navn til Digitaliseringsdirektoratet 1. januar 2020. (Wikipedia, 2019)

Nkom: Nasjonal kommunikasjonsmyndighet er en etat under Kommunal- og moderniseringsdepartementet, og de arbeider for bærekraftig konkurranse i post- og ekomsektoren, slik at brukere i hele landet kan tilbys gode og fremtidsrettete tjenester til konkurransedyktige priser. (Nasjonal kommunikasjonsmyndighet, 2019)

Innholdsfortegnelse

1.0 Innledning 10

1.1 Bakgrunn for oppgave 11

2.0 Teori 13

2.1 Aktører innen ISMS 13

2.2 PDCA metoden 24

2.3 Informasjonssikkerhet 25

2.4 ISO 27001 29

2.5 ISO 27002 35

2.6 GDPR 38

2.7 Artikkel “Integration of the GDPR requirements into the requirements of the SR EN ISO/IEC 27001:2018 standard, integration security management system in a software development company.” 46

3.0 Metode 50

3.1 Primærdata 50

3.2 Sekundærdata 51

4.0 Resultat (Empiri/Statistikk) 53

5.0 Diskusjon 60

5.1 Hvilke komplikasjoner har GDPR skapt for innføring av ISMS i bedrifter? 60

5.2 I hvilken grad hjelper ISO-standardene med å oppfylle kravene i GDPR? 63

5.3 Dagens modell for innføring av ISMS i bedrifter og veiledningsmateriell fra Difi, NorSIS, Datatilsynet og NSM 68

5.4 NS-EN ISO/IEC 27001:2017/NS-EN ISO/IEC 27002:2017 og dagens modell for et ledelsessystem for informasjonssikkerhet (ISMS) 72

6.0 Konklusjon 76

Referanser 79

Vedlegg 85

Figurliste

Figur 1: Illustrasjon av aktivitetene i et system for informasjonssikkerhet. Fra Difi «Systematiske aktiviteter.» (https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter) 14
Figur 2: Deminghjulet 24
Figur 3: Modell for innføring av ISMS. Figuren er hentet fra faget IINI2009 - Informasjonssikkerhet og produktforvaltning 2018 27
Figur 4: PDCA-modell brukt i ISMS-prosesser. Fra ISO Online Browsing Platform. ISO/IEC 27001:2005(en), 2005 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en) 30
Figur 5: Risk evaluation methodology. Fra «INTEGRATION OF THE GDPR REQUIREMENTS INTO THE REQUIREMENTS OF THE SR EN ISO/IEC 27001:2018 STANDARD, INTEGRATION SECURITY MANAGEMENT SYSTEM IN A SOFTWARE DEVELOPMENT» (https://atna-mam.utcluj.ro/index.php/Acta/article/view/1054) 47
Figur 6: 12041: Tiltak/rutiner ved administrasjon av IKT-sikkerheten (prosent), etter forvaltningsnivå, antall innbyggere, statistikkvariabel og år. Fra Statistisk Sentralbyrå, 29. mai 2018 (http://www.ssb.no/statbank/sq/10018006/) 59
Figur 7: Modell for innføring av ISMS. Figuren er hentet fra faget IINI2009 - Informasjonssikkerhet og produktforvaltning 2018 68
Figur 8: Illustrasjon av aktivitetene i et system for informasjonssikkerhet. Fra Difi «Systematiske aktiviteter.» (https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter) 68
Figur 9: Modell for ISMS med hovedkrav fra NS-EN ISO/IEC 27001:2017 75

Tabelliste

Tabell 1: Innholdet i ISO/IEC 27001:2005(en) og ISO/IEC 27001:2017(en) 31
Tabell 2: Innholdet i ISO/IEC 27001:2013(en) og NS-EN ISO 27001:2017(en) 32
Tabell 3: The risk handling plan for: confidential information resource- personal data. Fra «INTEGRATION OF THE GDPR REQUIREMENTS INTO THE REQUIREMENTS OF THE SR EN ISO/IEC 27001:2018 STANDARD, INTEGRATION SECURITY MANAGEMENT SYSTEM IN A SOFTWARE DEVELOPMENT» (https://atna-mam.utcluj.ro/index.php/Acta/article/view/1054) 49
Tabell 4: Datainnsamling basert på intervju og spørreskjema. Kilde: (Kristen, 2001, s. 124) 51
Tabell 5: Ulike typer sekundærdata. Kilde: (Ringdal, 2001, s. 120) 52
Tabell 6: Besvarelser fra Virksomhet 1 og Virksomhet 2 57
Tabell 7: 12042: Tiltak som del av internkontroll for informasjonssikkerhet (prosent), etter forvaltningsnivå, statistikkvariabel og år. Fra Statistisk Sentralbyrå, 29. mai 2018 (http://www.ssb.no/statbank/sq/10017378/) 57
Tabell 8: Utdrag fra tabellen viser antall gyldige ISO 27001 sertifikater i perioden 2006-2017 i Norge (ISO, u.d.). 57
Tabell 9: Top 10 countries for ISO/IEC 27001 certificates - 2016. Tabellen hentet fra «9. ISO Survey of certifications to management system standards - Full results» (https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1) .. 58
Tabell 10: 10852: Tiltak/rutiner ved administrasjon av IKT-sikkerheten i statlige virksomheter (prosent), etter sysselsettingsgruppe, statistikkvariabel og år. Fra Statistisk Sentralbyrå, 29. mai 2018 (http://www.ssb.no/statbank/sq/10019507/) 58
Tabell 11: Bruk av IKT i offentlig sektor. Andel som har opplevd IKT-sikkerhetsproblemer. Fra Statistisk Sentralbyrå, 28. mai 2018 (https://www.ssb.no/iktbruks) 59
Tabell 12: Karlegging av krav fra GDPR og sikkerhetstiltak fra ISO 27001 67
Tabell 13: Kartlegging av krav fra NS-EN ISO/IEC 27001:2017 og faser i modellen for ISMS 74

Tabell 14: Spørreskjema.....85
Tabell 15: ISO/IEC 27001 Europe. Hentet fra 9. ISO Survey of certifications to management system standards - Full results (https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1)..94

1.0 Innledning

Informasjon er en stadig større del av verdiene hos virksomheter. I takt med et økende trusselbilde, og strengere krav og regler, er det viktig for alle virksomheter å ha et systematisk arbeid med informasjonssikkerhet. For offentlige virksomheter er det ikke bare viktig, men også pålagt gjennom ulike regelverk. På bakgrunn av disse opplysningene, samt oppgaveforslaget har vi utarbeidet en problemstilling som vil forske på om den nye personvernsforordningen GDPR har påvirket arbeidet med ISMS som følge av strengere krav enn tidligere, hvorvidt ISO-standardene er et tilstrekkelig hjelpemiddel i dette arbeidet, samt en vurdering på dagens modell for innføring av ISMS og hvordan denne påvirkes.

Problemstilling

«Hvilke komplikasjoner har GDPR skapt for innføring av ISMS i bedrifter, i hvilken grad hjelper ISO-standardene med å oppfylle disse kravene og hvordan står dette i stil med dagens modell for innføring av ISMS i bedrifter?»

I denne oppgaven vil vi sammenligne en modell for innføring av styringssystem for informasjonssikkerhet fra NTNU, mot veiledninger og modeller fra norske aktører innen området. Videre vil vi sammenligne modellen mot krav og anbefalinger hentet fra standardene NS-ISO/IEC 27001:2017 og NS-ISO/IEC 27002:2017.

Vi skal også se på forordningen GDPR, for å finne ut om den påvirker innføringen av styringssystemet, og også om det å bruke ISO-standardene vil hjelpe virksomheter med å overholde krav i fra denne forordningen.

Til slutt har vi intervjuet to virksomheter for å prøve å finne ut hva som faktisk gjøres av sikkerhetsarbeid i praksis. Vi prøver også å finne ut av hvordan virksomhetene forholder seg til GDPR, og hvordan de jobber i forhold til NTNUs modell for innføring av styringssystem.

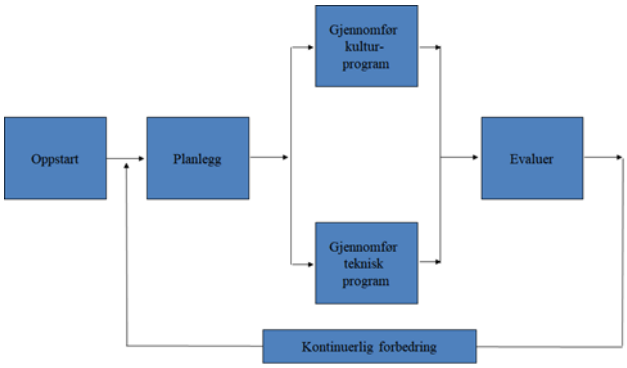
Oppgaven er strukturert slik at vi i teoridelen tar for oss beskrivelser om aktører og veiledninger innen styringssystem for informasjonssikkerhet, PDCA-metodikk, ISMS og NTNU sin modell for styringssystem, standardene ISO 27001 og ISO 27002 og GDPR. Til slutt beskrives en forskningsartikkel som omhandler implementering av GDPR-krav med sikringstiltak i SR EN ISO/IEC 27001:2018.

Videre kommer en resultatdel der vi oppgir svarene fra to intervju med to forskjellige virksomheter. Samt presentasjon av resultater fra andre sekundære kilder vi har valgt å benytte oss av videre til diskusjon.

I diskusjonsdelen ser vi på GDPR mot informasjonssikkerhet og vi ser i hvilken grad ISO-standardene hjelper til å oppfylle krav i GDPR.
Videre vil vi sammenligne NTNU sin modell for ISMS mot norske aktørers veiledninger, mot de to virksomhetene vi har intervjuet, og mot ISO-standardene.

1.1 Bakgrunn for oppgave

Selve bakgrunnen for oppgaven og den tidligere forskningen innen dette emnet har resultert i en modell for innføring av et styringssystem for informasjonssikkerhet:



Det er denne modellen vi er ute etter å analysere i denne oppgaven. Modellen er utarbeidet ved NTNU og baserer seg på prinsipper om beste praksis i henhold til den omfattende standarden ITIL V3. I ITIL V3 standarden beskrives det at den offisielle standarden for ISMS er ISO-27001 og at den modellen som blir presentert i ITIL V3 også er utarbeidet i henhold til denne standarden. (Van Bon, 2007) I vår formulering ønsker vi dermed å rette fokuset over mot den offisielle sikkerhetsstandarden ISO-27001 og vil ikke omtale bruken av ITIL V3.

Begrensninger:

NS-ISO/IEC 27001:2005 (Standard Norge, 2013) og NS-ISO/IEC 27001:2013 (Standard Norge, 2017) er tilbaketrukket og erstattet med NS-EN ISO/IEC 27001:2017.

Vitenskapelige artikkelen "*Integration of the GDPR requirements into the requirements of the SR EN ISO/IEC 27001:2018 standard, integration security management system in a software development company*" som er brukt i teoridelen refererer til SR ISO/IEC 27001:2018 som ikke er tilgjengelig som en åpen ressurs og derfor referanser i artikkelen til denne standarden kan ikke kontrolleres av prosjektgruppen.

NS ISO/IEC 27001:2018 beskriver 114 sikringstiltak. Det ble derfor beskrevet noen av sikringstiltak som eksempler i denne oppgaven.

GDPR er en stor og omfattende forordning som tar for seg mange ulike scenarier. Her velger vi å begrense GDPR til å ta med de viktigste artiklene som vil påvirke hvordan man er nødt til å forholde seg til GDPR i et ledelsessystem for informasjonssikkerhet, samt også inkludere hvilke rettigheter data subjektene har for å diskutere hvordan dette kan påvirke strukturen på ledelsessystemet.

Vi begrenser dermed GDPR ved å inkludere: kapittel 3 og kapittel 4, der i kapittel 4 vil det ligge et større fokus på kontrollør og prosessor, samt artikkel 32, 40 og 42.

I henhold til aktører har vi valgt å forholde oss til de aktørene som gir konkrete veiledninger for implementering av ISMS. Vi har også valgt å legge enda litt mer vekt på Datatilsynet, ettersom dette er Norge sin tilsynsmyndighet i henhold til GDPR. Som følge av at Nkom ikke er en aktør som gir direkte veiledninger vil de kun bli bragt opp i diskusjon mot andre aktører der de spiller en liten rolle.

2.0 Teori

Innledning

I denne delen av oppgaven presenteres den teoretiske bakgrunnen som baserer seg på sekundære kilder som standarder, forordninger, lovverk, artikler, bøker og videopptak av foredrag fra Sikkerhetskonferansen 2019. Kapitlet gir informasjon om viktige offentlige aktører som har ansvar for informasjonssikkerhet og deres veiledninger for informasjonssikkerhet. Videre introduseres og beskrives det PDCA kvalitetsforbedringsmetode, begrep «informasjon og informasjonssikkerhet», et styringssystem for informasjonssikkerhet sammen med modell for innføring av et styringssystem for informasjonssikkerhet. Det gjennomgås to viktige internasjonale standarder ISO 27001 og ISO 27002 relatert til informasjonssikkerhet. Det gis forklaringer om GDPR forordninger, databeskyttelsesprinsipper, rettigheter og forpliktelser. Til slutt vises til en vitenskapelig artikkel fra Romania som beskriver en case for implementering av GDPR krav med sikringstiltak i SR EN ISO/IEC 27001:2018.

2.1 Aktører innen ISMS

2.1.1 Difi – Direktoratet for forvaltning og IKT.

Hva er Difi?

Difi er et fagorgan for Kommunal- og moderniseringsdepartementet, og Nærings- og fiskeridepartementet innen fagområdene ledelse, organisering, offentlige anskaffelser og digitalisering i offentlig sektor. Difi forvalter også digital postkasse (statlig digital postkasse for borgere tiltenkt beskjeder fra stat og kommune), ID-porten (felles innloggingstjeneste til offentlige tjenester på internett), og Kontakt- og reservasjonsregisteret (fellesløsning for offentlige virksomheters tjenesteløsning, et register over borgernes digitale kontaktinfo og reservasjon)

Difi har et tett samarbeid med offentlige og private virksomheter som har ansvarsområder som grenser opp imot Difi sine områder. Samarbeid primært med stat og kommune for samordna, mer effektive, og mer brukerorienterte tjenester. Sekundære samarbeidsgrupper er borgere, og næringslivet. Målsetninger innen sekundærgruppa er at borgerne skal oppleve offentlig sektor som mer brukerorientert, og med mer bruk og gjenbruk av offentlige data, komponenter og løsninger er målet økte gevinster for næringslivet. Difi ønsker også samarbeid med private aktører for å få ut mest mulig potensialet i offentlige anskaffelser. (Direktoratet for forvaltning og IKT, 2019)

Hva sier Difi om styringssystem for informasjonssikkerhet?

«Alle virksomheter har behov for systematikk i styring og kontroll for å nå mål og resultatkrav, arbeide effektivt, etterleve lover og regler og ha pålitelig rapportering. Dette gjelder på flere områder.» (Difi, 2019)

Nettstedet til Difi forteller at formålet med et styringssystem for informasjonssikkerhet er at **offentlige** virksomheter skal ha nok styring og kontroll på informasjonssikkerheten, nærmere definert ved å ha nok kontroll og styring på integriteten, konfidensialiteten, og tilgjengelighet av informasjon. Og med dette menes informasjon internt, kommunikasjon med andre, og eksterne tjenester. Om bruksområdet tenkes informasjon som er kritisk for å nå virksomhetens behov for

effektiv drift, og informasjon som er underlagt spesielle krav, som lovfestede krav til saksbehandling, taushetsplikt, og personopplysningsloven, for å nevne noen eksempler.

«En obligatorisk standard skal følges med mindre du faller inn under en unntaksordning i forskrift. Anbefalte standarder skal benyttes med mindre du har gode grunner til å la være»
(Difi, 2019)

Difi sier det er **obligatorisk** for forvaltningsorgan som benytter elektronisk kommunikasjon til å ha internkontroll på informasjonssikkerhetsområdet. Omfang og innretning på internkontrollen skal være tilpasset risiko, og internkontrollen skal basere seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Difi oppgir ISO/IEC 27001:2013 som anbefalt å basere seg på (mulighet for lokale tilpasninger til hvilke krav man følger) ved oppretting av internkontroll på informasjonssikkerhet.

Difis modell for et system for informasjonssikkerhet.

Figur 1: Illustrasjon av aktivitetene i et system for informasjonssikkerhet. Fra Difi «Systematiske aktiviteter.» (https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter)

Systematiske aktiviteter i internkontroll for informasjonssikkerhet. Slike aktiviteter for styring og kontroll kalles også «styringssystem for informasjonssikkerhet» (Difi, u.d.):

- Ledelsens styring og oppfølging. Det er virksomhetsledelse som har ansvar for etablering av tilstrekkelig styring og internkontroll på informasjonssikkerhetsområder. Dette oppnås ved følging av lover og regler, etablering og oppfølging av et systematisk internkontrollarbeid i hele virksomheten, tilføring av nødvendige ressurser og gjennomføring av nødvendige endringer ved behov. (Difi, 2019) (Difi, u.d.).
- Risikovurdering gjennomføres for å identifisere, kartlegge, analysere og evaluere risiko som angår informasjonssikkerhet. Risikovurdering kan oppfatte hele virksomhet, enkelte

prosesser eller informasjonssystemer. «Det er lederens ansvar å sørge for at det gjennomføres nødvendige risikovurderinger innenfor eget ansvarsområde» (Difi, 2019).

- Risikohåndtering gjøres av utpekte ansvarlige i virksomheten, og i denne fasen foretas bestemmelser om hvordan risiko skal håndteres, og tiltak som følge av dette. Tiltak utarbeides i samsvar med vurderingene for akseptabel risiko.
  (Difi, 2019)
- Overvåking og hendelseshåndtering. Tekniske og manuelle rutiner må fange opp og sørge for oppfølging av feil, avvik og uønskede hendelser. Det er viktig at erfaringene man gjør seg i denne fasen tas med videre i sikkerhetsarbeidet.
  (Difi, 2019)
- Måling, evaluering og revisjon. Virksomheten tester ved hjelp av målinger om tiltak fungerer, og om pålegg blir etterlevd. Dette må gjennomføres både ved etablering og bruk av ulike tiltak. Målinger, evalueringer og internrevisjoner er viktig beslutningsgrunnlag for ledere på ulike nivå.
  (Difi, 2019)
- Kompetanse og kulturutvikling omhandler viktigheten av sikkerhetskulturen i virksomheten for at internkontrollen skal fungere etter hensikten. (Difi, 2019)
  En annen aktør, NSM, beskriver uttrykket sikkerhetskultur på denne måten:
  «Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsadferd.»
  (NSM, 2019)

Kommunikasjon legger til rette for læring, er kritisk for hendelseshåndtering, og gjør at virksomheten samlet kan jobbe med informasjonssikkerhet.
(Difi, 2019)

Difi forteller videre at deres eget veiledningsmateriell «internkontroll i praksis – informasjonssikkerhet» er basert på ISO/IEC 27001:2013, og konkretisert og tilpasset norske offentlige virksomheter. Difi sier det er anbefalt å søke til standarden ISO/IEC 27001:2013 som støtte og referanse ved etablering, forbedring og statusanalyse av internkontroll på informasjonssikkerhetsområdet.
Ved valg og etablering av risikoreduserende tiltak anbefaler Difi å finne støtte i anerkjente kilder, og tidsbruken for dette bør tilpasses risikoen. De viser til flere kilder, med standarden ISO/IEC 27002, faktaark, veiledere og norm for informasjonssikkerhet fra Helse og omsorgstjenesten, og veiledninger fra Nsm (Nasjonal Sikkerhetsmyndighet), Difi og Datatilsynet. Ved mer omfattende krav fra lov- og regelverk enn overnevnte standarder tilbyr, må dette identifiseres og etterleves av de virksomhetene som dette faller inn under. (Difi, 2019)

Veiledning fra Difi:

Difi har delt veiledningen sin for internkontroll (et styringssystem for informasjonssikkerhet) i tre deler.

Del 1 er for toppleder, og omhandler en oversikt og sjekkliste som forteller hva internkontroll er, og hva toppleder må gjøre.
Difi forteller at toppleder er ansvarlig for styring og kontroll på informasjonssikkerhetsområdet. Videre bør virksomheten kartlagt status i forhold til pålagt og anbefalt innhold i internkontrollarbeid. Fundamentet i internkontrollen ligger i styrende dokumenter som er klare i hvilke

sikkerhetsaktiviteter som skal gjennomføres, og hvem som har ansvar for hva. Dette skal utgjøre en systematisk aktivitet fordelt blant ledere og ansatte i hele virksomheten. I henhold til figur 4 ovenfor, skal virksomheten identifisere, vurdere, håndtere og følge opp ulike risikoer i alt virksomheten foretar seg. Dette skal skje systematisk og jevnlig, ettersom risikobildet kan endre seg.

Det påpekes i veilederen at alle ledere må sette seg inn i internkontroll og informasjonssikkerhet, og det må kommuniseres klart og tydelig ut til andre ansatte om man skal ha et velfungerende system. Ledelsen skal gå foran som et godt eksempel.
(Difi, 2019)

Del 2 i veiledningen omhandler en grunnleggende innføring av internkontrollen, og beskriver aktivitetene i figur 4 detaljert. Veiledningen tar for seg formål, forankring og bruksområde, og det blir bevisstgjort krav og behov til internkontroll, i tillegg til at det beskrives sentrale aktiviteter i oppretting, gjennomføring og forbedring av en internkontroll. Veiledningen også er sterkt støttet til ISO 31000, i tillegg til ISO 27001.
(Difi, 2019)

Del 3 omhandler grunnleggende begreper, og forklarer betydningen av de tre begrepene informasjonssikkerhet, internkontroll, og risiko.

«Behandling av informasjon er både kjerneaktivitet og en viktig støtteaktivitet i alle virksomheter. Det er en sentral del av alle arbeidsoppgaver. Effektiv og pålitelig informasjonsbehandling er avgjørende for at virksomheter skal kunne nå sine mål. Det er da viktig at man kan stole på informasjonen, at den er tilgjengelig og at man følger lover og regler. Informasjonssikkerhet handler om å ivareta dette.»
(Difi, 2019)

«Risiko handler om mulige avvik fra våre mål. Noen sier mulige avvik fra ønskede resultater eller ønskede tilstander. Det er det samme. Risiko kobles oftest til uønskede hendelser som har uønskede konsekvenser. Det er disse konsekvensene som er avvik fra det vi ønsker. For virksomheter vil det si avvik fra mål.»
(Difi, 2019)

2.1.2 Norsk senter for informasjonssikring.

Hva er NorSIS - Norsk senter for informasjonssikring?

"NorSIS er et ressurssenter opprettet av Fornyings- og administrasjonsdepartementet for rådgiving innen informasjonssikkerhet for alle norske private og offentlige virksomheter. Fra 1.4.2013 ble NorSIS faglig overført til Justis- og beredskapsdepartementet" (https.norsis.no).

NorSIS skal opptre som en nøytral, uavhengig og ikke kommersiell informasjonssikkerhetsinstans, og ønsker å samarbeide og tilby ekspertise mot offentlige og private virksomheter for å gjennomføre informasjonssikkerhetstiltak. NorSIS skal også så langt som mulig imøtekomme innbyggernes behov, og alle samfunnsgrupper skal kunne dra nytte av tjenestene til instansen.

"NorSIS' kjernevirksomhet er kunnskapsformidling og utvikling av en digital sikkerhetskultur for å skape bevissthet, påvirke holdninger og å endre sikkerhetsatferd i målgruppen." (https.norsis.no).

Tjenester som tilbys av instansen er:

- Nyheter via nettstedet https.norsis.no
- Foredrag, konferanser, og workshops. Både fra eget og eksternt initiativ.
- Over 100 veiledninger om sikkerhetstiltak.
- Prosjektsamarbeid med aktive partnere.
- Bygge opp og drifte faglige referanse- og arbeidsgrupper.
- Bruker media for å rette fokus på viktighet av informasjonssikkerhet.
- Bidra i samfunnsdebatten.
- Kontakt med internasjonale nettverk, forskningsmiljø og utdanningsinstitusjoner.

Totalt kan man oppsummere NorSIS med fire hovedtjenester.

Slettmeg.no
En gratis tjeneste som gir råd og veiledning til folk som føler seg krenket på internett og om hvordan man kan fjerne krenkende innhold. Man kan også kontakte tjenesten via sidens kontaktskjema, telefon, og e-post.

Nettvett.no
Et nettsted der man finner råd, informasjon og veiledning om sikrere bruk av internett. Målgruppe for nettstedet er enkeltpersoner - barn og voksne, forbrukere, og små og mellomstore bedrifter. Siden 2015 ble nettstedet driftet i samarbeid med NSM, og Nkom (nasjonal kommunikasjonsmyndighet, og nasjonal sikkerhetsmyndighet).

Nasjonal sikkerhetsmåned
I oktober 2011 ble det satt i gang en årlig kampanje for å øke kompetanse og bevissthet mot informasjonssikkerhet for næringslivet, det offentlige, og media. Formålet er å bidra til et mer robust digitalt samfunn, gjennom å forebygge, bevisstgjøre og støtte offentlig arbeid mot datakriminalitet. Nasjonal sikkerhetsmåned skjer også i samarbeid med EUs sikkerhetsorganisasjon, The European Union Agency for Network and Information Security (ENISA).

Security divas
En konferanse og nasjonalt initiativ som har utviklet seg til å bli et viktig nettverk for kvinner som jobber med eller studerer informasjonssikkerhet. Målsetningen er å få flere kvinner inn i informasjonssikkerhet i arbeidslivet.

Hva sier NorSis/nettvett.no om styringssystem for informasjonssikkerhet?

Gjennom nettstedet nettvett.no så kommer NorSIS, og samarbeidsaktørene NSM og NKom med flere råd og veiledninger til hvordan virksomheter, bedrifter og kommuner kan innføre et system for informasjonssikkerhet. Det henvises også til den internasjonale sikkerhetsstandarden ISO/IEC 27002, men nettvett.no tilbyr veiledning til å lage en forenklet håndbok for informasjonssikkerhet til de som finner den internasjonale standarden for omfattende.

«Informasjonssikkerhet er et løpende og langsiktig arbeid, som ikke alltid gir raske resultater. Virksomhetens leder er ansvarlig for informasjonssikkerheten i bedriften. Prioriteringer og styring av risiko knyttet til informasjonssikkerhet må derfor forankres hos ledelsen og ledelsen må vise engasjement i arbeidet.» (Nettvett.no, 2019)

Videre sier Nettvett.no at øverste leder er ansvarlig for informasjonssikkerheten i en virksomhet, og arbeidet med policy og sikkerhetsrutiner starter der.

I forbindelse med å utarbeide et system for informasjonssikkerhet, kommer nettvett.no med noen holdepunkter for sikkerhetsledelse.

> *Sikkerhetsledelse dreier seg om å styre sikkerhetsarbeidet slik at det bidrar så effektivt som mulig til å nå virksomhetens mål. Mer konkret handler sikkerhetsledelse om å vurdere, beslutte og følge opp tiltak for å avdekke og redusere sikkerhetsrisikoen. Sikkerhetsledelse skal bidra til å beskytte bedriftens verdier, informasjon og evnen til å løse prioriterte oppgaver.* (Nettvett.no, 2019)

Som en forenklet gjennomgang, sier nettvett.no under sikkerhetsledelse at ledelsen må beslutte akseptabelt risikonivå i virksomheten, og under dette kommer også risikovurdering, og risikostyring. Neste steg er sikkerhetsdokumentasjon. Der kommer krav og retningslinjer til informasjonssikkerhet, og en sikkerhetspolicy vil kunne fungere som et øverste nivå og som en beskrivelse til hvorfor man trenger ulike tiltak.
Steg tre er opplæring og bevisstgjøring av ansatte. Ledelsen skal være rollemodeller. Mange ansatte kan utføre sikkerhetsrisiko uten å selv være klar over hva det er som skjer. Med riktig bevisstgjøring og opplæring minsker faren for slike hendelser.
Til slutt skal ledelsens eierskap følges opp ved at sikkerhet inngår i etablert ledelsesoppfølging. Slik får man rapportering og bevisstgjøring om status for viktig risiko.

En policy for informasjonssikkerhet vil vise ledelsens målsetninger og hensikter for jobben med informasjonssikkerhet.
Alle ansatte skal gjøres kjent med policyen, og den bør gi svar på hvorfor informasjonssikkerhet er viktig i virksomheten, målene for informasjonssikkerheten, og kunne gi føringer for mer detaljerte retningslinjer for informasjonssikkerhet i virksomheten. Policyen vil synliggjøre for mellomledere og andre ansatte at informasjonssikkerhet er et prioriteringspunkt, og det vil bli enklere å velge sikkerhetstiltak når det er satt langsiktige målsetninger for informasjonssikkerhetsarbeidet. Videre får man en markør for omverdenen at virksomheten tar sikkerheten alvorlig, og dette kan gi økt trygghet for kunder, og kunne brukes til å sette sikkerhetskrav til leverandører. (Nettvett.no, 2019)

I forkant av utarbeidelsen av en sikkerhetspolicy, sier Nettvett.no at det bør foreligge en risikovurdering av virksomheten der man må finne svar på hvilke trusler mot informasjonssikkerhet bedriften er utsatt for. Ut fra dette finner man ut hvilken beskyttelse som er nødvendig, og hva som er i samsvar med bedriftens verdier, og langsiktige forretningsmål.

Nettvett.no har ingen standardpolicy som passer for alle bedrifter, men de oppgir noen punkter som bør dekkes i en sikkerhetspolicy.

- Hvorfor er informasjonssikkerhet viktig?
  Informasjonssikkerhet bør være forankret i virksomhetens behov, forretningsmål og eksterne krav. Ved å beskrive disse behovene, finner man bedre grunner til å fokusere på informasjonssikkerhet, man kan enklere gjøre sikkerhetstiltak, og det blir lettere å engasjere mennesker i sikkerhetsarbeidet når man presenterer behovet ut ifra virksomhetens målsetninger og behov. (Nettvett.no, 2019)

- Langsiktige og teknologinøytrale mål for fremtidig satsning. Hva som skal beskyttes, og på hvilket nivå må fremkomme. Virksomhetens ambisjonsnivå i forhold til informasjonssikkerhet må også beskrives. (Nettvett.no, 2019)
- Prinsippene for informasjonssikkerhet må komme frem. Risikovurdering kan brukes for å påpeke tiltak og satsningsområder. Andre prinsipper for behandling av informasjon må komme frem på overordnet nivå, og til sist må hvordan man følger opp policyen beskrives, samt konsekvenser av å bryte den. (Nettvett.no, 2019)
- Ansvar og roller beskrives klart, minimumskrav er beskrivelse av ansvar til øverste leder og medarbeidere. Øverste leder er hovedansvarlig, og må godkjenne policyen. Ut ifra virksomhetens størrelse og behov, kan det opprettes heltids/deltids stilling som informasjonssikkerhetsansvarlig. (Nettvett.no, 2019)

Når en policy er på plass, sier nettvett.no at policyen må følges opp, den må gjøres kjent, og den må brukes. Periodevis bør den gås igjennom, og oppdateres ved behov. Alle ansatte og nyansatte skal gjøre seg kjent med, og følge policyen. Ved behov skal det forekomme opplæring slik at policyen blir fulgt.

Interne krav, eksterne krav, og risiko er i stadig endring, og krever jevnlig endring i informasjonssikkerhetspolicyen. Gjeldende krav og retningslinjer må hele tiden oppdateres og finnes tilgjengelig for alle ansatte. Revisjon kan skje periodevis, eller ved større endringer som krever endring. Til slutt krever virksomheten mer detaljerte retningslinjer for informasjonssikkerhet. Disse skal gjenspeile seg i innholdet i policyen, og sørge for helhetstenking i sikkerhetsarbeidet. (Nettvett.no, 2019)

Når virksomhetens krav, målsetninger og ambisjoner, sikkerhetsledelse, sikkerhetspolicy, og risikovurdering er utarbeidet, kan man gå i gang med mer et mer detaljert sikkerhetsregelverk. Summen av alt dette blir da virksomhetens ISMS (Information Security Management System), eller system for informasjonssikkerhet.
Disse detaljerte reglene/rutinene er utarbeidet av nettvett.no (NorSIS, NKom, og NSM) som en forenklet utgave av ISO 27002.

I grove trekk omhandler regelverket:

- Anskaffelse, der det omhandler bla. lisenser, kontrakter, og krav til sikkerhet i kontrakter, og deponeringsavtaler, og krav til systemer.
- Sikkerhetshendelser og brudd på sikkerhetsbestemmelsene. Omhandler varsling og rutiner for ansatte og ledere angående håndtering og oppfølginger på uregelmessigheter.
- Beredskap. Går ut på beredskapsplaner, ansvar og prosedyrer på håndtering av kritiske sikkerhetshendelser.
- Personellsikkerhet, oppdelt i organisering og holdninger og opplæring. Bevisstgjøring på ansatte, kontraktører og tredjepartsbrukere sitt ansvar og roller innenfor informasjonssikkerhet.
- Fysisk sikring. Hvordan forhindre adgang til, og forstyrrelser/skader på lokaler, datasystemer, og informasjon. Omhandler sikring mot naturkatastrofer, sikring av lokaler og utstyr, adgangskontroll, utstyrsavhending og skytjenester.
- Behandling av informasjon. Omhandler rutiner om lagring, utveksling, virksomhetskritisk, privat informasjon. Og bruk av internett, e-post, og skytjenester.

Personopplysningsloven (lov om behandling av personopplysninger) og sikkerhetsloven (lov om nasjonal sikkerhet) kommer også under dette punkt.

- Teknisk sikkerhet. Sikre konfidensialitet, integritet, og tilgjengelighet til alle IKT-leveranser til virksomheten. Omhandler tilgangskontroll (fysisk og i systemer), og endringskontroll i systemer. Driftssikkerhet skal utredes med tanke på blant annet driftsprosedyrer, sikring av tilgjengelighet for et system, håndtering av ondsinnet programvare, sikkerhetskopiering og oppgradering av programvare.
  Nettverkssikkerhet skal utdypes med punkter som eksterne oppkoblinger, trådløse nettverk, brannmur og nettverksadskillelse.
  (Nettvett.no, 2019)

2.1.3 Datatilsynet

Hva er Datatilsynet?

Datatilsynet er et uavhengig forvaltningsorgan, og både tilsyn og et ombud, som har i oppgave å føre kontroll med at personvernregelverket etterleves, og å medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan tilknyttes dem.

Datatilsynet skal, ifølge deres hjemmeside:

I. Føre kontroll med at personvernregelverket etterleves, og at feil og mangler ved behandling av personopplysninger blir rettet. Dette gjøres blant annet gjennom tilsyn og saksbehandling
II. holde oss orientert om nasjonal og internasjonal utvikling når det gjelder behandling av personopplysninger.
   - *Ny personopplysningslov i 2018, og den består av nasjonale regler, og EU's personvernforordning GDPR – General Data Protection Regulation.*
III. identifisere farer for personvernet, og gi råd for hvordan farene kan unngås eller begrenses.
IV. være høringsinstans i saker som berører personvern
V. delta i råd og utvalg
VI. bistå bransjeorganisasjoner med å gi råd og utarbeide adferdsnormer for å sikre personopplysninger i virksomhetene
VII. stimulere til opprettelse av *personvernombud* og bygge kompetanse hos ombudene
VIII. ha en ombudsrolle overfor publikum, og gi råd og informasjon. Dette gjøres blant annet ved hjelp av våre nettsider, blogg og veiledere.
IX. få viktige saker på dagsorden i media og bidra til samfunnsdebatt om personvern
(Datatilsynet, 2019)

Personvernforordningen er lik for alle EU/EØS-land, og virksomheter i slike land må derfor stort sett følge samme lovgivning som norske virksomheter.
Personopplysningsloven, som vi har i Norge, gjelder når virksomheter i landet delvis eller helt foretar elektronisk (automatisk) behandling av personopplysninger, og i tillegg ved ikke-automatisk behandling av personopplysninger der opplysningene skal inngå i et strukturert register.
Personopplysningsloven gjelder **ikke** behandling av personopplysninger, som utføres av fysiske personer til rent personlig eller familiært bruk, eller som utføres av myndigheter i forbindelse med straffbare forhold, eller for utelukkende journalistiske, akademiske, eller kunstneriske og litterære formål.
(Datatilsynet, 2019)

Hva sier Datatilsynet om styringssystem for informasjonssikkerhet?

«Gjennom å ha god internkontroll og god informasjonssikkerhet sikrer virksomheten at den behandler personopplysninger lovlig, sikkert og forsvarlig.»
(Datatilsynet, 2019)

Videre sier Datatilsynet at personvernforordningen krever egnede tiltak hos behandlingsansvarlig, både tekniske og organisatoriske, for å sikre og påvise at personopplysninger behandles i henhold til regelverket. Ved behov skal tiltakene man har valgt endres og oppdateres, og dette kan oppsummeres som rutiner for oppfyllelse pliktene til virksomheten, og rettighetene til de registrerte, samt rutiner og tekniske tiltak for informasjonssikkerhet. Det forventes en systematisk tilnærming fra bedrifter mot etterlevelsen av regelverket, og for å imøtekomme dette må man sette seg inn i relevante bestemmelser for egen virksomhet, både mot ledelse og ansatte, og virksomhetene må opprette en internkontroll (ISMS/styringssystem for informasjonssikkerhet).

Datatilsynet foreslår at internkontrollen består av tre elementer.

1. Styrende elementer. Hovedsakelig ledelsens beslutninger og føringer for internkontroll.
2. Gjennomførende elementer. Hovedsakelig ansattes rutiner mot den enkeltes arbeidssituasjon.
3. Kontrollerende elementer. Fanger opp avvik fra systemet, og gjennomføre periodiske gjennomganger.
   (Datatilsynet, 2018)

Virksomheten må sikre forsvarlig behandling av personopplysninger ved å ivareta den registrertes rettigheter og friheter, samtidig som man etterlever virksomhetens mål ved behandlingen. Etter artikkel 24 i personvernforordningen, har man en forholdsmessighet mot behandlingens art, omfang, formål og sammenheng, og risiko for den registrertes rettigheter og frihet der virksomheten til slutt skal gjennomføre egnede tiltak. Internkontrollen skal derfor være både ledelsens verktøy for å ivareta ansvar og plikter i etterlevelsen av regelverket, og de ansattes verktøy for å kunne gjøre sine oppgaver forsvarlig og sikkert.
Datatilsynet presiserer at det ikke er verken nødvendig eller hensiktsmessig å opprette egen internkontroll for personvernregelverket dersom det finnes internkontroll for andre regelverk eller andre formål. Da er det bedre å inkludere kravene etter personregelverket i en utvidelse av det eksisterende systemet.

For å håndtere at personopplysninger og annen data blir ivaretatt tilfredsstillende, sier datatilsynet at virksomheten identifisere hvilke personopplysninger den har, og deretter gjennomføre en risikovurdering for å undersøke om de eksisterende sikkerhetstiltakene er gode nok. Hvis det avdekkes manglende tiltak i vurderingen, må nye tiltak vurderes igangsatt for å ivareta tilfredsstillende sikkerhetsnivå. Det må utføres og utarbeides kontrollrutiner jevnlig for å etterfølge at tiltakene blir utført, og at de virker etter hensikten. (Datatilsynet, 2019)

Tiltakene nevnt ovenfor, med tilhørende rutiner, vil da bli virksomhetens styringssystem for informasjonssikkerhet.

Hvordan gjennomføre og etablere internkontroll i praksis i forhold til Datatilsynets veiledning?

- Skaff kunnskap.
  Virksomheten er selv ansvarlig for å skaffe et minimum av kunnskap om personopplysningsloven, personvernforordningen, og andre lover og regler som måtte gjelde dem.
- Ledelsen har ansvaret.
  Ledelsen er ansvarlig for å opprette internkontroll, og ansvarsforhold og rutiner tilknyttet denne. Dette gjøres i forhold til akseptabel risiko for rettigheter og friheter.
- Formål med internkontrollen. Datatilsynet lister opp ivaretakelse av registrertes rettigheter, og kvalitetssikring for at offentlige krav følges. De nevner bedre informasjonssikkerhet/-kvalitet, og effektiviseringsgevinst. Videre nevnes det oppdagelser og håndtering av avvik som fordel, og redusert sjanse for feil grunnet manglende oppfølging av offentlig regelverk. Til slutt får man fordel av rutiner og instrukser ved at ansatte arbeider i samsvar med virksomhetens mål og policy.
  (Datatilsynet, 2019)

2.1.4 Nasjonal sikkerhetsmyndighet – NSM

Hva er NSM?

Norges ekspertorgan for informasjons- og objektsikkerhet, samt det nasjonale fagmiljøet for IKT-sikkerhet. NSM er også nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. NSM leverer en rekke tjenester innen ulike arbeidsområder og fagmiljø, og tjenestene kan grovt grupperes som IKT-sikkerhet, personellsikkerhet, og fysisk sikkerhet. De fører også tilsyn med virksomheter etter lov om forebyggende sikkerhetstjeneste.
Den operative delen av NSM som håndterer IKT-sikkerhetshendelser heter NorCert. (Computer Emergency Response Team)
(Nasjonal Sikkerhetsmyndighet, 2019)

Hva sier NSM om styringssystem for informasjonssikkerhet?

NSM har en publikasjon som heter «veileder i sikkerhetsstyring» fra 10.03.2015.
Denne veilederen er beregnet på virksomheter som trenger å etablere og videreutvikle et styringssystem for ikke bare informasjonssikkerhet, men sikkerhet generelt, og den støtter seg til ISO/IEC 2700x-serien, og NS 583x-serien.
Veilederen retter seg mot ansatte, for eksempel virksomhetsleder, sikkerhetsleder eller andre ansatte som har i oppgave å etablere og videreutvikle et styringssystem for sikkerhet.

NSM sin veileder sier at et helhetlig styringssystem for sikkerhet minimum bør inneholde disse punktene:

- God forankring hos ledelsen.
  Skal man ha et fungerende system må ledelsen følge opp og etterspørre resultater, og ledelsen må gå foran for å skape et miljø som gjør at medarbeidere tør å rapportere avvik, svakheter og sårbarheter. I tillegg til å ha ansvar i egen virksomhet, har ledelsen også ansvar for at sikkerheten hos underliggende virksomheter, og hos leverandører er ivaretatt.

- Ha tilfredsstillende sikkerhetsdokumentasjon. Dette går på forskjellige punkter:
    - Graden av forankring hos ledelsen i styrende sikkerhetsdokumentasjon.
    - Oversikt og tilgjengelighet for bedriftens sikkerhetsdokumentasjon.
    - Graden av dokumentasjon for sikringsrisikovurderingene.
    - Foreligge oppdatert instruks for å ivareta sikkerheten.
    - Foreligge oppdaterte instrukser innen relevante fagområder.
    - Instrukser for leders årlige evaluering, internrevisjoner, sikringsrisikovurderinger, beredskapssituasjoner, og sikkerhetstruende hendelser. I tillegg skal det foreligge tilfredsstillende dokumentasjon av dette.
    - Ansvarsforhold for oppdatering av sikkerhetsdokumenter.
    - Kjentgjøring av sikkerhetsdokumentasjonen rundt i virksomheten.
- Ha tydelig ansvarsfordeling og organisering.
  Enhver virksomhet organiserer sikkerhetsarbeidet selv, men en måte å gjøre det på er å å skille mellom strategiske (kravsettende og kontrollerende oppgaver), og utøvende (mer driftsrelaterte oppgaver) sikkerhetsfunksjoner. Alle ledere og ansatte skal i tillegg ha sine egne utøvende sikkerhetsoppgaver som et ledd i deres daglige arbeid.
- Ha konkrete målsetninger innen sikkerhetsarbeidet i virksomheten.
- Ha en strukturert metode for arbeidet med sikkerhetsstyring, for eksempel et styringshjul. Poenget med et slikt styringshjul er å ta høyde for de elementene hver enkelt virksomhet trenger for å få til en riktig prosess. Av hjulet skal det fremkomme en kontinuerlig prosess med regelmessig forbedring av sikkerhetsarbeidet. Sikkerhetshjulet som presenteres i NSM sin veiledning inneholder fem punkter:
    - Planlegging. Hvilke eksterne krav til sikkerhet gjelder? Status for sikkerhetstilstanden i virksomheten? Virksomhetens målsetninger innen sikkerhet?
    - Sikringsrisikovurdering. Hva er de mest kritiske verdiene? Hva er de største truslene mot verdiene? Hva er de største sårbarhetene til verdiene?
    - Hjulet må inneholde hvordan man identifiserer, implementerer, beslutter, og prioriterer forebyggende tiltak.
    - Oppfølging og kontroll. Hva skal revideres, og av hvem? Hvordan man følger opp intern avvikshåndtering, hvordan følge opp avvik under tilsyn, og hvordan følge opp sikkerhetsarbeidet i underlagte virksomheter.
    - Rapportering. Sikre at relevant informasjon rapporteres til riktig funksjon på riktig tidspunkt, sikre kontinuerlig rapportering, sikre at sluttårsrapportering blir innspill til planleggingsfase, og sikre at resultater fra ledelsens evalueringer danner grunnlag for nye mål innen sikkerhet.
      (NSM, 2019)

Som et ledd i sin virksomhet som nasjonalt sikkerhetsorgan har NSM årlige risikovurderinger for virksomheter i Norge sett under ett. Ut ifra rapporten Risiko 2019 (lansert 20.03.19), som er NSMs årlige tilstandsrapport for norske virksomheter, presenterer NSM seks faktorer som er spesielt viktig for å vurdere total risiko som virksomheter bør forholde seg til. Disse faktorene er:

1. **Ufullstendig risikobilde**. Man har ikke oversikt over ulike typer risiko, og områder med høy sikkerhetsrisiko, og får heller ikke optimalisert sikkerhetstiltak når man ikke vet hvilke tiltak som er best.

2. **Manglende sammenheng mellom tiltak**. Sikkerheten er avhengig av organisasjonens sikkerhet som helhet, og er dermed ikke sterkere enn sitt svakeste ledd.
3. **Svakt personellsikkerhetsarbeid.** En person på innsiden av virksomheten kan undergrave sikkerhetstiltak i både IKT-nettverk, og fysiske sikringer. Innsidere blir vanskeligere å oppdage ved svakt personellsikkerhetsarbeid.
4. **Økende digitalisering uten at løsningene bedres tilsvarende.** Vi opplever et økende tempo når det gjelder å digitalisere funksjoner som i dag ikke er heldigitaliserte, og hvis det ikke benyttes tilsvarende tempo på sikringstiltak, kan store verdier gå tapt.
5. **Dårlig oversikt over hva som bør sikres.** Med ny sikkerhetslov skal det utpekes flere skjermingsverdige objekter og infrastruktur, det vil si at tilgang til detaljert informasjon skal bare gis etter særskilt samtykke. Dette nevnes som en potensiell utfordring for norske myndigheter.
6. **Risikoreduserende tiltak både på offentlig og privat side.** Ettersom næringslivet leverer tjenester til det offentlige, trenger man sikkerhetstiltak på plass i begge sektorer, både privat og offentlig.
   (NSM, 2019)

2.2 PDCA metoden

PDCA sirkel eller Deminghjulet presenterer en fire-trinns iterativ tilnærming som brukes for kontroll og kontinuerlig forbedring av prosesser, tjenester eller produkter.
PDCA er en engelsk forkortelse og oppdelt, slik vist i Figur 1, i fire faser: Plan, Do, Check og Act som gjentas kontinuerlig. På norsk blir det ofte oversatt til Planlegg, Utfør, Kontroller og Korriger[1].

Figur 2: Deminghjulet

PDCA sirkel ble utviklet av Edward Demning som anses av mange som far til moderne kvalitetsstyring (Wikipedia, 2019). PDCA-metoden har vært mest brukt prosess- og styringssystemforbedringsmetode siden 1950 og grunnlag for nesten alle ISO-standarder (BSI, u.d.) Dette konseptet er et driftsprinsipp i ISO 9001:2015 som er verdens mest populære kvalitetsstyringsstandard (BSI, 2016). ISO 27001:2005 brukte PDCA sirkel på alle prosessene i ISMS (Wikipedia, 2019).

Et grunnleggende prinsipp for PDCA metoden baserer seg på iterative prosesser - for å komme nærmere et ønsket resultat må følgende trinn gjentas kontinuerlig:

- Plan (Planlegg). I denne fasen formuleres et tydelig problem eller mål og prosesser som kreves for å løse problemet og levere de ønskede resultater (Wikipedia, 2019).
- Do (Utfør). Planen fra forrige fasen blir vedtatt og endringer implementeres. Det foregår innsamling av data for å måle effektiviteten av endringer (Wikipedia, 2019).
- Check (Kontroller). Dataene og resultatene som er samlet i Do-fasen evalueres og sammenlignes med forventede resultater for å kartlegge likheter og forskjeller. Det evalueres planen som er vedtatt før for å se om det var gjennomført endringer underveis, hvilke endringer som fungerer bedre enn andre og om endringene kan forbedres (Wikipedia, 2019).

[1] Oversettelsen er hentet fra IINI2009 Informasjonssikkerhet og produktforvaltning

- Act (Korriger). Denne fasen kan også kalles «Adjust» på engelsk. Innsamlede dataene fra Do og Check faser brukes til å avdekke problemer med prosessen: avvik, ineffektivitet, muligheter for forbedring og andre problemer som resulterer i utfall som er mindre enn optimalt. Årsaken til problemet blir undersøkt, funnet og eliminert ved å korrigere prosessen. Avslutningsvis får prosessen forbedret instruksjoner, standarder eller mål. Do-fasen i nye syklusen bør ikke skape samme problemer ved effektive handlinger som er vedtatt i Act-fasen (Wikipedia, 2019).

I artikkelen *«Quality improvement methodologies–PDCA cycle, RADAR matrix, DMAIC and DFSS»* som introduserer og sammenligner ulike metoder for kontinuerlig kvalitetsforbedring av produkter, tjenester og prosesser i organisasjonen står det følgende om PDCA metoden: PDCA hjulet er mer enn bare metode – dette er et konsept av kontinuerlig forbedringsprosesser innebygd i organisasjonens kultur. Det viktigste aspektet av PDCA-prinsippet ligger i Act-fasen – når prosjekt er fulført og syklusen starter på nytt for gjennomføring av ytterligere forbedringer (Sokovic, Pavletic, & Pipan, 2010)

2.3 Informasjonssikkerhet

2.3.1 Informasjon og informasjonssikkerhet

Det samles inn og lagres enorme mengder av informasjon hver dag. Som eksempel henvises til artikkelen «Så mye lagret om deg» i nettavisen Tek.no (Tek.no, 2012). Den beretter om hvor mye informasjon som mobiloperatørene samler og lagrer om sine kunder*: «Da vi ba Telenor sende oss alt selskapet hadde av informasjon om én av våre journalister, skulle vi til slutt ende opp med en konvolutt med **150 tettskrevne A4-sider**. Her kunne vi følge de forrige 90 dagene av livet hans i detalj, fra han sto opp om morgenen til han la seg om kvelden»* (Tek.no, 2012).

Informasjon kan ha ulike betydninger avhengig av bruksområder. Det kan være bearbeidet talldata, noe som formidles mellom mennesker og kan presenteres i ulike former som digital, analog, fysisk eller logisk. ISO 27000 og ISO 27002 standardene utviklet mer spesifikke og oppfattende definisjoner av informasjon som eies av organisasjoner.

NS-EN ISO/IEC 27000:2017 definerer informasjon som:

> *«Informasjon er et aktivum som i likhet med andre viktige virksomhetsaktiva er avgjørende for en organisasjonsvirksomhet, og må derfor beskyttes på forsvarlig måte. Informasjon kan lagres i mange ulike formater: digitalt (datafiler som lages på optiske eller elektroniske medier), i materiell form (på papir) eller som kunnskaper til ansatte. Informasjons kan overføres på ulike måter: med kurer, elektronisk eller med verbal kommunikasjon. Uansett hvilken form informasjon har og på hvilken måte den overføres, trenger den å være beskyttet»* (Standard Norge, 2017).

NS-EN ISO/IEC 27002:2017 definerer informasjon som

> *«I vår sammenkoblede verden er informasjon og tilknyttede prosesser, systemer, nettverk og personell som er involvert i driften, håndtering, beskyttelsen av den, aktiva som, i likhet med andre viktige driftsmidler, er verdifulle for en organisasjonsvirksomhet, or derfor har krav på og trenger beskyttelse mot ulike risikoer»* (Standard Norge, 2017).

Informasjonssikkerhet er sikring av opplysninger ved å bruke prinsippene om konfidensialitet, integritet og tilgjengelighet (Datatilsynet, 2018).

Informasjonssikkerhet omfatter beskyttelse av:

- Konfidensialitet – at informasjonen ikke blir kjent for uvedkommende
- Integritet – at informasjonen ikke blir endret utilsiktet eller av uvedkommende
- Tilgjengelighet – at informasjonen er tilgjengelig for autoriserte ved behov
- Robusthet – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser (Datatilsynet, 2018)

NS-EN ISO/IEC 27001:2017 gir definisjon for et ledelsessystem for informasjonssikkerhet: *«Et ledelsessystem for informasjonssikkerhet bevarer konfidensialiteten, integriteten og tilgjengeligheten til informasjon ved å benytte en risikostyringsprosess, og dette gir tillit hos interesseparter ved at risikoer er tilstrekkelig håndtert. Det er forventet at ledelsessystemet for informasjonssikkerhet skaleres i samsvar med organisasjonens behov»* (Standard Norge, 2017)

*«Forvaltningsorgan (ethvert organ for stat og kommune, dvs. det vi kaller **offentlige virksomheter**) er gjennom eForvaltningsforskriftens § 15 **pålagt å ha** internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. eForvaltningsforskriften § 15 stiller krav om at **internkontrollen på informasjonssikkerhetsområdet skal basere seg på anerkjente standarder for styringssystem for informasjonssikkerhet**»* (Difi, u.d.)

Ved å etablere informasjonssikkerhet med egnet sikkerhetstiltak som fysiske og logiske tiltak, policyer, prosedyrer, rutiner og opplæring reduserer en disse risikoene og det reduseres innvirkninger på organisasjons aktiva. Det er viktig å overvåke, måle og forbedre sikkerhetstiltakene for å komme nærmest mulig organisasjonens sikkerhetsmål (Standard Norge, 2017). «I en mer generell forstand forsikrer dessuten en virkningsfull informasjonssikkerhet ledelsen og andre interessenter om at organisasjonens aktiva er rimelig trygge og beskyttet mot skade, og den åpner dermed for nye muligheter for virksomhet» (Standard Norge, 2017).

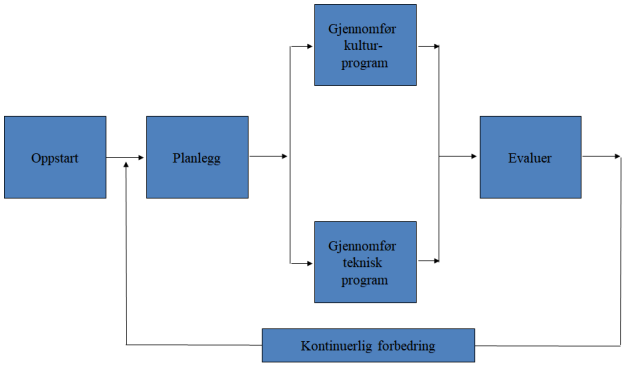
Digitalisering og digital transformasjon står på dagsorden i både private og offentlige virksomheter og baserer seg på bruk av digital teknologi til blant annet forbedring av tjenester eller oppretting av nye tjenester som gir økt verdi og konkurransefortrinn. Dette medfører et stadig større behov for høy grad av digital sikkerhet og personvern. Regjeringen vil bidra til å gjøre digitalt Norge sikrere. «Det arbeides for at IKT-sikkerhet skal styrkes i hele samfunnet for å møte utfordringene på området» (Regjeringen.no, 2019). «*Den nye sikkerhetsloven som trådte i kraft den 1. januar 2019 er modernisert og tilpasset en ny tid. Loven omhandler personellsikkerhet, infrastruktur - og objektsikkerhet i tillegg til IKT-sikkerhet. Den inneholder lovgivning som både angår de menneskelige, teknologiske og organisatoriske. En bakgrunn for nye lov er at statlige funksjoner er mer avhengige av støtte fra den private aktører*» sier statssekretær Toril Charlotte Ulleberg Reynolds på Sikkerhetskonferansen i Oslo i 2019 (NSM, 2019).

> «*Den nye sikkerhetsloven som trådte i kraft 1. januar 2019, gjelder spesielt datasikkerhet for fylkeskommunale, kommunale og statlige organer. De skjerpede kravene til IKT-objekter er basert på ISO-standarder. Nasjonal sikkerhetsmyndighet har utarbeidet et sett med prinsipper og tiltak som skal hjelpe statlige og kommunale organer med å oppfylle kravene i den nye sikkerhetsloven. Disse er basert på ISO 27000-serien som kom ut allerede i 2005 (og har blitt revidert flere ganger)*» (Standard Norge, 2019).

NSM opplyser at statlige, kommunale og fylkeskommunale virksomheter ved utsetting av tjenester skal kreve at leverandøren har et etablert styringssystem for informasjonssikkerhet og sertifisering i henhold til internasjonale standarder, for eksempel **ISO/IEC 27001:2017**. (Standard Norge, 2019).

2.3.2 Modell for innføring av et styringssystem for informasjonssikkerhet

I faget *IINI2009 Informasjonssikkerhet og produktforvaltning 2018* ved NTNU ble det presentert en modell for innføring av styringssystem for informasjonssikkerhet (ISMS). *Figur 3* viser seks sentrale faser for innføring av ISMS i en organisasjon.



Figur 3: Modell for innføring av ISMS. Figuren er hentet fra faget IINI2009 - Informasjonssikkerhet og produktforvaltning 2018

Denne modellen anbefaler at organisasjonens sikkerhetsarbeid planlegges, etableres, innføres og styres etter PDCA metode eller Deminghjulet for kontinuerlig forbedring av prosesser.

Videre skal det forklares kort seks faser i modellen for ISMS med utgangspunkt i faget IINI2009 - Informasjonssikkerhet og produktforvaltning 2018:

1. *Oppstart*
   Denne fasen inngår i Plan (Planlegg) fase i Deminghjulet og består av følgende hovedaktiviteter:
   - Lover og regler
   - Forankring
   - Aktører

   Krav til at organisasjon skal ha en sikkerhetsorganisasjon med risikovurdering, sikkerhetsrutiner og avvikshåndtering kan komme fra kunder, partnere eller lovpålagte nasjonale og internasjonale forskrifter. «Alle virksomheter bør ha en egeninteresse i et systematisk arbeid med informasjonssikkerhet. Offentlige virksomheter (forvaltningsorgan iht. forvaltningslovens § 1) er også pålagt dette gjennom ulikt regelverk» (Difi, u.d.).

   Innføring av ISMS starter med forankring av sikkerhetsarbeid i ledelsen som formulerer mål og strategi for arbeidet og overordnet sikkerhetspolicy for organisasjonen som skal kommuniseres og forankres i alle ansatte. Hensikten er å fortelle hvilke resultater ledelsen forventer av sikkerhetsarbeid i organisasjonen (Hjertø & Klefstad, Informasjonssikkerhetsstyring, 2018). Ledelsen har ansvar for at styringssystem for informasjonssikkerhet forvaltes i henhold til gjeldende og relevante avtaler, lover og forskrifter. Ledelsen skal definere og tilordne ansvar for informasjonssikkerhet i organisasjonen, for eksempel utpeke sikkerhetsleder. Ved oppbygging og innføring av ISMS kan det oppstå behov for å leie inn eksterne konsulenter som kan gi råd om hvordan ISMS kan etableres og implementeres og som har god innsikt i ISO 27000 serien. Ledelsen skal vurdere og ta beslutning om de trenger støtte fra en ekstern konsulentgruppe, skal det

utpekes interne aktører som har innblikk i organisasjonens eksisterende sikkerhetsrutiner eller de skal danne en kombinert gruppe for innføring av ISMS (Hjertø & Klefstad, Informasjonssikkerhetsstyring, 2018).

2. *Planlegg*
   Denne fasen befinner seg i Plan (Planlegg) fase i Deminghjulet. Ledelsen skal skaffe seg oversikt over eksisterende sikkerhetsrutiner i organisasjonen og dokumentere retningslinjene og måten folk jobber på for å kartlegge gapet mellom status og det nivået ledelsen ønsker å oppnå. Kartlegging av aktuelle trusler for organisasjonen og risikoanalyse er viktige hjelpemidler i dette arbeidet (Hjertø & Klefstad, Informasjonssikkerhetsstyring, 2018). For risikoanalysen kan organisasjon ta i bruk retningslinjer for informasjonssikkerhetsrisikostyring som er dokumentert i standard ISO/IEC 27005.
3. *Gjennomfør teknisk program*
   Teknisk program tilhører Do (Utfør) fase.
   ISO 27002 standard gir anbefalinger for hvordan å få på plass alt krav, retningslinjer og prosedyrer som skal gjelde for et velfungerende ISMS. Dette innebærer beredskapsplaner, drift og vedlikeholdsrutiner, krypteringsteknikker, fysiske sikringstiltak og driftsmiljø (Hjertø & Klefstad, Informasjonssikkerhetsstyring, 2018)
4. *Gjennomfør kulturprogram*
   Denne fasen tilhører også den andre fase Do (Ufør) i Deminghjulet. Informasjonssikring er 20% teknologi og 80% holdninger. Hensikten med kulturprogram er å forankre ISMS i alle ansatte, øke bevissthet angående sikkerhet, engasjere alle i arbeide med informasjonssikkerhet og sikre at alle har eierskap til ISMS prosessene. Arbeidet med kulturellprogram er utfordrende og består i å endre holdninger ved hjelp av opplæring, informasjon og medvirkning (Hjertø & Klefstad, Informasjonssikkerhetsstyring, 2018).
5. *Evaluer*
   Denne fasen hører hjemme i den tredje fasen Check (Kontroller) i Deminghjulet. Et ISMS som alle andre prosesser og aktiviteter skal kontinuerlig måles og evalueres. Evalueringer kan grupperes i interne evalueringer og eksterne evalueringer. Interne evalueringer gjennomføres av organisasjonen og inkluderer ledelsesgjennomgang, rutinemessig oppfølging av praksis og oppfølging av hendelser. Eksterne evalueringer gjennomføres av personer utenfor organisasjonen og kan utføres i forbindelse med sertifisering, overvåkende ekstern evaluering eller konsulterende ekstern evaluering. (Hjertø & Klefstad, Informasjonssikkerhetsstyring, 2018).
6. *Kontinuerlig forbedring*
   Resultatene fra evalueringsfase er input i denne fasen og skal brukes til å svare på spørsmålet *«hva som kan bli bedre».* Denne fasen hører hjemme i den fjerde og siste fasen Act (Korriger) i Demingshjulet. «*Kontinuerlig forbedring i planen vår finner vi ved fullført løp der vi går tilbake til start. Men vi starter sannsynligvis ikke hele det store ISMS prosjektet på nytt, nå har vi jo et solid grunnlag. Nå er tiden kommet til de små og målrettede forbedringene. I prinsippet gjennomfører vi imidlertid den samme syklusen: Vi planlegger nye tiltak, vi gjennomfører dem og vi måler hvor godt de fungerer, og så bruker vi resultatet til å starte på nytt, osv. osv.*» (Hjertø & Klefstad, Informasjonssikkerhetsstyring, 2018, s. 21)

2.4 ISO 27001

2.4.1 Bakgrunn til ISO 27001 og ISO 27002

«En standard er et dokument som beskriver krav, spesifikasjoner, retningslinjer eller egenskaper som skal brukes konsekvent for å sikre at materialer, produkter, prosesser og tjenester er forsvarlige og tilpasset sitt bruk» (NTNU, u.d.).

I 1995 publiserte British Standard Institute (BSI) en standard under betegnelsen *BS7799 – Code of Practice for information security management* som bestod av to deler (Sjølstad, Høie, Gulbrandsen, & Daler, 2010):

Del 1 (BS 7799-1): Code of Practice for information security management som er nå ISO/IEC 27002:2017.

NS-EN ISO/IEC 27002:2017 er den gyldige norske versjonen (Standard Norge, 2017).

Denne standarden gir retningslinjer og generelle prinsipper for hvordan opprette, iverksette, vedlikeholde og forbedre administrasjon av informasjonssikkerhet i en bedrift. Sikkerhetsmålene og sikkerhetstiltakene som er beskrevet i standarden kan brukes som anbefalinger til bruk for dem som er ansvarlige for å lede og styre sikkerhetsarbeidet i en virksomhet. Standarden var vedtatt av ISO som ISO/IEC 17799 i år 2000. I 2005 ble standarden revidert på nytt og inkludert i ISO 2000-serien i 2007 som ISO/IEC 27002:2005 (Wikipedia, 2019). NS-ISO/IEC 27002:2013 er tilbaketrukket og erstattet med NS-EN ISO/IEC 27002:2017 (Standard Norge, 2017).

Del 2 (BS 7799-2): Specification for Information Security Management Systems (som er nå ISO/IEC 27001:2017).

NS-EN ISO/IEC 27001:2017 er den gyldige norske versjonen (Standard Norge, 2017)

I NS-EN ISO/IEC 27001:2017 står det følgende om hovedformålet til dokumentet: *«Denne internasjonale standarden spesifiserer kravene til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet innenfor konteksten til en organisasjon»* (Standard Norge, 2017, s. 5).

2.4.2 Versjoner av ISO 27001

2002 versjonen av BS 7799-2 introduserte PDCA prinsippet og med dette tilpasset standarden med kvalitetsstandarden ISO 9000. BS 7799-2 ble vedtatt av ISO som ISO 27001 i 2005 (Wikipedia, 2018). Standarder er levende dokumenter og det kommer nye versjoner eller korrigeringer. ISO/IEC 27001:2005 er tilbaketrukket og erstattet med ISO/IEC 27001:2013 som er videre erstattet med BS EN ISO/IEC 27001:2017 (BSI, 2019). Standard.no opplyser at norske versjonen NS-ISO/IEC 27001:2013 er også tilbaketrukket or erstattet med NS-EN ISO/IEC 27001:2017 (Standard Norge, 2017) som er oversatt til norsk språk.

2.4.3 Endringer i ISO 27001:2017

Endringer som skiller ISO/IEC 27001:2013 fra ISO/IEC 27001:2017 er beskrevet i *Technical Corrigendum 1* som er publisert 2014-09-15 (ISO, 2014) *og Technical Corrigendum 2* som er publisert *2015-12-01* (ISO, 2015). *Technical Corrigendum 1* sier at informasjon må betraktes som aktiva og inkluderes i beholdningen *(Subclause A.8.1.1 Annex A). Technical Corrigendum 2* gjennomførte oppbygging av *Subclause 6.1.3* fra setning til punktliste for å tiltrekke oppmerksomhet og legge vekt på innholdet. Disse endringer er innført i NS-EN ISO/IEC 27001:2017.

> *«You may be aware that a new version of the ISMS standard has been published – BS EN ISO/IEC 27001:2017. Please be aware that the ISO version of the standard is not affected and*

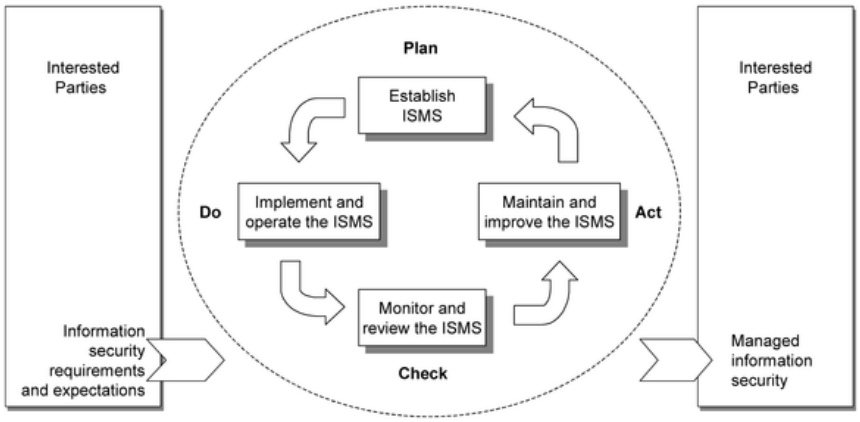
the changes do not introduce any new requirements. The change has been introduced to indicate approval by CEN/CENELEC for the EN designation. The updated BS does however incorporate two previously issued Corrigenda/Amendments in Clause 6.1.3 and Annex A clause 8.1» (UKAS, 2017).

ISO 27001:2013 og ISO 27001:2017 er en teknisk oppdatering av versjon 27001:2005. I tillegg fikk den nyere versjon en høynivåstruktur som er felles for alle de siste styringssystem standardene. Dette muliggjør enklere integrasjon og kombinering ved implementering av mer enn et styringssystem i organisasjonen, for eksempel ved implementering sammen med ISO 9001:2015 (Ledelsessystemer for kvalitet) eller 14001:2015 (Ledelsessystemer for miljø) (BSI, 2013).

«Standard Norge endret for noen år siden navn på alle styringssystemstandardene, herunder ISO 27001, fra styringssystem til ledelsessystem» (Difi). I denne oppgaven er det brukt både ledelsessystem og styringssystem som anses å bety det samme.

2.4.4 Tilnærming til etablering, implementering, drift, kontroll, vedlikehold og forbedring av ISMS i ISO 27001:2005

ISO IEC 27001:2005 (en) i underpunktet «0.2 Prosess aproach» (ISO, 2005) beskriver tilnærming til etablering, implementering, drift, kontroll, vedlikehold og forbedring av ISMS ved hjelp av PDCA prinsippet.



Figur 4: PDCA-modell brukt i ISMS-prosesser. Fra ISO Online Browsing Platform. ISO/IEC 27001:2005(en), 2005 (https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en)

Denne figuren viser at etablering og forbedring av ISMS foregår som kontinuerlig arbeid som aldri går over og baserer seg på PDCA trinn:

Plan (etablere ISMS): Etablere ISMS-politikk, mål, prosesser og prosedyrer som er relevante for å håndtere risiko og forbedre informasjonssikkerhet for å levere de resultatene som er i samsvar med organisasjonens overordnede retningslinjer og mål (ISO, 2005).

Do (implementere ISMS): Implementere ISMS-politikk, mål, prosesser og prosedyrer utarbeidet i fasen «Plan» (ISO, 2005).

Check (kontrollere ISMS): Vurdere prosessytelse mot ISMS-politikk og mål som er vedtatt i etableringsfasen (ISO, 2005).

Act (vedlikeholde og forbedre ISMS): Ta korrigerende og forebyggende tiltak basert på resultatene av den interne ISMS-revisjonen og ledelsesvurderinger for å oppnå kontinuerlig forbedring av ISMS (ISO, 2005).

Krav og forventninger til et sikkerhetssystem (Information security requirements and expectations, *Figur 2*) utarbeides av interessenter i organisasjonen (Interested Parties, *Figur 2*) og gjennom utformet prosesser og tiltak (ISMS) produseres det en styrt informasjonssikkerhet (Managed information security, *Figur 2*) som oppfyller disse kravene og forventninger.

«All references to PDCA were removed in ISO 27001:2013. Its use in the context of ISO 27001 is no longer mandatory» (Wikipedia, 2019).

NS-EN ISO/IEC 27001:2017 inneholder ikke krav til bruk av PDCA metoden. Tilnærming til styring av informasjonssikkerhet krav beskrives i sikringstiltakene i Tillegg A: «Policyene for informasjonssikkerhet skal gjennomgås med planlagte intervaller. Dersom betydelige endringer skjer, skal det sikres at de fortsatt er egnet, tilstrekkelige og virkningsfulle» (Standard Norge, 2017, s. 13). «Organisasjonens tilnærming til styring av informasjonssikkerhet og implementeringen av denne (dvs. sikringsmål, sikringstiltak, policyer, prosesser, prosesser og prosedyrer for informasjonssikkerhet) skal gjennomgås uavhengig **med planlagte intervaller eller dersom betydelige endringer skjer.** Informasjonssystemer skal regelmessig gjennomgås for samsvar med organisasjonens policyer og standarder for informasjonssikkerhet. (Standard Norge, 2017, s. 24).

NS-EN ISO/IEC 27002:2017 gir anbefalinger for å oppnå informasjonssikkerhet ved å *«implementere et eget sett med sikringstiltak, inkludert policyer, prosesser prosedyrer, organisatoriske strukturer og programvare- maskinvarefunksjoner. Det er nødvendig å etablere, implementere, overvåke, gjennomgå og forbedre disse sikringstiltakene der det er nødvendig, for å sikre at organisasjonens spesifikke sikkerhets- og virksomhetsmål nås»* (Standard Norge, 2017, s. 7)

2.4.5 Utvikling av struktur i ISO 27001 versjoner 2005, 2013 og 2017

I *Tabell 1* presenteres innholdet i versjoner ISO 27001:2005 og ISO 27001:2017. For bedre sammenligning av versjoner er det brukt engelskspråklige versjoner av standarder siden ISO/IEC 27001:2005 ikke var oversatt til norsk språk.

ISO/IEC 27001/Edition 2005	NS-EN ISO 27001/Edition 2017(en)
Introduction	Introduction
Scope	Scope
Normative references	Normative references
Terms and definition	Terms and definition
Information security management system	Context of the organization
Management responsibility	Leadership
Internal ISM audits	Planning
Management review of the ISMS	Support
ISMS improvement	Operation
	Performance evaluation
	Improvement

Tabell 1: Innholdet i ISO/IEC 27001:2005(en) og ISO/IEC 27001:2017(en)

I *Tabell 2* presenteres innholdet i versjoner ISO 27001:20013 og ISO 27001:2017. For bedre sammenligning av versjoner er det brukt engelskspråklige versjoner av standarder siden ISO/IEC 27001:2013 ikke var oversatt til norsk språk.

ISO/IEC 27001/E	NS-EN
Introduction	0. Introduction
Scope	1. Scope
Normative references	2. Normative references

	Terms and definition	3. Terms and definition	
	Context of the organization	4. Context of the organization	
	Leadership	5. Leadership	
	Planning	6. Planning	
	Support	7. Support	
	Operation	8. Operation	
	Performance evaluation	9. Performance evaluation	
	Improvement	10. Improvement	

Tabell 2: Innholdet i ISO/IEC 27001:2013(en) og NS-EN ISO 27001:2017(en)

2.4.6 Hovedkravene i NS-EN ISO/IEC 27001:2017

I punkt (*Clause*) 1. Omfang (*Scope*) opplyser NS-EN ISO/IEC 27001:2017 at **det ikke er akseptabel å ekskludere kravene som er beskrevet i punkt 4 til 10 dersom en organisasjon vil påstå at den er i samsvar med standarden** (Standard Norge, 2017, s. 5). Videre presenteres det en kort oppsummering av hovedkravene i standarden NS-EN ISO/IEC 27001:2017 med referanser til *Clauses*:

- *Clause 4. Organisasjonens kontekst.* Det skal bestemmes forhold med interne og eksterne interessenter som påvirker organisasjonens evne til å oppnå ønskede resultater av sitt ledelsessystem for informasjonssikkerhet. Kravene fra interesseparter kan omfatte regulatoriske og juridiske forpliktelser. Det er viktig å bestemme omfanget til ledelsessystemet for informasjonssikkerhet. Etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet skal utføres i samsvar med kravene i denne standarden (Standard Norge, 2017, ss. 5, 6).
- *Clause 5. Lederskap.* Den øverste ledelsen er ansvarlig for etablering av ledelsessystem for informasjonssikkerhet, informasjonssikkerhetspolicy og skal sikre at policy, ansvar og myndighet for roller er tildelt og kommunisert i organisasjonen. Ledelsen skal fremme kontinuerlig forbedring og sikre nødvendige ressurser for dette (Standard Norge, 2017, s. 6).
- *Clause 6. Planlegging.* ISO 27001 er risikobasert standard som betyr at ved planlegging av ledelsessystem for informasjonssikkerhet skal organisasjon utføre risikovurdering og definere prosess for håndtering av informasjonssikkerhetsrisikoene. Den skal etablere tiltak for håndtering av resultater fra risikovurdering som skal implementeres i informasjonssikkerhet styringssystem og virkninger av disse tiltakene skal evalueres (Standard Norge, 2017, s. 7).
- *Clause 7. Støtte.* Organisasjonen skal forsørge at nødvendige ressurser for etablering, implementering, vedlikehold og kontinuerlig forbedring av ISMS er definert og til stede. Dette innebærer å kartlegge kompetansebehov for innføring av ISMS og sikre at personene som skal utføre arbeid har den kompetansen tilegnet gjennom passende opplæring, utdanning eller erfaring. Personene skal være bevisst på informasjonssikkerhetspolicyen og konsekvenser for å ikke oppfylle kravene som er beskrevet i policyen. Intern og ekstern kommunikasjon av informasjonssikkerhetspolicyen i organisasjonen skal fastlegges ved å definere hva som skal kommuniseres, når og hvem som skal kommunisere og de prosessene som kommunikasjon skal foretas via. Organisasjons ledelsessystem for informasjonssikkerhet skal inneholde dokumentasjons som skal opprettes, håndteres, oppdateres og styres i henhold med denne standarden (Standard Norge, 2017, s. 9).
- *Clause 8. Drift.* Organisasjonen skal planlegge, implementere og styre prosessene for å oppfylle informasjonssikkerhetskrav og implementere tiltak for å håndtere risiko og muligheter. Risikovurdering skal utføres med planlagte intervaller eller når betydelige

endringer foreslås eller inntreffer med oppbevaring av dokumentasjon om resultatene av risikovurderingene av informasjonssikkerhet (Standard Norge, 2017, s. 10).

- *Clause 9. Prestasjonsevaluering.* Organisasjonen skal utføre prestasjonsevaluering av ledelsessystem for informasjonssikkerhet. Dette innebefatter å bestemme hva som skal overvåkes og måles, hvem og når det skal gjøres og metoder for overvåking, måling, analyse og evaluering for å sikre gyldige resultater. Organisasjon skal oppbevare dokumentasjon som bevis på overvåkings- og måleresultatene. Interne revisjoner skal gjennomføres med planlagte intervaller for å gi informasjon om ledelsessystem for informasjonssikkerhet. Resultatene rapporteres til relevant ledelse og dokumenteres. Organisasjonens øverste ledelse skal gjennomgå ledelsessystem for informasjonssikkerhet med planlagte mellomrom for å sikre at det fortløpende er velegnet, tilstrekkelig og virkningsfull. Resultatene skal omfatte beslutninger for kontinuerlig forbedring og skal dokumenteres (Standard Norge, 2017, s. 11).
- *Clause 10 Forbedring.* Organisasjonen skal håndtere avvik og iverksette korrigerende tiltak som er tilpasset virkningene av de avdekkete avvikene. Organisasjonen skal oppbevare dokumentasjon som bevis på avvikenes art og hvilke tiltak som var innført og resultatene av eventuelle korrigerende tiltak. Organisasjon skal kontinuerlig forbedre egenheten, tjenlighet og virkninger av ledelsessystem for informasjonssikkerhet (Standard Norge, 2017, s. 12).

2.4.7 Tillegg A NS-EN ISO/IEC 27001

Tillegg A inneholder en liste over 114 sikringsmål med sikringstiltak som skal brukes til håndtering av informasjonssikkerhetsrisikoene. Sikringsmålene er kategorisert i ulike grupper som er knyttet til fysisk og logisk organisasjonsstruktur, menneskelige ressurser, IT, leverandører og lovfestede forpliktelser blant annet personvern. Til sammen er det 14 grupper nummerert fra 5 til 18. Tillegg A er en viktig del av ISMS i organisasjonen - anbefalte sikringsmål er ikke obligatoriske og en organisasjon kan velge selv sikringsmålene som den finner gjeldende for implementering. Sikringsmål gir en ide om hva en organisasjon bør å ta hensyn til for å oppnå et sikkerhetsmål men ikke hvordan dette skal gjøres.

Videre skal det gjengis noen av sikringstiltak fra Tillegg A i ISO 27001 som er rettet mot beskyttelse av informasjon og personvern.

Informasjon er aktiva i en organisasjon Ifølge *Technical Corrigendum 1*. Dette gjenspeiles også i Tillegg A NS-EN ISO/IEC 27001:2017:

A.8 Forvaltning av aktiva (Standard Norge, 2017)

A.8.1 Ansvar for aktiva

Mål: Å identifisere organisasjonens aktiva og definere ansvar for tilstrekkelig beskyttelse.

A.8.1.1	Oversikt over aktiva	*Sikringstiltak* Informasjon, andre aktiva knyttet til informasjon og systemer for informasjonsbehandling skal identifiseres, og en oversikt over disse aktivaene skal utarbeides og vedlikeholdes.[2]

A.6 Organisering av informasjonssikkerhet (Standard Norge, 2017)

[2] Technical Corrigendum 1 til ISO/IEC 27001:2013

A.6.1 Intern organisering

Mål: Å etablere styringsrammeverk for å initiere og kontrollere implementering og forvaltning av informasjonssikkerhet i organisasjonen

A.6.1.3	Kontakt med myndigheter	*Sikringstiltak* Hensiktsmessig kontakt med relevante myndigheter skal opprettholders

A.8 Forvaltning av aktiva (Standard Norge, 2017)

A.8.2 Klassifisering av informasjon

Mål: Å sikre at informasjon har et tilstrekkelig beskyttelsesnivå i samsvar med dens betydning for organisasjon

A.8.2.1	Klassifisering av informasjon	*Sikringstiltak* Informasjons skal klassifiseres i henhold til juridiske krav, verdi, kritikalitet og sensitivitet forbundet med uautorisert utlevering eller modifisering.

A.12 Driftssikkerhet (Standard Norge, 2017)

A.12.3 Sikkerhetskopiering

Mål: Å beskytte mot tap av data.

A.12.3.1	Sikkerhetskopiering av informasjon	*Sikringstiltak* Sikkerhetskopiering av informasjon, programvare og systemavbildninger skal tas og testes regelmessig i samsvar med avtalt policy for sikkerhetskopiering.

A.15 Leverandørforhold (Standard Norge, 2017)

A.15.1 Informasjonssikkerhet i leverandørforhold.

Mål: Å sikre beskyttelse av virksomhetsaktiva som er tilgjengelig for leverandør.

A.15.1.1	Informasjonssikkerhetspolicy for leverandørforhold	*Sikringstiltak* Krav til informasjonssikkerhet for å redusere risikoer forbundet med leverandørtilgang til virksomhetsaktiva skal avtales med leverandør og dokumenteres.

A.18 Samsvar (Standard Norge, 2017)

A.18.1 Samsvar med juridiske og kontraktsmessige krav.

Mål: Å unngå brudd på juridiske, lovfestede, regulatoriske eller kontraktmessige forpliktelser knyttet til informasjonssikkerhet og på ethvert sikkerhetskrav.

A.18.1.4	Personvern og beskyttelse av personlig identifiserbar informasjon.	*Sikringstiltak* Personvern og beskyttelse av personlig identifiserbar informasjon skal sikres som påkrevd i relevante lover og forskrifter der det er aktuelt.

2.5 ISO 27002

2.5.1 Versjoner av ISO 27002

Det ble nevnt at Tillegg A i ISO 27001 ikke beskriver hvordan en organisasjon skal implementere sikringstiltak for å oppnå et sikringsmål. Dette er hvor ISO 27002 kommer inn og skal brukes som referanse ved valget av sikringstiltak ved implementering av et ISMS.

«Den engelskspråklige versjonen av europeisk standard EN ISO/IEC 27002:2017 ble fastsatt som Norsk Standard NS-EN ISO/IEC 27002:2017 i mai 2017. Denne standarden erstatter NS-ISO/IEC 27002:2013» (Standard Norge, 2017). Denne versjonen erstatter og opphever ISO/IEC 27002:2005, som har gjennomgått teknisk og strukturer revisjon (Standard Norge, 2017).

Livssyklusen til standarden er 5 år, dvs. at standarden er gjennomgått hvert femte år. *ISO/IEC 27002:2013* har fått endringer som er beskrevet i *Technical Corrigendum 1* publisert *2014-09-15* (ISO, 2014) *og Technical Corrigendum 2* publisert *2015-11-15* (ISO, 2015) og som er tatt med i NS-EN ISO/IEC 27002:2017*. Technical Corrigendum 1* berørte flere områder i standarden. Først og fremst sier *Subclause 8.1.1* i ISO/IEC 27002:2017 at informasjon må betraktes som aktiva og inkluderes i beholdningen. Endringer beskrevet i *Subclause 8.1.1 forårsaket endringer i Subclause 7.1.2*. hvor det ble erstattet «forvaltning av organisasjons aktiva» med «forvaltning av organisasjons informasjon». Samme gjelder endringer i *Subclause 8.1.3* hvor det innføres i tillegg til «organisasjons aktiva» begrepet «organisasjons informasjon». *Technical Corrigendum 2* i *Subclause 14.2.8* endrer henvisning til Systemakseptansetest fra *Subclause 14.1.9* til *Subclause 14.2.9* fordi *Subclause 14.1.9* er fjernet.

ISO/IEC WD 27002 er under utvikling nå og skal erstatte ISO/IEC 27002:2013 sammen med ISO/IEC 27002:2013/Cor 1:2014 og ISO/IEC 27002:2013/Cor 2:2015 (ISO, u.d.).

2.5.2 Veiledninger til implementering av sikringstiltak fra Tillegg A NS-EN ISO/IEC 27001:2017.

Standarden inneholder 5 innledende kapitler og 14 hovedkapitler med klassifiserte og spesifiserte sikringsmål og skisserte sikringstiltak med veiledninger til implementering. Veiledninger anses som beste praksis for å nå sikringsmål.

«Denne internasjonale standarden er utarbeidet for at organisasjon skal kunne bruke den som referanse når de skal velge sikringstiltak som en del av prosessen med å implementere et ledelsessystem for informasjonssikkerhet (et ISMS-system) basert på NS-EN ISO/IEC 27001» (Standard Norge, 2017, s. 7). Dvs. at ISO/IEC 27002 gir brukere råd og veiledninger for implementering av sikringstiltak (*controls på engelsk*) som vises i Tillegg A i ISO/IEC 27001.

Underpunkt 0.3 i NS-EN ISO/IEC 27002:2017 sier at sikringstiltakene i denne standarden kan betraktes som veiledende prinsipper for styring av informasjonssikkerhet. Sikringstiltak kan velges fra denne standarden eller fra andre sett med sikringstiltak, eller nye tiltak kan utarbeides for å dekke organisasjonens behov (Standard Norge, 2017, s. 8).

A.6 Organisering av informasjonssikkerhet (Standard Norge, 2017)

A.6.1 Intern organisering

Mål: Å etablere styringsrammeverk for å initiere og kontrollere implementering og forvaltning av informasjonssikkerhet i organisasjonen

A.6.1.3	Kontakt med myndigheter	*Sikringstiltak* Hensiktsmessig kontakt med relevante myndigheter bør opprettholders

Veiledning til implementering

Organisasjoner bør ha prosedyrer som angir når myndigheter (f. eks. politi, kontrollmyndigheter, tilsynsmyndigheter) bør kontaktes, hvem som bør gjøre det og hvordan identifiserte informasjonsbrudd bør rapporteres innen rimelig tid (f. eks. ved mistanke om lovbrudd) (Standard Norge, 2017).

A.8 Forvaltning av aktiva (Standard Norge, 2017)

A.8.2 Klassifisering av informasjon

Mål: Å sikre at informasjon har et tilstrekkelig beskyttelsesnivå i samsvar med dens betydning for organisasjon

A.8.2.3	Håndtering av aktiva	*Sikringstiltak* Det bør utarbeides og implementeres prosedyrer for håndtering av aktiva i samsvar med organisasjonens ordning for klassifisering av informasjon.

Veiledning til implementering

Det bør utarbeides prosedyrer for håndtering, behandling, lagring, og kommunikasjon av informasjon i samsvar men informasjonens klassifisering (8.2.1).

Følgende punkter bør vurderes (noen eksempler):

a) tilgangsbegrensninger som understøtter kravene til beskyttelse for hvert klassifiseringsnivå;
b) Føring av en formel fortegnelse over autoriserte mottakere av aktiva
c) Beskyttelse av midlertidige eller permanente kopier av informasjon på et nivå som er i samsvar med beskyttelsen av den opprinnelige informasjonen; (Standard Norge, 2017)

A.12 Driftssikkerhet (Standard Norge, 2017)

A.12.3 Sikkerhetskopiering

Mål: Å beskytte mot tap av data.

A.12.3.1	Sikkerhetskopiering av informasjon	*Sikringstiltak* Sikkerhetskopiering av informasjon, programvare og systemavbildninger bør tas og testes regelmessig i samsvar med avtalt policy for sikkerhetskopiering.

Veiledning til implementering

Organisasjon bør definere og utarbeide policy for sikkerhetskopiering av informasjon, programvare og systemer. Policyen for sikkerhetskopiering bør definere kravene til oppbevaring og beskyttelse. Organisasjon bør anskaffe tilfredsstillende fasiliteter for sikkerhetskopiering for å sikre at all vesentlig informasjon og programvare kan gjenopprettes etter en katastrofe eller en mediesvikt. Videre gir standarden anbefalinger for utforming av plan for sikkerhetskopiering, overvåking av utførelsen av sikkerhetskopiering, testing av ordninger for sikkerhetskopiering og oppbevaringsperiode for vesentlig virksomhetsinformasjon (Standard Norge, 2017).

A.15 Leverandørforhold (Standard Norge, 2017)

A.15.1 Informasjonssikkerhet i leverandørforhold.

Mål: Å sikre beskyttelse av virksomhetsaktiva som er tilgjengelig for leverandør.

A.15.1.1	Informasjonssikkerhetspolicy for leverandørforhold	*Sikringstiltak* Krav til informasjonssikkerhet for å redusere risikoer forbundet med leverandørtilgang til virksomhetsaktiva bør avtales med leverandør og dokumenteres.

Veiledning til implementering

Organisasjon bør identifisere og pålegge sikringstiltak for informasjonssikkerhet for spesifikt å håndtere leverandøraksess til organisasjonens informasjon i en policy. Disse sikringstiltakene bør omhandle prosesser og prosedyrer som skal implementeres av organisasjonen, samt prosessene og prosedyrene organisasjonen bør kreve at leverandører implementerer, inkludert:

a) identifisere og dokumentere hvilke typer leverandører, for eksempel, av IT-tjenester, logistikktjenester, økonomitjenester og komponenter i IT-infrastruktur som organisasjonen skal gi tilgang til informasjonen sin;
b) en standardisert prosess og et standardisert livsløp for styring av leverandørforhold;
c) definere hvilke typer informasjonsaksess ulike typer leverandør skal ha, og overvåke og kontrollere aksessen;
g) typer forpliktelser leverandør har for å beskytte organisasjonens informasjon;
h) håndtering av brudd og avvik forbunnet med leverandøraksess, inkludert ansvaret til både organisasjonen og leverandørene;

Annen informasjon

Sikringstiltak bør identifiseres og tas i bruk for å gi leverandørtilgang til systemer for informasjonsbehandling. Hvis det for eksempel er et spesielt behov for konfidensialitet for informasjonen, kan det benyttes taushetserklæring. Et annet eksempel er risikoer knyttet til databeskyttelse når leverandøravtalen omfatter overføring av eller tilgang til informasjon på tvers av grenser. Organisasjonen må være oppmerksom på at det juridiske eller kontraktmessige ansvaret for å beskytte informasjon forblir hos organisasjonen (Standard Norge, 2017)

A.18 Samsvar (Standard Norge, 2017)

A.18.1 Samsvar med juridiske og kontraktsmessige krav.

Mål: Å unngå brudd på juridiske, lovfestede, regulatoriske eller kontraktmessige forpliktelser knyttet til informasjonssikkerhet og på ethvert sikkerhetskrav.

A.18.1.4	Personvern og beskyttelse av personlig identifiserbar informasjon.	*Sikringstiltak* Personvern og beskyttelse av personlig identifiserbar informasjon bør sikres som påkrevd i relevante lover og forskrifter der det er aktuelt.

Veiledning til implementering

En organisasjons datapolicy for personvern og beskyttelse av personlig identifiserbar informasjon bør utarbeides og implementeres. Denne policyen skal kommuniseres til alle personer som er involvert i behandling av personlig identifiserbar informasjon (Standard Norge, 2017).

Samsvar med denne policyen og alle relevante lover og forskrifter om beskyttelse av personvern og beskyttelse av personlig identifiserbar informasjon krever en hensiktsmessig styringskultur og kontroll. Dette kan ofte best oppnås ved at det utnevnes en ansvarlig person, for eksempel en personvernleder, som bør gi veiledning til ledere, brukere og tjenesteleverandører om den enkeltes ansvar og de spesifikke prosedyrene som bør følges. Ansvaret for å håndtere personlig identifiserbar informasjon og sikre bevissthet rundt personvernprinsippene bør behandles i samsvar med relevante lover og forskrifter. Egnede tekniske og organisatoriske tiltak for å beskytte personlig identifiserbar informasjon bør implementeres (Standard Norge, 2017).

Annen informasjon

NS ISO/IEC 29100 gir et høynivårammeverk for beskyttelse av personlig identifiserbar informasjon i systemer for informasjons- og kommunikasjonsteknologi. Flere land har innført lovgiving som regulerer innsamling, behandling og overføring av personlig identifiserbar informasjon (generell informasjon om levende enkeltpersoner som kan identifiseres ut fra denne informasjonen) (Standard Norge, 2017).

2.6 GDPR

GDPR (General Data Protection Regulation) er en forordning vedtatt i EU som skal bidra til å styrke personvernet i behandling av personlige opplysninger. Implementasjonen av dette vedtaket tredde i kraft våren 2018 og beskriver nye lover som alle aktører innenfor EU, EØS og delvis noe av det som skjer utenfor EU, spesielt med tanke på overføring av personopplysninger ut av EU, er nå nødt til å følge. Vedtaket ble opprinnelig fremstilt som en måte for enkeltpersoner å få en større kontroll over hvilke personopplysninger som har blitt lagret av diverse aktører, både på nett i forbindelse med generelle gjøremål på internett og ved handel der virksomheten lagrer personopplysninger. EU valgte å utvide den første tanken til å lage et regelverk som alle medlemsland og aktører innenfor EU må følge. Vernet rundt denne forordningen er streng, og brudd på de lovene som skal følges under GDPR kan bøtelegges med store summer.

Sett i grove trekk har GDPR to hovedgrener til hvilken funksjon denne forordningen har. Den vil på den ene siden være gunstig for enkeltpersoner og hvilke rettigheter man har som borger innenfor EU med tanke på hvilke personopplysninger som lagres og hvordan disse opplysningene blir brukt. På den andre siden har man selve reglene som bedrifter og organisasjoner er nødt til å følge for å være i tråd med det nye lovverket.

2.6.1 GDPR – Enkeltpersoner

For privatpersoner sikrer GDPR at de skal ha mer kontroll over sine personopplysninger og hva som lagres av deres informasjon. Direkte så dikterer GDPR gjennom kapittel 3 (Artikkel 12 – 23) hvilke rettigheter man har som privatperson. Alle artiklene er i stor grad relevante for å få et godt syn på hvilke konkrete rettigheter man har, og her har blant annet artikkel 17, Right to erasure (retten til å bli glemt) blitt mye omtalt i medier. Selv om GDPR er delt inn i kapitler for hvilke virkeområder de er rettet mot, eksempelvis kapittel 3 er rettet mot privatpersoner (data subjekter) og kapittel 4 mot virksomheter (kontrollører og prosessor), vil det være høyst relevant for en virksomhet å gjøre seg kjent med rettighetene til privatpersoner og vice versa. I kapittel 3 så er det spesielt noen av artiklene som uthever seg mer enn andre, eller er viktige for å skape seg et helhetlig bilde.

Artikkel 12

Artikkel 12 dikterer hvilke av artiklene en kontrollør må forholde seg til og er overordnet en referanse til andre artikler som viser til rettighetene til data subjektet. Denne artikkelen legger grunnlaget for hvordan slik informasjon skal gis til en person som har en forespørsel om sine opplysninger. Det som vektlegges og som fremkommer tydelig i denne artikkelen er at det er veldig lite slingring for hva som ansees som akseptabelt når det kommer til utlevering av informasjon. Forordningen skal hjelpe til å beskytte og gi makt til data subjektet, når det kommer til deres personlige opplysninger, noe som kommer tydelig frem ved denne artikkelen:

> *«The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means. »*
> (The European Parliament and The Council of the European Union, 2016)

Dette utdraget er første paragraf fra denne artikkelen, som man kan se fra ordvalget og strukturen viser det til at data subjektet ikke skal trenge å ha noen spesifikk kompetanse for å forstå innholdet i den informasjonen som gis ut.

Artikkel 13 og 14

Disse artiklene beskriver respektivt hvilken informasjon som må oppgis der hvor personopplysninger har blitt samlet og hvilken informasjon som må gis før personopplysninger samles fra data subjektet. Effekten av disse artiklene i praksis kan lett sees i de fleste sitt daglige liv. En populær måte å samle inn personopplysninger ofte for å kunne tilby en bruker en bedre skreddersydd opplevelse på et nettsted ved hjelp av algoritmer er bruken av informasjonskapsler (Cookies). Informasjonskapsler er et verktøy som brukes av programmerere til å lagre data fra brukere, ofte lagres ting som personopplysninger i form av karakteristikker, samt bruksvaner og direkte handlinger på nettstedet. Til tross for at loven om å opplyse om bruken av informasjonskapsler har eksistert i et par års tid er det først etter GDPR at kravet om opplysning ved bruk faktisk er iøynefallende for sluttbrukeren. Et veldig vanlig eksempel på dette er at når man besøker en nettside vil man få et banner som bunntekst eller en pop-up melding på skjermen som forteller at nettsiden bruker informasjonskapsler for å forbedre brukeropplevelsen, du som bruker er da nødt til å enten godta eller avslå denne bruken.

Artikkel 15 – 22 - Rettigheter

Rett om tilgang

Data subjektet skal ha retten til å kreve tilgang til de opplysningene som har blitt lagret omhandlende dem. Slik som nevnt i artikkel 12 skal all tilgang og opplysninger som gis ut til data subjektet være formulert på en måte som kan fremstilles og tolkes av allmennheten. I tillegg til selve retten om tilgang er også kontrollør nødt til å oppfylle krav om hvordan de bruker denne informasjonen i sitt arbeid:

> *"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:*
>
> *2.7 the purposes of the processing;*
> *2.8 the categories of personal data concerned;*
> *2.9 the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;*
> *2.10 where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;*
> *2.11 the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;*
> *2.12 the right to lodge a complaint with a supervisory authority;*
> *2.13 where the personal data are not collected from the data subject, any available information as to their source;*
> *2.14 the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."* (The European Parliament and The Council of the European Union, 2016)

Retten til å rette

Data subjektet har til enhver tid retten til å fullføre ufullstendige opplysninger som er lagret om dem. Dette skal skje ved det forbeholdet at det ikke skal være unødige forsinkelser fra kontrollør på bakgrunn av å rette opp i disse opplysningene.

Retten til å bli glemt

Retten til å bli glemt er den mest omtalte rettigheten som blir beskrevet i GDPR. Flere større aktører blant annet Google har vært på banen med uttalelser i henhold til denne loven. Selve artikkelen beskriver hvilke rettigheter du har som subjekt når det kommer til sletting av personopplysninger som skulle foreligge. Fra et overordnet syn beskriver den at du som subjekt når som helst kan be kontrollør om å slette dine opplysninger, så lenge et av kravene er oppfylt:

“

1.1 *the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*
1.2 *the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;*
1.3 *the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);*
1.4 *the personal data have been unlawfully processed;*
1.5 *the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;*
1.6 *the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).”* (The European Parliament and The Council of the European Union, 2016)

Google har som aktør vært veldig spesifikke på at de ikke ønsker å gi alle det samme tilbudet når det kommer til denne rettigheten. Når GDPR først ble tredd i kraft mottok Google store mengder med forespørsler fra europeiske borgere som ønsket å få fjernet noen av sine fotspor fra Google sin søkemotor. I en artikkel fra januar 2019 blir det beskrevet at forholdet kun skal gjelde for EU der lovgivningen er gitt og at relevante saker skal bli liggende tilgjengelig for resten av verden. Ettersom dette kan sammenlignes med spørsmål om ytringsfrihet og sensur har dette vært en høyt profilert sak i domstoler og i medier, noe som har trukket en enorm oppmerksomhet mot denne delen av GDPR. For alle borgere innenfor EU derimot er sletting av opplysninger en lett prosess der Google har kommet med et eget skjema som er lett oversiktlig der man fyller ut opplysninger om hvem man er og hva man ønsker skal slettes. (Bowcott, 2019)

Paragraf nummer tre inneholder hvilke unntak som gjelder ved denne rettigheten. De unntakene som gjelder omhandler prosessering i henhold til statlige oppdrag, allmennhetens velvære, arkivering og dokumentasjon av historiske hendelser o.l., ytringsfrihet og for etablering, praktisering eller forsvar av juridiske krav.

Retten til flytting av data

Alle opplysninger som lagres hos kontrollør er nødt til å være flyttbare. Ved krav fra subjekt skal det være mulig å flytte data fra en kontrollør til en annen uten noen hindring. Samme regler gjelder for denne dataen og den skal være maskinleselig og strukturert. Der hvor det er teknisk mulig kan også subjekt gjøre krav på at dataen ikke utleveres til subjekt som mellomledd, men direkte til ny kontrollør.

Retten til å motstå

I samme linje som de andre rettighetene har også subjektet muligheten til å motstå når det kommer til spørsmål om behandling av deres personopplysninger. Denne rettigheten går også utover

profilering ved bruk av disse personopplysningene. Profilering er et begrep som omhandler å knytte en bruker opp mot en spesiell gruppe eller segment på bakgrunn av deres opplysninger, altså prosessen av å knytte en bruker opp mot en konkret profil. Som subjekt vil man også ha muligheten til å motstå dersom det skal komme til lys at deres personopplysninger har blitt benyttet i form av markedsføring fra kontrollør sin side. Denne rettigheten kan man heve til enhver tid der grunnlaget for unntak kun går ut på legitime årsaker fra kontrollør som overstiger subjektet sine rettigheter og frihet, eller for etablering, praktisering eller forsvar av juridiske krav.

2.6.2 GDPR – Bedrifter og organisasjoner

For bedrifter og organisasjoner sikrer GDPR et fornyet sett med lover som de nå vil være pliktige til å følge. I lovverket omtales de som kontrollører og prosessorer i henhold til hvilken oppgave de har i behandlingen av personopplysninger. En kontrollør er beskrevet som den personen/gruppen som bestemmer formålet ved behandling av personopplysninger.

> *"'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;"* (The European Parliament and The Council of the European Union, 2016)

Prosessoren blir beskrevet som den personen/gruppen som behandler informasjonen på vegne av kontrollør.

> *"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;"*

I flere sammenhenger vil kontrollør og prosessor være fra en og samme bedrift eller organisasjon. Det er først når det kommer eksterne aktører på banen at bedriften vil få noen andre retningslinjer å måtte forholde seg til. Stort sett er både kontrollør og prosessor pliktig til å følge de samme retningslinjene, og det er satt opp til lite slingring i selve lovgivningen på bakgrunn av disse rollene.

Kontrollør

Den overordnede forpliktelsen og oppgaven til kontrolløren er å tilse at de tekniske og organisasjons tiltakene er på plass ved behandling av personopplysninger, for å overholde de lovene som er gitt ved GDPR. Kontrolløren vil også være den rollen som er pliktig i delegering av personopplysninger til prosessor. Som nevnt tidligere er en av de viktige forordningene ved GDPR at personopplysninger kun hentes ut og behandles ved de spesifikke formålene de er ment til å brukes til, noe som igjen vil falle tilbake på ansvaret til kontrolløren.

> *"The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. [2]That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. [3]In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."* (The European Parliament and The Council of the European Union, 2016)

Dersom to eller flere kontrollører i fellesskap vurderer formålet og meningen med behandlingen av data skal da alle parter ansees som felles kontrollører. Det vil i et slikt tilfelle være viktig at hver av de respektive partene kommer til enighet om sitt ansvar for å overholde lovgivningen. Videre i dette tilfellet er det også viktig at de respektive partene får tildelt ansvarsområder på bakgrunn av deres roller og forhold til data subjektene.
En av de felles artiklene for både kontrollør og prosessor går ut på om personopplysninger behandles utenom EU, men at data subjektene går inn under EU. I dette tilfellet vil kontrollør og prosessor være nødt til å ha en representant som operer innen EU. Grunnlaget for denne artikkelen finnes under det geografiske virkeområdet for forordningen:

> *"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
>
> 1. *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
> 2. *the monitoring of their behaviour as far as their behaviour takes place within the Union."* (The European Parliament and The Council of the European Union, 2016)

Denne representanten er også pålagt til å være etablert i den medlemsstaten der data subjektene befinner seg.

Prosessor

Prosessoren sin forpliktelse vil være å forholde seg til oppgaven tildelt av kontrollør samtidig som de prosesserer data i henhold til lovene gitt i GDPR. En prosessor skal alltid handle på vegne av en kontrollør og er forpliktet under GDPR til å ikke vike unna fra de kravene som har blitt satt av kontrollør, som for eksempel å engasjere en annen prosessor i behandlingen. Kontrollør vil i tillegg være nødt til å bruke prosessorer som kan garantere overholdelse av de riktige tekniske og organisasjons tiltakene som kreves under behandlingen.

All databehandling av en prosessor skal styres av en bindende kontrakt mellom kontrollør og prosessor. Denne kontrakten skal være i henhold til avtale mellom kontrollør og prosessor, samt at den vil være nødt til å inneholde formål om behandlingen, hvilken type data som behandles og kategorier av data subjektene, forpliktelsene til prosessor og hvilke rettigheter kontrollør vil ha gjennom prosessen.

Artikkel 32 – Sikkerhet rundt behandling

Denne artikkelen beskriver hvilke handlinger kontrollør og prosessor vil være nødt til å implementere på bakgrunn av behandlingen av personopplysninger. Første paragrafen beskriver tiltak som skal vurderes og implementeres i henhold til hvilken risiko behandlingen medfører. Denne artikkelen, på lik linje med de andre artiklene som omhandler hvilke tiltak som skal implementeres lener seg i stor grad på bedriften sin evne innenfor risikostyring og risikoanalyse, noe som vil falle under bedriften sitt ISMS og hvilke evalueringsprosesser som allerede eksisterer under dette.

> *"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

1. *the pseudonymisation and encryption of personal data;*
2. *the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*
3. *the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
4. *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.*

2. *In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*
3. *Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.*
4. *The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law."* (The European Parliament and The Council of the European Union, 2016)

Artikkel 40 – Etiske retningslinjer (Codes of Conduct)

Som beskrevet i artikkel 32, refererer denne artikkelen til hvilke retningslinjer som kan implementeres av bedriften. Den beskriver hvordan medlemsstatene, sammen med tilsynsmyndighetene skal oppfordre til utarbeidelse av etiske retningslinjer for å sikre og bidra til en fullstendig implementering av GDPR. Der de også tar hensyn til de spesifikke behovene til alt fra mindre bedrifter til større bedrifter. Andre samarbeidspartnere kan i prosessen med å utarbeide disse retningslinjene komme på banen som eksterne aktører for kontrollør og prosessor, og skal i et slikt tilfelle sikre de overordnede kravene som allerede har blitt etablert under prosessering, samt også under enkeltpersoner sine rettigheter:

> *«Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to:*
>
> *(a) fair and transparent processing;*
>
> *(b) the legitimate interests pursued by controllers in specific contexts;*
>
> *(c) the collection of personal data;*
>
> *(d) the pseudonymisation of personal data;*
>
> *(e) the information provided to the public and to data subjects;*
>
> *(f) the exercise of the rights of data subjects;*
>
> *(g) the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained;*
>
> *(h) the measures and procedures referred to in Articles 24 and 25 and the measures to ensure security of processing referred to in Article 32;*

(i) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects;

(j) the transfer of personal data to third countries or international organisations; or

(k) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing, without prejudice to the rights of data subjects pursuant to Articles 77 and 79. » (The European Parliament and The Council of the European Union, 2016)

Artikkel 42 – Sertifisering

På lik linje som i artikkel 40 skal delen om sertifisering oppfordres og appellere til behovet i mindre bedrifter til større bedrifter. Sertifisering i henhold til GDPR beskrives i reguleringen som frivillig og skal gjøres tilgjengelig gjennom en åpen prosess. Et av punktene i denne artikkelen beskriver blant annet hvordan en sertifiseringsprosess ikke på noen måte betyr på noen som helst annet enn at bedriften var i tråd med GDPR på tidspunktet ved sertifisering. Dermed skal sertifiseringen ikke bety noe for selve driften hos kontrollør og prosessor, der brudd skal behandles på samme måten og på lik linje i henhold til det som er beskrevet i reguleringen.

«A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the tasks and powers of the supervisory authorities which are competent pursuant to Article 55 or 56.» (The European Parliament and The Council of the European Union, 2016)

GDPR – i Norge

Med tilknytning til EU gjennom EØS-avtalen er også Norge et av landene som må overholde GDPR. Innføringen av den nye personopplysningsloven tredde i kraft i Norge den 20. juli 2018. Dette vil si at alle aktører som opererer innenfor Norge er nødt til å overholde GDPR lovgivingen. I et intervju gir fagdirektør i Datatilsynet et bedre utsagn som setter de nye lovene i perspektiv:

«Har du ansatte, kunder eller klienter, så behandler du personopplysninger, og da gjelder lovverket. Sånn var det før også, men vi opplever at mange har satt i gang arbeid med dette etter at GDPR er blitt mye omtalt i mediene. Vi er bekymret for dem som ennå ikke har skjønt hvilke konsekvenser det har for dem» (NTB, 2018).

Innad i Norge har også flere aktører vært på banen med uttalelser, blant annet Neupart omhandlende hvordan GDPR ikke stiller krav til en full nyetablering av ISMS, men at man skal jobbe opp imot det tidligere grunnlaget man allerede har bygget gjennom ISO-27001:

«Datatilsynet anbefaler at man bruker ISO 27001 som utgangspunkt når man jobber med GDPR da mange av sikkerhetsprinsippene er identiske. Slik kan man spare både energi og tid på å bygge ut i stedet for å bygge nytt» forklarer Senior Security Advisor i Neupart Jesper E. Siig. (Neupart, 2017)

«Personvernforordningen stiller krav til tilstrekkelig informasjonssikkerhet ved innføring av egnede tekniske og organisatoriske tiltak. Vi anbefaler at man følger anerkjente standarder som beskriver styringssystem for informasjonssikkerhet, for eksempel "ISO/IEC 27001– Ledelsessystem for informasjonssikkerhet". Man kan også bruke rammeverk og veiledere som er utviklet av andre

organisasjoner, slik som Direktoratet for forvaltning og IKT (Difi) og Nasjonal sikkerhetsmyndighet (NSM)». (Datatilsynet, 2018)

I det første sitatet fra fagdirektør i Datatilsynet nevner han også noe om konsekvenser som kan følge for de som ikke enda har satt seg inn i det nye lovverket. Brudd på GDPR kan føre til gebyrer på opptil 20 millioner euro, eller 4 prosent av den årlige omsetningen dersom dette tallet utgjør mer. Eksempelvis har teknologigiganten Google måttet betale et gebyr på 50 millioner euro som følge av at de ikke henter inn et konkret samtykke fra datasubjektene de behandler. (Porter, 2019) Dette vil si at enkelte selskaper kan i teorien bli bøtelagt for flere milliarder kroner dersom de ikke klarer å overholde det nye regelverket. Dette kan føre til store økonomiske utfordringer ettersom implementeringen av et system som overholder dette lovverket ikke vil være gratis i drift det heller. Sett fra et perspektiv på små til mellomstore norske bedrifter kan dette være avgjørende for hvordan driften og de økonomiske nøkkeltallene utvikler seg etter en slik implementasjon, der et eventuelt brudd kan føre til katastrofale konsekvenser for bedriften.

Slike avvik og brudd på GDPR rapporteres her i Norge til Datatilsynet. Det er også de som er ansvarlig for vurdering av disse avvikene og det er deres ansvar å vurdere hvor det er nødvendig å legge ved et gebyr eller ikke. Selv om regelverk rundt behandling og bearbeiding av personopplysninger ikke er et nytt fenomen har GDPR bidratt til at kravene som stilles er mye strengere enn tidligere. Dette har blant annet ledet til en stor økning i rapporterte avvik, der tall fra Datatilsynet kort tid etter iverksetting i Norge viste at antall rapporterte avvik var over dobbelt så mange som ved samme tid året før. (NTB, 2018)

2.7 Artikkel "Integration of the GDPR requirements into the requirements of the SR EN ISO/IEC 27001:2018 standard, integration security management system in a software development company."

I dette kapittelet skal det gjengis kort innholdet i artikkelen «*Integration of the GDPR requirements into the requirements of the SR EN/IEC 27001:2018 standard, integration security system in a software development company*» som er publisert i det rumenske tidsskriftet «ACTA TECHNICA NAPOCENSIS, Series: Applied Mathematics, Mechanics, and Engineering» i 2018.

Denne artikkelen presenterer en ledelsesmessig tilnærming til informasjonssikkerhet som kombinerer kravene til GDPR og kravene som beskrevet i ISO 27001 standarden. Tilnærmingen er validert av en case i et programvareutviklingsselskap som beskriver metodikk og faser for risikovurdering, risikostyring, risikoreduksjon og risikohåndtering med hensyn til informasjonssikkerhetskrav fra GDPR og ISO 27001 standard.

Artikkelen starter med beskrivelsen av informasjon som en ressurs, som alle andre viktige forretningsressurser, er viktig i organisasjonens konkurranseevne, og dermed behovet for å være ordentlig beskyttet. For en virksomhet er informasjon ikke bare den som produseres av virksomheten. Informasjonen kan tilhøre kunder, leverandører og andre interessenter og har

kommet under selskapets eierskap gjennom forretningsprosesser i virksomheten og gjør den ansvarlig for informasjon (GAŞPAR & POPESCU, 2018, s. 85).

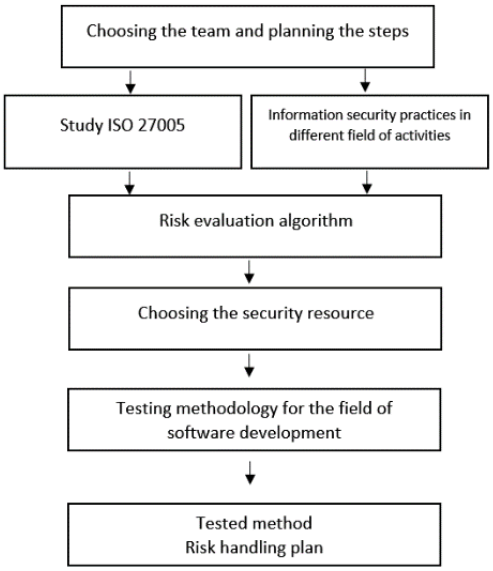
Informasjonssikkerhet er et hovedtema i ISO 27001:2013 (SR EN ISO/IEC 27001:2018) standard. GDPR pålegger en streng tilnærming ved forvaltning og beskyttelse av personopplysninger som brukes i en organisasjon (GAŞPAR & POPESCU, 2018, s. 86).

Det er obligatorisk å klassifisere informasjon. ISO 27001 nevner ikke måter for kvalifisering av infromasjons og tillater organisasjoner velge og implementre egne klassifiseringsstrategi (GAŞPAR & POPESCU, 2018, s. 86). De fleste metoder foreslår klassifisering av informasjons som:

- Offentlig eller ubegrenset informasjon
- Intern eller beskyttet informasjon
- Konfidensiell informasjon
- Hemmelig eller begrenset informasjon

Klassifisering av informasjons kan veriere og tilpasses organisasjonens behov og endringer i organisasjonen. Reglene for bruk og kontroll av informasjon bør være basert på informasjonens klassifisering (GAŞPAR & POPESCU, 2018, s. 86). Informasjonssikkerhet er utført ved å implementere en rekke sikringstiltak basert på risikostyringsprosess og administrert av et ISMS som omfatter retningslinjer, prosesser, rutiner, organisasjonsstrukturer, programvare og maskinvare for å beskytte den identifiserte informasjonsressurser. GDPR krever at alle organisasjoner som bruker personlig informasjon er forpliktet til å overholde strenge regler for måter de innsamler, bruker, prosesserer og lagrer informasjon uansett dens form, dvs. digital eller fysisk (GAŞPAR & POPESCU, 2018, s. 87). Implementering av SR EN ISO/IEC 27001:2018 hjelper organisasjonen til å kunne svare på GDPR-kravene som er et rammeverk for informasjonsbeskyttelse. Ifølge GDPR er personopplysninger kritisk konfidensiell informasjon som alle bedrifter må beskytte (GAŞPAR & POPESCU, 2018, s. 89).

Forskningsmetoden som er presentert i artikkelen baserer seg på følgende faser:



Figur 5: Risk evaluation methodology. Fra «INTEGRATION OF THE GDPR REQUIREMENTS INTO THE REQUIREMENTS OF THE SR EN ISO/IEC 27001:2018 STANDARD, INTEGRATION SECURITY MANAGEMENT SYSTEM IN A SOFTWARE DEVELOPMENT» (https://atna-mam.utcluj.ro/index.php/Acta/article/view/1054)

I den første fasen opprettes det team av de ansatte som er ansvarlige for styringssystem. Videre er utviklingen av prosessen planlagt og det utføres primærinnsamling og prosessering av informasjon.

Den andre fasen inkluderer analyse av SR ISO 27005:2016 «Information technology. Security techniques. Information security risk management» standard og praksis i informasjonssikkerhet i analyseteamet. Forfatterne henviser til SR EN/IEC ISO 27001:2018 som inneholder kravene knyttet til informasjonssikkerhet risikoevaluering og behandling. SR ISO/IEC 27005:2016 er en referansestandard for informasjonssikkerhet risikoevaluering og behandling (GAŞPAR & POPESCU, 2018, стр. 89).

For å gjennomføre forskningsmetoden ble det identifisert to typer ressurser («Choosing the security resource») i programvareutviklingsselskapet:

- Primære ressurser: forretningsprosesser, aktiviteter, informasjon og personlig informasjon (personal data) identifisert som primære ressurser.
- Støtteressurser: maskinvare, programvare, nettverk, ansatte, lokasjoner.

Med utgangspunkt i SR ISO/IEC 27005:2016 ble det dannet en risikohandlingsplan og risikostyringsmetoden som består av (GAŞPAR & POPESCU, 2018, стр. 89-90):

- Identifisering og evaluering av ISMS informasjons- og materielle ressurser og eiere av disse ressursene
- Identifisering av trusler og sårbarheter relatert til ressurser
- Evalueringen av virkningen på selskapets virksomhet når uønsket hendelse oppstår
- Evalueringen av den realistiske sannsynligheten for forekomst av uønskede hendelser
- Evaluering av risikonivå ved hjelp av en kvalitativ risikonivåmatrise
- Anbefalinger til valg av sikkerhetstiltak som beskrevet i SR ISO/IEC 27002:2018
- Opprettelse av risikoanalyserapport i henhold til SR ISO/IEC 27001: 2018 krav

Risikoanalyse i denne forskningsmetoden var gjennomført for informasjon som er klassifisert som konfidensielt (personal data) og som inneholder ansatte personlig informasjon. Disse dataene, i henhold til GDPR, må behandles og beskyttes gjennom egne metoder i programvareutviklingsselskapet (GAŞPAR & POPESCU, 2018, s. 92). Tabell 2 på side 93 «Risk evaluation for confidential information resource- personal data» inneholder risikoanalysen for tap av konfidensialitet, tre eksempler for sårbarhetsalternativer, mulige konsekvenser, tidligere gjennomførte tiltak og nye tiltak. Tabell 3 på side 93 «Risk evaluation for confidential information resource- personal data» inneholder trusler som tap av integritet og tilgjengelighet med sårbarhetsalternativer, mulige konsekvenser, tidligere gjennomførte tiltak og nye tiltak. I denne tabellen foreslås det ikke nye tiltak og bedriften skal forholde seg til allerede implementerte tiltak.

Figur 3 på side 94 i artikkelen beskriver sju trinn for rangering, evaluering, valg og implementering av risikoreduserende tiltak. På slutten oppsummerer forfatterne med en tabell «The risk handling plan for: confidential information resource - personal data» hvor de foreslår valgte tiltak, risikoansvarlig, implementeringsansvarlig og referanser til sikringstiltak i Tillegg A i ISO 27001 for å sikre konfidensialitet for personlig informasjon.

Influenced resource	Confidential information	Confidential information	Confidential information
Measure	Documents and the implementation of the GDPR requirements in the company	Cryptographic keys throughout information communication	The consistent review or access rights
Risk responsible	ISMS responsible	ISMS responsible	ISMS responsible
Measure implementation responsible	Security group	IT Manager	IT Manager
Ticket number	INSEC-49	INSEC-95	INSEC-98
The control reference from ISO 27001/ Appendix A	A 10.1.2	A 10.1.2	A 9.2.5

Tabell 3: The risk handling plan for: confidential information resource- personal data. Fra «INTEGRATION OF THE GDPR REQUIREMENTS INTO THE REQUIREMENTS OF THE SR EN ISO/IEC 27001:2018 STANDARD, INTEGRATION SECURITY MANAGEMENT SYSTEM IN A SOFTWARE DEVELOPMENT» (https://atna-mam.utcluj.ro/index.php/Acta/article/view/1054)

Artikkelen avsluttes med konklusjon om at integrasjon av GDPR krav i ISO 27001 er et nåtidstema i organisasjoner og leder organisasjonene som implementerer dette til ytelse. Forfatterne ønsker å møte selskapene som er interessert i denne prosessen for å oppnå ytelse ved å respektere GDPR-kravene og implementere informasjonssikkerhetsstandard (GAŞPAR & POPESCU, 2018, s. 95).

3.0 Metode

Innledning

I dette kapittelet skal den vitenskapelige fremgangsmåten for innsamling av data som skal danne grunnlaget for besvarelsen på problemstillingen i oppgaven beskrives. Metoden er den ikke teoretiske delen av oppgaven og handler om verktøy som skal benyttes for innsamling og analyse av informasjon, dvs. typer av data (primær- og sekundærdata) og undersøkelsesmetoder (kvalitativ og kvantitativ metode). Det er viktig at valg av metode tar utgangspunkt i den problemstillingen som skal studeres, og ikke omvendt å la metode dominere problemet. Valg av metode for innsamling av informasjon og opplysninger til denne oppgaven tar utgangspunkt i beskrivelsen av oppgaveforslag og problemstilling som forutsetter bruk av både sekundær- og primærdata.

3.1 Primærdata

Primærdata er de data som samles av forskeren selv, eller planlegges av forskeren for prosjektets formål. Normalt skilles det mellom følgende teknikker for innsamling av primærdata: spørreskjema, intervju, observasjoner eller fysisk/medisinsk måling (Ringdal, 2001). Fordelen med primærdata er at den samles inn spesielt for problemstillingen. Samtidig er det tids- og arbeidskrevende (Ringdal, 2001). Primærdata kan bli av kvantitativ eller kvalitativ art. Typiske kvantitative metoder er telefonintervju, spørreskjema i posten eller korte personlige intervjuer på gata. Innsamlet data er ofte behandlet av datamaskin og analyse foretas på bakgrunn av tallmaterialet (Mangfold, u.d.). Typiske kvalitative teknikker for å samle inn data er observasjoner, samtaler eller intervjuer. Kvalitativ metode tar utgangspunkt i å samle informasjon for å ta innsikt i et fenomen eller et problem, for eksempel hvordan nettstudenter kan forbedre motivasjonen og mestring.

> *«Et tradisjonelt bilde av forskjellen mellom kvantitativ og kvalitativ metode er at den kvalitative forskeren starter med å definere variabler og kategorier. Variablene stilles sammen i hypoteser, som testes mot data. Den kvalitative forskeren begynner med svært generelle begrep, som under forskningsprosessen gis mening og blir mer presist definert»* (Ringdal, 2001, s. 107).

«En hovedforskjell mellom kvantitative og kvalitative metoder er at de første gir talldata, og de andre tekstdata» (Ringdal, 2001, s. 108).

I dette prosjektet ble det valgt å samle inn primærdata av kvalitativ art med utgangspunkt i antall respondenter og problemstilling. Oppgaveforslaget anbefaler å ta kontakt med to til tre bedrifter for å kartlegge hvordan de forholder seg til styring av informasjonssikkerhet for å få vurdering av modellen for et ISMS som er beskrevet i teoridelen. For innsamling av primærdata ble det tatt kontakt med flere offentlige og private organisasjoner med både fysisk oppmøte og gjennom e-post. Ved valg av organisasjoner var det lagt vekt på tilstedeværelse av internkontroll på informasjonssikkerhetsområdet i organisasjonen. Positiv tilbakemelding kom fra to organisasjoner som ville bidra med informasjon til dette prosjektet og som ble intervjuet av et medlem i prosjektgruppen.

For intervjuene ble det utarbeidet et spørreskjema som var brukt som en intervjuguide og samtykkeerklæring med mal fra NSD med noen tilpasninger. Spørreskjemaet var utviklet med utgangspunkt i teorien som er presentert i teorikapittelet. Spørreskjema og samtykkeerklæring var sendt i forkant av intervju gjennom e-post slik at respondent hadde muligheter å forberede seg til intervju. Første versjonen av spørreskjemaet inneholdte 16 spørsmål. På slutten av det første

intervjuet ble det stilt spørsmål 17 og 18 som resultat av svarene på spørsmålene fra spørreskjemaet. Spørsmålene 17 og 18 ble lagt til spørreskjemaet og stilt også på det andre intervjuet. Spørsmål om sikkerhetspolicy som ble stilt i det andre intervjuet er ikke inkludert i spørreskjemaet men finnes i vedlegget. Det ble valgt å gjennomføre muntlig intervju med lydopptak slik at svarene registreres mer nøyaktig og fullstendig. Analysen av lydopptakene fra intervjuene ble gjennomført manuelt - svarene ble skrevet ned som tekstdata med noen tilpasninger for bedre struktur og lesbarhet.

Tabell 4 gir oversikt over flere dimensjoner ved innsamling av data og hvilken grad av nærheten og standardisering ble oppnådd ved bruk av ulike fremgangsmåter for innsamling av primærdata i prosjektet. Den ene dimensjonen er grad av nærheten. Medium representerer en fysisk avstand til respondenten og størst grad av nærheten ble oppnådd ved personlig besøk. Den andre dimensjonen er grad av standardisering. Virksomhetene som deltok i intervjuene fikk identiske spørreskjema og samtykkeerklæring gjennom e-post. Intervjuene ble utført av et medlem i prosjektgruppen med faglig innsikt i temaet for intervjuet slik at respondenten kunne få forklaringer til intervjuerens spørsmål. Selv om spørreskjema var sendt i forkant av intervjuet var det ikke krav til respondenten å forberede seg til intervju. Dette hadde både positive og negative innvirkninger. Det ga rom for improvisasjon fra respondenten sin side og nye interessante funn i løpet av intervju som med spørsmål 17 og 18 som var ikke i opprinnelige versjonen av spørreskjemaet. Samtidig var besvarelsene i det ene intervjuet hvor respondenten ikke hadde sett på spørsmålene i forkant av møtet preget med nokså lang betenkningstid og en del usikkerhet. Spørreskjemaet inneholder både lukkede spørsmål (ja/nei spørsmål) med muligheter til videreutvikling av svar og åpne spørsmål i situasjonen hvor respondenten ikke kunne velge mellom et av to alternativ (ja eller nei).

Grad av nærhet	Medium	Grad av standardisering	
		Lav	Høy
Lav	E-post	-	Spørreskjema som intervjuguide, samtykkeerklæring
Middels	-	-	-
Høy	Personlig besøk	Samtaleintervju med spørreskjema som intervjuguide	-

Tabell 4: Datainnsamling basert på intervju og spørreskjema. Kilde: (Kristen, 2001, s. 124)

3.2 Sekundærdata

Sekundærdata eller «skrivebordsdata» er data som er samlet inn av andre fra før, for eksempel forskere, forfattere eller statistikkbyrå. Sekundærdata er ikke avgrenset til forskningsdata og omfatter alt fra graffiti og tagging gjennom ulike typer dokumenter til statistikk fra SSB og forskningsdata (Ringdal, 2001). Sekundærdata har begrensninger i at den er avhengig av tid – jo lengre tilbake i tiden, jo mindre tilgjengelig data som finnes (Ringdal, 2001). Sekundærdata kan også være av kvalitativ og kvantitativ type. Typiske sekundære kvalitative data er samtaleintervju, livshistorier, muntlige historier eller feltnotater. Typiske sekundære kvantitative data er surveydata, tellinger eller regnskaper. Tilgjengelighet av kvalitative forskningsdata er meget dårlig i forhold til tilgjengelighet av kvantitative data som er meget god. «Det foreligger lite forskningsdata fra tida før 1960, mens datamengde øker fram mot vår tid» (Ringdal, 2001, s. 120). Det finnes store databanker

for flere typer kvantitative data som for eksempel Statistisk Sentralbyrå eller NSDs Database for statistikk om høgre utdanning (DBH).

Teoridelen består av sekundærdata som har både direkte og indirekte sammenheng med problemstillingen. Det ble valgt å bruke sekundærdata fordi utforskning av problemstillingen baserer seg på hendelser som skjedde i fortiden – utarbeidet standarder, veiledninger, lovverk, vitenskapelige artikler, konferanser, bøker mm. For å få tilgang til innholdet i NS, ISO standardene på standard.no ble det brukt NTNUs abonnement slik at standardene kunne leses/skrives ut innen 24 timer.

Tabell 5 viser en oversikt over sekundærdata som ble brukt i teoridelen og ordnet etter struktureringsgrad og på hvilke måter data ble til. Prosessdata er data som er skap gjennom samfunnets løpende aktivitet. Forskningsdata er produsert for forskningsformål (Ringdal, 2001, s. 120).

		Prosessdata	Forskningsdata
Struktureringsgrad	Lav	Video Grafikk (bilder og figurer) Medier Bøker Leksjoner fra NTNU Sikkerhetsrelaterte organer: • Difi • NorSIS • Datatilsynet • NSM	 Vitenskapelige artikler Leksjoner fra NTNU
	Høy	Offentlig forvaltning: • Lovdata Standarder: • ISO 27001 • ISO 27002 • ISO 27005 • ISO 27000 Forordninger: • GDPR	Offentlig statistikk fra • SSB • ISO

Tabell 5: Ulike typer sekundærdata. Kilde: (Ringdal, 2001, s. 120)

4.0 Resultat (Empiri/Statistikk)

Innledning

I dette kapitelet skat det presenteres kvalitative resultater fra muntlige intervjuene av to organisasjoner. Svarene ble registrert med lydopptak og skrevet ned som tekstdata. Tekstlige resultater er presentert videre som tabell for bedre sammenligning av intervjurespondentenes besvarelser på samme spørsmålene og som vedlegg hvor det finnes mer detaljerte svar. Spørsmålene som ble brukt på intervjuene finnes i Tabell 6 og i vedlegg. Med hensyn til konfidensialitet og sporbarhet som ble beskrevet i samtykkeerklæringen fikk organisasjonene anonymiserte navn som Virksomhet 1 og Virksomhet 2. Vedlegget inneholder også tilleggsspørsmål «*Har virksomheten utarbeidet en informasjonssikkerhetspolicy?»* som ble stilt til Virksomhet 2 men ikke til Virksomhet 1 og som ikke er inkludert i spørreskjema men brukes i analysedelen. Vi bruker også statistikk i form av tabeller og figurer fra SSB og ISO Survey som har nyttige talldata om sertifisering mot ISO 27001 i Norge og i verden, talldata om ISMS og om ulike tiltak/rutiner for informasjonssikkerhet og IKT-problemer i den norske offentlige sektoren.

Spørreundersøkelse

Virksomhet 1

Virksomhet 1 er en stor offentlig virksomhet på omtrent 400 årsverk. Respondenten har stilling som virksomhetsleder.

Virksomhet 2

Virksomhet 2 er en relativt nyetablert offentlig virksomhet og omfattes av omtrent 250 årsverk. Respondenten er ansvarlig for arbeidet med ISMS i virksomheten og har stilling som IT-sjef.

Nummer	Spørsmål	Virksomhet 1	Virksomhet 2
1	Hvem er ansvarlig for informasjonssikkerhetssystem i organisasjonen (stilling)?	Den øverste ledelsen og virksomhetsleder	Administrerende direktør og styret, IT-sjef
2	Hvem er ansvarlig for vedlikehold av informasjonssikkerhetssystemet i organisasjonen (stilling)?	Den øverste ledelsen er hovedansvarlig, og virksomhetsleder er ansvarlig i praksis.	Overordnet ansvar hos informasjonssikkerhetsansvarlig, og videre hos en sikkerhetsorganisasjon som virksomheten har beskrevet og bemannet.
3	Hvilket grunnlag hadde dere brukt for utvikling av styringssystem for	Veiledninger fra Datatilsynet, Difi, og NorSis.	Hovedsakelig veiledning fra Difi, men også fra Datatilsynet og standardene

	informasjonssikkerhet? For eksempel, veiledninger fra Datatilsynet, Difi, NoRSIS eller ISO 27001.		ISO 27005, og ISO 27002. Kurs for å forstå håndtering av den nye personvernloven.
4	Hvis dere brukte ISO 27001, hvilken versjon brukte dere for implementering av informasjonssikkerhet styringssystem?	Veiledningene fra spørsmål 3 baserte seg på ISO 27001 i fra 2013.	Difi sin veiledning baserte seg på ISO 27001 fra 2013.
5	Har organisasjonen opprettet sikkerhetssystem internt eller fått ekstern hjelp?	Internt, med unntak av det som omhandler GDPR.	Internt.
6	Har organisasjonen utarbeidet sikkerhetshåndbok?	Virksomhet har ikke sikkerhetshåndbok, men utarbeidet veiledere, regler, sikkerhetserklæringer og instrukser samlet i et system.	Virksomheten har et regelverk, men kaller ikke dette for en sikkerhetshåndbok.
7	Hvor ofte revideres sikkerhetshåndboka?	Intet gitt.	Virksomheten jobber med å utarbeide intervaller for revidering.
8	Når var den siste revideringen av sikkerhetshåndboka?	Intet gitt.	Fortløpende revidering, ettersom virksomheten er i gang med å implementere systemet sitt.
9	Ble sikkerhetsboka revidert i forbindelse med det nye personvernregelverket GDPR som trådte i kraft den 20. Juli 2018?	Nei.	Nei, men fire måneder i etterkant.

10	Hvordan spres innholdet i sikkerhetsboka?	Fra ledere og ut gjennom personalmøter, i muntlig-, digital- og i papirformat.	Virksomheten har en personalhåndbok per i dag, men vil senere følge samme fremgangsmåte som internkontrollen for øvrig. Det vil si at ansvarshavende for internkontroll kommuniserer ut til virksomheten.
11	Hva gjør virksomheten for å opprettholde fokus på informasjonssikkerhet, og hvordan sikrer dere at det opprettholdes fokus på informasjonssikkerhet?	Lite direkte fokus, men de har et rigid system med sentraldrift og tilgangsbegrensninger.	Administrerende direktør og styret gir instrukser videre til gjeldende ansvarsområder, hvor det er satt opp funksjoner, og IKT-funksjoner har ansvar for informasjonssikkerhet.
12	Gjennomføres det kultur- og teknisk program ved innføring, vedlikehold og forbedring av ISMS?	Det er fokus på sikkerhetsholdninger blant ansatte, og fokus på sikkerhet i fagsystemene som brukes.	Ja, men ikke systematisk enda.
13	Evalueres det ISMS i organisasjonen? Hvilke evalueringsmetoder interne og/eller eksterne som er tatt i bruk for å måle ISMS?	Ad hoc evalueringer. Sikkerhetsavvik blir evaluert for å finne ut hva som gikk galt, og hva som skal gjøres videre.	All drift av infrastruktur er satt ut, og med dette får de regelmessige gjennomganger slik at virksomheten sikrer samsvar med god praksis, og gjeldende standarder.
14	Hvordan sprer dere resultater av evalueringer i organisasjonen?	Spesielle hendelser tas opp i faste ledermøter, og spres videre ut i virksomheten.	Ingen intern spredning, men årlig rapportering til myndighetene.

15	Har organisasjonen fått sertifisert sikkerhetssystemet sitt?	Nei.	Nei.
16	Hva var årsaken til sertifisering/ikke sertifisering av ISMS?	Virksomhet har ikke behov for sertifisering. Det er en ressurskrevende prosess som skal gjennomføres hvert tredje år. Derimot ved kjøp av tjenester fra private aktører krever virksomhetene sertifisering mot sikkerhetsstandard.	Har ingen sertifisering, og ser heller ikke behovet. Dersom de skulle fått systemet sitt sertifisert, ville dette vært på bakgrunn av et eksternt krav.
17	Hvilke holdninger har virksomheten i forhold til digitalisering av tjenester?	Virksomheten jobber bevisst mot å digitalisere de tjenestene de har.	Stor grad av digitaliseringsbehov. Ved innsamling av data fra de ulike operative funksjoner utenom virksomheten, er det viktig med prosesstyrte rutiner for datainnsamling, og at det ikke skal foregå manuelt.
18	Hvordan ligger virksomheten i forhold til nye krav og regler som ble innført da GDPR trådte i kraft 20. juli 2018?	Virksomheten føler de ligger godt an, og at det hjalp med eksisterende rutiner for å håndtere og svare på krav fra den nye personvernloven.	Med utgangspunkt i Difi sin veiledning og med utgangspunkt i standardene var det mindre justeringer som måtte til for å håndtere krav i forbindelse med GDPR. I praksis utgjorde kravene fra GDPR en ekstra dimensjon i eksisterende system.

19	Hvordan jobber virksomheten sammenlignet med NTNU sin modell for ISMS?	Det jobbes ubevisst ganske likt metoden fra modellen, og virksomheten synes den tegner et bilde av en tenkemåte både de og andre virksomheter jobber ut ifra.	NTNU sin modell virker som et årshjul for systematisk aktivitet, som står i stil med måten virksomheten jobber ut ifra.

Tabell 6: Besvarelser fra Virksomhet 1 og Virksomhet 2

Statistikk fra SSB og ISO Survey

Prosent av offentlige virksomheter i Norge som har evaluert, forbedret eller fornyet ISMS i 2018.

	Evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet
	2018
Statlige virksomheter	81,7
Fylkeskommuner	87,5
Kommuner	52,3

Tabell 7: 12042: Tiltak som del av internkontroll for informasjonssikkerhet (prosent), etter forvaltningsnivå, statistikkvariabel og år. Fra Statistisk Sentralbyrå, 29. mai 2018 (http://www.ssb.no/statbank/sq/10017378/)

Resultatene fra undersøkelsen i perioden 2006-2017 viser antall av gyldige sertifikater per 31. desember 2017 i Norge. Undersøkelsen dekker ISO 27001 styringssystem for informasjonssikkerhet. Hele tabellen finnes i vedlegget.

ISO/IEC 27001 - Europe												
Year	*2006*	*2007*	*2008*	*2009*	*2010*	*2011*	*2012*	*2013*	*2014*	*2015*	*2016*	*2017*
Country												
Norway	15	22	16	17	25	31	16	26	70	49	81	87

Tabell 8: Utdrag fra tabellen viser antall gyldige ISO 27001 sertifikater i perioden 2006-2017 i Norge (ISO, u.d.).

ISO survey viser i sin undersøkelse ti land med flest ISO/IEC 27001 sertifikater i 2016:

Top 10 countries for ISO/IEC 27001 certificates - 2016		
1	Japan	8945
2	United Kingdom	3367
3	India	2902

4	China	2618
5	Germany	1338
6	Italy	1220
7	United States of Amerdica	1115
8	Taipei, Chinese	1087
9	Spain	752
10	Netherlands	670

Tabell 9: Top 10 countries for ISO/IEC 27001 certificates - 2016. Tabellen hentet fra «9. ISO Survey of certifications to management system standards - Full results» (https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1)

Innholdet i *Tabell 10* viser ulike tiltak/rutiner ved administrasjon av styringssystem for informasjonssikkerhet i statlige virksomheter og resultater i prosent for perioden 2013-2018.

		2013	2014	2015	2016	2017	2018
Alle ansatte	Har en skriftlig informasjonssikkerhetspolicy som er forankret i ledelsen	77,8	77,5	79,0	83,8	88,1	82,7
	En formelt utnevnt person er fagansvarlig for informasjonssikkerheten	82,1	81,4	83,8	85,1	91,1	90,9
	En beredskapsplan er oppdatert i løpet av de to siste årene	67,9	73,3	81,7	80,2	83,7	.
	Beredskapsøvelse gjennomføres minst en gang per år	.	29,2	31,0	33,3	43,6	41,3
	Har rutine for håndtering av sikkerhetshendelser	70,9	73,3	80,3	82,4	89,6	.
	Har dokumentert metodikk og maler for risikovurderinger	62,8	63,1	74,2	80,2	84,2	.
	Akseptabel risiko er klargjort av ledelsen, og er kommunisert videre til de ansatte	46,2	48,7	55,5	59,5	63,9	.
	Risikovurderinger gjennomføres systematisk og periodisk	.	57,2	69,0	72,5	79,2	76,4
	Ved nye risikovurderinger iverksettes nødvendig risikohåndtering	70,1	71,2	78,2	78,8	85,6	89,4
	Har årlige interne revisjoner av styringssystemet for informasjonssikkerhet	.	39,4	48,5	55,9	59,9	.
	Ledelsen har årlig gjennomgang av styringssystemet for informasjonssikkerhet	.	33,5	48,0	50,9	56,9	.
	Aktiviteter for opplæring og bevisstgjøring av ansatte og ledere gjennomføres minst én gang per år	.	.	.	.	.	67,8

Fotnoter

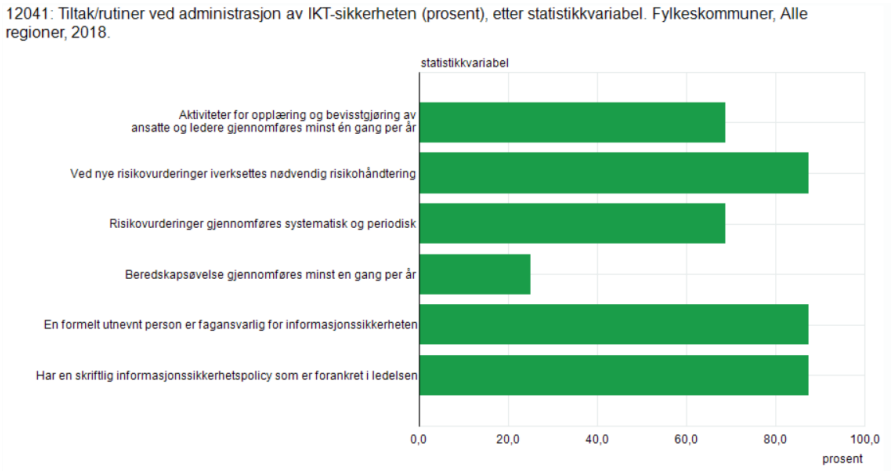
. = Tall kan ikke forekomme

statistikkvariabel

Ved nye risikovurderinger iverksettes nødvendig risikohåndtering
Uavhengig av nye eller endrede IKT-systemer

Tabell 10: 10852: Tiltak/rutiner ved administrasjon av IKT-sikkerheten i statlige virksomheter (prosent), etter sysselsettingsgruppe, statistikkvariabel og år. Fra Statistisk Sentralbyrå, 29. mai 2018 (http://www.ssb.no/statbank/sq/10019507/)

Diagrammet i *Figur 6* viser data for ulike tiltak/rutiner og resultater i prosent ved administrasjon av styringssystem for informasjonssikkerhet i fylkeskommuner i 2018.



Figur 6: 12041: Tiltak/rutiner ved administrasjon av IKT-sikkerheten (prosent), etter forvaltningsnivå, antall innbyggere, statistikkvariabel og år. Fra Statistisk Sentralbyrå, 29. mai 2018 (http://www.ssb.no/statbank/sq/10018006/)

Tabell 11 viser prosent av offentlige virksomheter i Norge som opplevde IKT-sikkerhetsproblemer i perioden 2016-2018 hvor noen resulterte i tap av informasjon.

	2016	2017	2018
	Prosent av statlige virksomheter	**Prosent av statlige virksomheter**	**Prosent av statlige virksomheter**
Virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid	23,0	21,3	10,6
Sammenbrudd i forbindelsen til internett eller andre eksterne nettverk[1]	10,8	11,4	11,1
Angrep av typen 'denial of service'[2]	16,7	18,8	11,5
Uautorisert tilgang til systemer eller data	9,0	15,3	15,4
Datatap pga. manglende backup	5,9	10,4	5,3
IT-misbruk av økonomisk karakter	5,4	7,9	8,2
Forsøk på identitetstyveri (phishing)	42,8	56,4	54,8
Virksomhetens IKT-utstyr har kommet på avveie	37,8	52,0	38,0

[1]Sammenbruddet ga merkbare virkninger i utførelsen av arbeidet

[2]Handlinger som forhindrer deler av at system eller nettverk i å fungere ordentlig

Tabell 11: Bruk av IKT i offentlig sektor. Andel som har opplevd IKT-sikkerhetsproblemer. Fra Statistisk Sentralbyrå, 28. mai 2018 (https://www.ssb.no/iktbruks)

5.0 Diskusjon

Innledning

I denne delen analyserer vi innsamlede sekundære og primære data for å besvare problemstillingen. Diskusjon består av fire punkter hvor det drøftes underspørsmålene som utgjør problemstillingen. Vi starter ved å beskrive hvilke komplikasjoner GDPR har skapt for innføring av ISMS i bedrifter ved hjelp av Google case. Ut fra krav og sikringstiltak i NS-EN ISO/IEC 27001:2017, NS-EN ISO/IEC 27001:2017, GDPR krav, vitenskapelig artikkel, statistiske og empiriske data undersøker vi i hvilken grad ISO sikkerhetsstandardene kan hjelpe med å oppfylle kravene i GDPR. Vi lager en tabell som foreslår hvilke sikringstiltak fra NS-EN ISO/IEC 27001:2017 kan hjelpe med arbeid mot implementering av personvernforordningen. Avslutningsvis vurderes modellen for innføring av ISMS mot veiledninger fra sikkerhetsaktører, resultater fra spørreundersøkelser, statistiske data og krav i NS-EN ISO/IEC 27001:2017 og NS-EN ISO/IEC 27002:2017.

5.1 Hvilke komplikasjoner har GDPR skapt for innføring av ISMS i bedrifter?

Slik som kommer frem av den fremstilte teorien er det ingen tvil om at GDPR stiller strengere krav til hvordan databehandlingen foregår i en bedrift enn tidligere. På selve siden om hvilke direkte komplikasjoner det dermed skaper er vi interessert i å diskutere både spørsmål om ressurser og bruk av ISO-standarder. Selv om GDPR har vært i utvikling over lengere tid, noe som har gitt bedrifter tid til å sette de korrekte tiltakene i verk har det for mange aktører, spesielt blant de større aktørene, vist seg å være et omfattende arbeid der noen av de større aktørene har måttet betale dyre dommer på bakgrunn av avgjørelser fra tilsynsmyndighetene. Til slutt har vi sett ut ifra vår forskning at det tilsynelatende er normal praksis for en andel norske bedrifter å ikke forholde seg til ISO-standarder når de implementerer ledelsessystemene sine, men heller å lene seg på veiledninger fra andre norske aktører som jobber tett mot informasjonssikkerhet. Dermed vil vi også diskutere hvilken påvirkning dette kan ha på et fullverdig system og se til om de veiledninger som ligger tilgjengelig for bedriftene i dag holder seg i tråd med GDPR, eller om slike veiledninger blir forenklet til en større grad der de ikke beskriver sentrale sikringstiltak.

GDPR og informasjonssikkerhet

Arbeid med informasjonssikkerhet og GDPR omtales som både avansert og ressurskrevende, og med god grunn. Påkrevde forordninger som GDPR og generelle lover om databehandling under staten sammen med anbefalte standarder for implementering, derav ISO-27K, hoper seg opp til å bli et omfattende arbeid som krever at man legger inn mye tid og ressurser for å kunne holde en god orden på informasjonssikkerheten i bedriften. Da GDPR ble innført i 2018 viste det på bakgrunn av tall fra Datatilsynet at antall avvik økte betraktelig i løpet av kort tid etter iverksetting. Dette gir både en tydelig indikator på at innføringen av GDPR har gått som planlagt med tanke på at folk nå rapporterer inn slike avvik oftere og er mer klar over sine egne rettigheter, samtidig så kan det også kaste et lys mot at bedrifter har møtt på problemer med overholdelse av den nye forordningen. Et nyttig verktøy for bedrifter i sammenheng med spørsmål om GDPR har vært å forholde seg til ISO-standard 27001. Slik som skal analyseres videre under neste forskningsspørsmål vil en streng og tett oppfølging av ISO 27001 allerede lede slike bedrifter på rett vei i henhold til GDPR.

GDPR og Google

En av de aktørene som har vært omtalt mye i mediene i henhold til GDPR er Google, og deres syn på forordningen samt hvilke komplikasjoner det har skapt for deres drift. En av de største mediesakene omhandlende GDPR har vært den kontroversielle artikkelen nummer 17, som beskriver data subjektet sin rettighet til å slettes eller "bli glemt". Google har som aktør vært tidlig ute på banen med uttalelser om at deres tilbud i henhold til GDPR ikke skal strekkes lenger ut enn kun innenfor medlemslandene i EU og EØS på bakgrunn av at i deres arbeid kan det stilles sentrale spørsmål om ytringsfrihet og sensur som kan overveies fra begge sider av saken. Hovedformålet til GDPR har vært å gi enkeltpersoner mer makt over hvilke personopplysninger bedrifter behandler om dem, stort sett i lys av dataanalytiske forhold. Til tross for at denne forordningen kun eksisterer innenfor EU er ikke personvern et glemt emne utenfor heller, dermed har mange enkeltpersoner utenfor EU vist stor interesse med de forskjellige rettighetene man har under GDPR. Her kommer spesifikt retten til å bli glemt inn. Enkeltpersoner ser på denne rettigheten som en rett de burde ha til tross for at deres lokasjon og databehandlere opptrer utenfor EU. Det er blant annet her Google har vært på banen med sine uttalelser om at dette skal være en særskilt rettighet for europeiske borgere og at disse rettighetene ikke skal gjelde for personer utenfor EU. Slik som ble nevnt tidligere har dette spørsmålet allerede vært oppe i domstoler og mye omtalt i medier, der hovedargumentasjonen går ut på spørsmål om ytringsfrihet og sensur. På den ene siden vil det være viktig å overveie andre menneskerettigheter, samt lovverk om dataregulering og om det skal opprettes særskilte behov for muligheten til å bli glemt vil det kunne oppmuntre bruk av sensur i enkelte land som ønsker å "kontrollere" folket i en større grad. For å komme seg mer i tråd med disse lovverkene implementerte Google for en stund tilbake forskjellige domener basert på hvilket land du surfer fra (eksempel .no, .dk, .uk osv). Noe som i praksis vil si fra et dataanalytisk standpunkt at du er mer sannsynlig for å finne artikler og nettsteder som besøkes av andre personer fra samme land som du surfer fra og dermed gjør det lettere å overholde forespørsler om fjerning av personopplysninger. Tidligere ble det nevnt at Google har implementert et eget skjema for utfylling dersom du er i en situasjon der du ønsker å få dine personopplysninger fjernet. Fremgangsmåten her fremstilles som transparent og lettleselig i henhold til GDPR der du fører inn hvilke URL-er det gjelder samt informasjon om deg. Det blir videre da sendt til behandling hos Google der du vil få en bekreftelse på behandlingsprosessen i en mail, samt bekreftelse da dine opplysninger har blitt fjernet.

Konkret på siden av komplikasjoner GDPR har skapt for Google har de nylig blitt pålagt et gebyr fra den franske tilsynsmyndigheten på bakgrunn av dårlig etterspørsel for samtykke fra datasubjektene. GDPR dikterer at kontrollør skal be datasubjektet om et genuint samtykke som er lettleselig og transparent i henhold til artikkel 12, noe som Google har feilet på. Dette resulterte i et gebyr på 50 millioner euro, som er det største gebyret som har blitt utlevert på bakgrunn av GDPR til dags dato (05.05.2019). I en uttalelse fra Google sin talsperson sier de at de er dypt engasjert for å holde de høye standardene for transparens og kontroll som blir satt av GDPR og har i ettertid anket gebyret med argumentasjon om hvilken effekt en slik kontroll vil ha på "publishers, content creators and tech companies in Europe and beyond". (Porter, 2019) Dette kan bidra til å illustrere nøyaktig hvor vanskelig arbeidet med GDPR kan være, i denne uttalelsen viser Google til virksomheter og enkeltpersoner som livnærer seg på å bli sett på internett. Det Google i all hovedsak bruker dataene sine til er å analysere dem og skreddersy annonsetilbud på bakgrunn av hva den enkelte bruker foretrekker. Noe som kan bli vanskelig å få gjennomført ved strengere regler enn det som allerede foreligger. På lang sikt kan dette påvirke de typene virksomheter som er økonomisk avhengig av å bli sett på internett.

Analyse av resultater

Som beskrevet ovenfor er arbeidet opp mot slike standarder omfattende og ressurskrevende, vi kan se ut ifra våre resultater fra to norske bedrifter at ingen av de undertegnede konkret har arbeidet opp mot ISO sine sikkerhetsstandarder, men heller lent seg på veiledninger fra diverse norske aktører som baserer seg på disse standardene. I begge intervjuene blir det beskrevet at et arbeid opp mot en slik standard blir såpass ressurskrevende at de heller ønsker å lene seg på veiledninger med mindre det kommer et eksternt krav om noe annet. Sett ut ifra den teorien som er fremlagt om de forskjellige veiledningene som ligger tilgjengelig fra norske informasjonssikkerhetsaktører baserer alle de konkrete veiledningene seg på ISO-sine sikkerhetsstandarder, i all hovedsak ISO-27001. Slik som har blitt diskutert tidligere vil bruk av denne standarden i stor grad hjelpe til når det kommer til det å holde seg i tråd med GDPR der standarden beskriver samtlige sikringstiltak som kan knyttes opp mot de kravene som blir satt av GDPR. Vi ønsker å utdype konkrete artikler i GDPR opp mot sikringstiltakene i ISO under neste forskningsspørsmål der vi går mer i dybden på hva dette innebærer. For norske bedrifter er det dermed et veldig godt utgangspunkt med å jobbe opp mot slike veiledninger, som vil sette et grunnlag for informasjonssikkerhet som både sikrer interne forhold i bedriften, med muligheter for å utvide systemene sine til den grad at de er helt i overholdelse med GDPR. Dette kommer også tydelig frem av de resultatene vi fikk fra våre kvalitative intervjuer, begge virksomhetene ble spurt om det forekom en revidering av sikkerhetshåndbok rundt tidspunktet der GDPR tredde i kraft i Norge, men ingen av bedriftene hadde gjort noen konkrete revideringer på dette området. Det skal visstnok nevnes at Virksomhet 1 fulgte dette svaret opp med at hovedfokuset i perioden var å kunne sikre behandlingen av personopplysninger for å vise frem til kunder, klienter og samarbeidspartnere at dette blir tatt på alvor og fra et markedsføringsperspektiv skaper tiltro til virksomheten. Virksomhet 2 hadde heller ingen revidering rundt dette tidspunktet, men i kort tid etter, og basert på de svarene som kommer frem av intervjuet har de også stått på i henhold til arbeidet med GDPR for at rutinene og systemene skal komme i tråd med den nye forordningen.

Tilrettelegging for overholdelse

I selve GDPR forordningen blir det beskrevet et par artikler som er lagt inn for å sikre at bedrifter skal kunne ha gode muligheter til å overholde forordningen uten at det skal foreligge enorme ressurskrevende oppgaver. Her referer vi til artikkel nummer 40 og i noen grad 42. Disse artiklene omhandler etiske retningslinjer for overholdelse, samt sertifisering av et ledelsessystem i henhold til GDPR. Viktige begreper som foreligger under disse artiklene er at forordningen spesifikt tilrettelegger for bedrifter av alle størrelser der både etiske retningslinjer og sertifisering av et system skal kartlegges ut ifra bedriften sitt behov og størrelse. Med andre ord vil ikke en lokal IT-forhandler måtte forholde seg til de samme kravene for overholdelse som en større bedrift som behandler opptil flere millioner forskjellige data subjekter daglig. Med tanke på det som har blitt nevnt tidligere om hvor krevende arbeidet opp mot slike standarder og forordninger er, vil disse få setningene være avgjørende for at GDPR faktisk skal kunne fungere i praksis. Med tanke på sertifisering er dette en prosess og etter eventuell sertifisering et bidrag til å skape et mer troverdig syn på bedriften utenfra. For mindre til mellomstore bedrifter skal det dermed være teoretisk mulig å kunne få en slik sertifisering ettersom kravene vil være noe lavere. Selvfølgelig er det ikke slik at en mindre bedrift kommer seg helt unna forordningen heller, man vil fortsatt være nødt til å følge alle lover om databehandling, oppbevaring, rettigheter til datasubjektene osv., men de to artiklene sikrer for de mindre bedriftene at det arbeidet skal være mer tilrettelagt for dem.

5.2 I hvilken grad hjelper ISO-standardene med å oppfylle kravene i GDPR?

ISO 27001 og 27002 som anerkjente internasjonale sikkerhetsstandarder

ISO 27001 er en anerkjent internasjonal standard for etablering av et ledelsessystem for informasjonssikkerhet som refererer til ISO 27002 for veiledninger til administrasjon av ISMS i organisasjoner. eForvaltningsforskrifter stiller krav til at alle offentlige virksomheter skal ha internkontroll på informasjonssikkerhetsområder som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Det er ikke krav til organisasjoner å ta i bruk ISO 27001 for innføring av ISMS. Fra spørreundersøkelsen kom det frem at både Virksomhet 1 og Virksomhet 2 valgte å bruke veiledninger for internkontroll på informasjonssikkerhetsområder som er utviklet av offentlige aktører Difi, NorSIS, NSM og Datatilsynet og som baserer seg på den anerkjente sikkerhetsstandarden ISO 27001:2013. Derimot for å bevise at organisasjonen har rimelig kontroll på informasjonssikkerhetsområder og organisasjonens aktiva er beskyttet mot skade må ISMS bli sertifisert mot standarden ISO 27001 av sertifiseringspartner. Det kan være kundene som krever sertifisering ved «outsoursing» av sine tjenester eller at organisasjonen selv ønsker en objektiv vurdering av ISMS fra eksterne aktører. I Tabell 8 fra ISO Survey kan en observere en betraktelig økning i antall gyldige sertifikater i Norge i perioden 2006-2017. På verdensbasis ifølge Tabell 9 er det Japan som hadde i 2016 flest organisasjoner som er sertifisert mot standarden ISO 27001, dvs. 8945. Dette tyder på en økt bevissthet til kravet om informasjonssikkerhet i organisasjoner. Tabellene 7 og 10 som er hentet fra Statistisk Sentralbyrå viser forskningsdata for rutiner og tiltak ved administrasjon av informasjonssikkerhet i offentlig sektor i Norge. Ved sammenligning av prosenttallene for de ulike aktivitetene i perioden 2013-2018 kommer det fram at offentlige virksomheter setter mer ressurser til administrasjon av informasjonssikkerhet. I 2018 hadde 81,7% av statlige virksomheter evaluert, fornyet eller forbedret styringssystem for informasjonssikkerhet. Dette kan mulig knyttes til GDPR personvernforordning som trådte i kraft i juni 2018. I 2013 iverksatte 70,1 % av offentlige virksomheter nødvendige sikkerhetstiltak etter nye risikovurderinger. I 2018 økte prosenttallet for samme aktivitet til 89,4%. Prosenten av offentlige virksomheter som opplevde virusangrep og tap av informasjon gikk ned fra 23,0 % i 2016 til 10,6 % i 2018 som vises i Tabell 11 fra SSB. Digitalisering av tjenester for effektivisering av offentlig sektor innebærer at statlige virksomheter leier digital spisskompetanse og tjenester, for eksempel skytjenester, fra private aktører. Konsekvensene av dette er at sikringsbehovet strekker seg utover virksomheten. Digitalisering av tjenester og informasjonsbehandling forutsetter bruk av IKT løsninger i organisasjoner. Tabell 11 fra SSB beskriver IKT-sikkerhetsproblemer som oppstod i offentlige virksomheter i perioden 2016-2018. Organisasjoner står ovenfor stadig nye trusler, risikoer og sårbarhet som må tas hensyn til. Ny sikkerhetslov tredde i kraft 1. januar 2019 i Norge har som formål å sikre Norges sikkerhetsinteresser og skal styrke IKT-sikkerhet i både privat og offentlig sektor. De internasjonale ISO sikkerhetsstandardene med sine prinsipper for sikring av informasjonens konfidensialitet, integritet og tilgjengelighet er en viktig støtte i arbeid for utvikling av IKT-sikkerhet i norske offentlige og private virksomheter. Private bedrifter som leverer tjenester til statlige virksomheter skal forholde seg til denne loven og det skal stilles krav at leverandøren av tjenester skal ha på plass et styringssystem for informasjonssikkerhet i henhold til en anerkjent standard ISO 27001. NSM har utviklet veiledninger som skal hjelpe både private og offentlige aktører å oppfylle kravene i den nye sikkerhetsloven. Veiledningene baserer seg på ISO-27000 serien. Overenstemmelse med ISO sikkerhetsstandardene beskytter organisasjonens informasjon og renomme. I 2018 vant Brønnøysundregister Fidusprisen for sitt store fokus på sikkerhetsarbeid

(NorSIS, 2018). «Brønnøysundregistrenes arbeid baserer seg på ISO 27001/27002-standarden og legger til grunn en risikobasert tilnærming på arbeidet» (ISF, 2019).

GDPR og ISO sikkerhetsstandarder

GDPR er et rammeverk for behandling av personlige opplysninger. Aktørene som opererer i Norge er pålagt å forholde seg til GDPR retningslinjer innenfor informasjonssikkerhet og personvern fra den 20. juni 2018 da personopplysningloven tredde i kraft i Norge.

Et koblingspunkt for ISO 27001 og GDPR er beskyttelse av personlig informasjon. Informasjon i dag regnes som en av de viktigste ressurser sammen med de materielle og menneskelige. Informasjon utsettes for tilsiktede eller utilsiktede trusler, uhell, ulykker eller uaktsomhet som gjør at det alltid foreligger informasonssikkerhetsrisiko som kan medføre brudd på informasjonssikkerhet med uønskede konsekvenser. Tabell 11 fra SSB viser at virusangrep førte til tap av informasjon i 10,6% av statlige virksomheter i 2018 og konsekvenser av angrep «denial of service» førte til sammenbruddet som ga merkbare virkninger i utførelsen av arbeidet i 11,5% av statlige virksomheter i 2018. Det produseres økende mengder av informasjon i organisasjoner som er krevende å kontrollere og beskytte. Tap av organisasjonens informasjon spesielt sensitive opplysninger kan være mer ødeleggende enn tap av fysisk aktiva. Informasjonstapet kan medføre store økonomiske og rettslige konsekvenser og uopprettelig skade på renomme.

ISO 27001 nevner begrepet «aktiva», dvs. noe som har verdi for organisasjonen. Sikringstiltak A.8.1.1 i Tillegg A NS-EN ISO/IEC 27001:2017 handler om å identifisere organisasjonens aktiva, hvor informasjon er definert som aktiva ifølge *Technical Corrigendum 1*, for å kartlegge ansvar for tilstrekkelig beskyttelse av aktiva. NS-EN ISO/IEC 27000:2017 og NS-EN ISO/IEC 27002:2017 sier at informasjon i likhet med alle andre virksomhetsaktiva er verdifull og avgjørende for organisasjonsvirksomhet og skal beskyttes mot ulike risikoer uansett hvilken form den har og hvordan den overføres. Informasjon i organisasjonen kan komme fra flere kilder: den kan oppstå som resultat av forretningsprosesser og kan tilhøre ulike aktører, for eksempel kunder, ansatte eller leverandør. Klassifisering av informasjon er derfor nødvendig for å utarbeide og implementere prosedyrer for å oppnå tilstrekkelig beskyttelse av informasjonen. Artikkelen «*Integration of the GDPR requirements into the requirements of the SR EN ISO/IEC 27001:2018 standard, integration security management system in a software development company»* som er gjennomgått i teoridelen foreslår en av metodene for klassifisering av informasjon for å finne egnede tiltak for tilstrekkelig beskyttelse av personlig informasjonen. Anbefalinger for klassifiseringen kan en finne i Tillegg A i sikringstiltaket A. 8.2.1 i NS-EN ISO/IEC 27001:2017 hvor det står at informasjon skal klassifiseres i henhold til juridiske krav, sensitivitet, verdi eller kritikalitet. Det skal implementeres prosedyrer for håndtering av informasjon i samsvar med organisasjonens ordning for klassifisering. Data om ansatte i casen i artikkelen ble klassifisert som personlig data og derfor skal prosesseres og beskyttes i samsvar med GDPR reguleringen. Et ledelsessystem for informasjonssikkerhet bevarer konfidensialiteten, integriteten og tilgjengeligheten til informasjon ved å benytte en risikostyringsprosess. Risikovurdering er den mest omfattende delen ved implementering av krav fra ISO 27001 og anbefalinger finnes i både *Clause 6 Planlegging* og *Clause 8 Drift*. Artikkelen beskriver hvordan kartlegging og klassifisering av informasjon med videre risikovurdering og kartlegging av trusler basert på ISO 27005 standarden for informasjonssikkerhetsstyring kan avdekke risiko vedrørende ansattes personlige informasjon. Til slutt kommer forfattere med et forslag til hvilke

sikringstiltak fra ISO 27001 standarden kan bli tatt i bruk som utgangspunkt for å respektere GDPR kravene til konfidensialitet når det gjelder personlig data.

I motsetning til GDPR gir ISO 27001 og 27002 klare instruksjoner i form av sikringsmål, sikringstiltak og veiledninger for å oppnå pålitelig informasjonssikkerhet. Tillegg A i NS-EN ISO/IEC 27001 inneholder 114 sikringstiltak som knyttet til fysisk og logisk tiltak, menneskelige ressurser, IT, leverandører og lovfestede forpliktelser. I teoridelen ble det beskrevet følgende sikringstiltak fra Tillegg A i NS-EN ISO/IEC 27001 med veiledninger fra NS-EN ISO/IEC 27002 som er rettet mot beskyttelse av informasjon og personvern:

- klassifisering av informasjon
- beskyttelse av informasjon mot tap
- beskyttelse av virksomhetsaktiva som er tilgjengelig for leverandør
- personvern og beskyttelse av personlig identifiserbar informasjon i samsvar med relevante lover og forskrifter
- hensiktsmessig kontakt med myndigheter

GDPR stiller strenge krav til innsamling, lagring, prosessering, overføring og forvaltning av personopplysninger som brukes i organisasjoner. De nevnte sikringstiltakene med veiledninger for implementering kan brukes som et startpunkt for videre utbygging av informasjonssikkerhetssystem ved implementering av GDPR krav. Senior Security Advisor i Neupart henviser til Datatilsynets anbefalingen til å bygge ut eksisterende informasjonssikkerhet i arbeidet mot implementering av GDPR-krav i organisasjonen. Datatilsynet anbefaler å følge den anerkjente standarden ISO 27001 eller veiledninger som er utviklet av Difi og NSM ved innføring av tekniske og organisatoriske tiltak for å tilfredsstille krav fra personvernforordningen. På intervjuene svarte Virksomhet 1 at det hjalp med eksisterende rutiner, som baserte seg på veiledninger og ISO 27001:2013, for å håndtere og svare på krav fra den nye personvernloven. Virksomhet 2 svarte at «*med utgangspunkt i Difi sin veiledning og standardene var det mindre justeringer som måtte til for å håndtere krav i forbindelse med GDPR. I praksis utgjorde kravene fra GDPR en ekstra dimensjon i eksisterende system*».

Med utgangspunkt i metoden i vitenskapelige artikkelen som er gjengitt i teoridelen, anbefalinger fra Datatilsynet og Neupart, og empiriske materialet som ble innsamlet til prosjektet ble det opprettet en tabell som inneholder en kort beskrivelse av GDPR-artikler og egnede sikringstiltak fra Tillegg A i NS-EN ISO/IEC 27001:2017 med kort forklaring av tiltakene. Denne tabellen har et veiledningsformål og viser anbefalinger for hvordan en organisasjon kan starte arbeid for å møte krav som er beskrevet i GDPR- artikler med utgangspunkt i sikringstiltak fra NS ISO/IEC 27001:2017. Det beskrives ikke veiledninger for sikringstiltakene fra ISO 27002 grunnet den omfattende størrelsen til informasjon.

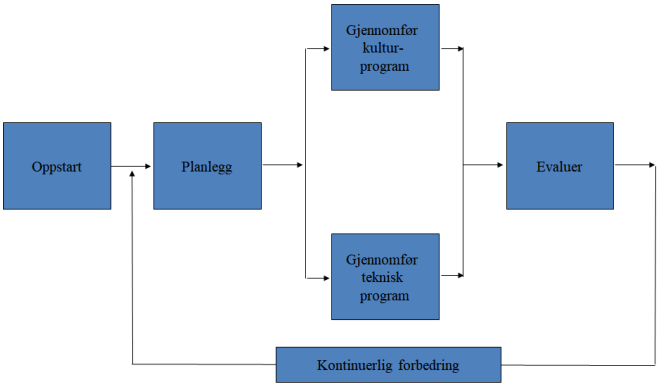
GDPR		ISO 27001	
Artikkel	Beskrivelse	Sikringstiltak	Beskrivelse
12	Kommunikasjon med datasubjektet skal være transparent, tydelig og lett forståelig.	A.8.2.1, A.9.2, A.13.2	Sikringstiltak gir anbefalinger om klassifisering, overføring av informasjon og styring av brukeraksess.
13	Informasjon skal gis til datasubjekt der personlig informasjon innsamles, med formål	A.8.2.1, A 8.2.3, A.13.2	Sikringstiltakene gir anbefalinger om utarbeidelse og implementering av prosedyrer for håndtering, behandling,

			kommunikasjon og overføring av informasjon i samsvar med organisasjonens ordning for klassifisering av informasjon
14	Samme prinsippet som ovenfor der informasjonen ikke har blitt innsamlet enda / eller innsamlet indirekte	A.8.2.1, A 8.2.3, A.13.2	Sikringstiltakene gir anbefalinger om utarbeidelse og implementering av prosedyrer for håndtering, behandling, kommunikasjon og overføring av informasjon i samsvar med organisasjonens ordning for klassifisering av informasjon
15	Datasubjektet skal ha tilgang til informasjon fra kontrollør om hvor deres informasjon lagres, hvem som har tilgang til denne informasjonen, hva den benyttes til og hvor lenge de skal prosessere dette.	A.8.1.1., A.8.2.1, A.6, A.9, A.15	Sikringstiltakene gir anbefalinger om prosedyrer for identifiserings av organisasjons aktiva, tildeling av ansvar for informasjonssikkerhet, tilgang til informasjon basert på klassifiseringsnivå, informasjonssikkerhet i leverandørforhold og styring av leverandørers tjenesteleveranser
16	Datasubjektet skal ha rettigheten til å rette/korrigere deres personlige opplysninger	A.8.2.1, A.8.2.3, A.9.2	Sikringstiltakene gir anbefalinger for identifisering og klassifisering av informasjon, utarbeidelse og implementering av prosedyrer for håndtering, behandling og kommunikasjon av informasjon, styring av brukeraksess til informasjon.
17	Datasubjektet har rettigheten til å bli glemt, eller med andre ord at all personlig informasjon slettes og skal ikke prosesseres lenger	A.8.2, A.6.1.2, A.18.1.4	Sikringstiltak gir anbefalinger om klassifisering av informasjon, merking og håndtering av informasjon basert på klassifisering, personvern og beskyttelse av personlig identifiserbar informasjon skal sikres som påkrevd i relevante lover og forskrifter. Sikringstiltak for å redusere mulighetene for uautorisert eller utilsiktet modifisering eller misbruk av informasjon.
20	Datasubjektet har som rettighet at all data som er innsamlet skal ha muligheten til å bli hentet ut på elektroniske kopier som skal kunne leses av datasubjektet uten å trenge spesifikke teknologier for dette (Artikkel	A.8.3 (spesielt A.8.3.1 «Forvaltning av flytbare medier»)	Sikringstiltak med anbefalinger for håndtering av medier i samsvar med organisasjonens klassifiseringsordninger

	13) og skal kunne levere dette til en ny kontrollør uten hindringer fra tidligere kontrollør		
21	Dersom personlige opplysninger fra datasubjektet blir benyttet av kontrollør til formål som profilering og markedsføring har datasubjektet retten til å motstå	A.8.1.1, A.8.2.1, A.8.2.3, A.9.2, A.18.1.4	Sikringstiltak gir anbefalinger for identifisering av oversikt av informasjon i organisasjonen, klassifisering av informasjon, styring av brukeraksess til informasjon, personvern og beskyttelse av personlig identifiserbar informasjon skal sikres som påkrevd i relevante lover og forskrifter
32	Organisasjoner (kontrollør og prosessor) må implementere de riktige tiltakene for å opprettholde en tilfreds sikkerhetsgrad på opplysningene de lagrer	A 8.2.1, A 8.2.3, A 18.1.4, A 10.1.1, A 10.1.2	Siktingstiltakene fra ISO 27001 som skal bidra til tilstrekkelig klassifisering av informasjon og valg av riktige sikringsmekanismer blant annet kryptografiske løsninger for å oppnå tilfredsstillende nivå for beskyttelse av informasjon og sikre informasjonens integritet, konfidensialitet og tilgjengelighet
40	Diverse aktører anbefales å tegne opp etiske retningslinjer som en veiledning mot å forholde seg til reguleringen	A.6.1, A.7.5, A.12.1	Sikringstiltak for etablering av styringsrammeverk for å initiere og kontrollere implementering og forvaltning av informasjonssikkerhet i organisasjonen, prosedyrer som angir når myndigheter (for eksempel tilsynsmyndigheter) skal kontaktes.
42	Frivillig sertifisering av organisasjonen som varer i perioder på 3 år	A.6.1.1., A.6.1.4, A.18.1.4	Sikringstiltakene som gir anbefalinger for intern organisering av informasjonssikkerhet, kontakt med spesielle interessegrupper, personvern og beskyttelse av personlig identifiserbar informasjon

Tabell 12: Karlegging av krav fra GDPR og sikkerhetstiltak fra ISO 27001

5.3 Dagens modell for innføring av ISMS i bedrifter og veiledningsmateriell fra Difi, NorSIS, Datatilsynet og NSM



Figur 7: Modell for innføring av ISMS. Figuren er hentet fra faget IINI2009 - Informasjonssikkerhet og produktforvaltning 2018

NTNU sin modell er utviklet for fagene IFUD1119, IINI2009 og IBED2003, og viser et styringssystem basert på metoden PDCA/Deminghjulet. Nøkkelordet kan sies å være kontinuerlig forbedring, altså at virksomheten skal ha et levende system, som hele tiden skal oppdateres og gjennomgås

NTNU sin modell sammenlignet med Difi sin modell.

Figur 8: Illustrasjon av aktivitetene i et system for informasjonssikkerhet. Fra Difi «Systematiske aktiviteter.» (https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter)

I Difi sin veiledning rettet mot norske offentlige virksomheter finner man også en anbefaling i et levende kontinuerlig system for informasjonssikkerhet. Ledelsens styring og oppfølging er trukket ut som eget punkt i modellen, noe som står i stil med kravet fra ISO 27001 der det påpekes at ledelsen er ansvarlig for etablering av ISMS, og at roller og ansvar er tildelt og kommunisert i organisasjonen. Videre finner man igjen Difi sine aktiviteter i NTNU sin modell, og omvendt.

Difi-modellens punkt *ledelsens styring og oppfølging* finner man igjen i NTNU-modellen sin *oppstartsfase*, der NTNU forteller at innføringen av et ISMS starter med forankring i ledelsen. Difis risikovurdering og risikohåndtering finner man igjen både i NTNUs *oppstarts-, og planleggingsfase*, og Difis *overvåking og hendelseshåndtering* finnes i NTNUs *evaluer.*

Måling, evaluering og revisjon fra Difi, finnes i *evaluering* fra NTNU, men *revisjon* nevnes ikke direkte i forklaringen om NTNUs modell. Dette kan være et definisjonsspørsmål, da det er mulig å inkludere revisjon under NTNU sitt punkt om evaluering.

Kompetanse og kulturutvikling hos Difi omhandler opplæringer og holdninger hos ledelse og ansatte, og dette finner man igjen i NTNUs *gjennomfør kulturprogram*.

Til slutt i Difis modell finner man *kommunikasjon*. Her finner man kanskje den største forskjellen mot NTNUs modell. NTNU beskriver en kommunikasjon av sikkerhetspolicy og mål og strategi mot ansatte i punktet *oppstart*, men har ikke direkte et fokus på kommunikasjon i de andre fasene sine. Likevel kan det tenkes at kommunikasjon av nye rutiner, målinger, evalueringer og lignende finnes i NTNUs gjennomfør kulturprogram, der ansatte skal inkluderes i sikkerhetssystemet gjennom opplæring, informasjon og medvirkning.

NTNU sin modell sammenlignet mot veiledning fra nettvett.no (NorSis, NSM, og nKom)

Nettvett.no retter seg mot små og mellomstore virksomheter, og har en litt mindre omfattende beskrivelse for ISMS enn Difi. Nettvett har ikke en visuell modell for veiledning, men de sier i likhet med NTNU at arbeidet med et ISMS starter og skal forankres hos ledelsen. Videre sier begge aktører at virksomheten skal definere krav og målsetninger for sikkerhetsarbeidet, og at det skal foreligge en sikkerhetspolicy. Begge nevner også risikohåndtering, og risikoanalyse.

NTNU har en *planleggingsfase* som omhandler sikkerhetsrutiner og risikoanalyse, og kartlegging av arbeidsmåte i forhold til virksomhetens målsetninger. Nettvett nevner at det som omhandler risiko og rutiner skal håndteres i et sikkerhetsregelverk som utarbeides for virksomheten. Virksomhetens status i forhold til målsetninger tas opp i sikkerhetspolicyen som nettvett.no sier skal utarbeides, og denne skal også gås igjennom både periodevis og ved behov.

NTNUs *gjennomfør kultur- og teknisk program* omhandler som tidligere nevnt punkter som prosedyrer, krav og holdninger til og opplæring av ansatte. Nettvett.no tar også for seg disse samme punktene i veiledningen til hvordan å utarbeide virksomhetens *sikkerhetsregelverk*.

Angående punktene *evaluering,* og *kontinuerlig forbedring* fra NTNU så forteller nettvett.no at de tar utgangspunkt i en sikkerhetspolicy for virksomheten, og at denne skal gås gjennom og oppdateres periodevis og ved behov, og at policyen også kan trenge periodevis revisjon, eller revisjon ved større endringer som følge av nye interne/eksterne krav, og ny risiko.

NTNU sin modell sammenlignet mot veiledning fra Datatilsynet.

Datatilsynet fokuserer sin veiledning på håndtering og sikker lagring av personopplysninger. De forenkler internkontrollen/styringssystemet for ISMS til tre elementer, der hele prosessen starter

med *styrende elementer*, hovedsakelig ledelsens beslutninger og føringer for internkontroll.
Dette står i stil til NTNUs to første faser, der ledelsen grovt oppsummert skal utarbeide policy og strategi for sikkerhetsarbeidet, samt skaffe oversikt over nåværende status på sikkerhetsrutiner og arbeidsmetode i forhold til virksomhetens mål.

Datatilsynets andre element i internkontrollen er de *gjennomførende elementer*, hovedsakelig ansattes rutiner mot den enkeltes arbeidssituasjon.
NTNU har delt opp ansattes opplæring og holdninger, og retningslinjer/prosedyrer og krav i to faser, *kulturprogram, og teknisk program*. Selv om vi har unnlatt å beskrive en del detaljer til innhold fra Datatilsynets veiledning, så kan innholdet i disse fasene sies å være sammenlignbart da de begge omhandler retningslinjer, ansattes holdninger og prosedyrer i et ISMS.

Datatilsynets tredje element *kontrollerende elementer*, omhandler det å fange opp avvik fra systemet, og å gjøre periodiske gjennomganger. Videre nevnes risikovurderinger, og innsetting av eventuelle nye tiltak som følge av dette, samt rutiner for kontrollering av at tiltak og rutiner virker etter hensikt, og faktisk blir utført av ansatte.
Dette minner om et levende system som kontinuerlig skal evalueres og forbedres, i likhet med det som beskrives i NTNUs modell. Selv om det altså benyttes andre navn på fasene i de ulike systemene, så er innholdet i dem ganske likt i de forskjellige modellene for ISMS.

NTNU sin modell sammenlignet mot NSM sitt styringshjul for sikkerhet.

Sikkerhetshjulet til NSM består av fem punkter, og det første, *planlegging,* går ut på å kartlegge eksterne sikkerhetskrav til virksomheten, samt status og målsetninger for virksomhetens sikkerhet. Tidligere beskriver NSM viktigheten av god forankring hos ledelsen når man skal utarbeide et system for sikkerhet, og med dette så vil første punkt i sikkerhetshjulet ligne mye på det NTNU beskriver i sine to første faser, *oppstart, og planlegging*.

Andre punkt i NSM sin modell er *sikringsrisikovurdering*. Her kartlegges kritiske verdier, største trusler mot verdier, og største sårbarheter mot verdiene. Dette finner man igjen i *planleggingsfasen* til NTNU, der det kartlegges trusler og risiko mot virksomheten.

Tredje punkt hos NSM forteller at virksomheten må inkludere hvordan man identifiserer, implementerer, beslutter og prioriterer forebyggende tiltak. Svarene på dette kommer ikke i ett bestemt punkt hos NTNU-modellen, men totalt sett gjennom alle punktene. Som følge av ledelsens målsetninger for virksomhetens sikkerhet i *oppstart og planleggingsfasen*, skal det gjennom kartlegging av trusler og risikoanalyse komme tiltak og prosedyrer som skal implementeres i virksomheten, videre skal disse evalueres, og eventuelt forbedres hvis de ikke fungerer etter hensikt.

NSMs fjerde fase, *oppfølging og kontroll*, går blant annet ut på avvikshåndtering, og revidering. NTNU nevner uttrykket avvikshåndtering som et krav i *planleggingsfasen*, men ikke ellers. I *evalueringsfasen* skal hendelser og prosesser og aktiviteter måles og evalueres, og det vil være naturlig at avvikshåndtering vil komme inn under denne fasen.

Femte fase hos NSM skal sikre at relevant informasjon rapporteres kontinuerlig til riktig funksjon på riktig tidspunkt, og at rapportene blir innspill til planleggingsfase, og at ledelsens evalueringer blir grunnlag for nye sikkerhetsmål. NTNU sier i bunn og grunn det samme med fasen *kontinuerlig forbedring*, der nye tiltak planlegges, gjennomføres og måles og brukes på nytt.

Dagens modell satt opp mot våre resultater og tall fra SSB

Slik som vi kan se ut ifra de resultatene vi har hentet inn fra undersøkelser hos to norske bedrifter stilte de seg begge positivt til den modellen vi allerede har for implementering av ISMS i en bedrift. Der virksomhet 1 mente at denne modellen absolutt illustrerer et bilde på hvordan de arbeider mot informasjonssikkerhet i sin drift, men at de ikke konkret har arbeidet opp mot en lignende modell hverken ved innføring eller kontinuerlig forbedring av sitt system. Virksomhet 2 beskrev modellen mer som et slags årshjul for systematisk aktivitet i bedriften, der informasjonssikkerhet går inn under dette som en av aktivitetene. Begge virksomhetene brakte også opp under dette spørsmålet at det de i all hovedsak ser på som en del av internkontrollen ikke var systematisk arbeid opp mot hverken tekniske eller kulturelle programmer, men la heller stor vekt på risikobasert analyse, noe som vil falle inn under evaluerings- og planleggingsdelen i modellen. På spørsmål om sikkerhetshåndbøker internt i bedriften ytret Virksomhet 1 at de ikke konkret hadde en sikkerhetshåndbok de arbeidet mot, men heller retningslinjer for hvordan man skal te seg som ansatt i bedriften. Her ble det gitt en begrunnelse om at slike sikkerhetshåndbøker ofte blir omfattende og at for den type virksomhet både med tanke på sektor og størrelse vil det ikke være realistisk med tanke på ressurser å utforme en slik sikkerhetshåndbok. Virksomhet 2 var noe på den samme siden der de har nedskrevne regler for atferd og sikkerhet, men de ville heller ikke beskrive dette som en sikkerhetshåndbok. Begge bedriftene har dermed i all hovedsak et større fokus på den tekniske siden av implementeringen/kontinuerlig forbedringen av sitt ISMS, der den kulturelle siden kan ansees til at man heller legger mer vekt på kompetent personell til å forholde seg til regler satt av lovverk og internt.

Under spørsmål om implementering og suksessrate ved innføring av ISMS generelt er det ansett som beste praksis at ved oppstart og videre arbeid skal det forekomme skriftlige informasjonssikkerhetspolicyer som skal være forankret i ledelsen. Begge de to virksomhetene som ble intervjuet nevnte at det formelle ansvaret ligger forankret i ledelsen, men at det i all hovedsak blir praktisert at IT-personell er de som jobber tettest opp mot informasjonssikkerhet i virksomhetene. I Tabell 10 viser det til at hele 82,7% av alle statlige virksomheter (fra målgruppen) har en slik informasjonssikkerhetspolicy som er forankret i ledelsen, der 90,9% av disse også har en formelt utnevnt person som er fagansvarlig for informasjonssikkerheten. Etter vurdering av beste praksis kan dette tilsynelatende være en nøkkel til å oppnå suksess med sitt arbeid om informasjonssikkerhet. Der ledelsen og styret alltid vil spille sentrale roller på viktige avgjørelser i henhold til informasjonssikkerhet, men at det formelle arbeidet forekommer hos en fagansvarlig kompetent person som har en større forståelse for emnet. Dette kan vurderes til å være spesielt viktig i en slik periode som har vært nå i forbindelse med GDPR, der en god forståelse av rammeverket til forordningen er essensielt for driften i en hvilken som helst virksomhet som behandler opplysninger om utenforstående personer.

Det vi videre kan se på i henhold til statistikken fra SSB og våre resultater fra virksomhetene er spørsmål om interne revisjoner av ISMS, risikoanalyse og ledelsen sin rolle i det praktiske arbeidet. Slik som kommer frem av resultatene fra virksomhetene blir interne revisjoner gjort på sparket uten noen planlagt konkret dato for revidering hos Virksomhet 1, mens Virksomhet 2 bygger på mange SLA-avtaler med underleverandører at dette sikrer at både revidering av deres systemer, samt de systemene som foreligger hos databehandler forekommer etter det som står beskrevet i SLA-avtalen. En kan se ut ifra disse svarene at det er noe varierende svar som kommer frem av intervjuene, dette kan også sammenlignes mot tallene fra SSB der på spørsmål om årlige interne revisjoner av styringssystemet for informasjonssikkerhet er det kun 59,9% av alle respondentene som faktisk har årlige interne revisjoner. Videre nevnte vi tidligere at begge bedriftene valgte å

vektlegge risikoanalyse som en viktig faktor da de ble presentert med NTNU sin modell for innføring av et ISMS. Dette står også i samsvar på hvordan dette arbeides med i praksis ved tallene fra SSB der gjennomføring av risikovurderinger systematisk og periodisk samsvarer med 76,4% av hvordan respondentene forholder seg til et slikt arbeid. Det vi kan trekke fra kontrastene mellom årlige revisjoner av styringssystemet og risikovurdering er at en høyere prosentandel åpenbart jobber tettere opp mot risikovurdering enn årlige revisjoner, dette gjenspeiles også hos begge virksomhetene som har blitt intervjuet og kan ansees som en del av normal praksis. På spørsmål om ledelsen sin rolle med unntak av selve forankring av policy kommer ledelsen dårlig ut i henhold til tallene, der kun 56,9% har årlig gjennomgang av sitt ISMS, dette kommer også delvis frem av intervjuene, der begge beskriver at selve arbeidet mot informasjonssikkerhet forekommer hos IT-ledelsen, mens policyen er forankret hos ledelsen. Til slutt nevnte vi tidligere at det tilsynelatende kunne vurderes at det tekniske arbeidet overgikk det kulturelle, noe som også vil stå i stil med det som er gitt fra tallene til SSB. Aktiviteter for opplæring og bevisstgjøring av ansatte og ledere gjennomføres én gang per år kun hos 67,8% av virksomhetene, der andel for de tekniske tiltakene som risikovurderinger og policyer blir betraktet av en langt større andel.

5.4 NS-EN ISO/IEC 27001:2017/NS-EN ISO/IEC 27002:2017 og dagens modell for et ledelsessystem for informasjonssikkerhet (ISMS)

PDCA-metode i dagens modell for ISMS og i ISO sikkerhetsstandardene

NS-EN ISO/IEC 27001:2017 og NS-EN ISO/IEC 27002:2017 er de norske gjeldende versjonene av internasjonale standarder ISO/IEC 27001 og ISO/IEC 27002. Standard er et levende dokument og blir stadig endret. Livssyklusen til sikkerhetsstandardene ISO/IEC 27001 og ISO/IEC 27002 er 5 år. I teoridelen er det kartlagt utvikling av ISO/IEC 27001 og ISO/IEC 27002 som tar utgangspunkt i standardene BS 7799-2 og BS 7799-1 tilsvarende som ble opprettet i 1995. Modellen for innføring av et styringssystem for informasjonssikkerhet som vi introduserte i teoridelen ble hentet fra faget IINI2009 - Informasjonssikkerhet og produktforvaltning 2018. Denne modellen skal vurderes opp mot de siste og gjeldende norske versjonene av sikkerhetsstandardene for innføring av et ledelsessystem for informasjonssikkerhet, dvs. NS-EN ISO/IEC 27001:2017 og NS-EN ISO/IEC 27002:2017.

Raske endringer i teknologi og digitalisering av samfunnet øker behovet for sikkerhetsstandarder med kontinuerlig revidering og innføring av korrigeringer i standardene slik at disse kan tilfredsstille dagens utfordringer på informasjonssikkerhet området. Standard er et anvendelig verktøy for utvikling av veiledninger som kan brukes av organisasjoner slik vi observerte dette i besvarelsene i spørreundersøkelsen. Veiledningsmaterieller for å opprette og vedlikeholde systematisk internkontroll[3] på informasjonssikkerhetsområdet som er utviklet av norske sikkerhetsaktører som NoRSIS, NSM og Difi baserer seg på ISO/IEC 27001:2013. Modellen for ISMS bygges på Deminghjulet prinsipper for kontinuerlig forbedring av prosessen: Plan (Planlegg), Do (Utfør), Check (Kontroller), Act (Korriger). PDCA metoden blir introdusert først i BS-7799-2 i 2002 for å tilpasse den til kvalitetsstyringsstandarder ISO 9000 og med dette gjøre ISMS en del av organisasjonens kvalitetssystem. Virksomhet 2 i spørreundersøkelsen jobber med å gjøre deres informasjonssikkerhet en del av eksisterende kvalitetssystem i organisasjonen. Mange av ISO standardene baserer seg på dette styringssystemforbedringskonseptet siden 1950. Standard ISO/IEC 27001:2005(en) introduserer modellen for etablering, drift, kontroll og kontinuerlig forbedring av et

[3] Internkontroll er et begrep som brukes av Difi i veiledningsmateriellet og betyr styringssystem eller ledelsessystem

styringssystem for informasjonssikkerhet ved hjelp av PDCA metoden. Figur 4 illustrerer innføring og drift av ISMS i ISO 27001:2005(en) der input i ISMS er krav og forventninger til informasjonssikkerhet som utarbeides av interessenter i organisasjonen. Etablering, drift, kontroll og forbedring av ISMS foregår som fire-trinns iterativ prosess som tar aldri slutt. Output i ISMS er en styrt informasjonssikkerhet som oppfyller kravene og forventninger til informasjonssikkerhet i organisasjonen. Standard ISO/IEC 27001:2005 gikk gjennom store endringer som resulterte i den nye standarden og den norske versjonen fikk navn NS-EN ISO/IEC 27001:2013. Standarden har fått en ny høynivåstruktur som gjør det enklere å kombinere og integrere den med flere styringssystem standarder som har samme strukturen. Denne høynivåstrukturen ble behold i standarden NS-EN ISO/IEC 27001:2017 hvor endringer som skiller denne standarden fra NS-EN ISO/IEC 27001:2013 introduserer ikke nye krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet. Den ene endringen i *Technical Corrigendum 1 som ble innført i* NS-EN ISO/IEC 27001:2017 sier at informasjon skal betraktes som organisasjons aktiva. Den andre endringer i *Technical Corrigendum 2* oppbygger innholdet i *Subclause 6.1.3* fra setning til punktliste for å legge vekt på innholdet. PDCA prinsippet er ikke obligatorisk mer og det finnes ikke noen referanser til bruk av denne metoden i verken NS-EN ISO/IEC 27001:2013 eller NS-EN ISO/IEC 27001:2017. Organisasjonen som skal innføre ISMS står fritt til å velge angrepsmåte for kontinuerlig forbedring av sikkerhetsstyringssystemet i organisasjonen. I spørreundersøkelsen svarte Virksomhet 2 at de bruker årshjul prinsippet for systematisk forbedring av informasjonssikkerhet i virksomheten. Selv om referanser til PDCA metoden er fjernet i de nye versjonene av sikkerhetsstandardene er dens konsept for kontinuerlig forbedring forankret i krav og anbefalinger for et ledelsessystem for informasjonssikkerhet som er spesifisert i standardene. Både NS-EN ISO/IEC 27001:2017 og NS-EN ISO/IEC 27002:2017 anbefaler gjennomgang av ISMS med planlagte intervaller for å oppnå sikkerhetsmål i organisasjonen. Ifølge NS-EN ISO/IEC 27002:2017 innebærer et ledelsessystem for informasjonssikkerhet planlegging av sikringstiltak som policyer, prosedyrer, organisatoriske strukturer, programvare- og maskinvarefunksjoner. Videre skal sikringstiltakene implementeres, overvåkes, gjennomgås og forbedres der det er nødvendig. Virksomhet 1 svarte at ved brudd eller avvik på retningslinjer foretar de evaluering av informasjonssikkerhet styringssystem for å finne ut hva som gikk galt, og hva som skal gjøres videre. NS-EN ISO/IEC 27001:2017 er risikobasertstandard. For kontinuerlig forbedring av ISMS skal det identifiserer, vurderes, planlegges og iverksettes nye tiltak for å modifisere eller håndtere risiko basert på risikoanalyse som utføres med planlagte intervaller. Forbedringssyklusen starter ved gjennomføring av korrigerende tiltak basert på indentifisert sårbarhet og risiko. PDCA prinsippet kan også identifiseres i oppbyggingen av NS-EN ISO/IEC 27001:2017. Standarden består av 14 *Clauses* hvor *Planlegging, Støtte/Drift, Prestasjonsevaluering* og *Forbedring* kan refereres til Planlegg, Utfør, Kontroller og Korriger fasene i Deminghjulet. I *Planlegging Clause* eller delen skal organisasjonen planlegge tiltak for å håndtere risikoene og muligheter som er nødvendig å håndtere, gjennomføre risikovurdering av informasjonssikkerhet for å identifisere informasjonssikkerhetsrisikoene, definere og benytte en prosess for håndtering av risikoene og fastsette informasjonssikkerhetsmål. I *Drift* delen skal organisasjon implementere tiltakene som er bestemt i Planlegging delen. I *Støtte* delen skal utføres det aktiviteter som rettet mot menneskelige ressurser i organisasjonen som baserer seg på risikoanalysen for informasjonssikkerhet. *Prestasjonsevaluering* omfatter overvåking, måling, analyse og evaluering av informasjonssikkerhetsprosesser og sikringstiltak. *Forbedring* delen innbefatter kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet ved å reagere på avvik, vurdere avvik og håndtere den med implementering av egnede korrigerende tiltak.

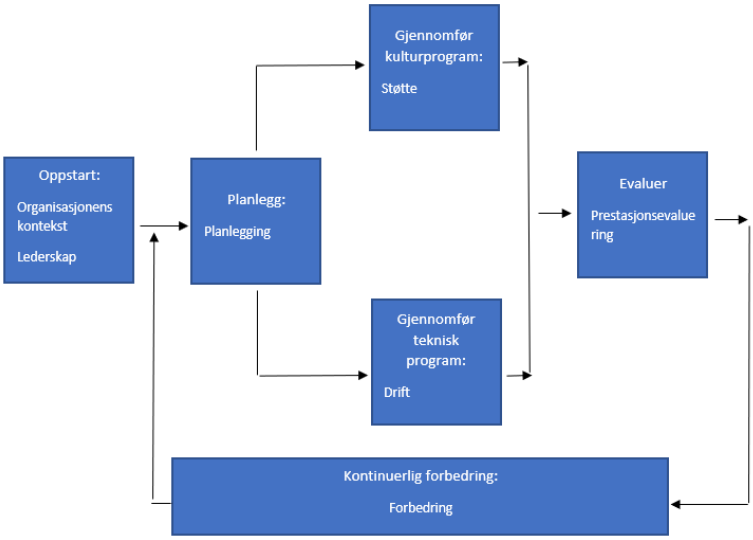
Kartlegging av hovedkrav i NS-EN ISO/IEC 27001:2017 og faser i dagens modell for ISMS

Modellen for ISMS som beskrives i denne oppgaven består av seks faser: Oppstart, Planlegg, Gjennomfør kulturprogram, Gjennomfør teknisk program, Evaluer og Kontinuerlig forbedring. NS-EN ISO/IEC 27001:2017 introduserer hovedkravene til etablering, implementering, vurdering og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet i 7 punkter (*Clause 4-10)*. Disse kravene er nødvendige hvis organisasjonen vil være i samsvar med standarden. Tabell 12 kartlegger hovedaktiviteter i kravene i NS-EN ISO/IEC 27001:2017 og i fasene i modellen for ISMS som er beskrevet i teoridelen.

NS-EN ISO/IEC 27001:2017	Modell for ISMS
Clause 4. Organisasjonens kontekst: Omfang av ISMS Interne og eksterne forhold Kravene og forventninger fra interessepartnere	*Oppstart fase:* Aktører Lover og regler Forankring i ledelsen Informasjonssikkerhetspolicy (mål og strategi)
Clause 5. Lederskap: Ledelsens forpliktelser, roller og myndighet Informasjonssikkerhetspolicy Informasjonssikkerhetsmål	
Clause 6. Planlegging: Risikovurdering og håndtering av informasjonssikkerhetsrisikoene	*Planlegg fase:* Trusselbilde Risikoanalyse
Clause 7. Støtte Kommunikasjon av policy til ansatte Kompetansebehov Bevissthet Engasjement Opplæring	*Gjennomfør kulturprogram fase:* Kommunikasjon av policy til ansatte Bevissthet Engasjement Opplæring
Clause 8. Drift: Implementering av sikringstiltak basert på risikovurdering med veiledninger fra ISO 27002	*Gjennomfør teknisk program fase:* Implementering av sikringstiltak vha. ISO 27002 Beredskapsplaner og drift Fysiske sikringstiltak Beskyttelse av PC, nettverk Kryptering
Clause 9. Prestasjonsevaluering: Overvåke, måle og evaluere et ledelsessystem for informasjonssikkerhet	*Evaluer fase:* Måling og evaluering av prosesser og aktiviteter innenfor ISMS
Clause 10. Forbedring: Håndtering av avvik med korrigerende tiltak og kontinuerlig forbedring	*Kontinuerlig forbedring fase:* Oppfølging og kontinuerlig forbedring

Tabell 13: Kartlegging av krav fra NS-EN ISO/IEC 27001:2017 og faser i modellen for ISMS

Ved å sammenligne aktivitetene i tabellen vil hovedkravene passe i ulike faser i modellen på følgende måte:



Figur 9: Modell for ISMS med hovedkrav fra NS-EN ISO/IEC 27001:2017

Vi ser at modellen gjenspeiler rekkefølgen av hovedkravene i standarden og aktivitetene som inngår i hovedkravene. *Organisasjonens kontekst* og *Lederskap* ble slått sammen og inngår i Oppstart fasen med utgangspunkt i aktiviteter som er felles for kravene og fasen. *Clauses Planlegging*, *Støtte*, *Drift*, *Prestasjonsevaluering og Forbedring* utgjør en kjerne i ISMS akkurat som tilsvarende faser Planlegg, Gjennomfør kulturprogram og teknisk program, Evaluer og Kontinuerlig forbedring i modellen. *Clause Forbedring* beskriver prinsipper for både forbedring og kontinuerlig forbedring av ISMS i underpunktet *10.2 Kontinuerlig forbedring* i standarden og derfor passer i Kontinuerlig forbedring fasen. Forbedringsprosessen starter ved å håndtere avvik og planlegge nye tiltak som skal bidra til ønskede endringer i ISMS, dvs. at *Clause Planlegging* starter en nye forbedringssyklus på samme måte som Planlegg fasen i modellen.

6.0 Konklusjon

Den konklusjonen vi kan trekke i henhold til GDPR er at denne nye forordningen stiller langt strengere krav til informasjonssikkerhet enn det man har vært vant med tidligere. Dette leder blant annet til at virksomheter og bedrifter er nødt til å sette et enda større fokus på de tekniske tiltakene i bedriften. Sett fra et perspektiv av et ledelsessystem vil ikke GDPR direkte påvirke de modellene for innføring vi har i dag, men slik som ble beskrevet i vår tabell for kartlegging av krav fra GDPR og sikringstiltak fra ISO-27k vil arbeidet opp mot slike standarder gi en større verdi for bedriften med tanke på å holde seg i tråd med de kravene som stilles. For å illustrere de komplikasjonene GDPR har skapt i praktisk forstand har vi benyttet oss av teknologigiganten Google som et eksempel, som har vært mye omtalt i medier i perioden både før og etter forordningen ble implementert. Når en ser på de vanskelighetene en av verdens mest ressurssterke bedrifter har fått erfare, gir dette en konkret pekepinn på at de kravene som stilles av denne forordningen har vært en komplisert oppgave å tilfredsstille. Vi drøftet også noe rundt hvordan dette påvirker bedrifter av mindre størrelse som ikke har de samme mulighetene til å legge ned store mengder med ressurser for å sikre en total overholdelse av forordningen, og hvordan utvalgte artikler skal være med på å hjelpe de som sitter i denne situasjonen. Dette er selvfølgelig noe til hjelp for de som faller inn under denne kategorien, mens realiteten vil være at dersom det ikke er på plass vil det kunne lede til store økonomiske konsekvenser for slike bedrifter av mindre størrelse. Det er dermed viktigere enn noensinne å legge ned et godt og systematisk arbeid med informasjonssikkerheten for å sikre overholdelse av GDPR.

SSB og ISO statistikken, veiledninger fra nasjonale sikkerhetsaktører, Brønnøysundregister sitt arbeid med informasjonssikkerhet og resultatene fra intervjuene som vi drøftet i diskusjonsdelen befester teorien om at sikkerhetsstandarder ISO 27001 og ISO 27002 er anerkjent i både Norge og hele verden og er til stor støtte ved oppretting av internkontroll på informasjonssikkerhetsområder i organisasjoner. Sertifisering mot ISO 27001 gjør det mulig for organisasjoner uansett størrelsen å ha et gyldig bevis på tilstrekkelig kontroll på informasjonssikkerhetsområdene og at de oppfyller lovfestete krav for informasjonssikkerhet. Tallene for sertifiserte styringssystemer for informasjonssikkerhet mot ISO 27001 økte betraktelig i perioden 2006-2017, dvs. fra 1064 gyldige sertifikater i 2006 til 14605 gyldige sertifikater i 2017 ifølge Tabell 15 som finnes i vedlegget. Dette kan oppfattes som en økt bevissthet rundt informasjonssikkerhet og organisasjoner er gradvis opptatt av å implementere pålitelige løsninger for å bygge et robust informasjonssikkerhetssystem. Sertifisering kan være et resultat av ulike hendelser, for eksempel krav fra kunder eller interne bestemmelser for å skape konkurransefortrinn, opprette og beholde kundenes tillit eller nå nye markeder. Begge respondentene som deltok i prosjektets spørreundersøkelse kommer fra offentlig sektor og i intervjuene svarte Virksomhet 1 at ved innkjøp av tjenester vil de gjerne velge leverandører som er sertifiserte mot ISO 27001. Virksomhet 2 svarte at hvis de skulle få systemet sitt sertifisert, ville dette vært på bakgrunn av et eksternt krav. Den nye sikkerhetsloven som trådte i kraft 1. januar 2019 i Norge innførte krav til internkontroll på informasjonssikkerhetsområdene i private bedrifter som leverer tjenester til offentlige aktører. I forbindelse med denne loven utviklet NSM en veiledning som baserer seg på ISO 27001 standard. Strengere krav til informasjonssikkerhet kan bidra til at flere vil benytte ISO sikkerhetsstandardene for oppretting av informasjonssikkerhet og vil vurdere og satse på sertifisering av sitt ISMS. Videre ble det vurdert hvordan sikringstiltak fra ISO 27001 med veiledninger fra ISO 27002 kan hjelpe med å oppnå etterlevelse med GDPR personvernforordningen. Her står ISO sikkerhetsstandardene igjen til stor hjelp med sine prinsipper for risikobaserte tilnærming og kontinuerlig forbedring av informasjonssikkerhet. Både ISO 27001 og GDPR vil forbedre informasjonssikkerhet og felles området for disse standardene er sikring av konfidensialitet, integritet og tilgjengelighet ved behandling av personlig informasjon. Datatilsynet, Senior Security Advisor i Neupart, artikkelen med case for implementering av GDPR krav i bedriften

anbefaler å ta i bruk ISO sikkerhetsstandarder og veiledninger fra Difi og NSM ved innføring av tekniske og organisatoriske tiltak for å tilfredsstille krav fra personvernforordningen. Både Virksomhet 1 og Virksomhet 2 påstår at deres internkontroll som baserte seg på veiledninger fra sikkerhetsaktører og derfor på ISO 27001:2013 var til stor hjelp med implementering av GDPR krav. Sikringstiltak med veiledninger fra ISO 27001 og ISO 27002 som er retter mot beskyttelse av informasjon og personvern kan være et startpunkt for å forenkle prosessen for implementering av personvernforordningen. Hovedaktiviteter som kartlegging av informasjon i organisasjonen, klassifisering av informasjon, behandling av personlig identifiserbar informasjon, leverandørforhold, beskyttelse mot tap og kontakt med tilsynsmyndigheter ved informasjonssikkerhetsbrudd kan brukes som generelle anbefalende prinsipper i arbeid mot GDPR krav. GDPR beskriver hva som skal gjøres i sine artikler men gir ikke veiledninger for tekniske eller organisatoriske tiltak, dvs. hvor en organisasjon skal starte og hvordan det skal gjøres slik at organisasjonen bli i samsvar med GDPR. Derfor i Tabell 10 som kartlegger GDPR artikler og ISO 27001 sikringstiltak foreslår vi mer spesifikke sikringstiltak (både tekniske og organisatoriske) som kan hjelpe med å imøtekomme kravene i artiklene. For eksempel, for implementering av artikkel 15 som krever at «*datasubjektet skal ha tilgang til informasjon fra kontrollør om hvor deres informasjon lagres, hvem som har tilgang til denne informasjonen, hva den benyttes til og hvor lenge de skal prosessere dette*» kan en starte med å identifisere informasjon som brukes i organisasjonen, klassifisere den, tildele ansvar for informasjonssikkerhet og tilgang til informasjon (brukeraksess) basert på klassifiseringsnivå, utarbeide retningslinjer og prosedyrer for informasjonssikkerhet i leverandørforhold og styring av leverandørers tjenesteleveranser. Det å ha disse tiltakene implementert garanterer ikke samsvar med GDPR men danner et godt grunnlag for videre arbeid mot personvernforordningen.

Fra de resultatene vi har hentet inn sammenlignet med dagens modell for innføring av ISMS og statistikker fra SSB kan vi konkludere med at det finnes en rød tråd i henhold til hva som ansees som beste praksis. Et av emnene som blir betraktet som en nøkkelfaktor for suksess med arbeidet om ISMS er at virksomheten skal ha sikkerhetspolicyer som er forankret hos ledelsen, og vi kan se både ut ifra våre resultater samt statistikker at dette er tilfellet for de fleste virksomheter. Videre under dette kan vi se at risikovurderinger og policyer er det som blir vektlagt mest hos virksomheter, noe som i stor grad samsvarer med de resultatene vi har hentet inn fra intervjuer. Dette peker i den retningen at slike tekniske tiltak blir mer vektlagt enn de kulturelle tiltakene som opplæring, sikkerhetshåndbøker og revidering av disse. Det som kan trekkes ut ifra denne informasjonen er at nå som det foreligger langt strengere krav til systemer og behandling av informasjon enn tidligere vil slike tekniske tiltak være nødt til å være på plass som et grunnlag for arbeid i alle virksomheter som behandler slike opplysninger. Begge virksomhetene ble presentert med dagens modell for innføring av ISMS og anser denne til å stemme godt overens med hvordan arbeidet blir gjort i deres respektive virksomhet. Det kan dermed konkluderes at denne modellen samsvarer godt med hvordan arbeidet blir utført i praksis, spesielt med tanke på at ingen av virksomhetene konkret hadde arbeidet opp mot en slik modell, men allikevel kunne gjense sine rutiner for informasjonssikkerhet i denne modellen.

Når man sammenligner NTNU-modellen/veiledningen for innføring av ISMS mot veiledningene fra nasjonale aktører, så finner man forskjellige navn på faser, og forskjellig rekkefølge på fasene ut fra hvilken veiledning man ser på. Men, ser man på veiledningene som en helhet, så ser man at man finner igjen de samme aktivitetene under samme fase eller en forskjellig fase, hos alle aktørene. Det som skiller veiledningene er omfanget og beskrivelsene i detalj av de forskjellige aktivitetene under fasene.

Alle veiledningene baserer seg på et prinsipp om kontinuerlig forbedring, der man skal måle, evaluere og forbedre, og alle veiledninger presiserer viktigheten av god forankring hos ledelsen når man skal igangsette et system for informasjonssikkerhet. Man kan se noen forskjeller i veiledningene, som at datatilsynet spisser seg litt mot håndtering av personopplysninger, og at nettvett.no med sin forenklede veiledning retter seg mot små og mellomstore bedrifter. Likevel inneholder de samme aktiviteter, og det blir opp til hver enkelt virksomhet å vurdere omfanget av sitt arbeid med informasjonssikkerhet, og at gjeldende krav og regelverk blir overholdt.

PDCA-metode er et utbredd konsept for kontinuerlig forbedring av prosesser, produkter og tjenester og er innført i de fleste ISO-standarder siden 1950. Vi undersøkte og sammenlignet utvikling av ISO 27001 standard som introduserte PDCA metoden først i 2002. ISO/IEC 27001:2005 introduserer og beskriver en modell for etablering, implementering, drift, kontroll og kontinuerlig forbedring av ISMS ved hjelp av PDCA metoden. I 2013 kom det en ny revidert ISO 27001 hvor referanser til PDCA metoden ble fjernet. Selv om det er ikke noen referanser til PDCA i NS-EN ISO/IEC 27001:2017 er metodens tilnærming for kontinuerlig forbedring forankret i standardens oppbygging og krav og anbefalinger for et ledelsessystem for informasjonssikkerhet.

Sammenligningen av hovedkravene fra standard NS-EN ISO/IEC 27001:2017 og fasene fra modellen for ISMS viser at standarden og modellen inneholder samme aktiviteter som utføres i samme rekkefølgen ved etablering, implementering, drift, vedlikehold og kontinuerlig forbedring av ISMS. Vi viste ved hjelp av Tabell 13 og Figur 9 at hovedkravene som er inndelt i *Clauses* i standarden tilsvarer fasene i modellen for ISMS. Denne modellen for ISMS som baserer seg på PDCA-prinsippet er i samsvar med nåværende hovedkravene for etablering, implementering, vedlikehold og kontinuerlig forbedring av et ISMS som er beskrevet i standarden NS-EN ISO/IEC 27001:2017 som også baserer seg på PDCA-prinsippet. Standard NS-EN ISO/IEC 27002:2017 har som formål å gi veiledninger med anbefalinger når organisasjon skal velge sikringstiltak som en del av prosessen med å implementere et ledelsessystem for informasjonssikkerhet basert på NS-EN ISO/IEC 27001:2017. Den brukes ikke dirkete til etablering av ISMS men fortsatt beskriver tilnærming til administrasjon av en ISMS, dvs. at sikringstiltak skal etableres, implementeres overvåkes, gjennomgås og forbedres med planlagte intervaller eller når det blir nødvendig.

Som en konklusjon for NTNU sin modell kan man si at den står i stil med dagens veiledninger og standarder, og at den dermed også vil hjelpe i forbindelse med krav ut fra GDPR. Vi kan vurdere de funnene vi har konkludert med til å en lang levetid. Dette ved det grunnlaget at modellen vi har vurdert er såpass standardisert ut ifra hva som ansees som beste praksis, samt at store endringer i henhold til ISO-standardene i all hovedsak kommer til å gå ut over sikringstiltakene og ikke det fundamentale ved en implementeringsprosess. På toppen av dette vil også GDPR være en forordning som kommer til å eksistere fremover og påvirke denne prosessen gjennom de konklusjonene vi har trukket.

Referanser

Bowcott, O. (2019, Januar 10). *The Guardian* . Retrieved from 'Right to be forgotten' by Google should apply only in EU, says court opinion: https://www.theguardian.com/technology/2019/jan/10/right-to-be-forgotten-by-google-should-apply-only-in-eu-says-court

BSI. (2013, Oktober). *BS EN ISO/IEC 27001:2017*. Retrieved from https://shop.bsigroup.com/ProductDetail/?pid=000000000030347472

BSI. (2016, april). *ISO 9001:2015 Your implementation guide.* Retrieved from https://www.bsigroup.com/LocalFiles/EN-AU/Whitepapers/ISO%209001%20PDFs%20(April%202016)/ISO%209001%20Implementation%20Guide.pdf

BSI. (2019). *BS ISO/IEC 27001:2005/BS 7799-2:2005*. Retrieved from https://shop.bsigroup.com/ProductDetail/?pid=000000000030126472

BSI. (n.d.). *Detailed Concepts of the Plan Do Check Act Process*. Retrieved from https://bsi.learncentral.com/shop/Course.aspx?id=12858&name=Detailed+Concepts+of+the+Plan+Do+Check+Act+Process

Datatilsynet. (2018, juni 19). *Veileder. Internkontroll og informasjonssikkerhet*. Retrieved from https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/?print=true

Datatilsynet. (2019, April 26). *Hvordan gjennomføre internkontroll i praksis*. Retrieved from Nettsted for Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/hvordan-gjennomfore-internkontroll-i-praksis/

Datatilsynet. (2019, Mars 11). *Lover og regler - Om personopplysningsloven*. Retrieved from Nettsted for Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/om-personopplysningsloven-og-nar-den-gjelder/

Datatilsynet. (2019, Mars 10). *Om oss, oppgaver*. Retrieved from Nettsted for Datatilsynet: https://www.datatilsynet.no/om-datatilsynet/oppgaver

Datatilsynet. (2019, Mars 11). *Veileder - Internkontroll og informasjonssikkerhet*. Retrieved from Nettsted for Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/

Difi. (2019, April 20). *Internkontroll, veileder for toppledere*. Retrieved from Nettsted til direktoratet for forvaltning og IKT.: https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/for_toppledere_-_internkontroll_informasjonssikkerhet.pdf

Difi. (2019, Mars 10). *internkontroll-stystringssystem-ledelsessyem-informasjonssikkerhet*. Retrieved from Webområde for Difi: https://www.difi.no/referansekatalogen/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet

Difi. (2019, April 29). *Systematiske aktiviteter.* Retrieved from https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter

Difi. (2019, April 20). *Veileder for internkontroll, grunnleggende innføring*. Retrieved from Nettsted for direktoratet for forvaltning og IKT: https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/grunnleggende_innforing_-_internkontroll_informasjonssikkerhet.pdf

Difi. (2019, April 20). *Veiledning til internkontroll, grunnleggende begreper*. Retrieved from Nettsted for direktoratet for forvaltning og IKT : https://internkontroll-infosikkerhet.difi.no/sites/sikkerhet/files/grunnleggende_begreper_-_internkontroll_informasjonssikkerhet.pdf

Difi. (n.d.). *Hva sier ISO/IEC 27001?* Retrieved from https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001

Difi. (n.d.). *Internkontroll i praksis - informasjonssikkerhet*. Retrieved from https://internkontroll-infosikkerhet.difi.no/

Difi. (n.d.). *Krav og anbefalinger*. Retrieved from https://internkontroll-infosikkerhet.difi.no/ledelsens-styring-og-oppfolging/godt-vite/krav-og-anbefalinger

Difi. (n.d.). *Ledelsens styring og oppfølging*. Retrieved from https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter/ledelsens-styring-og-oppfolging

Difi. (n.d.). *Regelverkskrav*. Retrieved from https://internkontroll-infosikkerhet.difi.no/regelverkskrav

Direktoratet for forvaltning og IKT. (2019, Mars 10). *Om difi*. Retrieved from Hjemmeside for Difi: https://www.difi.no/om-difi

GAŞPAR, M. L., & POPESCU, S. G. (2018, sep). INTEGRATION OF THE GDPR REQUIREMENTS INTO THE REQUIREMENTS OF THE SR EN ISO/IEC 27001: 2018 STANDARD, INTEGRATION SECURITY MANAGEMENT SYSTEM IN A SOFTWARE DEVELOPMENT COMPANY. *ACTA TECHNICA NAPOCENSIS, Series: Applied Mathematics, Mechanics, and Engineering*(61). Retrieved 2019, from https://atna-mam.utcluj.ro/index.php/Acta/article/view/1054

Hjertø, G., & Klefstad, B. (2018). Informasjonssikkerhetsstyring. *Leksjon 01-Informasjonssikkerhetsstyring*. Trondheim, Trøndelag, Norge: NTNU.

Hjertø, G., & Klefstad, B. (2018). Informasjonssikkerhetsstyring. *L12 - Sikkerhetspolicy – Oppfølging og kontinuerlig forbedring*. Trondheim, Trøndelag, Norge: NTNU.

ISF. (2019, april 10). Retrieved from https://isf.no/medlemsmoter1/2019/varmote-2019

ISO. (2005). *Online Browsing Platform. ISO/IEC 27001:2005*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-1:v1:en

ISO. (2014). *ISO/IEC 27001:2013/Cor.1:2014(en)*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:cor:1:v1:en

ISO. (2014). *ISO/IEC 27002:2013/Cor.1:2014(en)*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:cor:1:v1:en

ISO. (2015). *ISO/IEC 27001:2013/Cor.2:2015(en)*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:cor:2:v1:en

ISO. (2015). *ISO/IEC 27002:2013/Cor.2:2015(en)*. Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:cor:2:v1:en

ISO. (n.d.). *9. ISO Survey of certifications to management system standards - Full results*. Retrieved from https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

ISO. (n.d.). *ISO/IEC WD 27002*. Retrieved from https://www.iso.org/standard/75652.html

Mangfold. (n.d.). *Mangfold. Sammendrag kapittel 2*. Retrieved from https://mangfold.cappelendamm.no/vgsamf/tekst.html?tid=1006552

Nasjonal kommunikasjonsmyndighet. (2019, Mars 10). *Om nkom*. Retrieved from Nettsted for nasjonal kommunikasjonsmyndighet: https://www.nkom.no/om-nkom

Nasjonal Sikkerhetsmyndighet. (2019, Mars 23). *Om NSM*. Retrieved from Nettsted for NSM: https://www.nsm.stat.no/om-nsm/

NEK. (n.d.). *Kort om NEK*. Retrieved from https://www.nek.no/om-nek/kort-om-nek/

Nettvett.no. (2019, Mars 10). *Håndbok for informasjonssikkerhet* . Retrieved from nettvett.no: https://nettvett.no/handbok-for-informasjonssikkerhet/

Nettvett.no. (2019, Februar 28). *Informasjonssikkerhetspolicy*. Retrieved from https://nettvett.no/informasjonssikkerhetspolicy/

Nettvett.no. (2019, Februar 28). *Sikkerhetsledelse*. Retrieved from Nettvett: https://nettvett.no/sikkerhetsledelse/

Neupart. (2014, April 04). *Has 'Plan-Do-Check-Act´disappeared in the new ISO 27001?* . Retrieved from https://www.neupart.com/good-enough-it-risk-management/has-plan-do-check-actdisappeared-in-new

Neupart. (2017, september 12). *GDPR Samsvar: Du skal ikke bygge nytt – du skal bygge ut*. Retrieved from https://www.neupart.com/no/blog/samsvar-med-gdpr-du-skal-ikke-bygge-nytt-du-skal-bygge-ut

Nkom. (2019, Mars 11). *Om oss: nettsted for nasjonal kommunikasjonsmyndighet*. Retrieved from Nasjonal kommunikasjonsmyndighet: https://www.nkom.no/om-nkom

NorSIS. (2018, september 27). *Brønnøysundregistrene vant Fidusprisen 2018*. Retrieved from https://norsis.no/bronnoysundregistrene-vant-fidusprisen-2018/

Norsk Psykolog Forening. (2018, mai 25). *Norm for informasjonssikkerhet* . Retrieved from https://www.psykologforeningen.no/medlem/personvern/norm-for-informasjonssikkerhet

NSM. (2019, April 29). Retrieved from Om sikkerhetsstyring og Sikkerhetskultur: https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/

NSM. (2019, April 10). *Aktuelt: nettsted for Nasjonal Sikkerhetsmyndighet*. Retrieved from Nettsted for Nasjonal Sikkerhetsmyndighet: https://www.nsm.stat.no/aktuelt/risiko-2019/

NSM. (2019, mars 21). *Sikkerhetskonferansen 2019*. Retrieved from Sikkerhetskonferansen 2019 Program: https://www.nsm.stat.no/sikkerhetskonferansen/sikkerhetskonferansen2019/program/

NSM. (2019, Mars 23). *Veiledninger*. Retrieved from Nettsted for NSM: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf

NTB. (2018, Juli 31). *Tek*. Retrieved from Dobbelt så mange meldinger om avvik og fire ganger så stor trafikk på nettsidene: https://www.tek.no/artikler/dobbelt-sa-mange-meldinger-om-avvik-og-fire-ganger-sa-stor-trafikk-pa-nettsidene/442743

NTNU. (n.d.). *Standarder*. Retrieved from https://innsida.ntnu.no/wiki/-/wiki/Norsk/Standarder

Porter, J. (2019, January 21). *The Verge*. Retrieved from Google fined €50 million for GDPR violation in France: https://www.theverge.com/2019/1/21/18191591/google-gdpr-fine-50-million-euros-data-consent-cnil

Regjeringen.no. (2019, februar 12). *Digital sikkerhet*. Retrieved from https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/digital-sikkerhet/id2340011/

Ringdal, K. (2001). *Enhet og mangfold. Samfunnsvitenskapelig forskning og kvantitativ metode* (1. utgave, 2. opplag ed.). Bergen: Fagbokforlaget.

Sjølstad, T., Høie, T., Gulbrandsen, R., & Daler, T. (2010). *Håndbok i datasikkerhet : Informasjonsteknologi og risikostyring* (3 ed.). Trondheim: Tapir akademisk.

Sokovic, M., Pavletic, D., & Pipan, K. K. (2010, november). Quality improvement methodologies–PDCA cycle, RADAR matrix, DMAIC and DFSS. *Journal of achievements in materials*(43), pp. 476-483. Retrieved from http://pdfs.semanticscholar.org/e348/8a24ab1197670544b4e08dc6173f396eada9.pdf

SSB. (2018, mai 29). *Bruk av IKT i offentlig sektor. 10852: Tiltak/rutiner ved administrasjon av IKT-sikkerheten i statlige virksomheter (prosent), etter sysselsettingsgruppe, statistikkvariabel og år*. Retrieved from http://www.ssb.no/statbank/sq/10018031/

SSB. (2018). *Bruk av IKT i offentlig sektor. 12041: Tiltak/rutiner ved administrasjon av IKT-sikkerheten (prosent), etter forvaltningsnivå, antall innbyggere, statistikkvariabel og år*. Retrieved from http://www.ssb.no/statbank/sq/10018006/

SSB. (2018, mai 29). *Bruk av IKT i offentlig sektor. 12042: Tiltak som del av internkontroll for informasjonssikkerhet (prosent), etter forvaltningsnivå, statistikkvariabel og år*. Retrieved from http://www.ssb.no/statbank/sq/10017378/

SSB. (2018, mai 29). *Bruk av IKT i offentlig sektor. Andel som har opplevd IKT-sikkerhetsproblemer.* Retrieved from https://www.ssb.no/iktbruks

Standard Norge. (2013, november 01). *NS-ISO/IEC 27001:2005*. Retrieved from https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=529528

Standard Norge. (2017, mai). *Norsk Standard NS-EN ISO/IEC 27000:2017.* Retrieved from https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=942502

Standard Norge. (2017). *Norsk Standard NS-EN ISO/IEC 27001:2017.* Retrieved from http://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925900

Standard Norge. (2017, mai). *Norsk Standard NS-EN ISO/IEC 27002:2017.* Retrieved from https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=925901

Standard Norge. (2017). *NS-EN ISO/IEC 27002:2017*. Retrieved from https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=913018

Standard Norge. (2017). *NS-ISO/IEC 27001:2013*. Retrieved from https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=767576

Standard Norge. (2017, mai 01). *NS-ISO/IEC 27001:2013*. Retrieved from https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=665170

Standard Norge. (2019, februar 22). *Ny sikkerhetslov stiller strengere krav til IT-systemer* . Retrieved from https://www.standard.no/nyheter/nyhetsarkiv/ikt/nyheter-2019/ny-sikkerhetslov-stiller-strengere-krav-til-it-systemer-/

Standard Norge. (2019, februar 27). *Standard Norge*. Retrieved from https://www.standard.no/toppvalg/om-oss/standard-norge/

Tek.no. (2012, juni 04). *Så mye er lagret om deg*. Retrieved from https://www.tek.no/artikler/sa-mye-er-lagret-om-deg/109793

The European Parliament and The Council of the European Union. (2016). Regulation (EU) 2016/679. *General Data Protection Regulation*, 88.

UKAS. (2017, mai 11). *Technical Bulletin – BS EN ISO 27001 issued* . Retrieved from https://www.ukas.com/news/technical-bulletin-bs-en-iso-27001-issued/

Van Bon, J. (2007). *Foundations of ITIL V3.* Van Haren Publishing.

Wikipedia. (2017, september 27). *International Electrotechnical Commission*. Retrieved from https://no.wikipedia.org/wiki/International_Electrotechnical_Commission

Wikipedia. (2018, januar 16). *BS 7799*. Retrieved from https://en.wikipedia.org/wiki/BS_7799

Wikipedia. (2018, oktober 12). *ISO*. Retrieved from https://no.wikipedia.org/wiki/ISO

Wikipedia. (2018, juli 3). *Standard*. Retrieved from https://no.wikipedia.org/wiki/Standard

Wikipedia. (2019, April 29). Retrieved from Datatilsynet (Norge): https://no.wikipedia.org/wiki/Datatilsynet_(Norge)

Wikipedia. (2019, April 29). Retrieved from Om direktoratet for forvaltning og IKT: https://no.wikipedia.org/wiki/Direktoratet_for_forvaltning_og_IKT

Wikipedia. (2019, mars 20). *BSI Group*. Retrieved from https://en.wikipedia.org/wiki/BSI_Group

Wikipedia. (2019, februar 20). *ISO/IEC 27001*. Retrieved from https://en.wikipedia.org/wiki/ISO/IEC_27001

Wikipedia. (2019, februar 02). *PDCA*. Retrieved from https://en.wikipedia.org/wiki/PDCA

Vedlegg

Vedlegg 1

Spørreskjema

1	Hvem er ansvarlig for informasjonssikkerhetssystem i organisasjonen (stilling)?
2	Hvem er ansvarlig for vedlikehold av informasjonssikkerhetssystemet i organisasjonen (stilling)?
3	Hvilket grunnlag hadde dere brukt for utvikling av styringssystem for informasjonssikkerhet? For eksempel, veiledninger fra Datatilsynet, Difi, NoRSIS eller ISO 27001.
4	Hvis dere brukte ISO 27001, hvilken versjon brukte dere for implementering av informasjonssikkerhet styringssystem?
5	Har organisasjonen opprettet sikkerhetssystem internt eller fått ekstern hjelp?
6	Har organisasjonen utarbeidet sikkerhetshåndbok?
7	Hvor ofte revideres sikkerhetshåndboka?
8	Når var den siste revideringen av sikkerhetshåndboka?
9	Ble sikkerhetsboka revidert i forbindelse med det nye personvernregelverket GDPR som trådte i kraft den 20. Juli 2018?
10	Hvordan spres innholdet i sikkerhetsboka?
11	Hva gjør virksomheten for å opprettholde fokus på informasjonssikkerhet, og hvordan sikrer dere at det opprettholdes fokus på informasjonssikkerhet?
12	Gjennomføres det kultur- og teknisk program ved innføring, vedlikehold og forbedring av ISMS?
13	Evalueres det ISMS i organisasjonen? Hvilke evalueringsmetoder interne og/eller eksterne som er tatt i bruk for å måle ISMS?
14	Hvordan sprer dere resultater av evalueringer i organisasjonen?
15	Har organisasjonen fått sertifisert sikkerhetssystemet sitt?
16	Hva var årsaken til sertifisering av ISMS?
17	Hvilke holdninger har virksomheten i forhold til digitalisering av tjenester?
18	Hvordan ligger virksomheten i forhold til nye krav og regler som ble innført da GDPR trådte i kraft 20. juli 2018?
19	Hvordan jobber virksomheten sammenlignet med NTNU sin modell for ISMS?

Tabell 14: Spørreskjema

Vedlegg 2

Besvarelser fra spørreundersøkelse

Virksomhet 1

Virksomhet 1 er en stor offentlig virksomhet på omtrent 400 årsverk, og intervjuobjektet har stilling som virksomhetsleder i virksomheten.

Hvem er ansvarlig for informasjonssikkerhetssystem i organisasjonen (stilling)? Hvem er ansvarlig for vedlikehold av informasjonssikkerhetssystemet i organisasjonen (stilling)?

Hovedansvarlig for virksomhetens system for informasjonssikkerhet er formelt sett den øverste ledelsen, og det er virksomhetslederen, eller med andre ord den øverste ledelsens utøvende part, som til daglig håndterer, vedlikeholder, og styrer systemet.

Hvilket grunnlag hadde dere brukt for utvikling av styringssystem for informasjonssikkerhet? For eksempel, veiledninger fra Datatilsynet, Difi, NoRSIS eller ISO 27001.

Informasjonssikkerhetssystemet i virksomheten ble ikke utarbeidet direkte ut ifra sikkerhetsstandardene ISO 2700x, men det ble brukt veiledninger fra Datatilsynet, Direktoratet for forvaltning og IKT, og Norsk senter for informasjonssikring. Flere av disse aktørenes veiledningsmateriale baserer seg på ISO 2700x, henholdsvis i fra versjonen av 2013.

Har organisasjonen opprettet sikkerhetssystem internt eller fått ekstern hjelp?

Informasjonssikkerhetssystemet er utarbeidet internt i virksomheten, med unntak av håndteringen av personvernforordningen (GDPR). For håndteringen av personopplysninger har virksomheten benyttet seg av hjelpemiddelet «personvernappen», som er et system hjelper virksomheten med rutiner og protokoller for personopplysninger i forskjellige datasystem innad i virksomheten.

Har organisasjonen utarbeidet sikkerhetshåndbok?

Virksomheten har ikke en sikkerhetshåndbok for informasjonssystemet, men de har veiledere, små instrukser, sikkerhetserklæringer og regler som er samlet i et system, for eksempel rutiner og regler for e-post og internett, men de vil ikke definere dette som en sikkerhetshåndbok med tanke på at en sikkerhetshåndbok er typisk mye større i omfang enn det materialet som virksomheten benytter. Det er heller ingen planer i å innføre en sikkerhetshåndbok slik det ligger an per i dag, men heller i å fokusere på å holde et levende håndterbart sikkerhetsmateriale som fungerer for alle mulige brukere av datasystemene, heller enn et stort omfattende regelverk som kan oppleves uhåndterlig for de forskjellige yrkesgruppene som bruker det.

Hvordan spres innholdet i sikkerhetsboka?

Etter utarbeidelse av virksomhetens forskjellige rutiner, erklæringer og regler, spres disse gjennom bruk av administrative ledergrupper, det vil si ledere for avdelinger og undervirksomheter, og videre ut gjennom personalmøter. Sikkerhetsinnholdet spres både digitalt som for eksempel e-post, muntlig og via papirformat, og vil også senere havne i en Sharepoint-løsning som er på vei inn i virksomheten.

Ble sikkerhetsboka/regelverket revidert i forbindelse med det nye personvernregelverket GDPR som trådte i kraft den 20. Juli 2018?

Sikkerhetsrutinene og erklæringen har ikke blitt revidert i forbindelse med innføringen av GDPR, men noe må legges om i forhold til den nye personvernforordningen. Det som virksomheten har prioritert nå i første omgang i forhold til GDPR, er å få på plass protokoller som viser hvordan virksomheten håndterer personopplysninger.

Hva gjør virksomheten for å opprettholde fokus på informasjonssikkerhet, og hvordan sikrer dere at det opprettholdes fokus på informasjonssikkerhet?

Ifølge virksomheten er det et lite direkte fokus på informasjonssikkerhet, men de har tiltak ved at de kjører et rigid system med sentraldrift, og det er begrensninger på tilgang ved hjelp av brukerrettigheter, og sikkerhetsgrupper. Virksomheten har et forholdsvis strengt sikkerhetssystem, og det vil utvides med to faktors identifisering på nettet i fremtiden, i forhold til kun på enkelte fagsystemer per i dag. Målsetningen er et godt sikkert og håndterbart system for brukere.

Gjennomføres det kultur- og teknisk program ved innføring, vedlikehold og forbedring av ISMS?

Virksomheten mener videre at det er viktig med gode sikkerhetsholdninger blant de ansatte, og de har en it-sikkerhetserklæring som forklarer hva den enkelte bør gjøre av sikkerhetstiltak i sitt daglige arbeide. Det prates også om sikkerhet, holdninger og bevisstgjøring under kurs og opplæring for bruk av de forskjellige fagsystemene som finnes i virksomheten.

Fagsystemene består av gjennomprøvde, kostbare og standardiserte løsninger, og det kjøres prosedyrer og overvåkning på nye maskiner som blir satt inn i virksomheten med tanken på for eksempel oppdateringer.

Evaluering og revidering av virksomhetens informasjonssikkerhetssystem. Evalueres det ISMS i organisasjonen? Hvilke evalueringsmetoder interne og/eller eksterne som er tatt i bruk for å måle ISMS?

Virksomheten har ikke planlagte faste evalueringer, men de kjører ad hoc (ikke planlagt) intern evaluering. Dette kan typisk skje ved tilfeller ved brudd på retningslinjer innad i virksomheten. Ved slike brudd eller avvik på retningslinjer blir det foretatt evaluering for å finne ut hva som gikk galt, og hva som skal gjøres videre. Virksomheten har hjelpesystemer for inntrengere på nettverket. Det kjøres også risiko og sårbarhetsanalyse (ROS), og følger opp resultater med nødvendige tiltak, teknisk og kulturelt. Et eksempel som følge av en sikkerhetsanalyse er innkjøp av nødstrømsaggregat for å opprettholde drift under strømbrudd.

Hvordan sprer dere resultater av evalueringer i organisasjonen?

Ved spesielle hendelser tas det opp i faste ledermøter. Det tas opp overordnet, og ut mot ledere i hele virksomheten. Ledelsen starter med risikovurdering og evaluering, og nye tiltak kommer da videre nedover i virksomheten ved for eksempel personalmøter. Ledelsen er ansvarlig, og de sørger da for å spre informasjon om evalueringer og eventuelle nye tiltak og rutiner leddvis videre i virksomheten.

Har organisasjonen fått sertifisert sikkerhetssystemet sitt? Hva var årsaken til sertifisering/ikke sertifisering av ISMS?

Virksomheten har ingen planer om å sertifisere sikkerhetssystemet sitt for informasjonssikkerhet, da de føler det blir for omfattende, ressurskrevende og kostbart, og krever stadige resertifiseringer. Derimot ved kjøp av tjenester fra private aktører krever virksomheten sertifisering mot sikkerhetsstandard.

Hvilke holdninger har virksomheten i forhold til digitalisering av tjenester?

Virksomheten jobber bevisst mot å digitalisere de tjenestene de har, og ønsker å gjøre det enklest mulig i bruk for både kunder og ansatte. De ønsker gode systemer for å erstatte tungvinte manuelle løsninger, og vil videre søke skybaserte løsninger for enkelte systemer de har.
De ønsker også å legge til rette fordigital signatur for kundene, og å tilby løsninger som Chat-bot, som da vil være tilgjengelig for kundeveiledning døgnet rundt, uavhengig av kontortid.
Det finnes også stort sett digitale fagsystemer for det meste innen virksomheten, og dette forenkler håndtering og spredning av informasjon, og bedrer samspillet da man slipper å gi ut samme informasjon flere ganger, men heller har et system for håndteringen av den.

Hvordan ligger virksomheten i forhold til nye krav og regler som ble innført da GDPR trådte i kraft 20. juli 2018?

Virksomheten føler de ligger greit an. De har personvernombud, de har personvernappen, og det gås gjennom systemer for å se håndteringen av personopplysninger i de forskjellige systemene.

Det hjalp med eksisterende rutiner og informasjonssikkerhetssystem for å håndtere og svare på krav og regler fra den nye personvernloven. Virksomheten har eksisterende gode rutiner for å håndtere informasjon, og trengte da å dokumentere hvorfor de oppbevarer og hvordan de håndterer, men ikke å opprette nye rutiner. Virksomheten har hatt rutineinspeksjon fra Datatilsynet tidligere som gikk på håndtering av personopplysninger, og den gangen foreviste de samlede rutiner og regelverk, og håndteringen ble godkjent av tilsynet.

Virksomhet 1 sammenlignet med NTNU sin modell for informasjonssikkerhet.

Virksomheten synes at de ubevisst jobber likt som modellen i fra NTNU, og føler den tegner et bilde av en tenkemåte som både de og andre virksomheter handler ut ifra.
De har et system der de jobber ut ifra en risiko og sårbarhetsanalyse, og at evalueringene og nye tiltak som kommer ut ifra denne spres og innarbeides i virksomheten. De har også et kvalitetssystem der de legger inn ROS-analysene, og det kan legges inn og drøftes problemstillinger.

Virksomhet 2

Virksomhet 2 er relativt nyetablert offentlig virksomhet og er satt opp for å levere tjenester innen sin sektor. Både virksomhet, tjenestekatalog, og funksjonskatalog er nyopprettet, og virksomheten omfattes av omtrent 250 årsverk som er spredd ut over 25 lokasjoner. Respondenten har stilling som IT-sjef.

Hvem er ansvarlig for informasjonssikkerhet i virksomheten?

Formelt ansvar ligger hos administrerende direktør og styret, men rollen som informasjonssikkerhet og IKT-funksjon ligger hos intervjuobjektet/it-sjefen.

Hvem er ansvarlig for vedlikeholdet av informasjonssikkerhetssystemet i virksomheten?

Der har virksomheten beskrevet og bemannet en sikkerhetsorganisasjon. Overordnet ansvar ligger fremdeles hos informasjonssikkerhetsansvarlig som beskrevet tidligere. Virksomheten har opprettet et styringssystem for informasjonssikkerhet, der de følger Difis modell som gjør styringssystemet til en del av internkontrollen.

Hvilket grunnlag hadde dere brukt for utvikling av styringssystem for informasjonssikkerhet? For eksempel, veiledninger fra Datatilsynet, Difi, NoRSIS eller ISO 27001.

Virksomhet 2 har brukt Difi sin veiledning som utgangspunkt, og som følge av personvernforordningen som tredde i kraft i 2018, utarbeidet de ikke et eget prosjekt for å komme i samsvar med ny personlovgivning, men de gjorde heller dette til en del av det generelle informasjonssikkerhetsansvaret. På den måten ble regelverket om personopplysninger bygd inn i styringssystemet for informasjonssikkerhet. Rollen som personvernombud er også ansvarlig for internkontroll og kvalitet. Nærheten mellom internkontroll og kvalitet, og IKT-funksjoner har vært viktig for å få et operasjonelt system, og begge delene er en del av fellesfunksjoner som er organisert i stab i virksomheten. Samordning har vært viktig, for å unngå å få et fragmentert system. Virksomheten har altså funnet god hjelp i veiledningene til Difi, samt Datatilsynet, og også eksterne ressurser som kurs, for å få hjelp til å forstå forordningen fra 2018, og hvor og når den gjaldt i deres virksomhet. De opplevde ikke veiledningene til Datatilsynet og Difi som tilstrekkelige nok på det tidspunktet til å få en god nok forståelse av hvordan regelverket for personopplysninger gjaldt for deres virksomhet.

Virksomheten har også sett på flere standarder innen sammen område, som ISO 27005 for organisasjonsutvikling, og 27002 som omhandler tiltak. Veiledningen fra Difi støttet seg på ISO 27001 fra 2013.

Ble utarbeidelsen av informasjonssikkerhetssystemet gjort internt, eller ved ekstern hjelp?

Virksomheten utarbeidet systemet på egen hånd.

Har virksomheten en sikkerhetshåndbok?

Virksomheten har et regelverk, men de kaller ikke dette for en sikkerhetshåndbok.

Hvor ofte blir innholdet i sikkerhetshåndboka/regelverket revidert?

Virksomheten holder akkurat nå på å tilpasse systemet de har bygd for sikkerhetsorganisasjon, der de ser på intervaller for revidering, så det har de ikke et klart svar på akkurat nå.

Når var den siste revideringa av innholdet i sikkerhetshåndboka/regelverket?

Virksomheten har fortløpende revidering, i og med at de fortsatt holder på å implementere systemet sitt.

Ble sikkerhetsboka/regelverket revidert i forbindelse med det nye personvernregelverket GDPR som trådte i kraft den 20. Juli 2018?

Nei, virksomheten var ikke klar til å gjøre en revidering akkurat på det tidspunktet, men hadde første revidering omtrent fire måneder i etterkant av at forordningen tredde i kraft.

Hvordan spres innholdet i sikkerhetsboka?

Virksomheten følger samme fremgangsmåte som internkontrollen for øvrig, det vil si at alle områder av internkontrollen er samlet i en felles funksjon, og det er ansvarshavende for internkontrollene som også blir ansvarlig for å kommunisere ut til virksomheten. Foreløpig er ikke informasjonssikkerhetesystemet en del av internkontrollen, men det er i gang med å fases inn.
De har ikke en systematisk distribusjon av innholdet per nå, men de har en personalhåndbok som beskriver alt som er forventet av en medarbeider innenfor eksempel bruk av datamaskin, og mobil, men den er ikke god nok i forhold til dagens krav og regler angående GDPR, noe som virksomheten jobber med å implementere.

Hva gjør virksomheten for å opprettholde fokus på informasjonssikkerhet, og hvordan sikrer dere at det opprettholdes fokus på informasjonssikkerhet?

Administrerende direktør og styret gir instrukser videre til gjeldende ansvarsområder hvor det er satt opp funksjoner og IKT-funksjoner har ansvar for informasjonssikkerhet.

Operasjonelt og organisasjonsmessig så er strategien er bygget opp på klassifisering og digitalisering av informasjonselementer. Områder for samhandling eller dokumentdeling har innebygd støtte for klassifisering av virksomhetens rammer (tjenestekatalog, ansvarsområder og roller) og dermed også sikringstiltak.

Gjennomføres det kultur- og teknisk program ved innføring, vedlikehold og forbedring av ISMS?

Ja, men ikke systematisk, enda.

Evalueres det ISMS i organisasjonen? Hvilke evalueringsmetoder interne og/eller eksterne som er tatt i bruk for å måle ISMS?

Virksomheten bruker ikke ekstern hjelp i særlig grad, men all drift av infrastruktur er satt ut. Med dette får de også regelmessige oppfølginger av tjenesteavtaler med underleverandører, der områdene som omfatter databehandler og databehandleransvarlig blir gjennomgått slik at virksomheten sikrer samsvar med god praksis og gjeldende standarder.

Hvordan sprer dere resultater av evalueringer av ISMS i organisasjonen?

Evalueringene spres ikke internt, men det rapporteres til myndighetene en gang i året.

Har organisasjonen fått sertifisert sikkerhetssystemet sitt? Hva var årsaken til sertifisering/ikke sertifisering av ISMS?

Nei, og det er heller ikke definert som et mål. Hvis dette eventuelt skulle skje måtte det vært som følge av et eksternt krav.

Hvilke holdninger har virksomheten i forhold til digitalisering av tjenester?

Virksomheten har et betydelig ansvar som tjenesteleverandør. De legger til rette for og gjennomfører anskaffelser, og er opptatt av å utnytte leverandørmarkedet godt. Med tanke på at det er veldig mange anskaffelser innen deres sektor i løpet av et år, sitter virksomheten med et ansvar for å komme med gode beslutningsgrunnlag som skal legge til rette for rasjonelle og effektive innkjøp som skal gi gevinst. Der ligger det stor grad av digitaliseringsbehov ved at man har en god informasjonsarkitektur og systemarkitektur, som forvalter registerinformasjon/master data. Ved innsamling av data fra ulike operative funksjoner utenom virksomheten, og fra andre aktører er det viktig med prosesstyrte rutiner for datainnsamling, og at det ikke skal foregå manuelt.

Hvordan ligger virksomheten i forhold til nye krav og regler som ble innført da GDPR trådte i kraft 20. juli 2018?

Med utgangspunkt i Difi sin veiledning og med utgangspunkt i standardene (27001 også videre) var det mindre justeringer som måtte til for å håndtere krav i forbindelse med GDPR. I praksis utgjorde kravene fra GDPR en ekstra dimensjon i eksisterende system.

Virksomhet 2 sammenlignet med NTNU sin modell for informasjonssikkerhet.

Virksomheten synes at modellen fra NTNU virker som et årshjul for systematisk aktivitet i en virksomhet, der informasjonssikkerhet er en del av dette. Virksomhet 2 planlegger at informasjonssikkerhetsområdet skal bli en del av internkontrollen, og den er risikobasert, med et risikoregister. Det gjennomføres kontinuerlig risikovurdering med rapportering og innsetting av tiltak, og sånt sett står dette i stil med modellen fra NTNU.

Har virksomheten utarbeidet en informasjonssikkerhetspolicy? (Tilleggsspørsmål)

Virksomheten har en policy, og dette kom som et tidlig krav ut ifra virksomhetens styre for å møte krav til gjeldende regelverk omkring informasjonssikkerhet. IT-sjef ble også i denne sammenheng satt som informasjonssikkerhetsansvarlig.

Virksomheten har under utarbeidelsen av et ISMS støttet seg på veiledere fra Direktoratet for forvaltning og IKT/Difi, og noe av målsetningen var noe de kaller innebygd informasjonssikkerhet og personvern, og med det mener de at systemet skal fungere praktisk og operasjonelt for virksomhetens daglige drift, for eksempel i virksomhetens kultur og holdningsarbeid, og ikke bare være noe de lager for å imøtekomme krav og regelverk.

Vedlegg 3

Tabell fra ISO survey

ISO/IEC 27001 - Europe

Year	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
Country	1064	1432	2172	3563	4800	5289	6379	7952	8663	10446	12532	14605
Albania						3	2	7	8	22	44	15
Andorra									1	1	1	2
Armenia			1				3	7	3	22	22	37
Austria	16	23	32	37	54	59	28	75	87	91	146	146
Azerbaijan									2	2	2	5
Belarus				1	1	1	1	1	1	3	2	9
Belgium	4	9	15	19	26	29	31	47	43	53	98	127
Bosnia and Herzegovina				4	4	2	7	9	9	13	17	27
Bulgaria		8	23	60	116	132	208	278	330	273	261	250
Croatia	2	5	10	22	24	32	58	69	96	55	110	123
Cyprus				3	4	5	9	16	9	13	11	32
Czech Republic	27	77	88	264	529	301	264	399	276	381	507	463
Denmark	3	4	4	9	6	5	7	8	13	29	68	57
Estonia		1	1	1	1	1	2	2	3	2	4	9
Finland	1	14	13	18	23	27	28	32	33	44	54	72
France	5	9	14	15	31	46	66	94	155	227	209	342
Georgia								1	0	0	2	2
Germany	95	135	239	253	357	424	488	581	634	994	1338	1339
Gibraltar (UK)				1				0		5	3	3
Greece	3	5	20	28	44	45	49	77	62	136	150	727
Hungary	54	81	135	146	151	178	199	280	295	323	421	472
Iceland	10	11	13	16	20	21	20	26	31	29	57	60
Ireland	6	7	10	21	24	30	48	54	131	140	175	209
Italy	175	148	233	297	374	425	495	901	969	1013	1220	958
Latvia			1	2	6	9	9	18	24	24	30	42
Liechtenstein												1
Lithuania		2	3	7	11	14	19	23	25	35	43	85
Luxembourg	1	2	2	2	5	8	7	5	7	10	20	25
Malta		1	1	1	2	2	5	7	7	7	53	18
Moldova, Republic of	1	1	1	2	2	1	1	3	7	7	10	2
Monaco												2
Montenegro								1	5	1	0	2
Netherlands	41	41	56	76	97	125	190	316	335	455	670	913
Norway	15	22	16	17	25	31	16	26	70	49	81	87
Poland	11	45	75	187	229	233	279	307	310	448	657	705
Portugal	1	4	4	5	17	20	34	58	55	56	96	112
Romania	4	16	44	303	350	575	866	840	893	1078	513	440
Russian Federation	5	9	17	53	72	31	27	48	43	55	62	78
San Marino, Republic of						1	1	1	1	1	1	1

Serbia				3	8	9	25	43	101	142	146	133
Slovakia	4	12	28	50	70	111	127	159	162	232	212	173
Slovenia	5	12	16	27	33	31	13	49	58	50	57	70
Spain	23	93	203	483	711	642	805	799	698	676	752	803
Sweden	20	55	18	30	30	37	32	49	45	61	160	148
Switzerland	34	32	58	57	61	66	65	111	131	105	145	171
The Former Yugoslav Republic of Macedonia	1	1	4	6	7	7	5	9	9	13	13	27
Turkey	10	27	33	86	117	100	132	181	224	268	500	531
Ukraine	1	1	3	5	1	6	7	12	9	12	22	47
United Kingdom	486	519	738	946	1157	1464	1701	1923	2253	2790	3367	4503

Tabell 15: ISO/IEC 27001 Europe. Hentet fra 9. ISO Survey of certifications to management system standards - Full results (https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1)