Grunnleggende rammeverk for styrking av cybersikkerhet i kritisk infrastruktur

Norsk oversettelse av NIST CSF Version 1.1

16 April 2018

https://doi.org/10.6028/NIST.CSWP.6.nor

Oversatt av Tor-Ståle Hansen. Gjennomgått av TaikaTranslations LLC. Official U.S. Government Translation.

Den offisielle engelske versjonen av denne utgivelsen er tilgjengelig gratis fra National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.6

Translated by Tor-Ståle Hansen. Reviewed by TaikaTranslations LLC. Official U.S. Government Translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST): https://doi.org/10.6028/NIST.CSWP.6

Anerkjennelser

Anerkjennelser

Denne publikasjonen er et resultat av et samarbeid mellom industri, akademia og myndigheter. National Institute of Standards and Technology (NIST) lanserte prosjektet ved å kalle sammen private og offentlige organisasjoner og enkeltpersoner i 2013. Dette rammeverket for forbedring av cyber-, informasjonssikkerhet, og personopplysningsvern for kritisk infrastruktur ble første gang publisert i 2014 og revidert i løpet av 2017 og 2018, og har basert seg på arbeidsmøter, kommentarer, og tusenvis av direkte interaksjoner med interessenter fra alle sektorer i USA sammen med sektorer i verden for øvrig.
Drivkraften til å endre versjon 1.0 og endringene som vises i denne versjonen, er basert på:

- Tilbakemeldinger og spørsmål til NIST siden utgivelsen av versjon 1.0;
- 105 svar på forespørselen om informasjon (RFI) i desember 2015, og synspunkter på rammeverket for styrking av den digitale sikkerheten i kritisk infrastruktur;

Denne publikasjonen
NOR CSR (Norsk Cyber Sikkerhets Rammeverk), Grunnleggende rammeverk for styrking av cybersikkerhet i kritisk infrastruktur.

Versjon 1 (Mars 2023)

Spørsmål om denne publikasjonen rettes til:

Tor-Ståle Hansen
E-post: tor-stale.hansen@outlook.com

Originalpublikasjonen
Framework for Improving Critical Infrastructure Cybersecurity
Version 1.1
National Institute of Standards and Technology
April 16, 2018

Originalpublikasjonen er tilgjengelig fra: https://doi.org/10.6028/NIST.CSWP.6

Kommentarer til originalpublikasjonen:
National Institute of Standards and Technology
E-post: cyberframework@nist.gov

- Over 85 kommentarer til et foreslått andre utkast av versjon 1.1 fra 5. desember 2017;
- Over 120 kommentarer på et foreslått første utkast til versjon 1.1 av 10. januar 2017; og
- Innspill fra over 1200 deltakere på arbeidsmøter i 2016 og 2017.

I tillegg har NIST tidligere utgitt versjon 1.0 av Cybersecurity Framework med et følgedokument, NIST Roadmap for Improving Critical Infrastructure Cybersecurity. Dette veikartet fremhevet viktige "forbedringsområder" for videre utvikling, tilpasning og samarbeid. Gjennom innsats fra privat og offentlig sektor har noen forbedringsområder kommet så langt til å bli inkludert i denne versjon 1.1.

NIST takker alle som har bidratt.

Original publikasjonen NIST CSF: https://www.nist.gov/cyberframework/framework

Norsk utgave

Norsk utgave av NIST-publikasjoner er ikke utviklet eller gitt ut av NIST. NIST har gitt skriftlig tillatelse til å oversette NIST sine CSF og SP publikasjoner til norsk. I henhold til avtale gir NIST rettighetsinnehaveren til denne publikasjonen rettighetene til å oversette, skrive ut, kopiere, publisere og utgi avledede verk av disse publikasjonene i et hvilket som helst medium, eller autorisere andre til å gjøre det på sine vegne, over hele verden.

Denne utgivelsen er produsert og utgitt i henhold til skriftlig avtale med Applied Cybersecurity Division, Information Technology Laboratory, National Institute of Standards and Technology. ‘NIST CSF’ heter på norsk ‘NOR CSR (Norsk Cyber Sikkerhets Rammeverk) - Rammeverk for styrking av den digitale sikkerheten i kritisk infrastruktur’.

Kommentarer til norsk oversatt utgave rettes til:
Tor-Ståle Hansen
E-post tor-stale.hansen@outlook.com

Sammendrag

Samfunnet er avhengig av pålitelige offentlige og private sentrale organisatoriske funksjoner og teknologistøttet kritisk infrastruktur. Cybersikkerhetstrusler utnytter den økte kompleksiteten og tilkoblingene til kritiske infrastruktur, og setter cybersikkerhet, økonomi og offentlig sikkerhet og funksjon i fare. I likhet med finans- og omdømmerisiko påvirker cybersikkerhetsrisiko organisasjoner, virksomheter og samfunnet direkte med økonomisk tap, stress og i verste konsekvens tap av menneskeliv, og det kan få store funksjonelle- og infrastrukturmessige konsekvenser. For kommersielle og kostnadsdrevene virksomheter kan cybersikkerhetsrisikoer øke kostnadene, men kan også påvirke inntekter, og i noen sammenhenger ha en konkurransemessig effekt. Det kan skade en organisasjons evne til innovasjon og å skaffe og opprettholde ansatte og ikke minst markeder og kunder. Cybersikkerhetstiltak og risiko må derfor være en viktig og forsterkende komponent i en organisasjons samlede risikostyring, som styringsverktøy for strategisk og operative ledelse, og som en fast del av virksomhetens rapportering til og behandling i virksomhetens styre på linje med operasjonelle, økonomiske rapporteringer, saksbehandling og andre faste agendaer i styret.

For bedre å håndtere disse risikoene, oppdaterte Cybersecurity Enhancement Act of 2014[1] (CEA) rollen til National Institute of Standards and Technology (NIST) til å inkludere identifisering og utvikling av risikorammeverk for cybersikkerhet for frivillig bruk av eiere og operatører av kritisk infrastruktur. Gjennom CEA må NIST identifisere "en prioritert, fleksibel, repeterbar, ytelsesbasert og kostnadseffektiv tilnærming, inkludert informasjonssikkerhetstiltak og kontroller som frivillig kan vedtas av eiere og operatører av kritisk infrastruktur for å hjelpe dem med å identifisere, vurdere og håndtere cyberrisiko." Dette formaliserte NISTs tidligere arbeid med å utvikle Rammeverk Versjon 1.0 under Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity" (februar 2013), og ga veiledning for fremtidig rammeverkutvikling. Rammeverket som ble utviklet under EO 13636, og som fortsetter å utvikle seg i henhold til CEA, bruker et felles språk for å adressere og håndtere cybersikkerhetsrisiko på en kostnadseffektiv måte basert på forretnings- og virksomhetsbehov uten å stille ytterligere regulatoriske krav til organisasjonen.

Rammeverket fokuserer på å bruke forretningsdrivere til å veilede cybersikkerhetsaktiviteter og vurdere cybersikkerhetsrisikoer som en del av organisasjonens risikostyringsprosesser. Rammeverket består av tre deler: kjernen, nivå og profiler. ‘Grunnleggende rammeverk’ er et sett med cybersikkerhetsaktiviteter, resultater og informative referanser som er felles på tvers av sektorer og kritisk infrastruktur. Elementer av kjernen gir detaljert veiledning for utvikling av individuelle profiler. Gjennom bruk av profiler vil rammeverket hjelpe en organisasjon med å innrette og prioritere sine cybersikkerhetsaktiviteter med sine forretnings- og virksomhetskrav, risikotoleranser og ressurser. Nivåene gir en mekanisme for organisasjoner til å se og forstå egenskapene til deres tilnærming til håndtering av cybersikkerhetsrisiko, noe som vil hjelpe til med å prioritere og å oppnå cybersikkerhetsmål. Selv om dette dokumentet ble utviklet for å forbedre risikostyringen for cybersikkerhet i kritisk infrastruktur, kan rammeverket brukes av organisasjoner i alle sektorer eller industrier. Rammeverket gjør det mulig for organisasjoner – uavhengig av størrelse, grad av risiko eller sofistikert sikkerhet – å anvende prinsippene og beste praksis for risikostyring for å forbedre sikkerhet og motstandskraft for å oppnå forsvarlig sikkerhet.

Rammeverket gir en struktur for flere tilnærminger til cybersikkerhet ved å sette sammen standarder, retningslinjer og praksiser som sammen fungerer effektivt. Den refererer til globalt anerkjente standarder for cybersikkerhet, og rammeverk kan tjene som modell for internasjonalt samarbeid om å styrke cybersikkerhet i kritisk infrastruktur så vel som andre sektorer, innen privat og offentlig virksomhet.

[1] Se 15 U.S.C. § 272(e)(1)(A)(i). The Cybersecurity Enhancement Act of 2014 (S.1353) ble offentlig rett 113- 274 December 18, 2014 og kan bli funnet på: https://www.congress.gov/bill/113th-congress/senate- bill/1353/text

Rammeverket tilbyr en fleksibel måte å adressere cybersikkerhet, inkludert cybersikkerhet effekt på fysiske-, cyber-, organisasjon- og menneskelige dimensjoner. Den er anvendelig for organisasjoner som er avhengige av teknologi, enten deres cybersikkerhets fokus primært er på informasjonsteknologi (IKT/ICT), industrielle kontrollsystemer (OT/ICS), cyber-fysiske systemer (CPS), eller tilkoblede enheter mer generelt, inkludert tingenes internett (IoT). Rammeverket hjelper også med å håndtere personopplysningsvern ettersom det legger til grunn personvernkontroller. I tillegg tjener rammeverkets resultater som mål for virksomhetsutvikling og utviklingsaktiviteter.

Rammeverket er ikke en helhetlig (total) tilnærming for å håndtere all cybersikkerhetsrisiko for kritisk infrastruktur. Organisasjoner vil fortsatt ha unike risikoer – ulike trusler, ulike sårbarheter og ulike risikotoleranser. De vil også variere i hvordan de tilpasser praksis beskrevet i rammeverket. Organisasjoner kan bestemme aktiviteter som er viktige for kritiske tjenesteleveranser og kan prioritere investeringer for å maksimere effekten av innsatsen. Til syvende og sist er rammeverket rettet mot å redusere og bedre håndtere cybersikkerhetsrisikoer generelt.

For å ta hensyn til organisasjoners unike sikkerhetsbehov finnes det en lang rekke måter å bruke rammeverket på. Beslutningen om hvordan det skal brukes er overlatt til hver enkelt organisasjon - det er ingen mal eller fasit. En organisasjon kan for eksempel velge å bruke implementeringsnivåene for å artikulere tenkt risikostyringspraksis. En annen organisasjon kan bruke rammeverkets fem funksjoner til å analysere hele risikostyringsporteføljen; denne analysen kan være avhengig av mer detaljerte veiledninger, for eksempel kontrollkatalogen NOR SP 800-53 ‘Grunnleggende kontroller for styrking av digital sikkerhet i kritisk infrastruktur’. Noen ganger er det diskusjon om graden man er «i samsvar med», eller «hvor compliant man er» i forhold til rammeverket. Rammeverket kan også brukes som en struktur og språk for å organisere og uttrykke samsvar i forhold til en organisasjons egne krav til cybersikkerhet. Mangfoldet av måter rammeverket kan brukes på av en organisasjon betyr at setninger som er «i samsvar med», eller som sier «hvor compliant man er» kan være forvirrende og bety noe helt annet for ulike interessenter. Det er også viktig å påpeke at «100% compliant» er urealistisk og kan virke mot sin hensikt da det å være compliant overskygger kvaliteten og fokuset på adekvat sikkerhet.

Rammeverket er et levende dokument og vil fortsette å bli oppdatert og forbedret etter hvert som industrien gir tilbakemelding om forbedringer og utvidelser. NIST vil fortsette å koordinere med privat sektor og offentlige etater på alle nivåer. Etter hvert som rammeverket blir brukt i større grad, vil ytterligere erfaringer innlemmes i fremtidige versjoner. Dette vil sikre at rammeverket møter behovene til eiere og operatører av kritisk infrastruktur i et dynamisk og utfordrende miljø med nye trusler, risikoer og løsninger.

Utvidet og mer effektiv bruk og deling av beste praksis i dette frivillige rammeverket er de neste skrittene for å forbedre cybersikkerheten til kritisk infrastruktur, og gir utviklende veiledning for individuelle organisasjoner samtidig som den øker cyber-informasjonssikkerhets- og personopplysningsvern for kritisk infrastruktur, økonomi, helse, justis, forsvar og samfunnet ellers.

Innholdsfortegnelse

1.0 Innføring

Samfunnet er avhengig av pålitelig kritisk infrastruktur. Cybertrusler utnytter den økte kompleksiteten og tilkoblingen til kritisk infrastruktur og systemer, og setter landets sikkerhet, økonomi og offentlig sikkerhet og helse i fare. I likhet med finans- og omdømme-risiko påvirker cybersikkerhetsrisiko en virksomhets bunnlinje, tillit og troverdighet. Det kan øke kostnadene og påvirke inntektene, og det kan skade dens evne til innovasjon og å skaffe og opprettholde kunder. Cybersikkerhet er en viktig og forsterkende komponent i virksomhetens samlede risikostyring.

For å styrke motstandskraften til slik infrastruktur oppdaterte Cybersecurity Enhancement Act (CEA)[2] rollen til National Institute of Standards and Technology (NIST) til å tilrettelegge og støtte utviklingen av rammeverk for cybersikkerhet. Gjennom CEA må NIST identifisere en prioritert, fleksibel, repeterbar, ytelsesbasert og kostnadseffektiv tilnærming, inklusive tiltak og kontroller som kan benyttes av eiere og operatører av kritisk infrastruktur for å hjelpe dem med å identifisere, vurdere og håndtere cyber-risiko. Dette formaliserte NISTs tidligere arbeid med å utvikle Framework Versjon 1.0 under Executive Order 13636 «Improving Critical Infrastructure Cybersecurity», utgitt i februar 2013[3], og ga veiledning for den fremtidige utviklingen av rammeverket.

Kritisk infrastruktur[4] er i U.S. Patriot Act av 2001[5] definert som «systemer og eiendeler, enten fysiske eller virtuelle, [som er viktige for USA], og at manglende evne eller ødeleggelse av slike systemer og eiendeler vil ha en ødeleggende innvirkning på sikkerhet, nasjonal økonomisk sikkerhet, nasjonal folkehelse, eller generell sikkerhet, eller en kombinasjon av disse». På grunn av det økende presset fra eksterne og interne trusler, må organisasjoner som er ansvarlige for kritisk infrastruktur ha en konsistent og iterativ tilnærming til å identifisere, vurdere og administrere cybersikkerhetsrisiko. Denne tilnærmingen er nødvendig uavhengig av en organisasjons størrelse, trusseleksponering eller sofistikerte cybertrusler. Fellesskapet for kritisk infrastruktur inkluderer offentlige og private virksomheter, og andre enheter med en rolle i å bidra med å sikre kritisk infrastruktur. Medlemmer i en sektor utfører funksjoner som støttes av den brede kategorien teknologi, inkludert informasjonsteknologi (IKT/ICT), industrielle kontrollsystemer (OT/ICS), cyber-fysiske systemer (CPS) og tilkoblede enheter mer generelt, inkludert tingenes internett (IoT). Denne avhengigheten av teknologi, kommunikasjon, sammenkobling, organisasjon og operasjon har endret og utvidet de potensielle sårbarhetene og økt de potensielle risikoene. For eksempel, ettersom teknologien og dataene den produserer og behandler i økende grad brukes til å levere kritiske tjenester og støtte forretnings- og virksomhetsbeslutninger, må konsekvensene av en cyberhendelse vurderes hyppigere og basert på flere og bedre dekkende kontroller.

For å håndtere cybersikkerhetsrisikoer kreves en klar forståelse av organisasjonens forretningsdrivere og sikkerhetshensyn som er spesifikke for bruken av teknologi. Fordi hver organisasjons risikoer, prioriteringer og systemer er unike, vil verktøyene og metodene som brukes for å oppnå resultatene beskrevet av rammeverket variere.

Rammeverket anerkjenner rollen virksomheten innehar om det er behandlingsansvarlig eller databehandler, og begge skal beskytte personvernet og de sivile friheter for å skape bedre tillit, og inkludere metodikk og behandlingsprosesser for å beskytte individets personvern og friheter når kritisk infrastruktur behandler slik informasjon. Mange organisasjoner har allerede

[2] Se 15 U.S.C. § 272(e)(1)(A)(i). Cybersecurity Enhancement Act of 2014 (S.1353) ble offentlig lov 113-274 18. desember 2014 og kan finnes på: https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.
[3] Executive Order no. 13636, Improving Critical Infrastructure Cybersecurity, DCPD-201300091, February 12, 2013. https://www.gpo.gov/fdsys/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf
[4] The Department of Homeland Security (DHS) Critical Infrastructure program provides a listing of the sectors and their associated critical functions and value chains. http://www.dhs.gov/critical-infrastructure-sectors
[5] See 42 U.S.C. § 5195c(e)). The U.S. Patriot Act of 2001 (H.R.3162) became public law 107-56 on October 26, 2001 and may be found at: https://www.congress.gov/bill/107th-congress/house-bill/3162

prosesser for å håndtere personvern og sivile friheter. Metodikken er utformet for å utfylle slike prosesser og gi veiledning for å forenkle personvernrisiko i samsvar med en organisasjons tilnærming til cyberrisikostyring. Integrering av personvern og cybersikkerhet kan være til nytte for organisasjoner ved å øke kundenes tillit, muliggjøre mer standardisert deling av informasjon og forenkle operasjoner på tvers av juridiske regimer. Det følger også av lovgivning at behandling av personopplysninger avhenger av og er et lovpålagt behandlingsansvar, og at informasjonssikkerheten er ivaretatt i alle faser før, under og etter en behandling. Man skal, allerede før behandlingen starter, ha gjennomgått og vurdert behandlingens innvirkning på personvernet og individets friheter og rettigheter som følger av lovgivningen. Videre skal selve behandlingens lovlighet følge lovenes definisjoner om den behandlingsansvarliges plikter og ansvar.

Rammeverket forblir effektivt og støtter teknisk innovasjon fordi det er teknologinøytralt, samtidig som det refererer til en rekke eksisterende standarder, retningslinjer og praksiser som utvikler seg med teknologi. Ved å stole på de globale standardene, retningslinjene og praksisene som er utviklet, administrert og oppdatert av industrien, vil verktøyene og metodene som er tilgjengelige for å oppnå rammeverkresultatene skalere på tvers av landegrensene, erkjenne den globale karakteren til cybersikkerhetsrisikoer og utvikle seg med teknologiske fremskritt og forretningskrav. Bruken av eksisterende og nye standarder vil muliggjøre stordriftsfordeler og drive utviklingen av effektive produkter, tjenester og praksiser som oppfyller identifiserte markeds- og industribehov.

Markedskonkurranse fremmer også raskere spredning av disse teknologiene og praksisene, og realisering av mange fordeler i disse sektorene.

Rammeverket bygger på disse standardene, retningslinjene og praksisene, og gir en felles taksonomi og mekanisme for organisasjoner til å:

1) Beskrive nåværende modenhetsnivå med hensyn til cybersikkerhet;

2) Beskrive ambisjonsnivå for cybersikkerhet;

3) Identifisere og prioritere muligheter for forbedring innenfor konteksten av en kontinuerlig og repeterbar prosess;

4) Vurdere cybersikkerhetsstrategien;

5) Kommunisere internt og eksternt om cybersikkerhetsrisikoer.

Rammeverket er ikke en fullstendig, helhetlig eller total tilnærming til å håndtere cybersikkerhetsrisiko for kritisk infrastruktur. Organisasjoner vil fortsatt ha unike risikoer – ulike trusler, ulike sårbarheter, og ulike risikotoleranser. De vil også variere i hvordan de tilpasser praksis beskrevet i rammeverket. Organisasjoner kan bestemme aktiviteter som er viktige for kritiske tjenesteleveranser og kan ulikt prioritere investeringer for å maksimere effekten av innsatsen de legger inn. Til syvende og sist er rammeverket rettet mot å redusere og bedre håndtere cybersikkerhetsrisikoer, informasjonssikkerhet og personopplysningsvernet.

For å ta hensyn til organisasjoners unike sikkerhetsbehov finnes det en lang rekke måter å bruke rammeverket på. Beslutningen om hvordan den skal brukes er overlatt til hver enkelt organisasjon - det er ingen mal eller fasit. En organisasjon kan for eksempel velge å bruke implementeringsnivåene for å artikulere tenkt risikostyringspraksis. En annen organisasjon kan bruke rammeverkets fem funksjoner til å analysere hele risikostyringsporteføljen; denne analysen kan være avhengig av mer detaljerte veiledninger, for eksempel kontrollkatalogen NOR SP 800-53 ‘Grunnleggende kontroller for styrking av digital sikkerhet i kritisk

infrastruktur'. Noen ganger er det diskusjon om graden man er «i samsvar med», eller «hvor compliant man er» i forhold til rammeverket. Rammeverket kan også brukes som en struktur og språk for å organisere og uttrykke samsvar i forhold til en organisasjons egne krav til cybersikkerhet. Mangfoldet av måter rammeverket kan brukes på av en organisasjon betyr at setninger som er «i samsvar med», eller som sier «hvor compliant man er» kan være forvirrende og bety noe helt annet for ulike interessenter. Det er også viktig å påpeke at «100% compliant» er urealistisk og kan virke mot sin hensikt da det å være compliant overskygger kvaliteten og fokuset på adekvat sikkerhet.

Rammeverket utfyller, og erstatter ikke, en organisasjons risikostyringsprosess og sikkerhetsprogram eller portefølje. Organisasjonen kan bruke sine nåværende prosesser og utnytte rammeverket for å identifisere muligheter for å styrke og kommunisere sin håndtering av cybersikkerhetsrisiko samtidig som den er i tråd med bransjepraksis. Alternativt kan en organisasjon uten et eksisterende cybersikkerhetsprogram bruke rammeverket som referanse for å etablere det. Industrier og økosystem kan også benytte rammeverket for å normalisere konkurranse, men også for å etablere felles industrielle krav for cyber-, informasjonssikkerhet og personopplysningsvern i en hel industri.

Selv om rammeverket er utviklet for å forbedre risikostyringen for cybersikkerhet når det gjelder kritisk infrastruktur, kan det brukes av organisasjoner i enhver sektor av økonomien eller samfunnet. Det er ment å være nyttig for selskaper, offentlige etater og ideelle organisasjoner uavhengig av fokus eller størrelse. Den vanlige taksonomien av standarder, retningslinjer og praksis som den gir, er heller ikke spesifikk eller skreddersydd ett spesielt land - cybersikkerhet, informasjonssikkerhet og personopplysningsvern er globalt likt.

Organisasjoner utenfor USA kan også bruke rammeverket til å styrke sin egen cybersikkerhetsinnsats, og rammeverket kan bidra til å utvikle et felles språk for internasjonalt samarbeid om cybersikkerhet, informasjonssikkerhet og personopplysningsvern for kritisk infrastruktur.

1.1 Oversikt over rammeverket

Rammeverket er en risikobasert tilnærming til håndtering av cybersikkerhetsrisiko, og består av tre deler: kjernen, nivå og profiler. Hver komponent forsterker forbindelsen mellom forretnings- og virksomhetsdrivere, og cybersikkerhetsaktiviteter. Disse komponentene er:

- **Kjernen i rammeverket**, som er et sett med identifiserte grunnleggende aktiviteter, basert på grunnleggende resultater og relevante referanser som er vanlige på tvers av kritiske infrastrukturer og er industri- og sektoruavhengige. Kjerneaktivitetene i rammeverket presenterer bransjestandarder, retningslinjer og praksis på en måte som tillater kommunikasjon av cybersikkerhetsaktiviteter og resultater på tvers av organisasjonen fra utøvende nivå til implementerings-, drifts- og operasjonelt nivå. Kjernen i rammeverket består av fem funksjoner – Identifisere, Beskytte, Oppdage, Respondere, og Gjenopprette. Når de vurderes sammen, gir disse aktivitetene et overblikk over livssyklusen og modenhetsnivået til en organisasjons styring av cybersikkerhetsrisiko. Kjernen i rammeverket identifiserer deretter underliggende kategorier og underkategorier som er diskrete utfallskontroller for hver funksjon, og matcher dem med eksempler på informative referanser mot eksisterende andre standarder, retningslinjer og praksis for utfyllende eller flere kontroller på hver underkategori.

- **Implementeringsnivåer** (tiers), som gir kontekst for hvordan en organisasjon ser på cybersikkerhetsrisiko og prosessene for å håndtere denne risikoen. Nivåene

beskriver i hvilken grad en organisasjons risikostyringspraksis for cybersikkerhet viser egenskapene som er definert i rammeverket (f.eks. risiko- og trusselbevisst, repeterbar og adaptiv). Nivåene karakteriserer en organisasjons praksis over et spekter, fra Delvis (Tier 1) til Adaptiv (Tier 4). Disse nivåene reflekterer en progresjon fra uformelle, reaktive reaksjoner til tilnærminger som er smidige og informerte. Under utvelgelsesprosessen bør virksomheten vurdere gjeldende risikohåndteringspraksis, trusselmiljø, juridiske og regulatoriske krav, forretnings- og virksomhetsmål og organisatoriske begrensninger.

- **Rammeverksprofiler** (profil), som representerer resultatene basert på forretningsbehov som en organisasjon har valgt fra rammekategoriene og underkategoriene. Profilen kan karakteriseres som en tilpasning av standarder, retningslinjer og praksis til kjernen i et bestemt implementeringsscenario. Profiler kan brukes til å identifisere muligheter for å forbedre modenhetsnivået ved å sammenligne en gjeldende profils «som den er» tilstand med en mål-profil «å være»-tilstand. For å utvikle en profil kan en organisasjon gjennomgå alle kategoriene og underkategoriene og, basert på forretnings- og virksomhetsdrivere og en risikovurdering, bestemme hvilke som er de viktigste; den kan legge til kategorier og underkategorier etter behov for å håndtere organisasjonens risikoer. Den nåværende profilen kan deretter brukes til å støtte prioritering og måling av fremgang mot målprofilen, mens den tar hensyn til andre forretningsbehov, inkludert kostnadseffektivitet og innovasjon. Profiler kan brukes til å gjennomføre internrevisjon og kommunisere innenfor en organisasjon eller mellom organisasjoner.

1.2 Risikostyring og rammeverk for cybersikkerhet

Risikostyring er den pågående prosessen med å identifisere, vurdere og reagere på risiko. For å håndtere risiko bør organisasjoner forstå sannsynligheten for at en hendelse vil inntreffe og de potensielle resulterende konsekvensene. Med denne informasjonen kan organisasjoner bestemme det akseptable risikonivået for å oppnå sine virksomhetsmål og kan uttrykke dette som deres risikotoleranse.

Med en forståelse av risikotoleranse kan organisasjoner prioritere cybersikkerhetsaktiviteter, slik at organisasjoner kan ta informerte beslutninger om cybersikkerhetsutgifter.

Implementering av risikostyringsprogram gir organisasjoner muligheten til å kvantifisere og kommunisere justeringer av deres cybersikkerhetsprogram. Organisasjoner kan velge å håndtere risiko på forskjellige måter, inkludert å redusere risikoen, overføre risikoen, unngå risikoen eller akseptere risikoen, avhengig av den mulige innvirkningen på levering av kritiske tjenester. Rammeverket bruker risikostyringsprosesser for å gjøre organisasjoner i stand til å informere og prioritere beslutninger angående cybersikkerhet. Den støtter tilbakevendende risikovurderinger og validering av forretningsdrivere for å hjelpe organisasjoner med å velge riktig nivå for cybersikkerhetsaktiviteter som understøtter de ønskede resultater. Dermed gir rammeverket organisasjoner muligheten til dynamisk å velge og styre forbedringer i risikostyring for ICT og ICS.

Rammeverket er tilpasningsdyktig for å gi en fleksibel og risikobasert implementering som kan brukes med et bredt spekter av risikostyringsprosesser for cybersikkerhet. Eksempler på risikostyringsprosesser for cybersikkerhet inkluderer International Organization for Standardization (ISO) 31000:2009[6], ISO/International Electrotechnical Commission (IEC)

[6] International Organization for Standardization, Risk management – Principles and guidelines, ISO 31000:2009, 2009. http://www.iso.org/iso/home/standards/iso31000.htm

27005:2011[7], NIST Special Publication (SP) 800-39[8], og Electricity Subsector Cybersecurity Risk Management Process (RMP)-veiledningen[9].

1.3 Dokumentoversikt

Resten av dette dokumentet inneholder følgende seksjoner og vedlegg:

- **Del 2** beskriver rammekomponentene: kjernen, nivåene og profiler.
- **Del 3** presenterer eksempler på hvordan rammeverket kan brukes.
- **Del 4** beskriver hvordan man bruker rammeverket for selvevaluering og demonstrasjon av forsvarlig sikkerhetsnivå via internrevisjon.
- **Vedlegg A** presenterer kjernen i et tabellformat: funksjonene, kategoriene, underkategorier og informative referanser.
- **Vedlegg B** inneholder en ordliste med utvalgte termer.
- **Vedlegg C** viser akronymer brukt i dette dokumentet.

[7] International Organization for Standardization/International Electrotechnical Commission, Information technology – Security techniques – Information security risk management, ISO/IEC 27005:2011, 2011. https://www.iso.org/standard/56742.html
[8] Joint Task Force Transformation Initiative, Managing Information Security Risk: Organization, Mission, and Information System View, NIST Special Publication 800-39, March 2011.
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
[9] U.S. Department of Energy, Electricity Subsector Cybersecurity Risk Management Process, DOE/OE-0003, May 2012.
https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

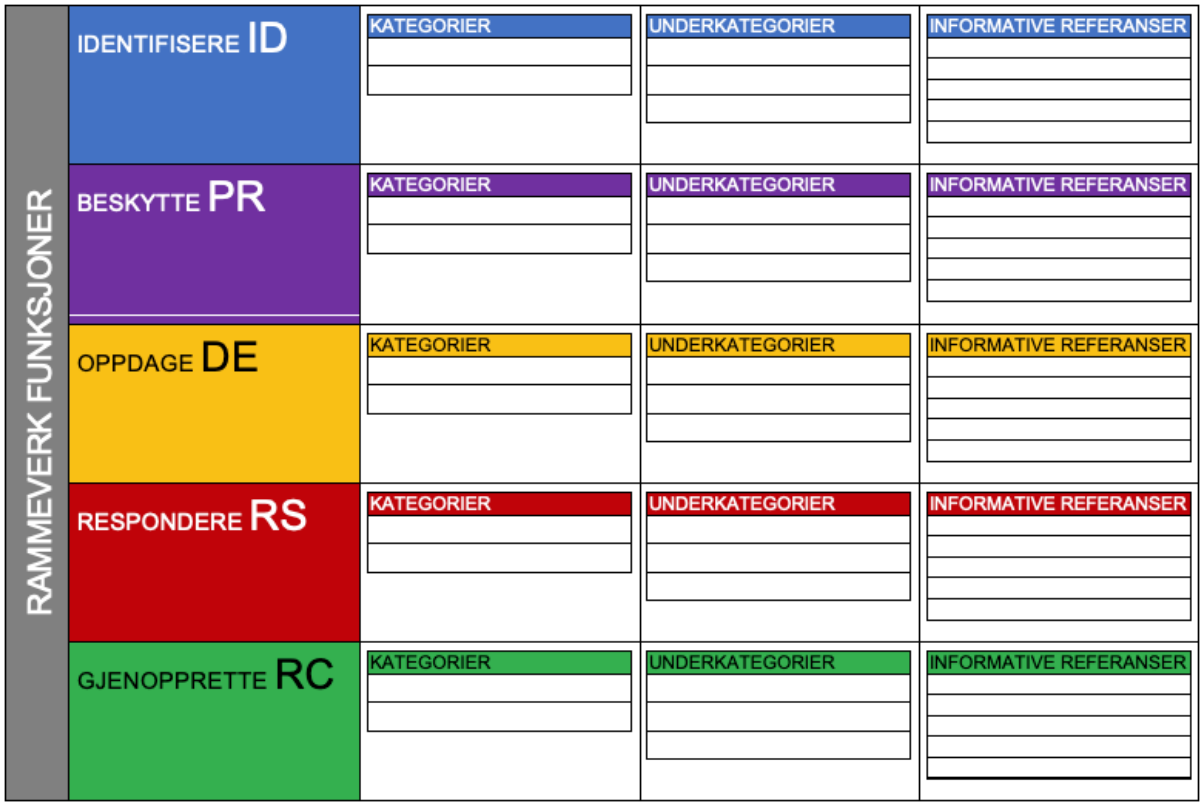
2.0 Rammeverket

Rammeverket gir et felles språk for å forstå, administrere og uttrykke cybersikkerhetsrisiko til interne og eksterne interessenter. Det kan brukes til å identifisere og prioritere handlinger for å redusere cybersikkerhetsrisiko, og det er et verktøy for å samkjøre policy-, forretningsmessige- og teknologiske tilnærminger for å håndtere denne risikoen. Rammeverket kan brukes til å håndtere cybersikkerhetsrisiko på tvers av hele organisasjoner, eller det kan fokuseres på levering av kritiske tjenester i en organisasjon. Ulike typer enheter – inkludert sektorkoordinerende strukturer, foreninger og organisasjoner – kan bruke rammeverket til forskjellige formål, inkludert opprettelse av felles profiler.

2.1 Grunnleggende om rammeverk

Grunnleggende rammeverk gir et sett med aktiviteter for å oppnå spesifikke cybersikkerhets-resultater, og refererer til eksempler i veiledningen for å oppnå disse resultatene.

Rammeverket er ikke en sjekkliste over handlinger som skal utføres. Den presenterer viktige resultater identifisert av områder som er grunnleggende for å håndtere risiko. Rammeverket består av fire elementer: funksjoner, kategorier, underkategorier og informative referanser, vist i figur 1:



Figur 1: Rammeverksstruktur

De grunnleggende elementene fungerer sammen på følgende vis:

- **Funksjoner (tema)** organiserer grunnleggende aktiviteter på sitt høyeste nivå. Disse funksjonene er; Identifisere (ID), Beskytte (PR), Oppdage DE), Respondere (RS) og Gjenopprette (RC), og er identifisert med individuelle fargekoder. De hjelper virksomheten med å definere sin håndtering av cybersikkerhetsrisiko ved å organisere informasjon, muliggjøre risikostyringsbeslutninger, adressere trusler og

forbedre ved å lære av tidligere aktiviteter. Funksjonene stemmer også overens med eksisterende metoder for hendelseshåndtering og hjelper til med å vise effekten av investeringer i cybersikkerhet. For eksempel støtter investeringer i planlegging og øvelser rettidig respons og gjenopprettingshandlinger, noe som resulterer i redusert innvirkning på tjenesteleveranser.

- **Kategorier (område)** er inndelingene av en funksjon i grupper av sikkerhets-resultater som er nært knyttet til behov og aktiviteter. Eksempler på kategorier inkluderer «Ressurshåndtering», «Identitetshåndtering og tilgangskontroll», «Deteksjonsprosesser» mf.

- **Underkategorier (minimum kontroll)** deler videre en kategori inn i spesifikke resultater av tekniske eller organisatoriske aktiviteter. De gir et sett med resultater som, selv om de ikke er uttømmende, bidrar til å støtte et minimum adekvat generelt forsvarlig sikkerhetsnivå i hver kategori. Eksempler på underkategorier inkluderer «Eksterne informasjonssystemer er katalogisert», «Langtidslagrede data er beskyttet» og «Varslinger fra deteksjonssystemer blir undersøkt.»

- **Informative referanser (eksterne referanser)** er spesifikke deler av standarder, retningslinjer og praksiser som er vanlige blant kritiske infrastruktursektorer som illustrerer eller beskriver en metode for å oppnå resultatene knyttet til hver underkategori. De informative referansene som presenteres i kjernen er illustrative og ikke uttømmende. De er basert på veiledning på tvers av sektorer som oftest refereres til i rammeverkets utviklingsprosess.

De fem kjernefunksjoner i rammeverket er definert nedenfor. Disse funksjonene er ikke ment å danne en seriell bane eller føre til en statisk ønsket slutt-tilstand. Snarere bør funksjonene utføres samtidig og kontinuerlig for å danne en operasjonell kultur som adresserer den dynamiske sikkerhetsrisikoen. Se vedlegg A for det fullstendige innholdet i rammeverket.

- **Identifisere** – Etablere en forståelse for håndtering av sikkerhetsrisiko for systemer, mennesker, eiendeler, data og evner. Aktivitetene i Identifisere-funksjonen er grunnleggende for effektiv bruk av rammeverket. Å forstå virksomhetskonteksten, ressursene som støtter kritiske funksjoner og de relaterte sikkerhetsrisikoene gjør det mulig for en virksomhet å fokusere og prioritere sin innsats, i samsvar med dens risikostyringsstrategi og -behov. Eksempler på utfallskategorier innenfor denne funksjonen inkluderer: Ressurshåndtering; Forretningsmiljø; Styresett; Risikovurdering; og Risikostyringsstrategi.

- **Beskytte** – Utvikle og implementere passende sikkerhetstiltak for å beskytte levering av kritiske tjenester. Beskyttelsesfunksjonen støtter muligheten til å forhindre eller begrense virkningen av en potensiell hendelse. Eksempler på utfallskategorier innenfor denne funksjonen inkluderer: Identitetshåndtering og tilgangskontroll; Bevissthet og opplæring; Datasikkerhet; Beskyttelse av informasjon og prosedyrer; Vedlikehold; og Beskyttelsesteknologi.

- **Oppdage** – Utvikle og implementere passende aktiviteter for å identifisere forekomsten av en sikkerhetshendelse. Oppdage-funksjonen muliggjør rettidig oppdagelse av hendelser som fører tileller har potensiale til å føre til en uønsket

hendelse. Eksempler på utfallskategorier innenfor denne funksjonen inkluderer: Avvik og uventede hendelser; Kontinuerlig overvåking; og Deteksjonsprosesser.

- **Respondere** – Utvikle og implementere passende aktiviteter for å iverksette tiltak når en hendelse er oppdaget. Respondere-funksjonen støtter muligheten til å begrense virkningen av en hendelse. Eksempler på utfallskategorier innenfor denne funksjonen inkluderer: Responsplanlegging; Kommunikasjon; Analyse; Skadebegrensning; og Forbedringer.

- **Gjenopprette** – Utvikle og implementere passende aktiviteter for å opprettholde planer for å gjenopprette eventuelle evner eller tjenester som ble svekket på grunn av en hendelse. Gjenopprettingsfunksjonen støtter rettidig gjenoppretting til normal eller en minimal akseptabel driftsstatus. Eksempler på utfallskategorier innenfor denne funksjonen inkluderer: Gjenopprettingsplanlegging; Forbedringer; og Kommunikasjon.

2.2 Implementeringsnivåer

Implementeringsnivåer («Tiers») gir kontekst for hvordan en virksomhet ser på cybersikkerhetsrisiko og prosessene som må på plass for å håndtere denne risikoen. Alt fra delvis (nivå 1) til adaptiv (nivå 4), beskriver nivåer med en økende grad av robusthet og kvalitet i risikostyringsprosessen. Tiers hjelper til med å bestemme i hvilken grad risikostyring er utledet fra forretningsbehov og integrert i en organisasjons overordnede risikostyringspraksis. Risikostyringshensyn inkluderer mange aspekter av cyber- og informasjonssikkerhet, inkludert i hvilken grad hensynet til personvern og rettslige friheter er integrert i en organisasjons styring av cybersikkerhetsrisiko og potensielle personvernrisikoer.

Nivåutvelgelsesprosessen vurderer en virksomhets gjeldende risikohåndteringspraksis, trusselmiljø, juridiske og regulatoriske krav, praksis i forhold til informasjonsdeling, forretnings- og virksomhetsmål, krav til leverandørkjedens cybersikkerhet og organisatoriske begrensninger. Organisasjoner må definere ønsket forsvarlig sikkerhetsnivå, og sikre at det valgte nivået oppfyller organisasjonens målsetninger, er gjennomførbart, og reduserer cybersikkerhetsrisikoen for kritiske eiendeler og ressurser til nivåer som er akseptable for organisasjonen, og personopplysningsvernet ivaretas i henhold til de lovbestemte krav som gjelder. Organisasjoner bør vurdere å utnytte ekstern veiledning innhentet fra myndigheter og eksterne.

Mens organisasjoner identifisert som nivå 1 (delvis) oppfordres til å vurdere å gå mot nivå 2 eller høyere, representerer ikke nivåene modenhet. Nivåene er ment å støtte organisasjonens beslutningstaking om hvordan man skal håndtere cybersikkerhetsrisiko, samt hvilke dimensjoner av organisasjonen som har høyere prioritet og kan motta ekstra ressurser. Progresjon til høyere nivåer oppmuntres når en kostnad-nytte-analyse indikerer en gjennomførbar og kostnadseffektiv reduksjon av cybersikkerhetsrisiko.

Vellykket implementering av rammeverket er basert på oppnåelse av resultatene beskrevet i organisasjonens mål-profiler og ikke på nivåbestemmelse. Likevel påvirker nivåvalg og -betegnelse naturligvis profiler. Nivåanbefalingen fra ledere på forretnings-/prosessnivå, som godkjent av toppledernivået, vil bidra til å sette den overordnede tonen for hvordan cybersikkerhetsrisikoen vil bli administrert i organisasjonen, og bør påvirke prioriteringen innenfor en mål-profil og vurderinger av fremgang i å håndtere hull.

Nivådefinisjonene er som følger:

Nivå 1: Delvis

- *Risikostyringsprosess* – Organisatorisk risikostyringspraksis for cybersikkerhet er ikke formalisert, og risiko håndteres på en ad hoc- og noen ganger reaktiv måte. Prioritering av cybersikkerhetsaktiviteter er kanskje ikke direkte informert av organisatoriske risiko-mål, trusselmiljøet eller krav til virksomhet/oppdrag.

- *Integrert risikostyringsprogram* – Det er begrenset bevissthet om cybersikkerhetsrisiko på organisasjonsnivå. Organisasjonen implementerer risikostyring på en uregelmessig basis fra sak til sak på grunn av variert erfaring eller informasjon fra eksterne kilder. Organisasjonen har kanskje ikke prosesser som gjør det mulig å dele cybersikkerhetsinformasjon i organisasjonen.

- *Ekstern deltakelse* – Organisasjonen forstår ikke sin rolle i det større økosystemet med hensyn til verken dets avhengigheter eller avhengige. Organisasjonen samarbeider ikke med eller mottar informasjon (f.eks. trusseletterretning, beste praksis, teknologier) fra andre enheter (f.eks. kjøpere, leverandører, avhengigheter, avhengige, forskere, myndigheter), og deler heller ikke informasjon. Organisasjonen er generelt uvitende om leverandørrisikoen ved produktene og tjenestene den leverer og som den bruker.

Nivå 2: Risikoinformert

- *Risikostyringsprosess* – Risikostyringspraksisen er godkjent av ledelsen, men kan ikke etableres som en organisasjonsomfattende policy. Prioritering av cybersikkerhetsaktiviteter og beskyttelsesbehov er direkte informert av organisatoriske risikomål, trusselmiljøet eller krav til virksomhet/oppdrag.

- *Integrert risikostyringsprogram* – Det er en bevissthet om cybersikkerhetsrisiko på organisasjonsnivå, men en organisasjonsomfattende tilnærming til håndtering av cybersikkerhetsrisiko er ikke etablert. Informasjon om nettsikkerhet deles i organisasjonen på uformell basis. Hensyn til cybersikkerhet i organisasjonsmål og programmer kan forekomme på noen, men ikke alle nivåer i organisasjonen. Cyber-risikovurdering av organisatoriske og eksterne eiendeler forekommer, men er vanligvis ikke repeterbar eller gjentakende.

- *Ekstern deltakelse* – Generelt forstår organisasjonen sin rolle i det større økosystemet med hensyn til enten sine egne avhengigheter eller avhengige, men ikke begge deler. Organisasjonen samarbeider med og mottar noe informasjon fra andre enheter og genererer noe av sin egen informasjon, men deler kanskje ikke informasjon med andre. I tillegg er organisasjonen klar over leverandørrisikoen knyttet til produktene og tjenestene den leverer og bruker, men handler ikke konsekvent eller formelt i forhold til disse risikoene.

Nivå 3: Repeterbar

- *Risikostyringsprosess* – Organisasjonens risikostyringspraksis er formelt godkjent og uttrykt som policy. Organisatoriske cybersikkerhetspraksiser oppdateres jevnlig basert på anvendelsen av risikostyringsprosesser på endringer i forretnings- og virksomhetskrav og et skiftende trussel- og teknologilandskap.

- *Integrert risikostyringsprogram* – Det finnes en organisasjonsomfattende tilnærming for å håndtere cybersikkerhetsrisiko. Risikoinformerte retningslinjer, prosesser og

prosedyrer blir definert, implementert etter hensikten og gjennomgått. Konsekvente metoder er på plass for å reagere effektivt på endringer i risiko. Personalet har kunnskap og ferdigheter til å utføre sine utpekte roller og ansvar. Organisasjonen overvåker konsekvent og nøyaktig cybersikkerhetsrisiko for organisasjonsressurser. Høytstående cybersikkerhetsledere og de som ikke er cybersikkerhetsledere kommuniserer regelmessig om cybersikkerhetsrisiko. Ledende ledere sikrer hensyn til cybersikkerhet gjennom alle operasjonslinjer i virksomheten.

- *Ekstern deltakelse* – Organisasjonen forstår sin rolle og avhengigheter også i det større økosystemet, og kan bidra til fellesskapets bredere forståelse av risikoer. Organisasjonen samarbeider med og mottar informasjon fra andre enheter regelmessig som utfyller internt generert informasjon, og deler informasjon med andre enheter. Organisasjonen er klar over leverandørkjederisikoen knyttet til produktene og tjenestene den leverer og som den bruker. I tillegg handler organisasjonen vanligvis formelt på disse risikoene, og i tillegg benytter organisasjonen mekanismer som skriftlige avtaler for å kommunisere grunnleggende krav, styringsstrukturer og policyimplementering, overvåking, dokumentasjon, compliance og rapportering.

Nivå 4: Adaptiv

- *Risikostyringsprosess* – Organisasjonen tilpasser sin cybersikkerhetspraksis basert på tidligere og nåværende cybersikkerhetsaktiviteter, inkludert erfaringer og prediktive indikatorer. Gjennom en prosess med kontinuerlig forbedring som inkluderer avanserte cybersikkerhetsteknologier og -praksis, tilpasser organisasjonen seg aktivt til et skiftende trussel- og teknologilandskap, og reagerer på en rettidig og effektiv måte på utviklende, sofistikerte trusler.

- *Integrert risikostyringsprogram* – Det er en organisasjonsomfattende tilnærming til å håndtere cybersikkerhetsrisiko som bruker risikoinformerte retningslinjer, prosesser og prosedyrer for å håndtere potensielle cybersikkerhetshendelser. Forholdet mellom cybersikkerhetsrisiko og organisatoriske mål er tydelig forstått og tatt i betraktning når beslutninger tas. Ledende ledere overvåker cybersikkerhetsrisiko i samme sammenheng som finansiell risiko og andre organisatoriske risikoer. Organisasjonsbudsjettet er basert på en forståelse av det nåværende og predikerte risikomiljøet og risikotoleransen. Forretningsenheter implementerer en ledervisjon og analyserer risikoer på systemnivå i sammenheng med de organisatoriske risiko-toleransene. Risikostyring av cybersikkerhet er en del av organisasjonskulturen og utvikler seg fra en bevissthet om tidligere aktiviteter og kontinuerlig bevissthet om aktiviteter på deres systemer og nettverk. Organisasjonen kan raskt og effektivt redegjøre for endringer i forretnings- og virksomhetsmål i hvordan risiko tilnærmes og kommuniseres.

- *Ekstern deltakelse* - Organisasjonen forstår sin rolle, avhengigheter og avhengige i det større økosystemet og bidrar til samfunnets bredere forståelse av risikoer. Den mottar, genererer og vurderer prioritert informasjon som informerer om kontinuerlig analyse av risikoene etter hvert som trussel- og teknologilandskapet utvikler seg. Organisasjonen deler denne informasjonen internt og eksternt med andre samarbeidspartnere. Organisasjonen bruker sanntids- eller nesten sanntidsinformasjon for å forstå og konsekvent handle på leverandørkjederisikoen knyttet til produktene og tjenestene den leverer og som den bruker. I tillegg kommuniserer den proaktivt ved å bruke formelle (f.eks. avtaler) og uformelle mekanismer for å utvikle og opprettholde sterke leverandørkjedeforhold.

2.3 Rammeprofiler

Rammeprofilen (profiler) er justeringen av funksjonene, kategoriene og underkategoriene med forretningskravene, risikotoleransen og ressursene til organisasjonen. En profil gjør det mulig for organisasjoner å etablere et veikart for å redusere cybersikkerhetsrisikoen som er på linje med organisasjons- og sektormål, vurderer juridiske og regulatoriske krav og bransjebestemmelser og reflekterer risikostyringsprioriteringer. Gitt kompleksiteten til mange organisasjoner, kan de velge å ha flere profiler, tilpasset spesielle komponenter og gjenkjenne deres individuelle behov.

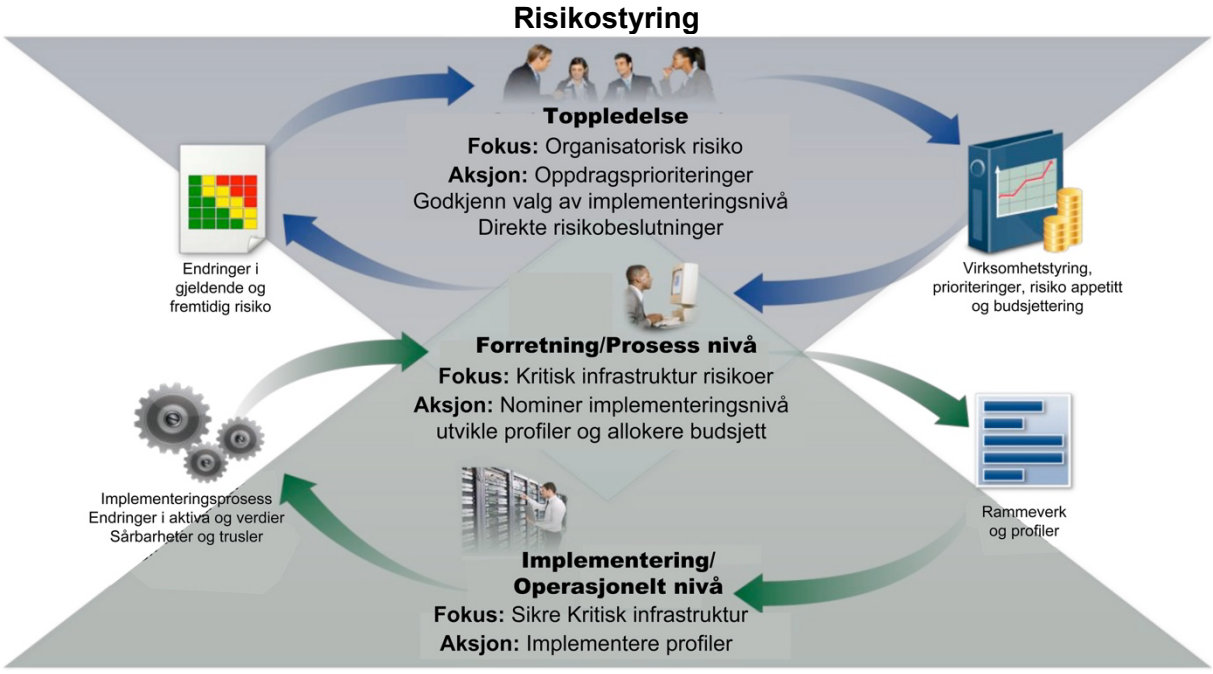
Profiler kan brukes til å beskrive gjeldende tilstand eller ønsket mål-tilstand for spesifikke cybersikkerhetsaktiviteter. Den nåværende profilen indikerer resultatene som nå oppnås. Mål-profilen indikerer resultatene som trengs for å oppnå de ønskede målene for risikostyring for cybersikkerhet. Profiler støtter forretnings- og virksomhetskrav, og hjelper til med å kommunisere risikoen innenfor og mellom organisasjoner. Dette rammeverket gir ikke profilmaler, noe som gir fleksibilitet i implementeringen.

Sammenligning av profiler (f.eks. gjeldende profil og mål-profil) kan avdekke hull som må løses for å oppfylle målene for styring av sikkerhetsrisiko. En handlingsplan for å tette disse hullene for å oppfylle en gitt kategori eller underkategori kan bidra til veikartet beskrevet ovenfor. Prioriteringen av å redusere hull er drevet av organisasjonens forretningsbehov og risikostyringsprosesser. Denne risikobaserte tilnærmingen gjør det mulig for en organisasjon å måle ressursene som trengs (f.eks. bemanning og finansiering) for å oppnå cybersikkerhetsmål på en kostnadseffektiv, prioritert måte. Videre er rammeverket en risikobasert tilnærming der anvendeligheten og oppfyllelsen av en gitt underkategori er underlagt profilens omfang.

2.4 Koordinering og implementering av rammeverk

Figur 2 beskriver en vanlig informasjonsflyt og beslutninger på følgende nivåer i en organisasjon:

- Ledelse (Styrende)
- Forretning/prosess (Gjennomførende-Kontrollerende)
- Implementering/Drift (Gjennomførende-Utøvende)



Figur 2 Implementering: eksempel på beslutnings- og informasjonsflyt

Det utøvende ledelsesnivået kommuniserer oppdragets prioriteringer, tilgjengelige ressurser og generell risikotoleranse til forretnings-/prosessnivået. Forretnings-/prosessnivået bruker informasjonen som input til risikostyringsprosessen, og samarbeider deretter med implementerings-/driftsnivået for å kommunisere forretningsbehov og opprette en profil. Implementerings-/driftsnivået kommuniserer fremdriften på profil-implementeringen til forretnings-/prosessnivået. Forretnings-/prosessnivået bruker denne informasjonen til å utføre en konsekvensutredning. Ledelse på forretnings-/prosessnivå rapporterer resultatene av den konsekvensanalysen til ledernivået for å informere organisasjonens overordnede risikostyringsprosess og til implementerings-/driftsnivået for bevissthet om virksomhetens påvirkning.

3.0 Hvordan bruke rammeverket

En organisasjon kan bruke rammeverket som en sentral del av sin systematiske prosess for å identifisere, vurdere og administrere cybersikkerhetsrisiko. Rammeverket er ikke utformet for å erstatte eksisterende prosesser; en organisasjon kan bruke sin nåværende prosess og legge den over på rammeverket for å finne hull i sin nåværende tilnærming til risiko for cyber-informasjonssikkerhet og personopplysningsvern, og med bakgrunn i det, utvikle et veikart for forbedring. Ved å bruke rammeverket som et risikostyringsverktøy for cybersikkerhet, kan en organisasjon bestemme aktiviteter som er viktigst for kritisk infrastruktur, og prioritere ressursene for å maksimere effekten av investeringen i dette arbeidet.

Rammeverket er utformet for å utfylle eksisterende forretnings- og cybersikkerhets operasjoner. Rammeverket kan tjene som grunnlaget for et nytt cybersikkerhetsprogram eller en mekanisme for å forbedre et eksisterende program. Rammeverket gir et middel til å uttrykke krav til cybersikkerhet til forretningspartnere og kunder, og kan bidra til å identifisere hull i en organisasjons cybersikkerhetspraksis. Den gir også et generelt sett med referanser og prosesser for å vurdere konsekvenser for personvern og sivile friheter i sammenheng med et cybersikkerhetsprogram.

Rammeverket kan brukes gjennom alle livssyklusfasene; fra planlegging, design, prosjektering, til drift, produksjon og helt gjennom dekommisjonering. Planfasen starter syklusen til ethvert system og legger grunnlaget for alt som følger. Cybersikkerhets- aspekter må deklareres og beskrives så tydelig som mulig allerede i planleggingsfasen. Planen må erkjenne at disse aspektene og kravene vil utvikle seg i løpet av resten av livssyklusen. Designfasen må ta hensyn til cybersikkerhetskrav som en del av en større multidisiplinær systemutviklingsprosess.[10] En viktig milepæl i designfasen er at valideringen av systemets cybersikkerhetsspesifikasjoner samsvarer med behovene og risikodisponeringen til organisasjonen som beskrevet i profilene. De ønskede cybersikkerhetsresultatene som er prioritert i en mål-profil må inkluderes når du a) utvikler systemet i byggefasen og b) kjøper eller outsourcer systemet i kjøpsfasen. Den samme mål-profilen fungerer som en liste over systemcybersikkerhetsfunksjoner som må vurderes når systemet distribueres for å bekrefte at alle funksjoner er implementert før produksjonssetting.

Cybersikkerhetsresultatene bestemmes ved å bruke rammeverket, og må da tjene som grunnlag for den pågående driften av systemet. Dette inkluderer sporadisk revurdering, innhenting av resultater i en gjeldende profil, for å verifisere at krav til cybersikkerhet og personopplysningsvernet fortsatt er oppfylt. Vanligvis betyr et komplekst nett av avhengigheter (f.eks. kompenserende og vanlige kontroller) blant systemer, at resultatene

[10] NIST Special Publication 800-160 Volume 1, System Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Ross et al, November 2016 (updated March 21, 2018), https://doi.org/10.6028/NIST.SP.800-160v1

som er dokumentert i mål-profiler for relaterte systemer må vurderes nøye når systemene tas ut av drift og dekommisjoneres.

De følgende avsnittene presenterer ulike måter organisasjoner kan bruke rammeverket på.

3.1 Grunnleggende gjennomgang av cybersikkerhetspraksis

Rammeverket kan brukes til å sammenligne en organisasjons nåværende aktiviteter med de cybersikkerhetsaktivitetene som er skissert i kjernen. Gjennom opprettelsen av en gjeldende profil kan organisasjoner undersøke i hvilken grad de oppnår resultatene beskrevet i kjerne-kategoriene og underkategoriene, på linje med de fem høynivåfunksjonene: Identifisere, Beskytte, Oppdage, Respondere og Gjenopprette. En organisasjon kan oppleve at den allerede oppnår ønskede resultater, og dermed administrere cybersikkerhet i forhold til den kjente risikoen. Alternativt kan en organisasjon fastslå at den har muligheter til å (eller må) forbedres. Organisasjonen kan bruke denne informasjonen til å utvikle en handlingsplan for å styrke eksisterende cybersikkerhetspraksis og redusere cybersikkerhetsrisiko. En organisasjon kan også oppleve at den overinvesterer for å oppnå visse resultater. Organisasjonen kan bruke denne informasjonen til å omprioritere ressurser.

Selv om de ikke erstatter en risikostyringsprosess, vil disse fem funksjonene på høyt nivå gi en kortfattet måte for topplederе og andre å destillere de grunnleggende konseptene for cybersikkerhetsrisiko slik at de kan vurdere hvordan identifiserte risikoer håndteres, og hvordan deres organisasjon stabler. opp på et høyt nivå mot eksisterende cybersikkerhets-standarder, retningslinjer og praksis. Rammeverket kan også hjelpe en organisasjon med å svare på grunnleggende spørsmål, inkludert "Hvordan har vi det?" Deretter kan de bevege seg på en mer informert måte for å styrke sin cybersikkerhetspraksis der og når det anses nødvendig.

3.2 Etablere eller forbedre et cybersikkerhetsprogram

De følgende trinnene illustrerer hvordan en organisasjon kan bruke rammeverket til å lage et nytt cybersikkerhetsprogram eller forbedre et eksisterende program. Disse trinnene bør gjentas etter behov for å kontinuerlig forbedre cybersikkerheten og personopplysningsvernet.

Trinn 1: **Prioriteringer og omfang**. Organisasjonen identifiserer sine forretnings- og virksomhetsmål, og organisasjonsprioriteringer på høyt nivå. Med denne informasjonen tar organisasjonen strategiske beslutninger angående implementeringer av cybersikkerhet og personopplysningsvern, og bestemmer omfanget av systemer og eiendeler som støtter den valgte strategien. Rammeverket kan tilpasses for å støtte de ulike forretningslinjene eller prosessene i en organisasjon, som kan ha ulike forretningsbehov og tilhørende risikotoleranse. Risikotoleranser kan reflekteres i mål-definert implementeringsnivå.

Trinn 2: **Orienter**. Når omfanget av cybersikkerhetsprogrammet er bestemt for virksomheten eller prosessen, identifiserer organisasjonen relaterte systemer og eiendeler, regulatoriske krav og overordnet risikotilnærming. Organisasjonen konsulterer deretter kilder for å identifisere trusler og sårbarheter som gjelder for disse systemene og eiendelene.

Trinn 3: **Opprett en nå-profil**. Organisasjonen utvikler en gjeldende nå-profil ved å indikere hvilke kategori- og underkategoriutfall fra kjernen som oppnås. Hvis et resultat delvis oppnås, vil det å legge merke til dette faktum bidra til å støtte påfølgende trinn ved å gi grunnlagsinformasjon.

Trinn 4: **Gjennomfør en risikovurdering**. Denne vurderingen kan styres av organisasjonens overordnede risikostyringsprosess eller tidligere risikovurderingsaktiviteter. Organisasjonen analyserer det operative miljøet for å se sannsynligheten for en cybersikkerhetshendelse og hvilken innvirkning hendelsen kan ha på organisasjonen. Det er viktig at organisasjoner identifiserer nye risikoer og bruker informasjon om cybertrusler fra

interne og eksterne kilder for å få en bedre forståelse av sannsynligheten og virkningen av cybersikkerhetshendelser.

Trinn 5: **Opprett en mål-profil**. Organisasjonen oppretter en mål-profil som fokuserer på vurderingen av rammekategoriene og underkategoriene som beskriver organisasjonens ønskede forsvarlige sikkerhetsnivå. Organisasjoner kan også utvikle sine egne tilleggskategorier og underkategorier for å ta hensyn til unike organisatoriske risikoer. Organisasjonen kan også vurdere påvirkninger og krav fra eksterne kilder som sektor, markeds- og kundekrav, og forretningspartnere når de oppretter en mål-profil. Mål-profilen må reflektere kriterier innenfor mål-implementeringsnivået.

Trinn 6: **Bestem, analyser og prioriter avvik**. Organisasjonen sammenligner gjeldende profil og mål-profil for å finne avvik. Deretter oppretter organisasjonen en prioritert handlingsplan for å håndtere avvik i henhold til prioriteringer fra oppdragsdrivere, kostnader og fordeler og risikoer, for å oppnå resultatene i mål-profilen. Organisasjonen bestemmer deretter ressurser, inkludert finansiering og arbeidsstyrke, som er nødvendige for å løse avvikene. Å bruke profiler på denne måten oppmuntrer organisasjonen til å ta kvalifiserte beslutninger om cybersikkerhetsaktiviteter, støtter risikostyring og gjør organisasjonen i stand til å utføre kostnadseffektive, målrettede forbedringer.

Trinn 7: **Implementer handlingsplan**. Organisasjonen bestemmer hvilke handlinger som skal iverksettes for å løse avvikene, hvis noen, identifisert i forrige trinn, og justerer deretter gjeldende cybersikkerhetspraksis for å oppnå mål-profilen. For ytterligere veiledning identifiserer rammeverket eksempler på informative referanser angående kategoriene og underkategoriene, men organisasjoner bør bestemme hvilke standarder, retningslinjer og praksis, inkludert de som er sektorspesifikke, som fungerer best for deres behov.
En organisasjon gjentar trinnene etter behov for kontinuerlig å vurdere og forbedre sin cybersikkerhet. For eksempel kan organisasjoner oppleve at hyppigere gjentakelse av orienteringstrinnet forbedrer kvaliteten på risikovurderinger. Videre kan organisasjoner overvåke fremdriften gjennom iterative oppdateringer av den nåværende profilen, og deretter sammenligne den nåværende profilen med mål-profilen. Organisasjoner kan også bruke denne prosessen til å tilpasse cybersikkerhetsprogrammet sitt til ønsket rammeimplementeringsnivå.

3.3 Kommunisere cybersikkerhetskrav med stakeholdere

Rammeverket gir et felles språk for å kommunisere krav mellom stakeholdere (interessenter og aktører) som er ansvarlige for levering av viktige kritiske infrastrukturprodukter og tjenester:

- En organisasjon kan bruke en mål-profil for å uttrykke cybersikkerhet og styringskrav i forhold til risiko til en ekstern tjenesteleverandør (f.eks. en skyleverandør som den eksporterer data til mv.).

- En organisasjon kan uttrykke sin cybersikkerhetstilstand gjennom en gjeldende profil for å rapportere resultater.

- En eier av kritisk infrastruktur, som har identifisert en ekstern partner som denne infrastrukturen er avhengig av, kan bruke en mål-profil for å formidle nødvendige kategorier og underkategorier.

- En kritisk infrastruktur-sektor kan etablere en mål-profil som kan brukes blant dens bestanddeler som en referanse for å bygge sektorens mål-profiler.

- En organisasjon kan bedre håndtere cybersikkerhetsrisiko blant interessenter ved å vurdere deres posisjon i den kritiske infrastrukturen og det digitale økosystemet ved å bruke implementeringsnivåer (tiers).

Kommunikasjon er spesielt viktig opp og ned i forsyningslinjer og leverandørkjeder. Forsyningslinjer og leverandørkjeder er komplekse, globalt distribuerte og sammenkoblede sett med ressurser og prosesser mellom flere organisasjonsnivåer, med hierarki av krav, kontroller og kontrakter. Forsyningslinjer og leverandørkjeder begynner med innkjøp av produkter og tjenester og strekker seg fra design, utvikling, produksjon, prosessering, håndtering og levering av produkter og tjenester til sluttbrukeren. Gitt disse komplekse og sammenkoblede relasjonene, er styring av forsyningslinje- og leverandørkjederisiko (SCRM) en kritisk organisasjonsfunksjon.[11]

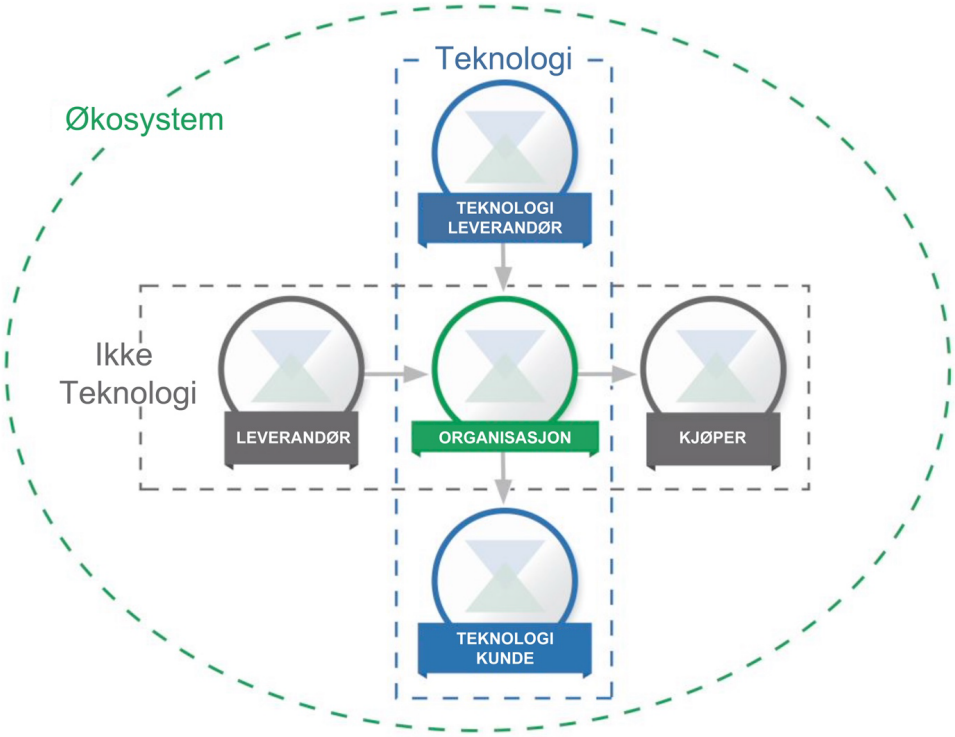
Cyber-SCRM er settet med aktiviteter som er nødvendige for å håndtere cybersikkerhetsrisiko knyttet til eksterne parter. Mer spesifikt adresserer cyber-SCRM både cybersikkerhetseffekten en organisasjon har på eksterne parter og cybersikkerhetseffekten eksterne parter har på en organisasjon.

Et hovedmål med cyber-SCRM er å identifisere, vurdere og redusere "produkter og tjenester som kan inneholde potensielt skadelig funksjonalitet, er forfalsket eller er sårbare på grunn av dårlig produksjons- og utviklingspraksis i forsyningslinjer og leverandørkjeder[12]." Cyber-SCRM-aktiviteter kan omfatte å:

- Fastsette krav til cybersikkerhet for leverandører, roller, ansvar, og dokumentasjon og compliance,
- Vedta cybersikkerhetskrav gjennom formell avtale (f.eks. kontrakter),
- Kommunisere til leverandører hvordan disse cybersikkerhetskravene vil bli verifisert og validert,
- Verifisere at krav til cybersikkerhet oppfylles gjennom en rekke ulike vurderinger, metoder, og
- Styre og administrere aktivitetene ovenfor.

Som vist i figur 3 omfatter Cybersecurity Supply Chain Risk Management (Cyber-SCRM) teknologileverandører og -kjøpere, så vel som ikke-teknologileverandører og -kjøpere, der teknologien minimalt består av informasjonsteknologi (IT), industrielle kontrollsystemer (ICS), cyber-fysiske systemer (CPS), og tilkoblede enheter mer generelt, inkludert tingenes internett (IoT). Figur 3 viser en organisasjon på et enkelt tidspunkt. Gjennom den normale forretningsdriften vil imidlertid de fleste organisasjoner være både oppstrøms leverandør og nedstrøms kjøper i forhold til andre organisasjoner eller sluttbrukere.

[11] Kommunikasjon av cybersikkerhetskrav (avsnitt 3.3) og kjøpsbeslutninger (avsnitt 3.4) omhandler bare to bruksområder av rammeverket for cyber SCRM og er ikke ment å adressere cyber SCRM omfattende.
[12] NIST Special Publication 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, Boyens et al, April 2015, https://doi.org/10.6028/NIST.SP.800-161



Figur 3: Leverandør-/kunde-økosystem

Partene beskrevet i figur 3 utgjør en organisasjons cybersikkerhets-økosystem. Disse relasjonene fremhever den avgjørende rollen til cyber-SCRM i å håndtere cybersikkerhetsrisiko i kritisk infrastruktur og den bredere digitale økonomien. Disse relasjonene, produktene og tjenestene de leverer, og risikoene de utgjør, bør identifiseres og tas med i organisasjonenes beskyttelses- og deteksjonsevner, så vel som deres respons- og gjenopprettingsprotokoller.

I figuren ovenfor refererer "Kjøper" til nedstrøms personer eller organisasjoner som bruker et gitt produkt eller en tjeneste fra en organisasjon, inkludert både for-profit- og non-profit-organisasjoner. "Leverandør" omfatter oppstrøms produkt- og tjenesteleverandører som brukes til en organisasjons interne formål (f.eks. IT-infrastruktur) eller integrert i produktene eller tjenestene som leveres til kjøperen. Disse vilkårene gjelder for både teknologibaserte og ikke-teknologibaserte produkter og tjenester.

Enten man vurderer individuelle underkategorier av kjernen eller de omfattende vurderingene til en profil, tilbyr rammeverket organisasjoner og deres partnere en metode for å sikre at det nye produktet eller tjenesten møter kritiske sikkerhetsresultater. Ved først å velge utfall som er relevante for konteksten (f.eks. overføring av personlig identifiserbar informasjon (PII), virksomhetskritisk tjenestelevering, dataverifiseringstjenester og produkt- eller tjenesteintegritet) kan organisasjonen evaluere partnere mot disse kriteriene. For eksempel, hvis det kjøpes et system som vil overvåke operasjonell teknologi (OT) for unormal cyberverkskommunikasjon, kan tilgjengelighet være et spesielt viktig mål for cybersikkerhet å oppnå, og bør drive en teknologileverandør evaluering mot gjeldende underkategorier (f.eks. ID.BE-4 , ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE AE-5).

3.4 Anskaffelsesprosess

Siden et rammeverks mål-profil er en prioritert liste over organisasjonskrav til cybersikkerhet, kan mål-profiler brukes til å informere beslutninger om kjøp av produkter og tjenester. Det kan variere fra kommunikasjon av cybersikkerhetskrav med interessenter (adressert i avsnitt

3.3) ved at det kanskje ikke er mulig å pålegge leverandøren et sett med cybersikkerhetskrav. Målet bør være å ta den beste anskaffelsesbeslutningen blant flere kvalifiserte leverandører, gitt en nøye fastsatt liste over krav til cybersikkerhet. Ofte betyr dette en viss grad av avveining, å sammenligne flere produkter eller tjenester med kjente avvik mot mål-profilen.

Når et produkt eller en tjeneste er kjøpt, kan profilen også brukes til å spore og adressere gjenværende cybersikkerhetsrisiko. For eksempel, hvis tjenesten eller produktet som ble kjøpt ikke oppfylte alle målene beskrevet i mål-profilen, kan organisasjonen håndtere den gjenværende risikoen gjennom andre beslutninger. Profilen gir også organisasjonen en metode for å vurdere om produktet oppfyller cybersikkerhetsresultater gjennom periodiske gjennomganger og testmekanismer.

3.5 Identifisere muligheter for nye eller reviderte informative referanser

Rammeverket kan brukes til å identifisere muligheter for nye eller reviderte standarder, retningslinjer eller praksis der ytterligere informative referanser vil hjelpe organisasjoner med å møte nye behov. En organisasjon som implementerer en gitt underkategori, eller utvikler en ny underkategori, kan oppdage at det er få informative referanser, om noen, for en relatert aktivitet. For å møte dette behovet kan organisasjonen samarbeide med teknologiledere og/eller standardorganer for å utarbeide, utvikle og koordinere standarder, retningslinjer eller praksis.

3.6 Metodikk for å beskytte personvern og sivile friheter

Denne delen beskriver en metodikk for å håndtere individuelle personvern og frihetsimplikasjoner som kan følge av cyber- og informasjonssikkerhet. Denne metodikken er ment å være et generelt sett med hensyn og prosesser siden implikasjoner for personvern og sivile friheter kan variere fra sektor til sektor, over tid, geografisk, og organisasjoner kan håndtere disse hensynene og prosessene med en rekke tekniske implementeringer. Ikke desto mindre gir ikke alle aktiviteter i et cybersikkerhetsprogram hensyn til personvern og sivile friheter. Lover, forskrifter, tekniske personvernstandarder, retningslinjer og ytterligere beste praksis må kanskje utvikles for å støtte forbedrede tekniske implementeringer. Personvern og cyber- og informasjonssikkerhet har en direkte sammenheng. En organisasjons cybersikkerhetsaktiviteter kan også skape risiko for personvern og sivile friheter når personlig informasjon behandles, samles inn, lagres, vedlikeholdes eller avsløres. Noen eksempler inkluderer: cybersikkerhetsaktiviteter som resulterer i overinnsamling eller overoppbevaring av personlig informasjon; avsløring eller bruk av personlig informasjon som ikke er relatert til cybersikkerhetsaktiviteter; og cybersikkerhetsaktiviteter som resulterer i tjenestenekt eller andre lignende mulige negative konsekvenser, inkludert noen typer hendelsesdeteksjon eller overvåking som kan hemme ytringsfriheten eller friheten til den det gjelder.

Rettssamfunnet har et ansvar for å beskytte personopplysningsvernet og sivile friheter som oppstår fra cybersikkerhetsaktiviteter. Som det refereres til i metodikken nedenfor, bør myndigheter og offentlige virksomheter som eier eller driver kritisk infrastruktur ha en prosess på plass for å støtte overholdelse av cybersikkerhetsaktiviteter med gjeldende personvernlover, forskrifter og avtaler.

For å håndtere behandling av personopplysninger kan organisasjoner vurdere hvordan deres cybersikkerhetsprogram skal inkludere konkrete personvernprinsipper som: dataminimering i behandling, avsløring og oppbevaring av personlig informasjonsmateriale relatert til cybersikkerhetshendelsen; bruke begrensninger utenfor cybersikkerhetsaktiviteter på all informasjon som samles inn spesifikt for cybersikkerhetsaktiviteter; åpenhet for visse cybersikkerhetsaktiviteter; individuelt samtykke og oppreisning for negative konsekvenser som oppstår ved bruk av personlig informasjon i cybersikkerhetsaktiviteter; datakvalitet, integritet og sikkerhet; og ansvarlighet og revisjon.

Ettersom organisasjoner vurderer kjernen i vedlegg A, kan følgende prosesser og aktiviteter betraktes som et middel for å håndtere de ovennevnte implikasjonene for personvern og sivile friheter:

Styring av cybersikkerhetsrisiko (governance)

- En organisasjons vurdering av cybersikkerhetsrisiko og potensielle risikoresponser tar hensyn til personvernimplikasjonene av cybersikkerhetsprogrammet.
- Personer med cybersikkerhetsrelatert personvernansvar rapporterer til riktig ledelse og får passende opplæring.
- Prosessen er på plass for å støtte overholdelse av cybersikkerhetsaktiviteter med gjeldende personvernlover, forskrifter, kontrakter og krav.
- Prosessen er på plass for å vurdere implementering av ovennevnte organisatoriske tiltak og kontroller.

Tilnærminger for å identifisere, autentisere og autorisere enkeltpersoner til å få tilgang til organisatoriske eiendeler og systemer

- Det tas skritt for å identifisere og adressere personvernimplikasjonene av identitetshåndtering og tilgangskontrolltiltak i den grad de involverer innsamling, avsløring eller bruk av personlig informasjon.

Bevisstgjøring og opplæringstiltak

- Gjeldende informasjon fra organisatoriske retningslinjer for personvern er inkludert i opplæring og bevisstgjøringsaktiviteter for cybersikkerhetsarbeidere.
- Tjenesteleverandører som leverer cybersikkerhetsrelaterte tjenester for organisasjonen, er informert om organisasjonens gjeldende personvernregler.

Deteksjon av unormal aktivitet og system- og aktivaovervåking

- Prosessen er på plass for å gjennomføre en personverngjennomgang av en organisasjons oppdagelse av unormal aktivitet og cybersikkerhetsovervåking.

Responsaktiviteter, inkludert informasjonsdeling eller andre avbøtende tiltak

- Prosessen er på plass for å vurdere og adressere hvorvidt, når, hvordan og i hvilken grad personopplysninger deles utenfor organisasjonen som en del av informasjonsdelingsaktiviteter for nettsikkerhet.
- Prosessen er på plass for å gjennomføre en personverngjennomgang av en organisasjons innsats for å redusere cybersikkerhet.

4.0 Internrevisjon og bruk av rammeverket

Grunnleggende rammeverk for styrking av cybersikkerheten i kritisk infrastruktur er utformet for å redusere risiko ved å forbedre styringen av cybersikkerhetsrisiko sett i forhold til organisasjonens forretnings- og virksomhetsmål. Ideelt sett vil organisasjoner som bruker rammeverket være i stand til å måle og tilordne verdier til risikoen deres sammen med kostnadene og fordelene ved tiltak som er tatt for å redusere risikoen til akseptable nivåer. Jo bedre en organisasjon er i stand til å måle risikoen, kostnadene og fordelene ved cybersikkerhetsstrategier, jo mer verdifull vil dens cybersikkerhetstilnærming være.
Over tid bør selvevaluering og måling forbedre beslutningstaking om investeringsprioriteringer. For eksempel, måling – eller i det minste robust karakterisering –

av aspekter ved en organisasjons cybersikkerhetstilstand og trender over tid kan gjøre det mulig for organisasjonen å forstå og formidle meningsfull risikoinformasjon til leverandører, kunder, brukere og andre. En organisasjon kan oppnå dette internt eller ved å søke en tredjeparts verifikasjon og revisjon. Hvis de gjøres riktig og med en forståelse av begrensninger, kan disse målingene gi grunnlag for sterke pålitelige relasjoner, både i og utenfor en organisasjon gjennom forbedret tillit.

For å undersøke effektiviteten til investeringer må en organisasjon først ha en klar forståelse av sine organisatoriske, forretningsmessige-, og virksomhetsmål, forholdet mellom disse målene og de understøttende cybersikkerhetsprogrammene, og hvordan disse diskrete cybersikkerhetsresultatene implementeres og administreres. Selv om målinger av alle disse elementene er utenfor rammeverkets omfang, støtter cybersikkerhetsresultatene til kjernen egenevaluering av investeringseffektivitet og cybersikkerhetsaktiviteter på følgende måter:

- Ta valg om hvordan ulike deler av cybersikkerhetsoperasjonen skal påvirke valget av mål-implementeringsnivåer,
- Evaluere organisasjonens tilnærming til risikostyring og cyberinformasjonssikkerhet og personopplysningsvern ved å bestemme de gjeldende implementeringsnivåene,
- Prioritering av cybersikkerhetsresultater ved å utvikle mål-profiler,
- Bestemme i hvilken grad spesifikke cybersikkerhetstrinn oppnås og ønsket cybersikkerhetsresultater ved å vurdere gjeldende profiler, og
- Måle graden av implementering for kontrollkataloger eller teknisk veiledning som er definert og valgt som informative referanser.

Organisasjoner bør være gjennomtenkte og kreative, men også forsiktige med måtene de bruker målinger på for å optimalisere bruken, samtidig som de unngår å stole på kunstige indikatorer for nåværende tilstand og fremgang i å forbedre risikostyringen for cybersikkerhet. Å bedømme cyberrisiko krever disiplin basert på kunnskap og erfaring, og bør revurderes med jevne mellomrom. Hver gang målinger brukes som en del av rammeprosessen, oppfordres organisasjoner til å tydelig identifisere og vite hvorfor disse målingene er viktige og hvordan de vil bidra til den generelle styringen av cybersikkerhetsrisiko. De bør også være tydelige om begrensningene for målinger som brukes.

For eksempel kan sporing av sikkerhetstiltak og forretningsresultater gi meningsfull innsikt i hvordan endringer i detaljerte sikkerhetskontroller påvirker fullføringen av organisasjonens mål. For å verifisere oppnåelse av noen organisatoriske mål krever at man analyserer dataene først etter at målet skulle ha blitt oppnådd. Denne typen etterslep er mer absolutt. Imidlertid er det ofte mer verdifullt å forutsi om en cybersikkerhetsrisiko kan oppstå, og virkningen det kan ha, ved å bruke et ledende mål. Organisasjoner oppfordres til å innovere og tilpasse hvordan de inkorporerer målinger i deres bruk av rammeverket med full forståelse for deres nytte og begrensninger.

Vedlegg A: Grunnleggende rammeverk

Dette vedlegget presenterer kjernen: en liste over funksjoner, kategorier, underkategorier og informative referanser som beskriver spesifikke cybersikkerhetskontroller som er felles på tvers av alle sektorer for kritisk infrastruktur. Det valgte presentasjonsformatet for kjernen antyder ikke en spesifikk implementeringsrekkefølge, eller antyder en grad av betydning for kategoriene, underkategoriene og informative referanser. Kjernen presentert i dette vedlegget representerer et felles sett med aktiviteter for håndtering av cybersikkerhetsrisiko. Selv om rammeverket ikke er uttømmende, kan det utvides, slik at organisasjoner, sektorer og andre enheter kan bruke underkategorier og informative referanser som er kostnadseffektive og effektive og som gjør dem i stand til å håndtere cybersikkerhetsrisikoen. Aktiviteter kan velges fra kjernen under profilopprettingsprosessen, og ytterligere kategorier, underkategorier og informative referanser kan legges til profilen. En organisasjons risikostyringsprosesser, juridiske/regulatoriske krav, forretnings-/oppdragsmål og organisatoriske begrensninger styrer valget av disse aktivitetene under opprettelsen av profilen. Personopplysninger betraktes som en komponent av data eller eiendeler som er referert til i kategoriene ved vurdering av sikkerhetsrisiko og beskyttelse.

Mens de tiltenkte resultatene identifisert i funksjonene, kategoriene og underkategoriene er de samme for IT og ICS, er driftsmiljøene og hensynene til ICT og ICS forskjellige. ICS har en direkte effekt på den fysiske verden, inkludert potensielle risikoer for helse og sikkerhet for enkeltpersoner og eiendeler og innvirkning på miljøet. I tillegg har ICS unike krav til ytelse og pålitelighet sammenlignet med ICS, og målene om sikkerhet og effektivitet må vurderes ved implementering av cybersikkerhetstiltak. For ICS anbefales et parallelt program hvor man for eksempel ser på IEC 61508-standarden for sikkerhetsintegritets- nivåer.
For enkel bruk gis hver komponent i kjernen en unik identifikator. Funksjoner og kategorier har hver sin unike alfabetiske identifikator, som vist i tabell 1. Underkategorier innenfor hver kategori er referert numerisk; den unike identifikatoren for hver underkategori er inkludert i tabell 2.

Ytterligere støttemateriale, inkludert informative referanser, knyttet til rammeverket kan finnes på NIST-nettstedet på http://www.nist.gov/cyberframework/.

Tabell 1: Unike identifikatorer for funksjoner og kategorier

Funksjon	Kategori ID	Kategori navn
IDENTIFISERE (ID)	ID.AM	Ressurshåndtering
	ID.BE	Forretningsmiljø
	ID.GV	Styresett
	ID.RA	Risikovurdering
	ID.RM	Strategi for risikostyring
	ID.SC	Risikostyring for leverandørkjeden
BESKYTTE (PR)	PR.AC	Identitetsbehandling og tilgangskontroll
	PR.AT	Bevissthet og opplæring
	PR-DS	Datasikkerhet
	PR.IP	Informasjonsbeskyttelsesprosesser og prosedyrer
	PR.MA	Vedlikehold
	PR.PT	Beskyttende teknologi
OPPDAGE (DE)	DE.AE	Uregelmessigheter og hendelser
	DE.CM	Kontinuerlig overvåking av sikkerhet
	DE.DP	Gjenkjenningsprosesser
RESPONDERE (RS)	RS.RP	Planlegging av svar
	RS.CO	Kommunikasjon
	RS.AN	Analyse
	RS.MI	Klimatiltak
	RS.IM	Forbedringer
GJENOPPRETTE (RC)	RC.RP	Planlegging av gjenoppretting
	RC.IM	Forbedringer
	RC.CO	Kommunikasjon

Tabell 2: Kontroller

Funksjon	Kategori	Underkategori	Informativ referanse
IDENTIFISERE (ID)	**Ressurshåndtering (ID.AM)**: Dataene, personalet, enhetene, systemene og fasilitetene som gjør det mulig for organisasjonen å oppnå forretningsformål, identifiseres og administreres i samsvar med deres relative betydning for organisatoriske mål og organisasjonens risikostrategi.	**ID.AM-1**: Fysiske enheter og systemer i organisasjonen er lagerført	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1. **NOR SP 800-53 ver. 1** CM-8, PM-5
		ID.AM-2: Programvareplattformer, systemer og applikasjoner i organisasjonen er lagerført	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NOR SP 800-53 ver. 1** CM-8, PM-5
		ID.AM-3: Kommunikasjon og dataflyt i organisasjonen kartlegges	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NOR SP 800-53 ver. 1** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Eksterne informasjonssystemer er katalogisert	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NOR SP 800-53 ver. 1** AC-20, SA-9
		ID.AM-5: Ressurser (f.eks. maskinvare, enheter, data, tid, personell og programvare) prioriteres basert på deres klassifisering, kritikkverdighet og forretningsverdi	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NOR SP 800-53 ver. 1** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersikkerhetsroller og -ansvar for hele arbeidsstyrken og tredjepartsinteressenter (f.eks. leverandører, kunder og partnere) er etablert	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013 A**.6.1.1 **NOR SP 800-53 ver. 1** CP-2, PS-7, PM-11
	Forretningsmiljø (ID.BE): Organisasjonens oppdrag, mål, interessenter og aktiviteter blir forstått og prioritert; denne informasjonen brukes til å informere om cybersikkerhetsroller, ansvar og beslutninger om risikostyring.	**ID.BE-1**: Organisasjonens rolle i forsyningskjeden identifiseres og kommuniseres	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NOR SP 800-53 ver. 1** CP-2, SA-12
		ID.BE-2: Organisasjonens plass i kritisk infrastruktur og dens industrisektor er identifisert og kommunisert	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NOR SP 800-53 ver. 1** PM-8
		ID.BE-3: Prioriteringer for organisasjonsoppdrag, mål og aktiviteter etableres og kommuniseres	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NOR SP 800-53 ver. 1** PM-11, SA-14
		ID.BE-4: Avhengigheter og kritiske funksjoner for levering av kritiske tjenester etableres	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3

			NOR SP 800-53 ver. 1 CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Krav til motstandskraft for å støtte levering av kritiske tjenester er etablert for alle driftstilstander (f.eks. under tvang/angrep, under utvinning, normal drift)	**COBIT 5** BAI03.02, DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NOR SP 800-53 ver. 1** CP-2, CP-11, SA-13, SA-14
	Styresett (ID.GV): Retningslinjene, prosedyrene og prosessene for å administrere og overvåke organisasjonens regulatoriske, juridiske, risiko-, miljø- og operasjonelle krav er forstått og informerer ledelsen om cybersikkerhetsrisiko.	**ID.GV-1**: Organisatorisk cybersikkerhetspolicy er etablert og kommunisert	**CIS CSC** 19 **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 **ISA** 62443-2-1:2009 4.3.2.6 **ISO/IEC** 27001:2013 A.5.1.1 **NOR SP 800-53 ver. 1** -1 kontroller fra alle sikkerhetskontrollfamilier
		ID.GV-2: Cybersikkerhetsroller og -ansvar er koordinert og på linje med interne roller og eksterne partnere	**CIS CSC** 19 **COBIT 5** APO01.02, APO10.03, APO13.02, DSS 05.04 **ISA** 62443-2-1:2009 4.3.2.3.3 **ISO/IEC** 27001:2013 A.6.1.1, A.7.2.1, A.15.1.1 **NOR SP 800-53 ver. 1** PS-7, PM-1, PM-2
		ID.GV-3: Juridiske og regulatoriske krav angående nettsikkerhet, inkludert forpliktelser om personvern og sivile friheter, er forstått og administrert	**CIS CSC** 19 **COBIT 5** BAI02.01, MEA03.01, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.7 I**SO/IEC** 27001:2013 A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 **NOR SP 800-53 ver. 1** -1 kontroller fra alle sikkerhetskontrollfamilier
		ID.GV-4: Styrings- og risikostyringsprosesser adresserer cybersikkerhetsrisikoer	**COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 **ISO/IEC** 27001:2013 Clause 6 **NOR SP 800-53 ver. 1** SA-2, PM-3, PM-7, PM- 9, PM-10, PM-11
	Risikostyring (ID.RA): Organisasjonen forstår cybersikkerhetsrisikoen for organisasjonsdrift (inkludert oppdrag, funksjoner, image eller omdømme), organisatoriske eiendeler og enkeltpersoner.	**ID.RA-1**: Verdi- / eiendels-sårbarheter er identifisert og dokumentert	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NOR SP 800-53 ver. 1** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Etterretning om cybertrusler mottas fra fora og kilder for informasjonsdeling	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NOR SP 800-53 ver. 1** SI-5, PM-15, PM-16
		ID.RA-3: Trusler, både interne og eksterne, identifiseres og dokumenteres	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Clause 6.1.2 **NOR SP 800-53 ver. 1** RA-3, SI-5, PM-12, PM-16

		ID.RA-4: Potensielle forretningspåvirkninger og sannsynligheter er identifisert	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NOR SP 800-53 ver. 1** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Trusler, sårbarheter, sannsynligheter og påvirkninger brukes til å bestemme risiko	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NOR SP 800-53 ver. 1** RA-2, RA-3, PM-16
		ID.RA-6: Risikoreaksjoner identifiseres og prioriteres	**CIS CSC** 4 **COBIT 5** APO12.05, APO13.02 **ISO/IEC 27001:2013** Clause 6.1.3 **NOR SP 800-53 ver. 1** PM-4, PM-9
	Risikostyringsstrategi (ID.RM): Organisasjonens prioriteringer, begrensninger, risikotoleranser og forutsetninger er etablert og brukt til å støtte beslutninger om operasjonell risiko.	**ID.RM-1**: Risikostyringsprosesser er etablert, administrert og godkjent av organisasjonsinteressenter	**CIS CSC** 4 **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 **NOR SP 800-53 ver. 1** PM-9
		ID.RM-2: Organisatorisk risikotoleranse er bestemt og tydelig uttrykt	**COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.2.6.5 **ISO/IEC 27001**:2013 Clause 6.1.3, Clause 8.3 **NOR SP 800-53 ver. 1** PM-9
		ID.RM-3: Organisasjonens bestemmelse av risikotoleranse er informert om dens rolle i kritisk infrastruktur og sektorspesifikk risikoanalyse	**COBIT 5** APO12.02 **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 **NOR SP 800-53 ver. 1** SA-14, PM-8, PM-9, PM-11
	Risikostyring i forsyningskjeden (ID.SC): Organisasjonens prioriteringer, begrensninger, risikotoleranser og forutsetninger er etablert og brukt til å støtte risikobeslutninger knyttet til styring av forsyningskjederisiko. Organisasjonen har etablert og implementert prosessene for å identifisere, vurdere og administrere forsyningskjederisikoer.	**ID.SC-1**: Risikostyringsprosesser for cyberforsyningskjeden identifiseres, etableres, vurderes, administreres og godkjennes av organisasjonens interessenter	**CIS CSC** 4 **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 **ISA 62443-2-1:2009** 4.3.4.2 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NOR SP 800-53 ver. 1** SA-9, SA-12, PM-9
		ID.SC-2: Leverandører og tredjepartspartnere av informasjonssystemer, komponenter og tjenester blir identifisert, prioritert og vurdert ved hjelp av en risikovurderingsprosess for cyberforsyningskjeden	**COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NOR SP 800-53 ver. 1** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Kontrakter med leverandører og tredjepartspartnere brukes til å implementere passende tiltak utformet for å oppfylle målene til en organisasjons cybersikkerhetsprogram og Cyber Supply Chain Risk Management Plan.	**COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 **NOR SP 800-53 ver. 1** SA-9, SA-11, SA-12, PM-9

		ID.SC-4: Leverandører og tredjepartspartnere vurderes rutinemessig ved å bruke revisjoner, testresultater eller andre former for evalueringer for å bekrefte at de oppfyller sine kontraktsmessige forpliktelser.	**COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 **ISA 62443-2-1:2009** 4.3.2.6.7 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 **NOR SP 800-53 ver. 1** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Planlegging og testing av respons og gjenoppretting utføres med leverandører og tredjepartsleverandører	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.17.1.3 **NOR SP 800-53 ver. 1** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
BESKYTTE (PR)	**Identitetsstyring, autentisering og tilgangskontroll (PR.AC)**: Tilgang til fysiske og logiske eiendeler og tilhørende fasiliteter er begrenset til autoriserte brukere, prosesser og enheter, og administreres i samsvar med den vurderte risikoen for uautorisert tilgang til autoriserte aktiviteter og transaksjoner.	**PR.AC-1**: Identiteter og legitimasjon utstedes, administreres, verifiseres, trekkes tilbake og revideres for autoriserte enheter, brukere og prosesser	**CIS CSC** 1, 5, 15, 16 **COBIT 5** DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.5.1 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 **NOR SP 800-53 ver. 1** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Fysisk tilgang til eiendeler administreres og beskyttes	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 **NOR SP 800-53 ver. 1** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Fjerntilgang administreres	**CIS CSC** 12 COBIT 5 APO13.01, DSS01.04, DSS05.03 ISA 62443-2-1:2009 4.3.3.6.6 **ISA 62443-3-3:2013** SR 1.13, SR 2.6 **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 **NOR SP 800-53 ver. 1** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Tilgangstillatelser og autorisasjoner administreres, og inkluderer prinsippene om minste privilegium og oppgavedeling	**CIS CSC** 3, 5, 12, 14, 15, 16, 18 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.7.3 **ISA 62443-3-3:2013** SR 2.1 **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 **NOR SP 800-53 ver. 1** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Nettverksintegritet er beskyttet (f.eks. nettverkssegregering, nettverkssegmentering)	**CIS CSC** 9, 14, 15, 18 **COBIT 5** DSS01.05, DSS05.02 **ISA 62443-2-1:2009** 4.3.3.4 **ISA 62443-3-3:2013** SR 3.1, SR 3.8 **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 **NOR SP 800-53 ver. 1** AC-4, AC-10, SC-7

		PR.AC-6: Identiteter er bevist og bundet til legitimasjon og hevdet i interaksjoner	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NOR SP 800-53 ver. 1** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Brukere, enheter og andre eiendeler er autentisert (f.eks. enkeltfaktor, multifaktor) i forhold til risikoen ved transaksjonen (f.eks. enkeltpersoners sikkerhets- og personvernrisiko og andre organisatoriske risikoer)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NOR SP 800-53 ver. 1** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Bevissthet og opplæring (PR.AT): Organisasjonens personell og partnere får opplæring om cybersikkerhetsbevissthet og er opplært til å utføre sine cybersikkerhetsrelaterte oppgaver og ansvar i samsvar med relaterte retningslinjer, prosedyrer og avtaler.	**PR.AT-1**: Alle brukere er informert og opplært	**CIS CSC** 17, 18 **COBIT 5** APO07.03, BAI05.07 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 **NOR SP 800-53 ver. 1** AT-2, PM-13
		PR.AT-2: Privilegerte brukere forstår deres roller og ansvar	**CIS CSC** 5, 17, 18 **COBIT 5** APO07.02, DSS05.04, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NOR SP 800-53 ver. 1** AT-3, PM-13
		PR.AT-3: Tredjepartsinteressenter (f.eks. leverandører, kunder, partnere) forstår deres roller og ansvar	**CIS CSC** 17 **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 **NOR SP 800-53 ver. 1** PS-7, SA-9, SA-16
		PR.AT-4: Høytstående ledere forstår sine roller og ansvar	**CIS CSC** 17, 19 **COBIT 5** EDM01.01, APO01.02, APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NOR SP 800-53 ver. 1** AT-3, PM-13
		PR.AT-5: Fysisk og cybersikkerhetspersonell forstår sine roller og ansvar	**CIS CSC** 17 **COBIT 5** APO07.03 **ISA 62443-2-1:2009** 4.3.2.4.2 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NOR SP 800-53 ver. 1** AT-3, IR-2, PM-13

	Datasikkerhet (PR.DS): Informasjon og poster (data) administreres i samsvar med organisasjonens risikostrategi for å beskytte konfidensialitet, integritet og tilgjengelighet til informasjon.	**PR.DS-1**: Data-at-rest er beskyttet	**CIS CSC** 13, 14 **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 **ISA 62443-3-3:2013** SR 3.4, SR 4.1 **ISO/IEC 27001:2013** A.8.2.3 **NOR SP 800-53 ver. 1** MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit er beskyttet	**CIS CSC** 13, 14 **COBIT 5** APO01.06, DSS05.02, DSS06.06 **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 **NOR SP 800-53 ver. 1** SC-8, SC-11, SC-12
		PR.DS-3: Eiendeler administreres formelt gjennom fjerning, overføringer og disponering	**CIS CSC** 1 **COBIT 5** BAI09.03 **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 **NOR SP 800-53 ver. 1** CM-8, MP-6, PE-16
		PR.DS-4: Tilstrekkelig kapasitet for å sikre at tilgjengeligheten opprettholdes	**CIS CSC** 1, 2, 13 **COBIT 5** APO13.01, BAI04.04 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 **NOR SP 800-53 ver. 1** AU-4, CP-2, SC-5
		PR.DS-5: Beskyttelse mot datalekkasjer er implementert	**CIS CSC** 13 **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 **ISA 62443-3-3:2013** SR 5.2 **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 **NOR SP 800-53 ver. 1** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integritetskontroll-mekanismer brukes til å verifisere programvare, fastvare og informasjonsintegritet	**CIS CSC** 2, 3 **COBIT 5** APO01.06, BAI06.01, DSS06.02 **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 **NOR SP 800-53 ver. 1** SC-16, SI-7
		PR.DS-7: Utviklings- og testmiljøet(-miljøene) er atskilt fra produksjonsmiljøet	**CIS CSC** 18, 20 **COBIT 5** BAI03.08, BAI07.04 **ISO/IEC 27001:2013** A.12.1.4 **NOR SP 800-53 ver. 1** CM-2
		PR.DS-8: Integritetskontroll-mekanismer brukes til å verifisere maskinvareintegritet	**COBIT 5** BAI03.05 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISO/IEC 27001:2013** A.11.2.4 **NOR SP 800-53 ver. 1** SA-10, SI-7

	Informasjonsbeskyttelsesprosesser og -prosedyrer (PR.IP): Sikkerhetspolicyer (som tar for seg formål, omfang, roller, ansvar, ledelsesforpliktelse og koordinering mellom organisasjonsenheter), prosesser og prosedyrer vedlikeholdes og brukes til å administrere beskyttelse av informasjonssystemer og eiendeler.	**PR.IP-1**: En grunnlinjekonfigurasjon av informasjonsteknologi/industriell kontrollsystemer opprettes og vedlikeholdes med sikkerhetsprinsipper (f.eks. konseptet med minst funksjonalitet)	**CIS CSC** 3, 9, 11 **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NOR SP 800-53 ver. 1** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: En livssyklus for systemutvikling for å administrere systemer er implementert	**CIS CSC** 18 **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 **ISA 62443-2-1:2009** 4.3.4.3.3 **ISO/IEC 27001:**2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 **NOR SP 800-53 ver. 1** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Kontrollprosesser for konfigurasjonsendringer er på plass	**CIS CSC** 3, 11 **COBIT 5** BAI01.06, BAI06.01 **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 **ISA 62443-3-3:2013** SR 7.6 **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 **NOR SP 800-53 ver. 1** CM-3, CM-4, SA-10
		PR.IP-4: Sikkerhetskopier av informasjon utføres, vedlikeholdes og testes	**CIS CSC** 10 **COBIT 5** APO13.01, DSS01.01, DSS04.07 **ISA 62443-2-1:2009** 4.3.4.3.9 **ISA 62443-3-3:2013** SR 7.3, SR 7.4 **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 **NOR SP 800-53 ver. 1** CP-4, CP-6, CP-9
		PR.IP-5: Retningslinjer og forskrifter vedrørende det fysiske driftsmiljøet for organisasjonsmidler er oppfylt	**COBIT 5** DSS01.04, DSS05.05 **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 **ISO/IEC 27001:**2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 **NOR SP 800-53 ver. 1** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data blir destruert i henhold til retningslinjer	**COBIT 5** BAI09.03, DSS05.06 **ISA 62443-2-1:2009** 4.3.4.4.4 **ISA 62443-3-3:2013** SR 4.2 **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 **NOR SP 800-53 ver. 1** MP-6
		PR.IP-7: Beskyttelsesprosesser er forbedret	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 **NOR SP 800-53 ver. 1** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effektiviteten til beskyttelsesteknologier er delt	**COBIT 5** BAI08.04, DSS03.04 **ISO/IEC 27001:2013** A.16.1.6 **NOR SP 800-53 ver. 1** AC-21, CA-7, SI-4

		PR.IP-9: Responsplaner (Incident Response and Business Continuity) og gjenopprettingsplaner (Incident Recovery and Disaster Recovery) er på plass og administreres	**CIS CSC** 19 **COBIT 5** APO12.06, DSS04.03 **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 **NOR SP 800-53 ver. 1** CP-2, CP-7, CP-12, CP- 13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Respons- og gjenopprettingsplaner testes	**CIS CSC** 19, 20 **COBIT 5** DSS04.04 **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 ISA 62443-3-3:2013 SR 3.3 **ISO/IEC 27001:2013** A.17.1.3 **NOR SP 800-53 ver. 1** CP-4, IR-3, PM-14
		PR.IP-11: Cybersikkerhet er inkludert i personalpraksis (f.eks. deprovisjonering, personellscreening)	**CIS CSC** 5, 16 **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 **NOR SP 800-53 ver. 1** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: En sårbarhetsplan er utviklet og implementert	**CIS CSC** 4, 18, 20 **COBIT 5** BAI03.10, DSS05.01, DSS05.02 **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 **NOR SP 800-53 ver. 1** RA-3, RA-5, SI-2
	Vedlikehold (PR.MA): Vedlikehold og reparasjoner av industrielle kontroll- og informasjonssystemkomponent er utføres i samsvar med retningslinjer og prosedyrer.	**PR.MA-1**: Vedlikehold og reparasjon av organisatoriske eiendeler utføres og logges med godkjente og kontrollerte verktøy	**COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.7 **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 **NOR SP 800-53 ver. 1** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Fjernvedlikehold av organisasjonsressurser godkjennes, logges og utføres på en måte som forhindrer uautorisert tilgang	**CIS CSC** 3, 5 **COBIT 5** DSS05.04 **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 **NOR SP 800-53 ver. 1** MA-4
	Beskyttelsesteknologi (PR.PT): Tekniske sikkerhetsløsninger administreres for å sikre sikkerheten og motstandskraften til systemer og eiendeler, i samsvar med relaterte retningslinjer, prosedyrer og avtaler.	**PR.PT-1**: Revisjons-/loggposter bestemmes, dokumenteres, implementeres og gjennomgås i samsvar med retningslinjer	
		PR.PT-2: Flyttbare medier er beskyttet og bruken er begrenset i henhold til retningslinjer	**CIS CSC** 8, 13 **COBIT 5** APO13.01, DSS05.02, DSS05.06 ISA 62443-3-3:2013 SR 2.3 **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 **NOR SP 800-53 ver. 1** MP-2, MP-3, MP-4, MP- 5, MP-7, MP-8

		PR.PT-3: Prinsippet om minst mulig funksjonalitet er inkorporert ved å konfigurere systemer for å gi kun viktige funksjoner	**CIS CSC** 3, 11, 14 **COBIT 5** DSS05.02, DSS05.05, DSS06.06 **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 **ISO/IEC 27001:2013** A.9.1.2 **NOR SP 800-53 ver. 1** AC-3, CM-7
		PR.PT-4: Kommunikasjons- og kontrollnettverk er beskyttet	**CIS CSC** 8, 12, 15 **COBIT 5** DSS05.02, APO13.01 **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 **NOR SP 800-53 ver. 1** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC- 38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mekanismer (f.eks. feilsikringer, lastbalansering, hot swap) implementeres for å oppnå motstandskrav i normale og ugunstige situasjoner	**COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 **ISA 62443-2-1:2009** 4.3.2.5.2 **ISA 62443-3-3:2013** SR 7.1, SR 7.2 ISO/IEC 27001:2013 A.17.1.2, A.17.2.1 **NOR SP 800-53 ver. 1** CP-7, CP-8, CP-11, CP- 13, PL-8, SA-14, SC-6
OPPDAGE (DE)	**Avvik og hendelser (DE.AE)**: Unormal aktivitet oppdages, og den potensielle virkningen av hendelser er forstått.	**DE.AE-1**: En grunnlinje for nettverksoperasjoner og forventede datastrømmer for brukere og systemer er etablert og administrert	**CIS CSC** 1, 4, 6, 12, 13, 15, 16 **COBIT 5** DSS03.01 **ISA 62443-2-1:2009** 4.4.3.3 **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 **NOR SP 800-53 ver. 1** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Oppdagede hendelser analyseres for å forstå angrepsmål og metoder	**CIS CSC** 3, 6, 13, 15 **COBIT 5** DSS05.07 **ISA 62443-2-1:**2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 **NOR SP 800-53 ver. 1** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Hendelsesdata samles inn og korreleres fra flere kilder og sensorer	**CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 **COBIT 5** BAI08.02 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 **NOR SP 800-53 ver. 1** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Virkningen av hendelser bestemmes	**CIS CSC** 4, 6 **COBIT 5** APO12.06, DSS03.01 **ISO/IEC 27001:2013** A.16.1.4

			NOR SP 800-53 ver. 1 CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Terskler for hendelsesvarsling er etablert	**CIS CSC** 6, 19 **COBIT 5** APO12.06, DSS03.01 **ISA 62443-2-1:2009** 4.2.3.10 **ISO/IEC 27001:2013** A.16.1.4 **NOR SP 800-53 ver. 1** IR-4, IR-5, IR-8
	Kontinuerlig sikkerhets-overvåking (DE.CM): Informasjonssystemet og aktiva overvåkes for å identifisere cybersikkerhetshendelser og verifisere effektiviteten til beskyttelsestiltak.	**DE.CM-1**: Nettverket overvåkes for å oppdage potensielle cybersikkerhetshendelser	**CIS CSC** 1, 7, 8, 12, 13, 15, 16 **COBIT 5** DSS01.03, DSS03.05, DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **NOR SP 800-53 ver. 1** AC-2, AU-12, CA-7, CM- 3, SC-5, SC-7, SI-4
		DE.CM-2: Det fysiske miljøet overvåkes for å oppdage potensielle cybersikkerhetshendelser	**COBIT 5** DSS01.04, DSS01.05 **ISA 62443-2-1:2009** 4.3.3.3.8 **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 **NOR SP 800-53 ver. 1** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personalaktivitet overvåkes for å oppdage potensielle cybersikkerhetshendelser	**CIS CSC** 5, 7, 14, 16 **COBIT 5** DSS05.07 **ISA 62443-3-3:2013** SR 6.2 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 **NOR SP 800-53 ver. 1** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Skadelig kode er oppdaget	**CIS CSC** 4, 7, 8, 12 **COBIT 5** DSS05.01 **ISA 62443-2-1:2009** 4.3.4.3.8 **ISA 62443-3-3:2013** SR 3.2 **ISO/IEC 27001:2013** A.12.2.1 **NOR SP 800-53 ver. 1** SI-3, SI-8
		DE.CM-5: Uautorisert mobilkode er oppdaget	**CIS CSC** 7, 8 **COBIT 5** DSS05.01 **ISA 62443-3-3:2013** SR 2.4 **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 **NOR SP 800-53 ver. 1** SC-18, SI-4, SC-44
		DE.CM-6: Ekstern tjeneste-leverandørs aktivitet overvåkes for å oppdage potensielle cybersikkerhetshendelser	**COBIT 5** APO07.06, APO10.05 **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 **NOR SP 800-53 ver. 1** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Overvåking for uautorisert personell, tilkoblinger, enheter og programvare utføres	**CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 **COBIT 5** DSS05.02, DSS05.05 **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 **NOR SP 800-53 ver. 1** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Sårbarhetsskanninger utføres	**CIS CSC** 4, 20 **COBIT 5** BAI03.10, DSS05.01 **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 **ISO/IEC 27001:2013** A.12.6.1 **NOR SP 800-53 ver. 1** RA-5
	Deteksjonsprosesser (DE.DP): Deteksjonsprosesser og prosedyrer vedlikeholdes og testes for å sikre bevissthet om unormale hendelser.	**DE.DP-1**: Roller og ansvar for deteksjon er godt definert for å sikre ansvarlighet	**CIS CSC** 19 **COBIT 5** APO01.02, DSS05.01, DSS06.03 **ISA 62443-2-1:2009** 4.4.3.1 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 **NOR SP 800-53 ver. 1** CA-2, CA-7, PM-14

		DE.DP-2: Deteksjonsaktiviteter overholder alle gjeldende krav	**COBIT 5** DSS06.01, MEA03.03, MEA03.04 **ISA 62443-2-1:2009** 4.4.3.2 **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 **NOR SP 800-53 ver. 1** AC-25, CA-2, CA-7, SA- 18, SI-4, PM-14
		DE.DP-3: Deteksjonsprosesser er testet	**COBIT 5** APO13.02, DSS05.02 **ISA 62443-2-1:2009** 4.4.3.2 **ISA 62443-3-3:2013** SR 3.3 **ISO/IEC 27001:2013** A.14.2.8 **NOR SP 800-53 ver. 1** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Informasjon om hendelsesdeteksjon kommuniseres	**CIS CSC** 19 **COBIT 5** APO08.04, APO12.06, DSS02.05 **ISA 62443-2-1:2009** 4.3.4.5.9 **ISA 62443-3-3:2013** SR 6.1 **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 **NOR SP 800-53 ver. 1** AU-6, CA-2, CA-7, RA- 5, SI-4
		DE.DP-5: Deteksjonsprosesser blir kontinuerlig forbedret	**COBIT 5** APO11.06, APO12.06, DSS04.05 **ISA 62443-2-1:2009** 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6 **NOR SP 800-53 ver. 1**, CA-2, CA-7, PL-2, RA- 5, SI-4, PM-14
RESPONDERE (RS)	**Responsplanlegging (RS.RP):** Responsprosesser og prosedyrer utføres og vedlikeholdes for å sikre respons på oppdagede cybersikkerhetshendelser.	**RS.RP-1**: Responsplan utføres under eller etter en hendelse	**CIS CSC** 19 **COBIT 5** APO12.06, BAI01.10 **ISA 62443-2-1:2009** 4.3.4.5.1 **ISO/IEC 27001:2013** A.16.1.5 **NOR SP 800-53 ver. 1** CP-2, CP-10, IR-4, IR-8
	Kommunikasjon (RS.CO): Responsaktiviteter koordineres med interne og eksterne interessenter (f.eks. ekstern støtte fra rettshåndhevende organer).	**RS.CO-1:** Personell kjenner sine roller og operasjonsrekkefølge når det er behov for respons	**CIS CSC** 19 **COBIT 5** EDM03.02, APO01.02, APO12.03 **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 **NOR SP 800-53 ver. 1** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Hendelser rapporteres i samsvar med etablerte kriterier	**CIS CSC** 19 **COBIT 5** DSS01.03 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 **NOR SP 800-53 ver. 1** AU-6, IR-6, IR-8
		RS.CO-3: Informasjon deles i samsvar med responsplaner	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.2 **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 **NOR SP 800-53 ver. 1** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Koordinering med interessenter skjer i samsvar med responsplaner	**CIS CSC** 19 **COBIT 5** DSS03.04 **ISA 62443-2-1:2009** 4.3.4.5.5 **ISO/IEC 27001:2013** Clause 7.4 **NOR SP 800-53 ver. 1** CP-2, IR-4, IR-8
		RS.CO-5: Frivillig informasjonsdeling skjer med eksterne interessenter for å oppnå bredere situasjonsbevissthet om nettsikkerhet	**CIS CSC** 19 **COBIT 5** BAI08.04 **ISO/IEC 27001:2013** A.6.1.4 **NOR SP 800-53 ver. 1** SI-5, PM-15

	Analyse (RS.AN): Analyse utføres for å sikre effektiv respons og støtte gjenopprettingsaktiviteter.	**RS.AN-1**: Meldinger fra deteksjonssystemer undersøkes	**CIS CSC** 4, 6, 8, 19 **COBIT 5** DSS02.04, DSS02.07 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 ISA 62443-3-3:2013 SR 6.1 **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 **NOR SP 800-53 ver. 1** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: Virkningen av hendelsen er forstått	**COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 **NOR SP 800-53 ver. 1** CP-2, IR-4
		RS.AN-3: Kriminaltekniske undersøkelser utføres	**COBIT 5** APO12.06, DSS03.02, DSS05.07 **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 **ISO/IEC 27001:2013** A.16.1.7 **NOR SP 800-53 ver. 1** AU-7, IR-4
		RS.AN-4: Hendelser er kategorisert i samsvar med responsplaner	**CIS CSC** 19 **COBIT 5** DSS02.02 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISO/IEC 27001:2013** A.16.1.4 **NOR SP 800-53 ver. 1** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Prosesser er etablert for å motta, analysere og svare på sårbarheter som avsløres til organisasjonen fra interne og eksterne kilder (f.eks. intern testing, sikkerhetsbulletiner eller sikkerhetsforskere)	**CIS CSC** 4, 19 **COBIT 5** EDM03.02, DSS05.07 **NOR SP 800-53 ver. 1** SI-5, PM-15
	Redusering (RS.MI): Aktiviteter utføres for å forhindre utvidelse av en hendelse, dempe dens virkninger og løse hendelsen.	**RS.MI-1**: Hendelser er begrenset	**CIS CSC** 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6 **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 **NOR SP 800-53 ver. 1** IR-4
		RS.MI-2: Hendelser mitigeres	**CIS CSC** 4, 19 **COBIT 5** APO12.06 **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 NOR SP 800-53 ver. 1 IR-4
		RS.MI-3: Nylig identifiserte sårbarheter reduseres og dokumenteres med eventuelt aksepterte residualrisikoer og kompenserende tiltak	**CIS CSC** 4 **COBIT 5** APO12.06 **ISO/IEC 27001:2013** A.12.6.1 **NOR SP 800-53 ver. 1** CA-7, RA-3, RA-5
	Forbedringer (RS.IM): Organisatoriske responsaktiviteter forbedres ved å inkludere erfaringer fra nåværende og tidligere deteksjons-/responsaktiviteter.	**RS.IM-1**: Responsplaner inkluderer erfaringer	**COBIT 5** BAI01.13 **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NOR SP 800-53 ver. 1** CP-2, IR-4, IR-8
		RS.IM-2: Responsstrategier er oppdatert	**COBIT 5** BAI01.13, DSS04.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NOR SP 800-53 ver. 1** CP-2, IR-4, IR-8

GJENOPPRETTE (RC)	**Gjenopprettingsplanlegging (RC.RP):** Gjenopprettingsprosesser og prosedyrer utføres og vedlikeholdes for å sikre gjenoppretting av systemer eller eiendeler som er påvirket av cybersikkerhetshendelser.	**RC.RP-1**: Gjenopprettingsplan utføres under eller etter en cybersikkerhetshendelse	**CIS CSC** 10 **COBIT 5** APO12.06, DSS02.05, DSS03.04 **ISO/IEC 27001:2013** A.16.1.5 **NOR SP 800-53 ver. 1** CP-10, IR-4, IR-8
	Forbedringer (RC.IM): Planlegging og prosesser for gjenoppretting forbedres ved å inkludere lærdom i fremtidige aktiviteter.	**RC.IM-1**: Gjenopprettingsplaner inkluderer lærdom	**COBIT 5** APO12.06, BAI05.07, DSS04.08 ISA 62443-2-1:2009 4.4.3.4 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NOR SP 800-53 ver. 1** CP-2, IR-4, IR-8
		RC.IM-2: Gjenopprettings-strategier er oppdatert	**COBIT 5** APO12.06, BAI07.08 **ISO/IEC 27001:2013** A.16.1.6, Clause 10 **NOR SP 800-53 ver. 1** CP-2, IR-4, IR-8
	Kommunikasjon (RC.CO): Restaureringsaktiviteter koordineres med interne og eksterne parter (f.eks. koordineringssentre, internett-leverandører, eiere av angripende systemer, ofre, andre CSIRTer og leverandører).	**RC.CO-1**: PR administreres	**COBIT 5** EDM03.02 **ISO/IEC 27001:2013** A.6.1.4, klausul 7.4
		RC.CO-2: Omdømme repareres etter en hendelse	**COBIT 5** MEA03.02 **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Gjenopprettings-aktiviteter kommuniseres til interne og eksterne interessenter så vel som ledere og ledergrupper	**COBIT 5** APO12.06 **ISO/IEC 27001:2013** Clause 7.4 **NOR SP 800-53 ver. 1** CP-2, IR-4

Informasjon om informative referanser beskrevet i vedlegg A kan finnes på følgende steder:

- Kontrollmål for informasjon og relatert teknologi (COBIT): http://www.isaca.org/COBIT/Pages/default.aspx
- CIS Critical Security Controls for Effective Cyber Defense (CIS Controls): https://www.cisecurity.org
- American National Standards Institute/International Society of Automation (ANSI/ISA)-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems: Etablering av et Industrial Automation and Control Systems Security Program: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116731
- ANSI/ISA-62443-3-3 (99.03.03)-2013, Security for Industrial Automation and Control Systems: System Security Requirements and Security Levels: https://www.isa.org/templates/one-column.aspx?pageid=111294&productId=116785
- ISO/IEC 27001, Informasjonsteknologi -- Sikkerhetsteknikker -- Styringssystemer for informasjonssikkerhet -- Krav: https://www.iso.org/standard/54534.html
- NOR SP 800-53 ver. 1 - NIST Special Publication 800-53 Revisjon 4, Security and Privacy Controls for Federal Information Systems and Organizations, april 2013 (inkludert oppdateringer fra 22. januar 2015). https://doi.org/10.6028/NIST.SP.800-53r4. Informative referanser er bare tilordnet kontrollnivået, selv om enhver kontrollforbedring kan være nyttig for å oppnå et underkategoriresultat.

Tilordninger mellom underkategoriene og de spesifiserte seksjonene i de informative referansene er ikke ment å definitivt avgjøre om de spesifiserte seksjonene i de informative referansene gir det ønskede underkategoriresultatet.

Informative referanser er ikke uttømmende, ved at ikke alle elementer (f.eks. kontrollkrav) i en gitt informativ referanse er tilordnet underkategorier.

Vedlegg B: Begrepsfastsettelse

Dette vedlegget definerer utvalgte begreper som brukes i publikasjonen og korrelasjon mot engelskspråklige begreper.

Tabell 3: Ordliste

Buyer	Kjøper	Menneskene eller organisasjonene som bruker et gitt produkt eller en gitt tjeneste mot vederlag.
Category	Kategori	Underinndelingen av en funksjon i grupper av cybersikkerhetsresultater, nært knyttet til programmatiske behov og spesielle aktiviteter. Eksempler på kategorier inkluderer «Ressurshåndtering», «Identitetshåndtering og tilgangskontroll» og «Deteksjonsprosesser».
Critical Infrastructure	Kritisk infrastruktur	Systemer og eiendeler, enten fysiske eller virtuelle, er så viktige for USA at manglende evne eller ødeleggelse av slike systemer og eiendeler vil ha en ødeleggende innvirkning på cybersikkerhet, nasjonal økonomisk sikkerhet, nasjonal folkehelse eller sikkerhet, eller en hvilken som helst kombinasjon av disse sakene.
Cybersecurity	Cybersikkerhet	Forebygging av skade på, beskyttelse av og gjenoppretting av datamaskiner, elektroniske kommunikasjonssystemer, elektroniske kommunikasjonstjenester, trådkommunikasjon og elektronisk kommunikasjon, inkludert informasjonen, for å sikre tilgjengelighet, integritet, autentisering, konfidensialitet og ikke-benektelse.
Cybersecurity Event	Cybersikkerhetshendelse	En endring av nettsikkerhet som kan ha innvirkning på organisasjonsdrift (inkludert oppdrag, evner eller omdømme).
Cybersecurity Incident	Uønsket hendelse relatert til cybersikkerhet	En cybersikkerhetshendelse som har blitt fastslått å ha en innvirkning på organisasjonen, noe som gir behov for respons og gjenoppretting.
Detect (function)	Oppdage (funksjon)	Utvikle og implementere passende aktiviteter for å identifisere forekomsten av en cybersikkerhetshendelse.
Framework	Rammeverk	En risikobasert tilnærming for å redusere cybersikkerhetsrisiko som består av tre deler: rammekjernen, rammeprofilen og rammeimplementeringsnivåene. Også kjent som "Cybersecurity Framework."
Framework Core	Rammeverkskjerne	Et sett med cybersikkerhetsaktiviteter og referanser som er vanlige på tvers av kritiske infrastruktursektorer og er organisert rundt bestemte utfall. Rammekjernen består av fire typer elementer: funksjoner, kategorier, underkategorier og informative referanser.
Framework Implementation Tier	Rammeimplementeringsnivå	En linse for å se egenskapene til en organisasjons tilnærming til risiko – hvordan en organisasjon ser på cybersikkerhetsrisiko og prosessene på plass for å håndtere denne risikoen.
Framework Profile	Rammeverkprofil	En representasjon av resultatene som et bestemt system eller organisasjon har valgt fra rammekategoriene og underkategoriene.
Function	Funksjon	En av hovedkomponentene i rammeverket. Funksjoner gir det høyeste nivået av struktur for å organisere grunnleggende cybersikkerhetsaktiviteter i kategorier og underkategorier. De fem funksjonene er Identifisere, Beskytte, Oppdage, Svare og Gjenopprette.
Identify (function)	Identifisere (funksjon)	Utvikle organisasjonsforståelsen for å håndtere cybersikkerhetsrisiko for systemer, eiendeler, data og evner.
Informative Reference	Informativ referanse	En spesifikk del av standarder, retningslinjer og praksiser som er vanlig blant sektorer med kritisk infrastruktur, som illustrerer en metode for å oppnå resultatene knyttet til hver underkategori. Et eksempel på en informativ referanse er ISO/IEC 27001 Control A.10.8.3, som støtter underkategorien "Data-in-transit er beskyttet" til kategorien "Datasikkerhet" i "Beskytte"-funksjonen.
Mobile Code	Mobilkode	Et program (f.eks. skript, makro eller annen bærbar instruksjon) som kan sendes uendret til en heterogen samling av plattformer og kjøres med identisk semantikk.
Protect (function)	Beskytte (funksjon)	Utvikle og implementere passende sikkerhetstiltak for å sikre levering av kritiske infrastrukturtjenester.

Privileged User	Privilegert bruker	En bruker som er autorisert (og derfor klarert) til å utføre sikkerhetsrelevante funksjoner som vanlige brukere ikke er autorisert til å utføre.
Recover (function)	Gjenopprette (funksjon)	Utvikle og implementere passende aktiviteter for å opprettholde planer for motstandskraft og for å gjenopprette eventuelle evner eller tjenester som ble svekket på grunn av en cybersikkerhetshendelse.
Respond (function)	Svare (funksjon)	Utvikle og implementere passende aktiviteter for å iverksette tiltak angående en oppdaget cybersikkerhetshendelse.
Risk	Risiko	Et mål på i hvilken grad en enhet er truet av en potensiell omstendighet eller hendelse, og typisk en funksjon av: (i) de negative virkningene som vil oppstå hvis omstendigheten eller hendelsen inntreffer; og (ii) sannsynligheten for forekomst.
Risk Management	Risikostyring	Prosessen med å identifisere, vurdere og reagere på risiko.
Subcategory	Underkategori	Underinndelingen av en kategori i spesifikke resultater av tekniske og/eller ledelsesaktiviteter. Eksempler på underkategorier inkluderer "Eksterne informasjonssystemer er katalogisert", "Data-at-rest er beskyttet" og "Varslinger fra deteksjonssystemer blir undersøkt."
Supplier	Leverandør	Produkt- og tjenesteleverandører som brukes til en organisasjons interne formål (f.eks. IT-infrastruktur) eller integrert i produktene av tjenester levert til den organisasjonens kjøpere.
Taxonomy	Taksonomi	Et klassifiseringsskjema.

Vedlegg C: Akronymer

Dette vedlegget definerer utvalgte akronymer som brukes i publikasjonen.

ANSI	American National Standards Institute
CEA	Cybersecurity Enhancement Act av 2014
CIS	Center for Internet Security
COBIT	Control Objectives for Information and Related Technologies. Kontrollrammeverk for informasjon og relatert teknologi
CPS	Cyber-fysiske systemer
CSC	Critical Security Control
DHS	Department of Homeland Security
EO	Executive Order, US Presidentordre
ICS	Industrielle kontrollsystemer
IEC	International Electrotechnical Commission
IoT	Tingenes internett
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Organization for Standardization
IT	Informasjonsteknologi
NIST	National Institute of Standards and Technology
OT	Operativ teknologi
PII	Personlig identifiserende informasjon
RFI	Forespørsel om informasjon
RMP	Risikostyringsprosess
SCRM	Supply Chain Risk Management
SP	Spesialpublikasjon

NOR CSR - Grunnleggende rammeverk for styrking av cybersikkerheten i kritisk infrastruktur - versjon 1 (Mars 2023)

ISBN 978-82-693086-1-1