IN5080 Semesteroppgave

Kandidatnr 15026
Kandidatnr 15011
Kandidatnr 15039

Department of informatics
The faculty of mathematics and neutral science

UNIVERSITY OF OSLO
APRIL 2025

Innholdsfortegnelse

Oppgave A: Vurdering av modenheten til UiOs LSIS

Modenhetsnivåene

CMMI, eller Capability Maturity Model Integration, er en prosessforbedringsmodell utviklet for programvareutvikling på 1990-tallet. Siden den gang har CMMI utviklet seg for å tilpasse seg det moderne markedet, og inkluderer nå mer enn bare programvareutvikling. CMMI ble først utviklet av Software Engineering Institute ved Carneige Mellon University, men blir i dag publisert av CMMI Institute ved ISACA. Modellen brukes i dag til blant annet å vurdere modenhet av cybersikkerhetsprosesser i private og offentlige virksomheter. Målet med modellen er å vurdere nåværende modenhet i forhold til ønsket nivå slik at man kan prioritere investeringene i cybersikkerhet riktig og forbedre sitt nivå (Universitetet i Oslo [UiO], 2025).

CMMI består av fem, men i praksis seks, nivåer for modenhet, og deles inn i umoden styring av cybersikkerhet (nivå 0-2) og moden styring av cybersikkerhet (nivå 3-5). Nivå 0, som kjennetegnes av fravær på sikkerhetstiltak og fokus på cybersikkerhet, er egentlig ikke definert som et nivå, men siden det er en reell mulighet for en bedrift å være på dette nivået er det derfor relevant å inkludere (UiO, 2025). Hvert modenhetsnivå bygger på det tidligere, men legger til nye krav (CMMI Institute, n.d.).

“Nivå 1: Initiell”
Kjennetegnes av få og tilsynelatende tilfeldige sikkerhetstiltak. Det mangler mulighet for kvalitetskontroll og oppfølging, og det eksisterer ingen overordnet plan for cybersikkerheten til en virksomheten (UiO, 2025).

“Nivå 2: Ledet”
Dette nivået kjennetegnes ved at det i større grad er et fokus på sikkerhet, men ikke fra toppledelsen. Det blir foretatt noen risikovurderinger med tilhørende tiltak, men virksomhetens holdning er i stor grad fortsatt reaktiv. Prosesser forblir udokumenterte (UiO, 2025).

“Nivå 3: Definert”
På dette nivået har sikkerhet blitt et fokusområde for toppledelsen, og det eksisterer en overordnet policy for virksomheten hvor cybersikkerhet er definert som en målsetning. Prosjekter og prosesser relatert til cybersikkerheten følger til en viss grad anerkjente standarder (UiO, 2025).

“Nivå 4: Kvantifisert”
Nivå 4 skiller seg fra de lavere nivåene ved at bedriften har innført en helhetlig risikostyring hvor sikkerhetsprosjekter, -prosesser og -tiltak er målbare etter definerte metrikker. En virksomhet på dette nivået har et erfarent sikkerhetsteam med sterkt lederskap, budsjett og støtte fra toppledelsen (UiO, 2025).

“Nivå 5: Optimaliserende”
Dette siste og øverste nivået vil i tillegg til å dekke alle kjennetegnene ved de lavere nivåene, også samle inn metrikker og KPI-er for cybersikkerhet. Disse kan brukes så virksomheten kan gjøre bedre investeringer og fordeling av ressurser, samt er med å skape mer objektive estimater for sannsynlighet og konsekvens i risikovurderinger (UiO, 2025).

Dokumentene består av 14 kapitler fordelt over 3 deler: styrende, gjennomførende og kontrollerende. Den styrende delen inneholder grunnleggende prinsipper for arbeidet (Universitetet i Oslo [UiO], 2018), slik som sikkerhetsmål, -strategi og -organisering (UiO, 2020, Kapittel 1). Denne delen av LSIS bør leses av ledere, men er også noe flere bør være kjent med (UiO, 2018). Den gjennomførende delen beskriver i detalj hva som skal gjøres og av hvem (UiO, 2018). Dette inkluderer rutiner, verktøy, avvikshåndtering m.m. (UiO, 2020, Kapittel 1). Denne delen er hovedsakelig rettet mot ledere, IT-ansatte på alle nivåer samt vitenskapelige ansatte og ansatte i administrative stillinger (UiO, 2018). Til slutt så forklarer den kontrollerende delen hvordan vi vet at vi når målene om at informasjonen er rett sikret og forvaltet og er utviklet for ledere og IT-ansatte på alle nivåer (UiO, 2018).

Modenhetsnivå for UiOs ledelsessystem for informasjonssikkerhet

UiOs LSIS kan med sikkerhet klassifiseres som et av nivåene med moden styring av cybersikkerhet. Universitetet har et omfattende dokumentert ledelsessystem med klare roller og ansvarsområder samt et system med systematisk tilnærming inkludert årlige revisjoner, definerte policyer og dokumenterte prosesser. Dette alene gjør at vi er over nivå 0 og 1. I tillegg har UiOs LSIS ikke bare reaktive tiltak, men også proaktive tiltak som ROS-analyser, penetrasjonstester og port scanning, og krav om grundig dokumentasjon av sikkerhetsprosesser i hele LSIS-en. Dette vil gjøre at vi oppfyller alle krav om nivå 2 og vi kan gå videre til de øvre modne nivåene. Videre er også alle kriterier for nivå 3 oppfylt. Det er en tydelig ledelsesforankring med universitetsdirektøren som øverste ansvarlig. Systemet har en formell policy med definerte sikkerhetsroller og ansvar, og følger retningslinjer fra UNINETT samt standarder fra blant annet NSM og Difi.

Nivå 4
UiO utfører risikovurderinger annethvert år med definerte skalaer fra 1-4 på både konsekvens og sannsynlighet (UiO, 2025, Kapittel 7). Dette gjør at risiko kan kvantifiseres og måles, som igjen gjør at vi kan sammenligne ulike risikoer før eventuelle tiltak, med restrisiko etter tiltak. Vi kan også systematisk sammenligne risiko over tid. I kapittel 14 beskrives UiOs internkontroll, som inneholder flere elementer som kan gi målbare metrikker for sikkerhetsarbeidet. ROS-analyser, internkontroll via nettskjema, stedlige kontroller, brevkontroller og tekniske kontroller kan alle gi kvalifiserbare resultater (UiO, 2019, Kapittel 14). Internkontrollen skal ende i rapporter, og i kapittel 6 beskrives årsrapporten fra informasjonssikkerhetsarbeidet. Rapporten inneholder blant annet status på vedtatte mål, krav og styringsparametere samt aktivitetene i internkontrollarbeidet (UiO, 2022, Kapittel 6). Dette tyder på at det finnes målbare metrikker som er fastsatt og måles jevnlig.

Universitetet i Oslo har et erfarent sikkerhetsteam med klare roller, definert i kapittel 4 (UiO, 2023, Kapittel 4), og et system for regelmessig rapportering gjennom årsrapporter, rapporter fra stedlige kontroller og fortløpende avviksrapportering. Enhet for intern revisjon (EIR) har ansvar for å etterse at internkontroll er tilfredsstillende etablert for all virksomhet.

Samlet vil dette resultere i at UiOs LSIS oppfyller kravene for nivå 4 av modenhet på CMMI-skalaen.

Nivå 5

Ettersom det er innsamling og videre bruk av metrikker og KPI-er som skiller nivå 4 og 5 må vi se nærmere på hva UiOs LSIS sier om dette. Konkret informasjon om KPI-er og metrikker er noe mangelfullt, men vi bygger videre på det vi allerede vet. For å oppnå nivå 4 av modenhet, kreves det at sikkerhetsprosjekter, -prosesser og -tiltak er målbare etter definerte metrikker, noe som vil si at metrikker eksisterer som et overordnet mål for cybersikkerheten hos universitetet og er noe vi kan sammenligne resultatene våre mot. Vi vet også at det samles inn data fra forskjellige komponenter i internkontrollen som havner i en eller flere rapporter, blant annet årsplanen. Denne planen redegjør for prioriterte tiltak for informasjonssikkerhetsarbeidet, noe som kan bidra til bedre bruk av ressursene. Årsplanen inneholder data som samles inn i internkontrollen og presenteres. Etter at årsplanen er gjennomgått kan det forekomme en revisjon og mulig endringer. Disse endringene vil være optimaliserte dersom innsamling og bruk av KPI-er er gjennomført på en hensiktsmessig og systematisert måte, men det får vi ingen konkret informasjon om i dokumentene.

I kapittel 7, om risiko- og sårbarhetsanalyser, står det at grunnlaget for sikring av alle IT-systemer er grunnsikringen, beste praksis fra leverandører og sikring basert på erfaring og tilpasninger til det gjeldende trusselbildet (UiO, 2025, Kapittel 7). Hvordan man velger å tolke dette, har stor innvirkning på hvorvidt UiOs LSIS er oppe på nivå 5 eller ikke. Grunnsikring og best practice er ikke basert på innsamlede metrikker og KPI-er, men derimot kan man tolke “erfaringer og tilpasninger” til å gjelde dette, ettersom innsamlede data kan tolkes som erfaring. Videre står det at ekstra sikring utover grunnsikringen skal være basert på en risikovurdering. En slik vurdering vil gi et kvantifiserbart resultat, som vi samler inn og eventuelt bruker til å videre sikre cybersikkerheten.

Ledelsessystemet dekker delvis kravene til nivå 5, men det mangler tydelige rammer på hvordan de indsamlede metrikkene og KPI-ene skal brukes til å fremme bedre cybersikkerhet. Det bør beskrives et formelt system for hvordan man kan drive kontinuerlig forbedring basert på disse dataene. Dette vil også inkludere hvordan vi kan bruke tidligere innsamlet data til å lage mer objektive estimater for risikovurderingene våre. Da det ikke forekommer et slikt formelt system, eller noe særlig beskrivelse av KPI-er, kan man ikke fastslå at dokumentene oppfyller alle krav til dette øverste nivået av modenhet. Det finnes derimot mye som tyder på at man er i nærheten av å kunne nå det. Derfor vil en endelig konklusjon være at UiOs ledelsessystem for informasjonssikkerhet er på nivå 4, men med noen av kjennetegnene til nivå 5.

Oppgave B: Sammenligning av sikkerhetstiltak fra ulike kilder

Tabellen under sammenligner begrepene som brukes for tiltaket «sikkerhetskopiering» fra ISO/IEC 27002 og tilsvarende tiltak i andre kilder:

Kilde	Begrep brukt
ISO/IEC 27002	**Backup**
NIST Cybersecurity Framework (CSF) 2.0	**Data Backup** (funksjonsområde: "Recover" under "Recovery Planning")
CIS Critical Security Controls (CSC)	**Data Recovery Capabilities** (Kontroll #11)
NSMs grunnprinsipper for IKT-sikkerhet	**Sikkerhetskopiering** (under prinsippet "Beskytte data")
NIST SP 800-53	**System Backup** (Kontroll CP-9)

Tabellen viser distinkt at alle kildene beskriver tiltaket, men bruker litt forskjellige betegnelser som reflekterer deres fokus og detaljeringsgrad.

Hyppighet av sikkerhetskopiering

- **ISO/IEC 27002:** Anbefaler at frekvensen bør besluttes basert på organisasjonens risikovurderinger og behov for tilgjengelighet. Ingen konkret tidsangivelse.

- **NIST CSF 2.0:** Angir generelt at hyppigheten må samsvare med kontinuitetsbehov, uten å spesifisere nøyaktige tidsintervaller.

  CIS CSC: Gir tydelig anbefaling om daglig eller kontinuerlig sikkerhetskopiering av kritiske data for raskest mulig gjenoppretting.

- **NSM:** Poengterer viktigheten av regelmessighet, tilpasset dataverdi og endringstakt, uten å gi spesifikke intervaller.

- **SP 800-53:** Som ISO, anbefaler frekvens basert på risikovurdering og organisasjonens spesifikke behov.

Kryptering og sikker lagring

- **ISO/IEC 27002:** Krever tydelig sikker og kryptert lagring av sikkerhetskopiene, inkludert fysisk og logisk beskyttelse.

- **NIST CSF 2.0:** Understreker at sikkerhetskopier må sikres og krypteres som del av organisasjonens overordnede sikkerhetsstrategi.

- **CIS CSC:** Spesifiserer at sikkerhetskopier bør være fysisk separert («air-gapped»), krypterte og tilgangskontrollers for å hindre uautorisert tilgang og datalekkasjer.

- **NSM:** Poengterer betydningen av fysisk og logisk sikker lagring, inkludert kryptering, tilpasset norske krav og operative anbefalinger.

- **SP 800-53:** Har eksplisitte krav til kryptering og sikker fysisk/logisk oppbevaring av sikkerhetskopier med tydelig tilgangsstyring.

Testing av gjenopprettingsprosedyrer

- **ISO/IEC 27002:** Krever regelmessig testing av gjenopprettingsprosedyrer, men gir ikke spesifikke tidsintervaller eller metoder.

- **NIST CSF 2.0:** Understreker viktigheten av testing av sikkerhetskopier og gjenopprettingsprosedyrer som en integrert del av kontinuitetsplanleggingen.

- **CIS CSC:** Anbefaler bestemte og regelmessige tester av datagjenopprettingsprosedyrer for å sikre deres effektivitet og operasjonelle pålitelighet.

- **NSM:** Gir generell anbefaling om rutinemessig testing, men uten konkretisering av metoder eller intervaller.

- **SP 800-53:** Krever dokumenterte, regelmessige tester av gjenopprettingsprosedyrer med klare krav om dokumentasjon og oppfølging av resultatene.

Samlet sett gir ISO/IEC 27002 og SP 800-53 generelle rammer for sikkerhetskopiering, mens CIS CSC gir tydelige, operasjonelle anbefalinger. NIST CSF inkluderer tiltaket som en del av en bred kontinuitetsstrategi, og NSM tilbyr praktiske, nasjonalt tilpassede råd som reflekterer norske forhold og behov.

Oppgave C: DPIA og Risikovurdering av Apo-Nett

Oppgave C.1

Apo-Nett-løsningen tar for seg en rekke personopplysninger som er knyttet til kundene. De planlegger å behandle disse opplysningene for å tilby tjenestene sine som et nettapotek. Behandlingen består av innsamling, lagring og bruk av personopplysninger for å blant annet administrere kundeforhold, behandle bestillinger og sørge for at relevante lover og regler blir fulgt. For Apo-Nett er det derfor nødvendig å gjøre det mulig for registrering, autentisering, kjøpshistorikk, og betaling og levering av varer. Behandlingsgrunnlaget er i henhold til GDPR artikkel 6, inkludert kontraktmessing, nødvendighet, juridiske forpliktelser, samtykke, og berettiget interesse. I tillegg er også noe av behandlingsgrunnlaget i henhold til GDPR artikkel 9 som tar for seg behandling av særlige kategorier av personopplysninger. Om Apo-Nett bruker en amerikansk skyleverandør og eksterne utviklere fra India, slik som designerne foreslår, skal overføringen av personopplysninger ut av EØS gå gjennom et særskilt grunnlag og et overføringsgrunnlag identifisert. Et overføringsgrunnlag kan være standard personvernbestemmelser (SCCs) som er vedtatt av EU-kommisjonen og er mellom Apo-Nett og tredjeparten. Siden India ikke anses til å gi tilstrekkelig personvern så iverksettes det også supplerende tiltak. (datatilsynet.no, 2023)

De ulike kategoriene av personopplysninger som behandles, hvorfor de er nødvendige for Apo-Nett og grunnlag er følgende (lovdata.no, 2022):

1. ***Navn***. Dette er nødvendig at Apo-Nett har på grunn av identifisering av kunden i systemet, adressere leveranser og eventuelt når kundeservice trengs. Løsningen funker ikke uten navn fordi det blir vanskelig å administrere kundekontoer og kjøpsordre. Behandlingsgrunnlaget er GDPR art. 6(1)(b) som er nødvendig for å oppfylle en kontrakt.
2. ***E-postadresse***. Dette brukes for kontoregistrering, pålogging og som kommunikasjonskanal. Hvis kunden samtykker brukes dette også til markedsføring. E-postadresse er viktig for blant annet sikkerhetsformål, f.eks varsle påleggingsforsøk. Behandlingsgrunnlaget er GDPR art. 6(1)(a) - samtykke om markedsføring, 6(1)(b)- oppfylle kontrakt, og 6.(1)(f)- berettiget interesse.
3. ***Telefonnummer***. Dette brukes til å ta kontakt med kunden enten ved problemer eller med oppdateringer fra transportører, men kan også brukes til tofaktorerings. Behandlingsgrunnlaget er GDPR6(1)(b)(f).
4. ***Kjønn (frivillig)***. Brukes til personalisering av produktanbefalinger. Behandlingsgrunnlag GDPR art. 6(1)(a) - samtykke.
5. ***Fødselsdato (frivillig)***. Nødvendig for aldersverifisering, samt tilpasset anbefalinger. Behandlingsgrunnlag GDPR art. 6(1)(a)(c).
6. ***Lokalt brukernavn og passord.*** Uten denne løsningen må Apo-nett bruke eksterne identifiserings-løsninger, noe som ekskluderer brukere uten løsningene, og gir derfor mulighet til kunder å logge inn direkte. Behandlingsgrunnlag GDPR art. 6(1)(b).
7. ***Internett-ID***. Dette forenkler innlogging til de som har eksisterende brukere, reduserer risikoen for glemt passord og bidrar til en økt brukervennlighet. Behandlingsgrunnlag GDPR art. 6(1)(a).

8. ***Fødselsnummer***. Påkrevd for sterk autentisering som BankID, samt er nødvendig for kjøp av reseptbelagte legemidler. Behandlingsgrunnlag GDPR art. 6(1)(c) og GDPR art.9(2)(h) for helsetjenester.
9. ***Kjøpshistorikk***. Gir kunder mulighet til å ha en ryddig oversikt over tidligere kjøp, nødvendig for kundeservice, samt kan være påkrevd for regnskap. Behandlingsgrunnlag GDPR art. 6(1)(b)(c).

En DPIA skal gjennomføres om behandlingen av personopplysninger vil medføre høy risiko for personvern, fysiske personers rettigheter og friheter ifølge GDPR art.35(1). Da skal en vurdering av hvilke konsekvenser behandlingen vil ha bli gjort. Dette skal også være spesielt nødvendig i tilfeller der systematisk og omfattende vurdering av personlige aspekter er basert på automatisert behandling, behandling av særlige kategorier som skjer i større grad, og i tilfelle en systematisk overvåking av et offentlig tilgjengelig område. (lovdata.no, 2022) I Apo-Nett sin løsning, er det flere faktorer som fører til at en DPIA bør være nødvendig. Apo-Nett behandler sensitive personopplysninger, blant annet fødselsnummer, som ifølge GDPR art.9 krever sterkere beskyttelse. Behandlingen av de andre personopplysningene - navn, telefonnummer, kjøpshistorikk - er en stor mengde data, og om det skjer en lekkasje eller andre feil vil dette forårsake høy risiko. En annen ting er at ifølge Apo-nett sin løsning vil de dele kjøpshistorikk med tredjeparter, f.eks. treningssentre, for å tilby helseprodukter som passer med deres aktivitet. Personopplysningene til kunden kan dermed bli brukt til andre hensikter enn hva kunden har gitt eksplisitt samtykke til. Til slutt skal Apo-Nett bruke en amerikansk skyleverandør som medfører til overføring utenfor EØS.

Ifølge GDPR artikkel 9 er visse personopplysninger regnet som særlige kategorier av personopplysninger - også kalt sensitive personopplysninger. Dette er en rekke kategorier med opplysninger som krever mer til å kunne behandles og kan føre til større personvernkonsekvenser. Apo-Nett vil at kundedatabasen skal inneholde de følgende sensitive personopplysningene:

Fødselsnummer skal brukes i sammenheng med login med sterk ID, det vil si autentisering med tjenester som BankID. Etter dagens lov regnes ikke fødselsnummer som sensitive personopplysninger, men det er tilleggskrav for bruk av dette som identifikasjonsmiddel samt klare grenser for hvordan det skal brukes. Det kan kun brukes ved saklig behov for sikker identifisering av en person ifølge personopplysningsloven § 12. Det skal heller ikke brukes for å administrere kundeforhold, med mindre det er saklig behov. (Datatilsynet, 2023). I Apo-Nett sin foreslåtte løsning vil de bruke login med sterk ID, dvs. fødselsnummer med autentisering med et virkemiddel som BankID. Dette går under behandlingsgrunnlaget GDPR art.6 om juridisk forpliktelse der det er krav om sikker identifikasjon for reseptbelagte legemidler, samt behandlingsgrunnlag for helseopplysninger art.9 om data nødvendig for helsetjenester. Løsningen nevner også forslaget om at fødselsnummeret lagres i kundedatabasen, men dette er ikke noe som er nødvendig for administrasjon av kundeforhold. Derfor er dette et brudd på personopplysningsloven § 12. Dessuten innebærer bruk av autentisering ved sterk ID høy risiko for misbruk og muligens identitetstyveri om tjenesten ikke implementeres med nok beskyttelse mot hacking eller lekkasje. Noen sikkerhetstiltak som reduserer dette er for eksempel å implementere multifaktorautentisering, ikke lagre passord i klartekst - altså bruk av hashing på passord , sørge for at en plan for gjenoppretting av data er etablert, samt kryptere fødselsnummer under lagring og overføring. Bruken av fødselsnummer som autentiseringsmetode i seg selv er et personvernproblem, og det må veies nøye opp mot nødvendigheten av det med tanke på at høy sikkerhet er også nødvendig. Så lenge sikkerhetstiltakene er gjennomført, og at en hendelsesrespons blir opprettet, kan risikoen reduseres og behandlingen blir akseptabel.

Annet enn fødselsnummer er det flere potensielle personvernkonsekvenser på andre personopplysninger som Apo-Nett foreslår å lagre i kundedatabasen. Informasjon som e-postadresse, telefonnummer, kjøpshistorikk og helseinformasjon som er knyttet til kunden, og dens behandling innebærer forskjellige risikoer og konsekvenser. E-postadresser og telefonnummer, som i Apo-Nett skal brukes til kontakt med kundene og til markedsføring, anses ikke som sensitive personopplysninger, og risikoen for misbruk av disse er relativt lav. Men, om disse opplysningene blir delt med f.eks. tredjepartsleverandører uten å informere og samtykke fra kunden, kan dette antyde til brudd på personvernet. Tiltak for å unngå dette er at Apo-Nett må eksplisitt hente inn samtykke for bruk av disse opplysningene til spesifikke årsaker som markedsføring eller til tredjepartsleverandører som et treningsstudio. Apo-Nett vil også lagre kjøpshistorikken til kunder for å kunne tilby relevante produkter og passende tjenester basert på tidligere ordre. Denne informasjonen kan også bli delt med tredjepartsleverandører og brukt til uautorisert markedsføring, og derfor kan de også unngås med de samme tiltakene som gjelder samtykke og innføre tiltak som bruker krypterte kanaler for overføring. Kjønn og fødselsdato er frivillige opplysninger kunder gir til Apo-Nett, og de blir brukt til å tilpasse produkter til forskjellige kundegrupper. Disse opplysningene er ikke sensitive, og risikoen for at de blir brukt feil er relativt lav. Så lenge opplysningene ikke blir benyttet til diskriminerende formål, er personvernkonsekvensene akseptable.

Oppgave C.2

For å sikre en hensiktsmessig og grundig risikovurdering er det avgjørende å etablere et oversiktlig og tydelig register over virksomhetens kritiske verdier. Apo-Nett håndterer ulike informasjonskategorier og systemer med varierende grad av sensitivitet og viktighet for virksomhetens drift. Gjennom en strukturert tilnærming kan virksomheten bedre forstå hvilke verdier som krever høyest sikkerhetsnivå, og dermed tilrettelegge for målrettede sikkerhetstiltak.

Under følger en detaljert beskrivelse av tre sentrale verdier hos Apo-Nett, inkludert relevante attributter som beskriver verdienes art, betydning og hvilke typer sikkerhetsbrudd som potensielt kan være alvorlige. For hver verdi er det også gitt en forklaring og utdyping av viktigheten med hensyn til konsekvenser ved sikkerhetsbrudd.

Kundedatabasen

Kundedatabasen representerer en av de mest kritiske verdiene for Apo-Nett og inneholder en omfattende mengde sensitiv informasjon om kundene. Denne databasen inneholder ikke bare grunnleggende personopplysninger som navn, telefonnummer og lokal passordinformasjon, men også omfattende kjøpshistorikk. Kjøpshistorikken inkluderer informasjon om kjøpte produkter, både standardprodukter som vitaminer og mer sensitive varer som reseptbelagte

medisiner. Denne typen data er svært sensitiv da den kan avsløre detaljerte opplysninger om kundens helsetilstand, livsstil eller medisinske utfordringer.

Sikkerhetsbrudd mot kundedatabasen kan innebære alvorlige konsekvenser som lekkasje av personopplysninger og sensitive helseopplysninger, noe som potensielt kan føre til juridiske sanksjoner, store bøter og omfattende tap av tillit blant kundene. Det vil også kunne medføre vesentlig skade på Apo-Netts omdømme, som igjen kan føre til tap av kunder og redusert inntektsstrøm. Bevaring av dataens integritet, altså at informasjonen ikke utilsiktet eller uautorisert endres, samt opprettholdelse av konfidensialitet, er derfor avgjørende.

Klientplattformen

Klientplattformen fungerer som det primære grensesnittet mellom Apo-Nett og kundene. Det er denne plattformen kundene interagerer med for å bestille produkter, administrere sine kontoer og få tilgang til viktige tjenester. Plattformens kontinuerlige drift og tilgjengelighet er derfor en forutsetning for at virksomheten skal kunne tilby sine tjenester effektivt og uten avbrudd.

Sikkerhetsbrudd, spesielt tjenestenektangrep (Denial of Service, DoS), mot klientplattformen kan føre til nedetid, som vil si at kundene ikke lenger får tilgang til sine tjenester eller kan gjennomføre transaksjoner. Slike brudd påvirker direkte virksomhetens ytelse ved tap av salg. Ved lengre nedetid kan det oppstå alvorlige skadevirkninger på Apo-Netts merkevare og omdømme. Et velfungerende brukergrensesnitt krever at virksomheten sikrer tilgjengeligheten og robustheten av klientplattformen gjennom tekniske og organisatoriske sikkerhetstiltak, som redundans og beredskapsplaner for rask gjenoppretting ved eventuelle hendelser.

Skytjenesten

Apo-Nett har valgt å benytte seg av en ekstern amerikansk leverandør for drift av sin skytjeneste. Denne tjenesten ivaretar essensielle sikkerhetsfunksjoner som nettverkssikkerhet, overvåking av sikkerhetshendelser, hendelsesrespons og håndtering av cyberangrep. Siden skytjenesten utgjør selve infrastrukturen og bakbenet for Apo-Nett sine nettbaserte tjenester, utgjør den en kritisk ressurs for virksomhetens operasjonelle evne og sikkerhetsstyring.

En sikkerhetshendelse eller angrep rettet mot skytjenesten vil kunne få betydelige konsekvenser. Eksempelvis kan sensitive data bli kompromittert eller det kan oppstå omfattende og langvarig nedetid. I tillegg er det viktig å ta hensyn til at angrep mot skytjenesten potensielt også kan påvirke flere kunder enn Apo-Nett alene, og dermed øke skadeomfanget anselig. For å begrense slike risikoer kreves det grundig og systematisk risikostyring og kontinuerlig overvåking av skytjenesten samt tydelige avtaler rundt sikkerhetsansvar og oppfølging med leverandøren.

Inspirert av boka «Informasjonssikkerhet: Teori og praksis» (s. 252), presenteres følgende attributter for å tydeliggjøre og strukturere hver verdi ytterligere:

Attributt	Beskrivelse
Nummer	Hver verdi/ressurs får tildelt en unik identifikator
Type verdi / klasse	Eksempelvis fysisk infrastruktur, data, personinfo, systemer, applikasjoner, tjenester og ansatte (roller)
Eier	Den avdeling eller enhet som er ansvarlig for verdien
Lokasjon	Den fysiske eller logiske plasseringen av verdien
Funksjon/forretningsprosess	Funksjoner eller prosesser som støttes eller avhenger av verdien
Data-klassifisering	Klassifisering basert på dataens sensitivitet
Konsekvensvurdering	Vurdering av konsekvenser ved brudd på sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet (KIT)

Verdi	Kundedatabasen	Klientplattform	Sky-leverandør
Nummer	1	2	3
Type verdi/klasse	Personlig informasjon	Applikasjon	Fysisk infrastruktur (gitt fysiske maskiner)
Eier	Apo-Nett	Apo-Nett / Kunde	Amerikansk leverandør av valgt skytjeneste
Lokasjon	MySQL database	Kundens enhet	PaaS sky-infrastruktur
Funksjon	Samling av kundeinformasjon	Brukergrensesnitt for kunde	Ansvarlig for nettverkssikkerhet og håndtering av angrep
Data-klassifisering	Sensitiv informasjon	Brukerenhet	Drift
Konfidensialitet	5	1	1
Integritet	5	1	1
Tilgjengelighet	2	5	5

Når det gjelder konsekvensvurderinger og vurdering av KIT-aspektene (konfidensialitet, integritet og tilgjengelighet) for de beskrevne verdiene, er flere ulike faktorer analysert og vurdert i sammenheng. Disse inkluderer potensielt tap av omsetning, reduksjon av ytelse, brudd på juridiske krav, skade på virksomhetens omdømme og økonomiske kostnader knyttet til gjenoppretting etter sikkerhetshendelser. Hver verdi har fått en samlet score på en skala fra 1 (lav risiko) til 5 (høy risiko), hvor en høy score indikerer at verdien krever omfattende beskyttelsestiltak og høy sikkerhetsprioritet.

Begrunnelse for KIT-vurderinger i detalj:

- **Kundedatabase:** Denne databasen er vurdert som høyst sensitiv når det gjelder konfidensialitet og integritet. Enhver u-autorisert tilgang eller manipulering av informasjon vil føre til omfattende konsekvenser, inkludert juridiske sanksjoner og varig omdømmeskade.

- **Klientplattform:** Vurderingen fokuserer primært på tilgjengelighet, gitt plattformens direkte rolle i kundeinteraksjoner og virksomhetens inntektsgenerering. Driftsstans innebærer umiddelbart tap av inntekt og redusert kundeopplevelse.

- **Skytjeneste:** Tilgjengelighet og kontinuerlig drift er av største viktighet, ettersom tjenesten håndterer sikkerhetsrelaterte avhandlinger som overvåking, hendelseshåndtering og nettverkssikkerhet. Manglende evne til å håndtere og respondere på hendelser øker risikoen for alvorlige sikkerhetsbrudd som igjen kan lamme hele virksomhetens tjenestetilbud.

Ved å forstå og ivareta disse vurderingene sikrer Apo-Nett effektiv risikostyring og robust beskyttelse av kritiske verdier.

Oppgave C.3

A - Kvalitativt nivå for akseptabel risiko

I denne oppgaven har vi valgt å bruke tolkningen av ordinale risikonivåer fra forelesningen om risikovurdering som grunnlag. Her har vi valgt at "(5) lav risiko" er akseptabelt, alt over dette bør håndteres.

Det er to høye risikonivåer og et middels risikonivå for Apo-Nett før risikohåndteringen.
Risiko *R1*, datainnbrudd og eksponering av kundedata, har en veldig høy sannsynlighet og en stor konsekvens og vurderes derfor som en ikke akseptabel risiko. For å senke risikoen til *R1*, må Apo-Nett ifølge NSMs grunnprinsipper for IKT sikkerhet ha kontroll på tilganger (2.6.1) og beskytte data (2.7) uansett hvor visualisert infrastruktur man velger. *R1* krever tiltak for å bruke multi-faktor autentisering for å autentisere brukere (2.6.7) og kryptering av lagring som holder konfidensiell data som kan mistes eller kompromitteres (2.7.3). Apo-nett må også etablere sikkerhetsovervåkning (3.2.6) med tanke på personopplysninger som eksisterer i kundedatabasen og gjennomføring av analyser på logger. Implementering av gjenoppretting om data blir tapt er også hensiktsmessig for å hindre tap (2.9.) (NSM, 2024). *R1* senkes til middels risikonivå. For å få dette ned på et forsvarlig lavt nivå anbefaler vi at Apo-nett heller velger utviklere med kompetanse innen sikkerhet, men siden oppgaveteksten tar utgangspunkt i utviklere fra India uten sikkerhetskompetanse så gjør denne risikoanalysen også det.

Risiko *R2*, tjenestenektangrep, har en høy sannsynlighet og en liten konsekvens. For at risiko R2 skal endres til et mer akseptabelt risikovivå må Apo-nett ta for seg NSMs grunnprinsipper om å ha tydelige strukturer og prosesser, sikkerhetspolicier og en konkret plan for hendelseshåndtering (4.1). Teknologiske tiltak som å innføre hendelsesdeteksjon(3.2) og brannmurer hjelper også å senke risikoen til lavt risikonivå.

Risiko *R3*, angrep på webapplikasjonen, har en veldig høy sannsynlighet og en betydelig konsekvens og vurderes som en ikke akseptabel risiko før nye sikkerhetstiltak implementeres.. Tiltak som kan redusere risiko *R3* til lavt risikonivå er også ifølge NSMs grunnprinsipper å utarbeide flere planer og forberede virksomheten på håndtering om et angrep skjer - sikkerhetspolicyer, beredskapsplan (4.1) og en god kontrakt med skylderandøren (2.1.10). I tillegg må passordpolicyen forbedres med å implementere multi-faktor autentisering og redusere tilganger, samt noen teknologiske tiltak som input-validering og å installere en web-applikasjon brannmur (2.4.4) (NSM, 2024)

B - Trusselscenarior med risikovurdering

R1

Trussel:

Datainnbrudd og eksponering av kundeopplysninger på grunn av svakheter i lagring og håndtering av autentisering som fødselsnummer og passord. Angripere skaffer seg uautorisert tilgang til Apo-Nett via teknikker som phishing, SQL-injection eller lekket passord. Angriperen får tilgang til sensitive opplysninger og eksponerer dem eller selger dem videre.

Sårbarheter:

Innloggingsdata er håndtert på en dårlig måte, blant annet at passord er lagret i klartekst, fødselsnummer er lagret i kundedatabasen og mangel på MFA som gjør phising og bruteforce mulig.

Berørte verdier

Personopplysninger - både sensitive og ikke, helseopplysninger fra kjøpshistorikken, tilgangsdata og potensielt systemdata er de mest kritiske verdiene. Dette betyr brudd på konfidensialitet.

Konsekvenser

Det er både juridiske, økonomiske og omdømmemessige konsekvenser på brudd av konfidensialitet. For kunder er mulig konsekvenser av svindel, manglende tilgang på tjenester og tap av tillit. Apo-Nett får økonomisk tap på grunn av bøter, og juridiske konsekvenser på grunn av brudd på GDPR og personopplysningsloven.

Eksisterende sannsynlighets-reduserende og konsekvens-reduserende tiltak

Det finnes enkelte tiltak som kan bidra til å redusere sannsynligheten, men ikke forhindre. Apo-Nett bruker sterk ID for kjøp av reseptbelagte medisiner, ansatte bruker Active Directory og skyleverandøren håndterer mye av sikkerheten. Ingen spesifikke tiltak som reduserer konsekvensene siden Apo-nett mangler en beredskapsplan for hendelser.

Evne til deteksjon av event eller hendelse

Utføre logganalyse, nettverksovervåkning og automatiserte sikkerhetstester er noen metoder som kan oppdage hendelsen, men Apo-Nett har ingen dedikerte sikkerhetsovervåkningstiltak for å fange opp dette.

Begrunnelse av sannsynlighet og konsekvens

På grunn av de mangelfulle sikkerhetsrutinene og lagring av sensitive data regnes sannsynligheten som veldig høy (5). Persondata som kan bli stjålet er sensitive og kan lede til identitetstyveri, som påvirker kundetilitet , utløser skade for enkeltpersoner og høye bøter for virksomheten. Konsekvensen regnes som stor (4).

Kvalitativt risikonivå og Kvantitativt risikonivå

S = 50 og V = 1000000

“S” er kalibreringsfaktor for den snarest forventede hendelse.

“V” er kalibreringsfaktoren for det verste forventet tap.

P	K	R	P	Q	R
5	4	9.0	50.0	1.00E+05	5.00E+06

Disse tallene tilsier at det vil skje en hendelse av denne trusselen 50 ganger i året, og vil koste 1*(10^5) = 100000kr når det skjer. Det vil i snitt hvert år koste bedriften:
5*(10^6) = 5 000 000 kr.

Anbefalte nye sikkerhetstiltak

Organisatoriske: Dataminisering og begrenset lagringstid på sensitive data i kundedatabasen.
Utarbeide prosedyrer for lekkasje og angrep, samt jevnlige beredskapsøvelser og analyser av logger.
Menneskelige: Opplæring i angrep, særlig i phishing-angrep. Endre passordrutiner og innføre bruk av sterke passord og multifaktorautentisering.
Teknologiske: Kryptering av sensitiv data, MFA og zero-trust arkitektur.

Begrunnelse for sannsynlighet og konsekvens etter nye tiltak

Sannsynligheten blir noe redusert med nye tiltak, og sannsynligheten estimeres til sannsynlig (4).
Konsekvensen blir ikke veldig mindre påvirket om hendelsen skjer, og reduseres til betydelig (3).

Kvalitativt risikonivå og Kvantitativt risikonivå etter håndtering

P	K	R	P	Q	R
4	3	7.0	5.0	1.00E+04	5.00E+04

Disse tallene tilsier at det vil skje en hendelse av denne trusselen 5 ganger i året, og vil koste 1*(10^4) = 10000kr når det skjer. Det vil i snitt hvert år koste bedriften:
5*(10^4) = 50 000 kr. Dette er hva risikoen vil koste selskapet i året etter at tiltak er innført.

R2

Trussel:

Trusselaktører kan utføre et tjenestenektangrep på web applikasjon ved å overbelaste front-end-webtjener eller back-end webtjener med store mengder trafikk. Trusselaktøren vil sette systemet ut av drift så ingen legitim trafikk når frem og pasienter ikke får benyttet seg av tjenestene til Apo-Nett.

Sårbarheter:

Det stilles ikke krav om kompetanse for DevOps-utviklerne som skal utvikle og drifte web-plattformen, og skyleverandøren dekker ikke sikkerheten av Apo-nett sine plattformer. Dette vil føre til en plattform med et ukjent antall sårbarheter, samt ingen som følger opp sikkerheten.

Berørte verdier

Verdi: Dynamisk nettside. Tilgjengelighet: Uautorisert angrep på webapplikasjonen kan føre til nedetid. Dette vil påvirke brukernes tilgang til apoteket.

Konsekvenser

Tap av tilgjengeligheten kan føre til økonomiske konsekvenser og tap av tillit og omdømme blant kundene.

Eksisterende sannsynlighets-reduserende og konsekvens-reduserende tiltak

Apo-Nett konfigurerer nettverksinstillinger etter behov, men det mangler en plan for hendelseshåndtering og beredskap. Her antar vi at skyleverandøren ikke vil gjøre noe siden det er målrettede angrep på web-applikasjonen og dermed ikke deres ansvarsområde. Ingen spesifikke tiltak som reduserer konsekvensene

Evne til deteksjon av event eller hendelse

Her antar vi at skyleverandøren har tilgang på logger, analyse av nettverkstrafikk etc. slik som det består beskrevet i case-teksten, men siden angriperne målrettet går for servere utenfor skyleverandørens ansvarsområde, infrastrukturen, så vil de ikke gjøre noe med det. Derfor har Apo-Nett ingen evne til deteksjon av en slik hendelse.

Begrunnelse av sannsynlighet og konsekvens

På grunn av manglende beredskap og plan for hendelseshåndtering, samt mangel på sikkerhetskompetanse hos utviklerne, vil sannsynligheten beregnes som sannsynlig (4).
Dersom brukere ikke får til å bruke nettbutikken, vil dette gi økonomiske konsekvenser for Apo-Nett. Dette utløser hovedsakelig skade for bedriften selv, og derfor vil det ikke være like alvorlig som om det i tillegg hadde påvirket f.eks. brukernes personopplysninger. Brukerne vil også kunne benytte seg av andre lignende tjenester i mellomtiden, så det gir ikke store konsekvenser for hver enkelt bruker. Konsekvensen regnes som liten (2).

Kvalitativt risikonivå og Kvantitativt risikonivå

S = 50 og V= 1000000

P	K	R	P	Q	R
4	2	**6.0**	5.0	1.00E+03	5.00E+03

Disse tallene tilsier at det vil skje en hendelse av denne trusselen 5 ganger i året, og vil koste 1*(10^3) = 1000kr når det skjer. Det vil i snitt hvert år koste bedriften:

5*(10^3) = 5000

Anbefalte nye sikkerhetstiltak

Organisatoriske: opprett en tydelige strukturer og prosesser for sikkerhetsstyring, tydelige sikkerhetspolicyer, samt implementer en konkret plan for hendelseshåndtering og dokumentasjon
Menneskelige: Sikkerhetsopplæring med spesialisert DDoS-opplæring for teknisk personell
Teknologiske: innføre enten egen hendelsesdeteksjon som vil utløse alarmer ved unormal trafikk, eller leie inn et sikkerhetsfirma med en SOC som kan ta seg av det. Innføre bedre brannmurer som kan hjelpe til med å stoppe lignende angrep.

Begrunnelse for sannsynlighet og konsekvens etter nye tiltak

Sannsynligheten blir redusert spesielt med tanke på organisatoriske og tekniske tiltak, og er nå på et nivå (3) mulig. Konsekvens blir ikke påvirket av de nye tiltakene og vil fortsette å være betydelig (2)

Kvalitativt risikonivå og Kvantitativt risikonivå etter håndtering

P	K	R	P	Q	R
3	2	**5.0**	0.5	1.00E+03	5.00E+02

Disse tallene tilsier at det vil skje en hendelse av denne trusselen 0.5 ganger i året, og vil koste 1*(10^3) = 1000kr når det skjer. Det vil i snitt hvert år koste bedriften:

5*(10^2) = 500 kr

R3

Trussel:

Trusselaktør utnytter sårbarhet i Apo-Nett sin webapplikasjonen med angrepsvektor som cross-site scripting, SQL-injection eller bruteforce-angrep

Sårbarheter:

DevOps utviklerne har ikke fokus på sikkerhet som kan føre til sårbarheter som manglende inputvalidering, manglende MFA og andre ukjente sårbarheter som gjør det mulig å gjennomføre angrep på applikasjonen.

Berørte verdier

Verdi: brukeropplysninger / informasjonsopplysninger.
Konfidensialitet: Angriper har tilgang til personopplysninger som i trusselscenario 1.
Integritet: Angriper kan redigere innhold og informasjon, noe som vil gi et brudd på integritet.
Tilgjengelighet: Angriper kan endre på eller slette informasjon fra databaser, og dermed gjøre tjenesten utilgjengelig for de legitime brukerne.
Personvern: Angriper har tilgang til personopplysninger som i trusselscenario 1

Konsekvenser

Konsekvenser kan være at deres applikasjon eller databasen endres, men det er også juridiske og økonomiske konsekvenser som man ser i trusselscenario 1. Eksempler på konkrete konsekvenser kan være at brukere kan miste muligheten til å logge inn, eller at adresse for mottak av vare endres til angriperens adresse og dermed økonomisk tap for kunden.

Eksisterende sannsynlighets-reduserende og konsekvens-reduserende tiltak

Det er noen tiltak som er plass, men de er ikke tilstrekkelige til å beskytte webapplikasjonen. Noen av dem er sikringen av webgrensesnitt og bruk av sterk autentisering for kunder. De eksisterende tiltakene gir liten beskyttelse mot konsekvensene om hendelsen skjer.

Evne til deteksjon av event eller hendelse

Apo-Nett har veldig begrensete metoder for å fange et angrep, der skyleverandørens overvåkning av nettverkstraffikk og mulige feilmeldinger i systemet kan oppdages manuelt, er en av de som Apo-Nett har.

Begrunnelse av sannsynlighet og konsekvens

Det er ingen spesifikke tiltak mot et angrep på webapplikasjonen, som gjør at sannsynligheten for et angrep er veldig snarest (5). På grunn av brukeropplysninger i kundedatabasen som kan bli lekket, samt tjenesten kan bli utilgjengelig av et angrep vurderes konsekvensen som betydelig (3).

Kvalitativt risikonivå og Kvantitativt risikonivå

S = 50 og V= 1000000

P	K	R	P	Q	R
5	3	8.0	50.0	1.00E+04	5.00E+05

Disse tallene tilsier at det vil skje en hendelse av denne trusselen 50 ganger i året, og vil koste 1*(10^4) = 10000kr når det skjer. Det vil i snitt hvert år koste bedriften:
5*(10^5) = 500 000 kr

Anbefalte nye sikkerhetstiltak

Organisatoriske: Utarbeide en sikker kontrakt med skyleverandøren og en beredskapsplan, sterkere sikkerhetsrutiner inkludert sterkere passordrutiner og MFA og tilgangskontroll, implementere klare sikkerhetspolicyer og redusere mengden lagret sensitive data.
Menneskelige: Sterkere passordrutiner og implementere MFA, samt strengere tilgangskontroll.
Teknologiske: Implementere input-validering, sikkerhetsoppdateringer og installere en webapplikasjon brannmur.

Begrunnelse for sannsynlighet og konsekvens etter nye tiltak

Sannsynligheten blir noe redusert til usannsynlig (2), mens konsekvensene forblir som de er om hendelsen skjer, så betydelig (3).

Kvalitativt risikonivå og Kvantitativt risikonivå etter håndtering

P	K	R	P	Q	R
2	3	5.0	0.1	1.00E+04	5.00E+02

Disse tallene tilsier at det vil skje en hendelse av denne trusselen 0.1 ganger i året, og vil koste 1*(10^4) = 10000kr når det skjer. Det vil i snitt hvert år koste bedriften:
5*(10^2) = 500 kr

C - Visualisering

Matrise:

	(5) SS: Svært stor risiko, håndteres med høy prioritet.
	(4) S: Stor risiko, skal håndteres.
	(3) M: Moderat risiko, tiltak bør vurderes.
	(2) L: Liten risiko, kan aksepteres.
	(1) SL: Svært liten risiko, kan ignoreres.

Risiko før sikkerhetstiltak:

(5) Snarest			**R3**	**R1**	
(4) Sannsynlig		**R2**			
(3) Mulig					
(2) Usannsynlig					
(1) Sjeldent					
Sannsynlighet/ Konsekvens	**(1) Ubetydelig**	**(2) Liten**	**(3) Betydelig**	**(4) Stor**	**(5) Verst**

Risiko etter sikkerhetstiltak:

(5) Svært sannsynlig					
(4) Sannsynlig			**R1**		
(3) Mulig		**R2**			
(2) Usannsynlig			**R3**		
(1) Sjeldent					
Sannsynlighet/ Konsekvens	**(1) Ubetydelig**	**(2) Liten**	**(3) Betydelig**	**(4) Stor**	**(5) Verst**

Kilder

CSC (Critical Security Controls) fra CIS (Centre for Internet Security) Hentet 24.mars, 2025 fra
https://www.cisecurity.org/controls

CMMI Institute. (n.d.). Appraisals. Hentet 25. mars, 2025, fra
https://cmmiinstitute.com/learning/appraisals/levels

Datatilsynet.no. (2023, mars 16). *Virksomhetenes plikter*. Overføring av personopplysninger ut av EØS. Hentet mars 24, 2025, fra
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overforing-av-personopplysninger-ut-av-eos/overforingsgrunnlag/

Datatilsynet.no. (2023, juli 26). *Fødselsnummer*. Datatilsynet. Hentet mars 19, 2025, fra
https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/fodselsnummer/

Forskrift om rekvirering og utlevering av legemidler. (2005). *Forskrift om rekvirering og utlevering av legemidler m.m.*. Hentet mars 24, 2025, fra
https://lovdata.no/dokument/SF/forskrift/2022-06-02-977/KAPITTEL_5#KAPITTEL_5

ISO/IEC 27002 Sikkerhetstiltak (utdrag) Hentet mars 25, 2025 fra
https://www.uio.no/studier/emner/matnat/ifi/IN5080/v25/forelesningsvideoer/utdrag-fra-iso-iec-27002.pdf

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

Lovdata.no. (2022, januar 01). *Artikkel 6.Behandlingens lovlighet*. Lov om behandling av personopplysninger (personopplysningsloven). Hentet mars 24, 2025, fra
https://lovdata.no/lov/2018-06-15-38

Lovdata.no. (2022, januar 1). *Avsnitt 3 Vurdering av personvernkonsekvenser og forhåndsdrøftinger*. Lov om behandling av personopplysninger (personopplysningsloven). Hentet mars 24, 2025, fra
https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_35#gdpr/ARTIKKEL_35

The NIST Cybersecurity Framework (CSF) 2.0. Hentet mars 24, 2025, fra
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

NSM. (2024, mai 31). *NSMs Grunnprinsipper for IKT-sikkerhet v2.1*. NSMs Grunnprinsipper for IKT-sikkerhet v2.1. Hentet april 1, 2025, fra

https://nsm.no/getfile.php/1313975-1717589722/NSM/Filer/Dokumenter/Veiledere/NSMs%20Grunnprinsipper%20for%20IKT-sikkerhet%20v2.1.pdf

Personopplysningsloven (2018). *Lov om behandling av personopplysninger: Artikkel 6*. Hentet 24.mars,2025
https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_6#gdpr/ARTIKKEL_6

Personopplysningsloven (2018). *Lov om behandling av personopplysninger: Artikkel 25.Innebygd personvern og personvern som standardinnstilling*. Hentet 24.mars, 2025
https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_25#gdpr&#x2f:ARTIKKEL_25

Personopplysningsloven (2018). *Lov om behandling av personopplysninger: Artikkel 32.Sikkerhet ved behandlingen*. Hentet 24.mars, 2025, fra
https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_32#gdpr&#x2f:ARTIKKEL_32

SP 800-53 Security and Privacy Controls for Systems and Organizations. Hentet 25.mars 2025, fra
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Universitetet i Oslo. (2025). *CMMI for cybersikkerhetsstyring.* https://www-int.uio.no/studier/emner/matnat/ifi/IN5080/v25/forelesningsvideoer/cmmi-for-cybersikkerhet.pdf

Universitetet i Oslo. (2018, 14. desember). *Kort introduksjon til LSIS*. Hentet 25. mars 2025, fra
https://www.uio.no/tjenester/it/sikkerhet/lsis/intro.html

Universitetet i Oslo. (n.d.). L*edelsessystem for informasjonssikkerhet*. Hentet 25. mars 2025, fra
https://www.uio.no/tjenester/it/sikkerhet/lsis/

Universitetet i Oslo. (2020, 30. september). *Ledelsessystem for informasjonssikkerhet: Kapittel 1: Innledning*.
https://www.uio.no/tjenester/it/sikkerhet/lsis/1.html

Universitetet i Oslo. (2017, 17. oktober). *Ledelsessystem for informasjonssikkerhet: Kapittel 3: Mål og strategi*.
https://www.uio.no/tjenester/it/sikkerhet/lsis/3.html

Universitetet i Oslo. (2023, 8. juli). *Ledelsessystem for informasjonssikkerhet: Kapittel 4: Sikkerhetsorganisasjon og ledelse.*
https://www.uio.no/tjenester/it/sikkerhet/lsis/4.html

Universitetet i Oslo. (2022, 5. april). *Ledelsessystem for informasjonssikkerhet: Kapittel 6: Sikkerhetsplan*.
https://www.uio.no/tjenester/it/sikkerhet/lsis/6.html

Universitetet i Oslo. (2025, 17. mars). *Ledelsessystem for informasjonssikkerhet: Kapittel 7: Risiko- og sårbarhetsanalyser.*
https://www.uio.no/tjenester/it/sikkerhet/lsis/7.html

Universitetet i Oslo. (2019, 19. august). *Ledelsessystem for informasjonssikkerhet: Kapittel 14: Internkontroll og sikkerhetsrevisjon.*
https://www.uio.no/tjenester/it/sikkerhet/lsis/14.html