

# NIST rammeverk for cyber- og informasjonssikkerhet

Nasjonalt institutt for standarder og teknologi

Denne publikasjonen er tilgjengelig gratis fra: <https://doi.org/10.6028/NIST.CSWP.29.nor>

februar 26, 2024



Oversatt av Tor-Ståle Hansen. Oversatt med tillatelse fra Nasjonalt institutt for standarder og teknologi (NIST). Oversettelsen er under kontrakt gjennomgått av TaikaTranslations LLC {133ND23PNB770271} på vegne av NIST. Amerikansk offisielt godkjent oversettelse. Alle rettigheter er forbeholdt, USAs handelsdepartement.

Translated for NIST by TaikaTranslations LLC under contract {133ND23PNB770271}. Official U.S. Government Translation. All rights reserved, US Secretary of Commerce.

## Abstrakt

NIST Cybersecurity Framework (CSF) 2.0 gir veiledning til sivil industri, offentlige myndigheter og andre organisasjoner for å håndtere cybersikkerhetsrisikoer. Rammeverket tilbyr en taksonomi av høy-nivå cybersikkerhetsprofiler som kan brukes av enhver organisasjon - uavhengig av størrelse, sektor, eller modenhet – for bedre å forstå, vurdere, prioritere og kommunisere sin innsats innen cybersikkerhet. Rammeverket dikterer ikke hvordan resultatene skal oppnås. Snarere er det koblinger til ressurser som gir ytterligere veiledning om praksis og kontroller som kan brukes til å oppnå disse resultatene. Dette dokumentet beskriver NIST Rammeverket 2.0, dets komponenter, og noen av de mange måtene den kan brukes på.

## Søkeord

cybersikkerhet; rammeverk for cybersikkerhet; csf; styring av risiko for cybersikkerhet; cybersikkerhetsrisiko; ledelse; risikostyring; profiler; nivåer.

## Publikum

Personer som er ansvarlige for å utvikle og lede cybersikkerhetsprogrammer er det primære publikum for rammeverket, og kan brukes av andre som er involvert i risikostyring – inkludert ledere, styrever, fagfolk innen anskaffelser, teknologer og risiko ledere, advokater, HR-funksjoner, cybersikkerhet- og risikostyringsrevisorer, personvernombud og informasjonsarkitekter – for å veilede deres cybersikkerhetsrelaterte beslutninger. I tillegg kan rammeverket være nyttig for de som utarbeider og påvirker styringssystemer, ledelsessystemer, lover mv. (f.eks. foreninger, profesjonelle organisasjoner og lovgivende myndigheter) som setter og kommuniserer prioriteringer for risikostyring innen cybersikkerhet.

## Supplerende innhold

NIST vil fortsette å bygge og være vert for flere ressurser for å hjelpe organisasjoner med å implementere rammeverket, inkludert veiledninger og profiler. Alle ressurser gjøres offentlig tilgjengelig på NIST sine internettsider. Forslag til flere ressurser å referere til på NIST Rammeverket-nettstedet kan alltid deles med NIST på [cyberframework@nist.gov](mailto:cyberframework@nist.gov).

## Merknad I leserne

Med mindre annet er angitt, er dokumenter som siteres, refereres eller utdrag i denne publikasjonen ikke helt innlemmet i denne publikasjonen.

Før versjon 2.0 ble Cybersecurity Framework kalt «Framework for Improving Critical Infrastructure Cybersecurity.» Denne tittelen brukes ikke for Rammeverket 2.0.

## Anerkjennelser

Rammeverket er resultatet av et flerårig samarbeid på tvers av industri, akademisk og regjeringer i USA og rundt om i verden. NIST anerkjenner og takker alle de som har bidratt til denne reviderte rammeverket. Informasjon om Rammeverket-utviklingsprosessen finner du på NIST Rammeverkets nettsider. Erfaringer om bruk av rammeverket kan alltid deles med NIST via mail til: [cyberframework@nist.gov](mailto:cyberframework@nist.gov).



Innholdsfortegnelse

1.Oversikt over rammeverk for cybersikkerhet (Rammeverket) ..... 2

2.Introduksjon til Rammeverket-kjernen ..... 3

3.Introduksjon til Rammeverket-profiler og -nivåer ..... 7

    3.1 Rammeverket-profiler ..... 7

    3.2 Rammeverket -nivå ..... 8

4.Introduksjon til elektroniske ressurser som supplerer Rammeverket ..... 10

5.Forbedre kommunikasjon og integrasjon av cybersikkerhetsrisiko ..... 11

    5.1 Forbedre risikostyringskommunikasjon ..... 11

    5.2 Forbedre integrasjonen med andre risikostyringsprogrammer ..... 12

Vedlegg A. Rammeverket Core ..... 16

Vedlegg B. Beskrivelser av Rammeverkets Nivåer ..... 25

Vedlegg C. Ordliste..... 27



## Forord

Cybersecurity Framework (CSF) 2.0 (her etter også bare kalt Rammeverket) er utviklet for å hjelpe organisasjoner i alle størrelser og sektorer – inkludert industri, myndigheter, academia og ideelle organisasjoner – med å håndtere og redusere cybersikkerhetsrisikoer. Det er nyttig uavhengig av modenhetsnivå og teknisk raffinement av en organisasjons cybersikkerhetsprogrammer. Likevel omfavner Rammeverket ikke en one-size-fits-all-tilnærming. Hver organisasjon har både felles og unike risikoer, samt varierende risikoappetitt og toleranser, spesifikke oppdrag og mål for å oppnå disse oppdragene. Av nødvendighet vil måten organisasjoner implementerer Rammeverket variere.

Ideelt sett vil Rammeverket bli brukt til å håndtere cybersikkerhetsrisikoer sammen med andre risikoer i bedriften, inkludert de som er økonomiske, personvern, forsyningskjede, omdømmemessige, teknologiske eller fysiske av natur.

Rammeverket beskriver ønskede resultater som er ment å bli forstått av et bredt publikum, inkludert ledere, managere og utøvere, uavhengig av deres cybersikkerhetskompetanse. Fordi disse resultatene er sektor-, land- og teknologinøytrale, gir de en organisasjon den fleksibiliteten som trengs for å håndtere sine unike risikoer, teknologier og oppdragshensyn. Resultatene er kartlagt direkte til en liste over potensielle sikkerhetskontroller for umiddelbar vurdering for å redusere cybersikkerhetsrisikoer.

Selv om det ikke er foreskrivende, hjelper Rammeverket brukerne med å lære om og velge bestemte utfall. Forslag til hvordan spesifikke resultater kan oppnås, gis i en voksende pakke med elektroniske ressurser som utfyller Rammeverket, inkludert en rekke hurtigstartveiledninger (QSG-er). Ulike verktøy tilbyr også nedlastbare formater for å hjelpe organisasjoner som velger å automatisere noen av prosessene sine. QSG-ene foreslår innledende måter å bruke Rammeverket på og inviterer leseren til å utforske Rammeverket og relaterte ressurser i større dybde. Tilgjengelig via NIST Rammeverkets nettsted, bør Rammeverket og disse tilleggsressursene fra NIST og andre sees på som en "Rammeverket-portefølje" for å bidra til å håndtere og redusere risiko. Uansett hvordan den brukes, ber Rammeverket brukerne om å vurdere sin cybersikkerhetsstilling i kontekst og deretter tilpasse Rammeverket til deres spesifikke behov.

Rammeverket 2.0 bygger på tidligere versjoner og inneholder nye funksjoner som fremhever viktigheten av styring og forsyningskjeder. Spesiell oppmerksomhet rettes mot QSG-ene for å sikre at Rammeverket er relevant og lett tilgjengelig for mindre organisasjoner så vel som deres større kolleger. NIST gir nå implementeringseksempler og informative referanser, som er tilgjengelige online og oppdateres regelmessig. Oppretting av organisasjonsprofiler for nåværende tilstand og måltilstand hjelper organisasjoner med å sammenligne hvor de er i forhold til hvor de ønsker eller trenger å være, og lar dem implementere og vurdere sikkerhetskontroller raskere.

Cybersikkerhetsrisikoer utvides hele tiden, og håndtering av disse risikoene må være en kontinuerlig prosess. Dette gjelder uansett om en organisasjon nettopp har begynt å

konfrontere sine cybersikkerhetsutfordringer eller om den har vært aktiv i mange år med et sofistikert, ressurssterkt cybersikkerhetsteam. Rammeverket er designet for å være verdifullt for alle typer organisasjoner og forventes å gi passende veiledning over lang tid.

## 1. Oversikt over rammeverk for cybersikkerhet (Rammeverket)

Dette dokumentet er versjon 2.0 av NIST Cybersecurity Framework (Framework eller Rammeverket). Det inneholder følgende komponenter:

- **Rammeverket-kjernen**, kjerneelementet i Rammeverket, som er en taksonomi av cybersikkerhetsresultater på høyt nivå som kan hjelpe enhver organisasjon med å håndtere cybersikkerhetsrisikoer. Rammeverket-kjernekomponentene er et hierarki av funksjoner, kategorier og underkategorier som beskriver hvert resultat. Disse resultatene kan forstås av et bredt publikum, inkludert ledere, managere og utøvere, uavhengig av deres cybersikkerhetskompetanse. Fordi resultatene er sektor-, land- og teknologinøytrale, gir de en organisasjon den fleksibiliteten som trengs for å håndtere sine unike risikoer, teknologier og oppdragshensyn.
- **Rammeverket-organisasjonsprofiler**, som er en mekanisme for å beskrive en organisasjons nåværende og/eller målrettede cybersikkerhetsholdning når det gjelder Rammeverket-kjernens resultater.
- **Rammeverket-nivåer**, som kan brukes på Rammeverket-organisasjonsprofiler for å karakterisere grundigheten i en organisasjons risikostyring og ledelsespraksis for cybersikkerhet. Nivåer kan også gi kontekst for hvordan en organisasjon ser på cybersikkerhetsrisikoer og prosessene som er på plass for å håndtere disse risikoene.

Dette dokumentet beskriver hvilke ønskelige resultater en organisasjon kan ha ambisjoner om å oppnå. Det *foreskriver* ikke resultater eller *hvordan* de kan oppnås. Beskrivelser av *hvordan* en organisasjon kan oppnå disse resultatene er gitt i en pakke med elektroniske ressurser som utfyller Rammeverket og er tilgjengelige via [NIST Rammeverket-nettstedet](#). Disse ressursene gir ytterligere veiledning om fremgangsmåter og kontroller som kan brukes til å oppnå resultater, og er ment å hjelpe en organisasjon med å forstå, ta i bruk og bruke Rammeverket. De inkluderer:

- [Informative referanser](#) som peker på kilder til veiledning om hvert utfall fra eksisterende globale standarder, veiledninger, rammeverk, forskrifter, retningslinjer, etc.
- [Eksempler](#) på Implementering som illustrerer potensielle måter å oppnå hvert resultat
- [Hurtigstartveiledninger](#) som gir praktisk veiledning om bruk av Rammeverket og Rammeverkets nettbaserte ressurser, inkludert overgang fra tidligere Rammeverket-versjoner til versjon 2.0
- [Felleskapsprofiler og organisasjonsprofilmal](#) som hjelper en organisasjon med å sette Rammeverket ut i praksis og sette prioriteringer for å håndtere cybersikkerhetsrisikoer



En organisasjon kan bruke Rammeverket-kjernen, profilene og nivåene med tilleggsressursene for å forstå, vurdere, prioritere og kommunisere cybersikkerhetsrisikoer.

- **Forstå og vurdere:** Beskriv den nåværende eller ønskede cybersikkerhetsstillingen til deler av eller hele organisasjonen, identifiser hull og vurder fremdriften mot å håndtere disse hullene.
- **Prioriter:** Identifiser, organiser og prioriter handlinger for å håndtere cybersikkerhetsrisikoer som samsvarer med organisasjonens oppdrag, juridiske og forskriftsmessige krav og forventninger til risikostyring og styringsforventninger.
- **Kommunisere:** Tilby et felles språk for å kommunisere i og utenfor organisasjonen om cybersikkerhetsrisikoer, evner, behov og forventninger.

Rammeverket er designet for å brukes av organisasjoner i alle størrelser og sektorer, inkludert industri, myndigheter, academia og ideelle organisasjoner, uavhengig av modenhetsnivået til deres cybersikkerhetsprogrammer. Rammeverket er en grunnleggende ressurs som kan vedtas frivillig og gjennom statlig politikk og mandater. Rammeverkets taksonomi og refererte standarder, retningslinjer og praksis er ikke landsspesifikke, og tidligere versjoner av Rammeverket har blitt utnyttet med suksess av mange regjeringer og andre organisasjoner både i og utenfor USA.

Rammeverket bør brukes sammen med andre ressurser (f.eks. rammeverk, standarder, retningslinjer, ledende praksis) for bedre å håndtere cybersikkerhetsrisikoer og informere den overordnede styringen av informasjons- og kommunikasjonsteknologi (IKT) risiko på bedriftsnivå. Rammeverket er et fleksibelt rammeverk som er ment å skreddersys for bruk av alle organisasjoner uavhengig av størrelse. Organisasjoner vil fortsette å ha unike risikoer – inkludert ulike trusler og sårbarheter – og risikotoleranser, samt unike oppdragsmål og krav. Dermed vil organisasjoners tilnærminger til risikostyring og deres implementering av Rammeverket variere.

Resten av dette dokumentet er strukturert som følger:

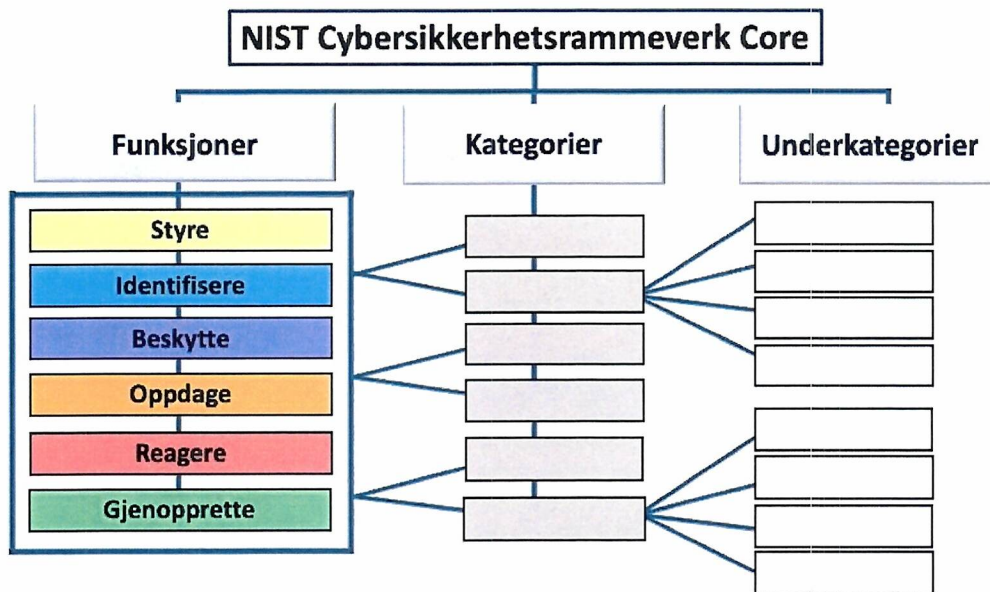
- Del 2 forklarer det grunnleggende om Rammeverket-kjernen: funksjoner, kategorier og underkategorier.
- Del 3 definerer begrepene Rammeverket-profiler og -nivåer.
- Del 4 gir en oversikt over utvalgte komponenter i Rammeverkets pakke med elektroniske ressurser: informative referanser, implementeringseksempler og hurtigstartveiledninger.
- Del 5 drøfter hvordan en organisasjon kan integrere Rammeverket med andre risikostyringsprogrammer.
- Vedlegg A er Rammeverket-kjernen.
- Vedlegg B inneholder en tenkt illustrasjon av Rammeverket-nivåene.
- Vedlegg C er en ordliste med Rammeverket-terminologi.

## 2. Introduksjon I Rammeverket-kjernen

Vedlegg A er Rammeverk-kjernen - et sett med cybersikkerhetsprofiler ordnet etter funksjon, deretter kategori og til slutt underkategori, som vist på fig. 1. Disse resultatene er ikke en



sjekkliste over handlinger som skal utføres; Spesifikke tiltak for å oppnå et resultat vil variere etter organisasjon og brukstilfelle, og det samme vil personen som er ansvarlig for disse handlingene. I tillegg innebærer ikke rekkefølgen og størrelsen på funksjoner, kategorier og underkategorier i kjernen sekvensen eller viktigheten av å oppnå dem. Strukturen i kjernen er ment å resonere mest med de som har ansvar for å operasjonalisere risikostyring i en organisasjon.



Figur 1. Rammeverketkjernen struktur

Rammeverkets kjernefunksjoner – STYRE, IDENTIFISERE, BESKYTTE, OPPDAGE, REAGERE og GJENOPPRETTE – organiserer cybersikkerhetsprofiler på overordnet nivå.

- **STYRE (GV)** – *Organisasjonens risikostyringsstrategi, forventninger og retningslinjer for cybersikkerhet etableres, kommuniseres og overvåkes.* STYRE-funksjonen gir resultater for å informere om hva en organisasjon kan gjøre for å oppnå og prioritere resultatene av de andre fem funksjonene i sammenheng med sitt oppdrag og interessentforventninger. Styringsaktiviteter er avgjørende for å innlemme cybersikkerhet i en organisasjons bredere strategi for risikostyring (ERM). STYRE adresserer en forståelse av organisatorisk kontekst; etablering av cybersikkerhetsstrategi og risikostyring av cybersikkerhet i forsyningskjeden; roller, ansvar og myndigheter; retningslinjer; og tilsynet med cybersikkerhetsstrategien.
- **IDENTIFISERE (ID)** – *Organisasjonens nåværende cybersikkerhetsrisikoer er forstått.* Å forstå organisasjonens eiendeler (f.eks. data, maskinvare, programvare, systemer, fasiliteter, tjenester, mennesker), leverandører og relaterte cybersikkerhetsrisikoer gjør det mulig for en organisasjon å prioritere innsatsen i samsvar med risikostyringsstrategien og oppdragsbehovene identifisert under STYRE. Denne funksjonen inkluderer også identifisering av forbedringsmuligheter for organisasjonens retningslinjer, planer, prosesser,

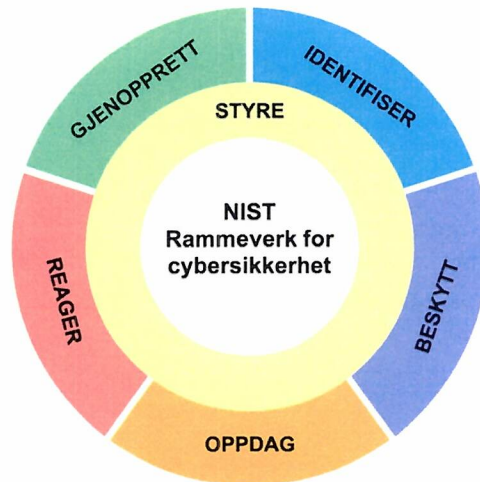
prosedyrer og praksis som støtter risikostyring for cybersikkerhet for å veilede innsatsen under alle seks funksjonene.

- **BESKYTTE (PR)** — *Sikkerhetstiltak for å håndtere organisasjonens cybersikkerhetsrisikoer brukes.* Når eiendeler og risikoer er identifisert og prioritert, støtter BESKYTT muligheten til å sikre disse eiendelene for å forhindre eller redusere sannsynligheten for og virkningen av uønskede cybersikkerhetshendelser, samt å øke sannsynligheten for og virkningen av å utnytte muligheter. Utfall som dekkes av denne funksjonen inkluderer identitetsadministrasjon, autentisering og tilgangskontroll; bevissthet og trening; datasikkerhet; plattformsikkerhet (dvs. sikring av maskinvare, programvare og tjenester på fysiske og virtuelle plattformer); og motstandsdyktigheten til teknologisk infrastruktur.
- **OPPDAGE (DE)** — *Mulige cybersikkerhetsangrep og kompromisser blir funnet og analysert.* OPPDAG muliggjør rettidig oppdagelse og analyse av uregelmessigheter, indikatorer på kompromiss og andre potensielt uønskede hendelser som kan indikere at cybersikkerhetsangrep og hendelser oppstår. Denne funksjonen støtter vellykket hendelsesrespons og gjenopprettingsaktiviteter.
- **REAGERE (RS)** — *Tiltak angående en oppdaget cybersikkerhetshendelse iverksettes.* REAGER støtter evnen til å begrense effekten av cybersikkerhetshendelser. Utfall innenfor denne funksjonen dekker hendelseshåndtering, analyse, begrensnings, rapportering og kommunikasjon.
- **GJENOPPRETTE (RC)** — *Eiendeler og operasjoner som er berørt av en cybersikkerhetshendelse, gjenopprettes.* GJENOPPRETT støtter rettidig gjenoppretting av normal drift for å redusere effekten av cybersikkerhetshendelser og muliggjøre hensiktsmessig kommunikasjon under gjenopprettingsarbeidet.

Mens mange risikostyringsaktiviteter for cybersikkerhet fokuserer på å forhindre at negative hendelser oppstår, kan de også støtte å dra nytte av positive muligheter. Tiltak for å redusere cybersikkerhetsrisiko kan være til nytte for en organisasjon på andre måter, for eksempel å øke inntektene (f.eks. først tilby overflødig anleggsplass til en kommersiell hostingleverandør for å være vert for egne og andre organisasjoners datasentre, og deretter flytte et stort finansielt system fra organisasjonens interne datasenter til vertslleverandøren for å redusere cybersikkerhetsrisiko).

Figur 2 viser Rammeverket-funksjonene som et hjul fordi alle funksjonene er relaterte til hverandre. For eksempel vil en organisasjon kategorisere eiendeler under IDENTIFISER og iverksette tiltak for å sikre disse eiendelene under BESKYTT. Investeringer i planlegging og testing i STYRE- og IDENTIFISER-funksjonene vil støtte rettidig oppdagelse av uventede hendelser i OPPDAG-funksjonen, samt muliggjøre hendelsesrespons og gjenopprettingshandlinger for cybersikkerhetshendelser i funksjonene REAGER og

GJENOPPRETT. STYRE er i midten av hjulet fordi det informerer hvordan en organisasjon vil implementere de andre fem funksjonene.



Figur 2. Rammeverksfunksjoner

Funksjonene bør behandles samtidig. Handlinger som støtter STYRE, IDENTIFISER, BESKYTT, og OPPDAG bør alle skje kontinuerlig, og handlinger som støtter REAGER og GJENOPPRETT, bør være klare til enhver tid og skje når cybersikkerhetshendelser oppstår. Alle funksjoner har viktige roller knyttet til cybersikkerhetshendelser. STYRE-, IDENTIFISER- og BESKYTT-resultater bidrar til å forhindre og forberede seg på hendelser, mens STYRE, OPPDAG, REAGER og GJENOPPRETT-resultater bidrar til å oppdage og håndtere hendelser.

Hver funksjon er oppkalt etter et verb som oppsummerer innholdet. Hver funksjon er delt inn i kategorier, som er relaterte cybersikkerhetsresultater som samlet utgjør funksjonen.

*Underkategorier* deler videre hver kategori inn i mer spesifikke resultater fra tekniske og ledelsesaktiviteter. Underkategoriene er ikke fullstendige, men de beskriver detaljerte resultater som støtter hver kategori.

Funksjonene, kategoriene og underkategoriene gjelder for all IKT som brukes av en organisasjon, inkludert informasjonsteknologi (IT), tingenes internett (IoT) og operativ teknologi (OT). De gjelder også for alle typer teknologimiljøer, inkludert sky-, mobil- og kunstig intelligens-systemer. Rammeverket-kjernener fremtidsrettet og ment å gjelde for fremtidige endringer i teknologier og miljøer.



### 3. Introduksjon | Rammeverket-profiler og -nivåer

Denne delen definerer konseptene for Rammeverket-profiler og -nivåer.

#### 3.1 Rammeverket-profiler

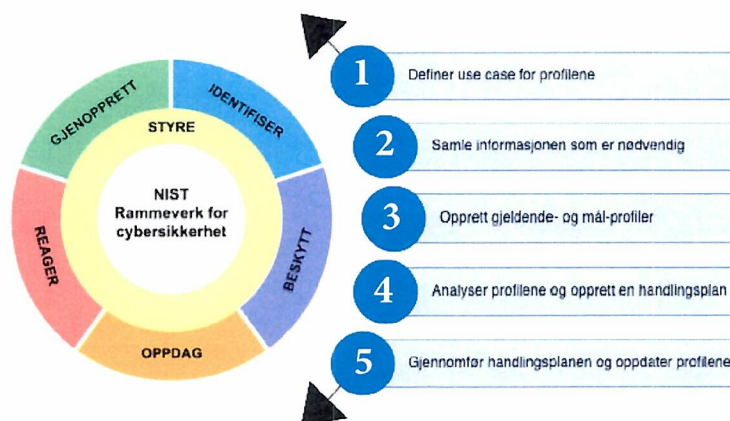
En *Rammeverket-organisasjonsprofil* beskriver en organisasjons nåværende og/eller målrettede cybersikkerhetsholdning når det gjelder kjernens resultater. [Organisasjonsprofiler](#) brukes til å forstå, skreddersy, vurdere, prioritere og kommunisere kjernens resultater ved å vurdere en organisasjons oppdragsmål, interessentforventninger, trussellandskap og krav. En organisasjon kan deretter prioritere sine handlinger for å oppnå bestemte resultater og kommunisere denne informasjonen til interessenter.

Hver organisasjonsprofil inneholder ett eller begge av følgende:

1. En gjeldende profil spesifiserer kjerne-resultatene som en organisasjon for øyeblikket oppnår (eller forsøker å oppnå) og karakteriserer hvordan eller i hvilken grad hvert resultat oppnås.
2. En målprofil spesifiserer de ønskede resultatene som en organisasjon har valgt og prioritert for å oppnå sine risikostyringsmål for cybersikkerhet. En målprofil vurderer forventede endringer i organisasjonens holdning til cybersikkerhet, for eksempel nye krav, innføring av ny teknologi og trender innen trusselletterretning.

En fellesskapsprofil er en grunnlinje for Rammeverket-resultater som opprettes og publiseres for å adressere felles interesser og mål blant en rekke organisasjoner. En fellesskapsprofil er vanligvis utviklet for en bestemt sektor, undersektor, teknologi, trusseltype eller annet brukstilfelle. En organisasjon kan bruke en fellesskapsprofil som grunnlag for sin egen målprofil. Eksempler på fellesskapsprofiler finner du på [NIST Rammeverket-nettstedet](#).

Trinnene vist i fig. 3 og oppsummert nedenfor illustrerer en måte en organisasjon kan bruke en organisasjonsprofil for å informere om kontinuerlig forbedring av cybersikkerheten.



Figur 3. Trinn for å opprette og bruke Cybersikkerhetsrammeverkprofiler

1. **Definer omfang for de organisasjonelle profilene.** Dokumenter overordnede fakta og forutsetninger som profilen vil være basert på for å definere omfanget. En organisasjon kan ha så mange organisasjonsprofiler som ønsket, hver med forskjellig omfang. En profil kan for eksempel henvende seg til en hel organisasjon eller være knyttet til en organisasjons økonomisystemer eller for å motvirke trusler om løsepengevirus og håndtere løsepengevirus som involverer disse finanssystemene.
2. **Samle inn informasjonen som trengs for å forberede organisasjonsprofilen.** Eksempler på informasjon kan omfatte organisasjonsretningslinjer, prioriteringer og ressurser for risikostyring, virksomhetsrisikoprofiler, BIA-registre (Business Impact Analysis), cybersikkerhetskrav og standarder etterfulgt av organisasjonen, praksiser og verktøy (f.eks. prosedyrer og sikkerhetstiltak) og arbeidsroller.
3. **Opprett organisasjonsprofilen.** Bestem hvilke typer informasjon profilen skal inneholde for de valgte Rammeverket-resultatene, og dokumenter den nødvendige informasjonen. Vurder risikoimplikasjonene av den nåværende profilen for å informere målprofilplanlegging og prioritering. Du bør også vurdere å bruke en fellesskapsprofil som grunnlag for målprofilen.
4. **Analyser gapene mellom gjeldende profil og målprofil, og opprett en handlingsplan.** Gjennomfør en gapanalyse for å identifisere og analysere forskjellene mellom nåværende profil og målprofil, og utvikle en prioritert handlingsplan (f.eks. risikoregister, risikodetaljrapport, handlingsplan og milepæler [POA&M]) for å håndtere disse hullene.
5. **Implementere handlingsplanen, og oppdatere organisasjonsprofilen.** Følg handlingsplanen for å håndtere hullene og flytte organisasjonen mot målprofilen. En handlingsplan kan ha en overordnet tidsfrist eller være pågående.

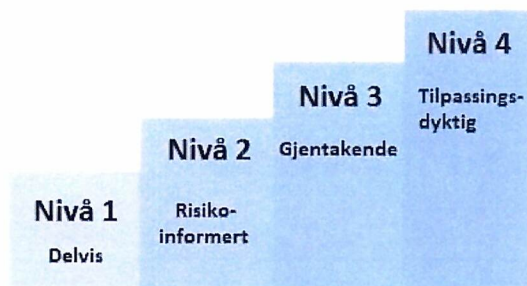
Gitt viktigheten av kontinuerlig forbedring, kan en organisasjon gjenta disse trinnene så ofte som nødvendig.

Det finnes flere bruksområder for organisasjonsprofiler. En gjeldende profil kan for eksempel brukes til å dokumentere og kommunisere organisasjonens cybersikkerhetsfunksjoner og kjente forbedringsmuligheter med eksterne interessenter, for eksempel forretningspartnere eller potensielle kunder. En målprofil kan også bidra til å uttrykke organisasjonens risikostyringskrav og forventninger til leverandører, partnere og andre tredjeparter som et mål for disse partene å oppnå.

### 3.2 Rammeverket -nivåer

En organisasjon kan velge å bruke nivåene til å informere sine gjeldende profiler og målprofiler. Nivåer karakteriserer grundigheten i en organisasjons styring og styringspraksis for cybersikkerhetsrisiko, og de gir kontekst for hvordan en organisasjon ser på cybersikkerhetsrisikoer og prosessene som er på plass for å håndtere disse risikoene. Nivåene, som vist i fig. 4 og antydnet i vedlegg B, gjenspeiler en organisasjons praksis for å håndtere cybersikkerhetsrisiko som delvis (Nivå 1), risikoinformert (Nivå 2), gjentakende (Nivå 3) og tilpassingsdyktig (Nivå 4). Nivåene beskriver en progresjon fra uformelle, ad hoc-responser til

tilnærminger som er smidige, risikoinformerte og kontinuerlig forbedres. Valg av nivåer bidrar til å sette den generelle tonen for hvordan en organisasjon skal håndtere sine cybersikkerhetsrisikoer.



Figur 4. Cybersikkerhetsrammeverkets nivåer

Nivåer bør utfylle en organisasjons risikostyringsmetodikk for cybersikkerhet i stedet for å erstatte den. En organisasjon kan for eksempel bruke nivåene til å kommunisere internt som en målestokk for hele organisasjonens<sup>1</sup> tilnærming til håndtering av cybersikkerhetsrisiko. Progresjon til høyere nivåer oppmuntres når risikoer eller mandater er større eller når en kostnad til nytte-analyse indikerer en gjennomførbar og kostnadseffektiv reduksjon av negative cybersikkerhetsrisikoer.

[NIST Rammeverket-nettstedet](#) gir ytterligere informasjon om bruk av profiler og nivåer. Den inneholder pekere til [NIST-vertsbaserte organisasjonsprofilmaler](#) og et repositorium med [felleskapsprofiler](#) i en rekke maskinlesbare og menneskebrukbare formater.

---

<sup>1</sup> For formålene med dette dokumentet har begrepene «hele organisasjonen» og «foretak» samme betydning.



#### 4. Introduksjon I elektroniske ressurser som supplerer Rammeverket

NIST og andre organisasjoner har produsert en pakke med elektroniske ressurser som hjelper organisasjoner med å forstå, ta i bruk og bruke Rammeverket. Siden de driftes på nettet, kan disse tilleggsressursene oppdateres oftere enn dette dokumentet, som oppdateres sjelden for å gi brukerne stabilitet og være tilgjengelige i maskinlesbare formater. Denne delen gir en oversikt over tre typer elektroniske ressurser: informative referanser, implementeringseksempler og hurtigstartveiledninger.

[Informative referanser](#) er tilordninger som indikerer relasjoner mellom kjernen og ulike standarder, retningslinjer, forskrifter og annet innhold. Informative referanser bidrar til å informere om hvordan en organisasjon kan oppnå kjernens resultater. Informative referanser kan være sektor- eller teknologispesifikke. De kan være produsert av NIST eller en annen organisasjon. Noen informative referanser er smalere i omfang enn en underkategori. For eksempel kan en bestemt kontroll fra [SP 800-53](#), *Sikkerhets- og personvernkontroller for informasjonssystemer og organisasjoner*, være en av mange referanser som trengs for å oppnå resultatet beskrevet i en underkategori. Andre informative referanser kan være på høyere nivå, for eksempel et krav fra en policy som delvis adresserer mange underkategorier. Når du bruker Rammeverket, kan en organisasjon identifisere de mest relevante informative referansene.

[Implementeringseksempler](#) gir illustrative eksempler på konsise, handlingsorienterte trinn for å bidra til å oppnå resultatene av underkategoriene. Verb som brukes til å uttrykke Eksempler inkluderer dele, dokumentere, utvikle, utføre, overvåke, analysere, vurdere og utøve. Eksempelene er ikke en omfattende liste over alle handlinger som kan tas av en organisasjon for å oppnå et resultat, og de representerer heller ikke en grunnlinje av nødvendige tiltak for å håndtere cybersikkerhetsrisikoer.

[Hurtigstartveiledninger \(QSG-er\)](#) er korte dokumenter om spesifikke Rammeverket-relaterte emner og er ofte skreddersydd for bestemte målgrupper. QSG-er kan hjelpe en organisasjon med å implementere Rammeverket fordi de destillerer bestemte deler av Rammeverket til handlingsbare "første trinn" som en organisasjon kan vurdere på veien for å forbedre sin cybersikkerhetsstilling og styring av tilhørende risiko. Veiledningene revideres i egne tidsrammer, og nye hjelpelinjer legges til etter behov.

Forslag til nye informative referanser for Rammeverket 2.0 kan alltid deles med NIST på [olir@nist.gov](mailto:olir@nist.gov). Forslag til andre ressurser å referere til på NIST Rammeverkets nettsted, inkludert flere QSG-emner, bør rettes til [cyberframework@nist.gov](mailto:cyberframework@nist.gov).

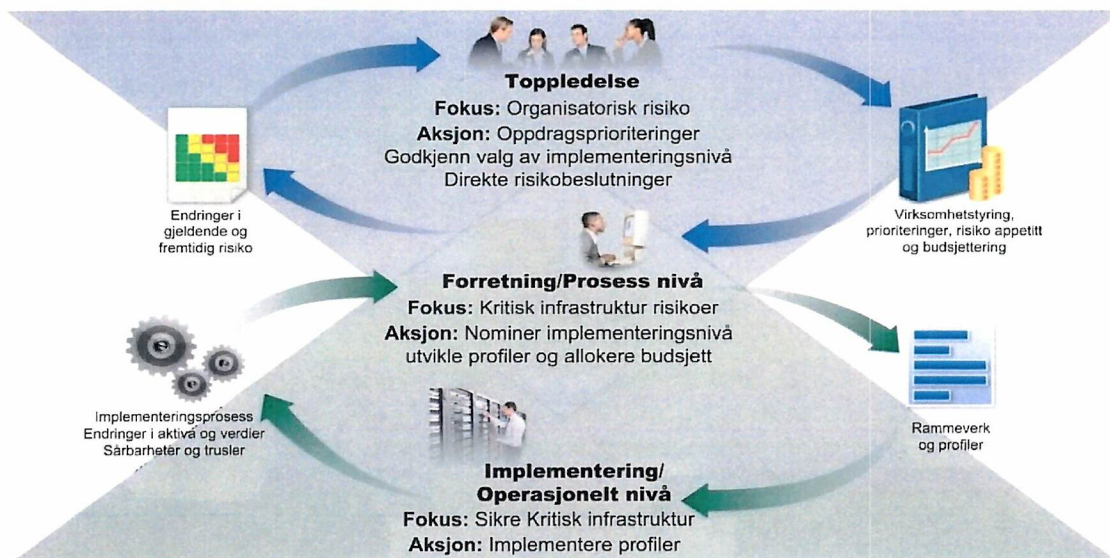
## 5. Forbedre kommunikasjon og integrasjon av cybersikkerhetsrisiko

Rammeverkets bruk vil variere basert på en organisasjons unike oppdrag og risikoer. Med en forståelse av interessentenes forventninger og risikoappetitt og toleranse (som beskrevet i STYRE), kan en organisasjon prioritere cybersikkerhetsaktiviteter for å ta informerte beslutninger om utgifter og handlinger knyttet til cybersikkerhet. En organisasjon kan velge å håndtere risiko på en eller flere måter - inkludert å redusere, overføre, unngå eller akseptere negative risikoer og realisere, dele, styrke eller akseptere positive risikoer - avhengig av potensielle virkninger og sannsynligheter. Det er viktig at en organisasjon kan bruke Rammeverket både internt for å administrere sine cybersikkerhetsfunksjoner og eksternt for å overvåke eller kommunisere med tredjeparter.

Uavhengig av Rammeverkets bruk, kan en organisasjon dra nytte av å bruke Rammeverket som veiledning for å hjelpe den med å forstå, vurdere, prioritere og kommunisere cybersikkerhetsrisikoer og handlingene som vil håndtere disse risikoene. De valgte resultatene kan brukes til å fokusere på og implementere strategiske beslutninger for å forbedre cybersikkerhetsstillinger og opprettholde kontinuitet i oppdragsviktige funksjoner, samtidig som man tar hensyn til prioriteringer og tilgjengelige ressurser.

### 5.1 Forbedre risikostyringskommunikasjon

Rammeverket gir grunnlag for forbedret kommunikasjon om forventninger, planlegging og ressurser til cybersikkerhet. Rammeverket fremmer toveis informasjonsflyt (som vist i øverste halvdel av fig. 5) mellom ledere som fokuserer på organisasjonens prioriteringer og strategisk retning og managere som håndterer spesifikke cybersikkerhetsrisikoer som kan påvirke oppnåelsen av disse prioriteringene. Rammeverket støtter også en lignende flyt (som vist i nederste halvdel av fig. 5) mellom ledere og utøvere som implementerer og driver teknologiene. Venstre side av figuren indikerer viktigheten av at utøvere deler sine oppdateringer, innsikt og bekymringer med managere og ledere.



Figur 5. Bruk av Rammeverket forbedrer kommunikasjon og risikostyring



Forberedelse til å opprette og bruke organisasjonsprofiler innebærer å samle informasjon om organisatoriske prioriteringer, ressurser og risikoretning fra ledere. Managere samarbeider deretter med utøvere for å kommunisere forretningsbehov og skape risikoinformerte organisasjonsprofiler. Tiltak for å lukke eventuelle gap identifisert mellom nåværende profil og målprofil vil bli implementert av managere og utøvere og vil gi viktige innspill til systemnivåplaner. Etter hvert som måltilstanden oppnås i hele organisasjonen – inkludert gjennom kontroller og overvåking som brukes på systemnivå – kan de oppdaterte resultatene deles gjennom risikoregistre og fremdriftsrapporter. Som en del av den løpende vurderingen får managere innsikt for å gjøre justeringer som ytterligere reduserer potensielle skader og øker potensielle fordeler.

STYRE-funksjonen støtter organisatorisk risikokommunikasjon med **ledere**. Ledernes diskusjoner involverer strategi, spesielt hvordan cybersikkerhetsrelaterte usikkerheter kan påvirke oppnåelsen av organisatoriske mål. Disse styringsdiskusjonene støtter dialog og enighet om risikostyringsstrategier (inkludert cybersikkerhetsrisiko i leverandørkjeden); roller, ansvar og myndigheter; retningslinjer; og tilsyn. Når ledere etablerer prioriteringer og mål for cybersikkerhet basert på disse behovene, kommuniserer de forventninger om risikoappetitt, ansvarlighet og ressurser. Ledere er også ansvarlige for å integrere risikostyring av cybersikkerhet med ERM-programmer og risikostyringsprogrammer på lavere nivå (se avsnitt 5.2). Kommunikasjonen reflektert i den øverste halvdelen av fig. 5 kan inkludere hensyn til ERM og programmene på lavere nivå og dermed informere managere og utøvere.

De overordnede cybersikkerhetsmålene satt av ledere er informert av og videreføres til **ledere**. I en kommersiell enhet kan disse gjelde for en bransje- eller driftsavdeling. For statlige virksomheter kan dette være hensyn til divisjons- eller filialnivå. Ved implementering av Rammeverket vil managere fokusere på hvordan man kan oppnå risikomål gjennom felles tjenester, kontroller og samarbeid, som uttrykt i målprofilen og forbedret gjennom handlingene som spores i handlingsplanen (f.eks. risikoregister, risikodetaljrapport, POA&M).

**Utøvere** fokuserer på å implementere måltilstanden og måle endringer i operasjonell risiko for å planlegge, gjennomføre og overvåke spesifikke cybersikkerhetsaktiviteter. Etter hvert som kontroller implementeres for å håndtere risiko på et akseptabelt nivå, gir utøvere managere og ledere informasjonen (f.eks. nøkkelindikatorer, nøkkelrisikoindikatorer) de trenger for å forstå organisasjonens cybersikkerhetsstilling, ta informerte beslutninger og opprettholde eller justere risikostrategien tilsvarende. Ledere kan også kombinere disse cybersikkerhetsrisikodataene med informasjon om andre typer risiko fra hele organisasjonen. Oppdateringer av forventninger og prioriteringer inkluderes i oppdaterte organisasjonsprofiler etter hvert som syklusen gjentas.

## 5.2 Forbedre integrasjonen med andre risikostyringsprogrammer

Hver organisasjon står overfor mange typer IKT-risiko (f.eks. personvern, forsyningskjede, kunstig intelligens) og kan bruke rammeverk og styringsverktøy som er spesifikke for hver risiko. Noen organisasjoner integrerer IKT og alle andre risikostyringstiltak på høyt nivå ved hjelp av ERM, mens andre holder innsatsen atskilt for å sikre tilstrekkelig oppmerksomhet på hver enkelt. Små organisasjoner kan av sin natur overvåke risiko på bedriftsnivå, mens større selskaper kan opprettholde separat risikostyringsinnsats integrert i ERM.



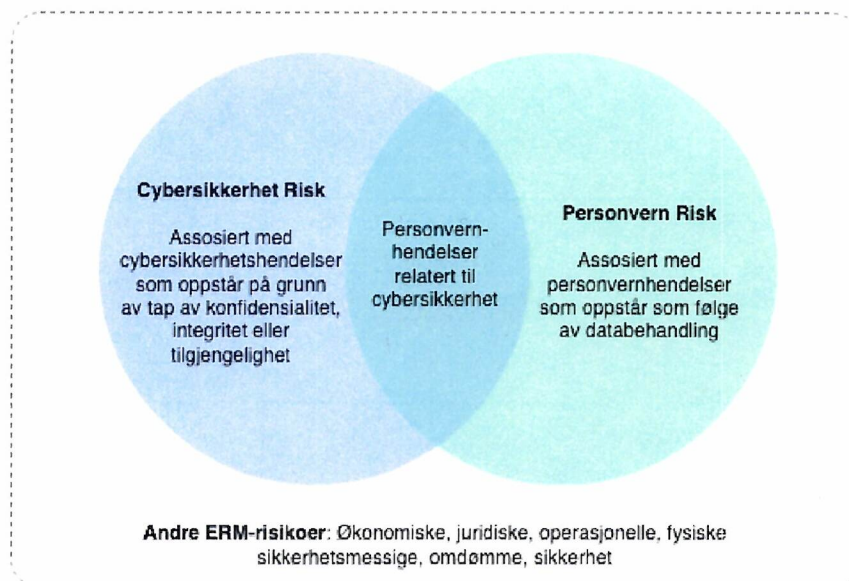
Organisasjoner kan bruke en ERM-tilnærming for å balansere en portefølje av risikohensyn, inkludert cybersikkerhet, og ta informerte beslutninger. Ledere får betydelig informasjon om nåværende og planlagte risikoaktiviteter når styrings- og risikostrategier integreres med resultater fra tidligere bruk av Rammeverket. Rammeverket hjelper organisasjoner med å oversette terminologien for risikostyring innen cybersikkerhet og cybersikkerhet til et generelt risikostyringsspråk som ledere forstår.

NIST-ressurser som beskriver det gjensidige forholdet mellom risikostyring av cybersikkerhet og ERM inkluderer:

- NIST Cybersecurity Framework 2.0 - [Hurtigveiledning for Enterprise Risk Management](#)
- NIST Interagency Report (IR) 8286, [Integrering av cybersikkerhet og Enterprise Risk Management \(ERM\)](#)
- IR 8286A, [Identifisering og estimering av cybersikkerhetsrisiko for helhetlig risikostyring](#)
- IR 8286B, [prioritering av cybersikkerhetsrisiko for risikostyring i bedrifter](#)
- IR 8286C, [Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight](#)
- IR 8286D, [bruk av Business Impact Analysis for å informere om risikoprioritering og respons](#)
- SP 800-221, [Bedriftspåvirkning av informasjons- og kommunikasjonsteknologirisiko: Styre og håndtere IKT-risikoprogrammer innenfor en virksomhetsrisikoportefølje](#)
- SP 800-221A, [Informasjons- og kommunikasjonsteknologi \(IKT\) risikoutfall: Integrering av IKT-risikostyringsprogrammer med Enterprise Risk Portfolio](#)

En organisasjon kan også finne Rammeverket gunstig for å integrere risikostyring for cybersikkerhet med individuelle IKT-risikostyringsprogrammer, for eksempel:

- **Risikostyring og vurdering av cybersikkerhet:** Rammeverket kan integreres med etablerte risikostyrings- og vurderingsprogrammer for cybersikkerhet, for eksempel [SP 800-37, Risikostyringsrammeverk for informasjonssystemer og organisasjoner](#), og [SP 800-30, Veiledning for gjennomføring av risikovurderinger](#) fra NIST Risk Management Framework (RMF). For en organisasjon som bruker [NIST RMF og dens pakke med publikasjoner](#), kan Rammeverket brukes til å utfylle RMFs tilnærming til å velge og prioritere kontroller fra [SP 800-53, sikkerhets- og personvernkontroller for informasjonssystemer og organisasjoner](#).
- **Personvernrisiko:** Mens cybersikkerhet og personvern er uavhengige disipliner, overlapper deres mål under visse omstendigheter, som illustrert i fig. 6.



**Figur 6. Integrering av cybersikkerhet og personvernrisikoe**

Risikostyring av cybersikkerhet er avgjørende for å håndtere personvernrisiko knyttet til tap av konfidensialitet, integritet og tilgjengelighet av enkeltpersoners data. For eksempel kan datainnbrudd føre til identitetstyveri. Imidlertid kan personvernrisiko også oppstå ved hjelp av midler som ikke er relatert til cybersikkerhetshendelser.

En organisasjon behandler data for å oppnå oppdrags- eller forretningsformål, noe som noen ganger kan føre til *personvern*hendelser der enkeltpersoner kan oppleve problemer som følge av databehandlingen. Disse problemene kan uttrykkes på ulike måter, men NIST beskriver dem som alt fra verdighetseffekter (f.eks. Forlegenhet eller stigma) til mer konkrete skader (f.eks. Diskriminering, økonomisk tap eller fysisk skade). [NIST Privacy Framework](#) og Rammeverket kan brukes sammen for å håndtere de ulike aspektene av cybersikkerhet og personvernrisiko. I tillegg har NISTs [Privacy Risk Assessment Methodology \(PRAM\)](#) en katalog med eksempelproblemer for bruk i personvernrisikovurderinger.

- **Leverandørkjederisikoe:** En organisasjon kan bruke Rammeverket til å fremme tilsyn med cybersikkerhetsrisikoe og kommunikasjon med interessenter på tvers av forsyningskjeder. Alle typer teknologi er avhengig av et komplekst, globalt distribuert, omfattende og sammenkoblet økosystem for forsyningskjeder med geografisk varierte ruter og flere nivåer av outsourcing. Dette økosystemet består av enheter i offentlig og privat sektor (f.eks. innkjøpere, leverandører, utviklere, systemintegratorer, eksterne systemtjenesteleverandører og andre teknologirelaterte tjenesteleverandører) som samhandler for å forske, utvikle, designe, produsere, anskaffe, levere, integrere, drive, vedlikeholde, avhende og på andre måter utnytte eller administrere teknologiprodukter og -tjenester. Disse interaksjonene er formet og påvirket av teknologier, lover, retningslinjer, prosedyrer og praksis.

Gitt de komplekse og sammenkoblede forholdene i dette økosystemet, er risikostyring i forsyningskjeden (SCRM) avgjørende for organisasjoner. Cybersecurity SCRM (C-SCRM) er en systematisk prosess for å håndtere eksponering for cybersikkerhetsrisiko gjennom forsyningskjeder og utvikle passende responsstrategier, retningslinjer, prosesser og prosedyrer. Underkategoriene i Rammeverket C-SCRM-kategorien [GV. SC] gir en sammenheng mellom utfall som fokuserer utelukkende på cybersikkerhet og de som fokuserer på C-SCRM. SP 800-161r1 (Revisjon 1), [\*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations\*](#), gir grundig informasjon om C-SCRM.

- **Risiko fra nye teknologier:** Etter hvert som nye teknologier og nye anvendelser av teknologi blir tilgjengelige, blir nye risikoer tydelige. Et moderne eksempel er kunstig intelligens (AI), som har cybersikkerhets- og personvernrisikoer, samt mange andre typer risikoer. [\*NIST Artificial Intelligence Risk Management Framework \(AI RMF\)\*](#) ble utviklet for å bidra til å håndtere disse risikoene. Behandling av AI-risiko sammen med andre bedriftsrisikoer (f.eks. økonomiske, cybersikkerhet, omdømme og personvern) vil gi et mer integrert resultat og organisatoriske effektiviteter. Hensyn og tilnærminger til risikostyring av cybersikkerhet og personvern gjelder for design, utvikling, implementering, evaluering og bruk av AI-systemer. AI RMF Core bruker funksjoner, kategorier og underkategorier for å beskrive AI-resultater og bidra til å håndtere risikoer relatert til AI.



## Vedlegg A. Rammeverket Core

Dette vedlegget beskriver funksjonene, kategoriene og underkategoriene til Rammeverket-kjernen. Tabell 1 viser Rammeverket 2.0 sin kjernefunksjon og kategorinavn og unike alfabetiske identifikatorer. Hvert funksjonsnavn i tabellen er knyttet til sin del av vedlegget. Rekkefølgen på funksjoner, kategorier og underkategorier av kjernen er ikke sekvensielle; Uoverensstemmelser i nummereringen indikerer delkategorier for Rammeverket 1.1 som ble flyttet i Rammeverket 2.0

**Tabell 1. Rammeverket 2.0 kjernefunksjon og kategorinavn og identifikatorer**

Funksjon	Kategori	Kategori-Identifikator
<b>Styre (GV)</b>	Organisasjonskontekst	GV.OC
	Strategi for risikostyring	GV.RM
	Roller, ansvar og myndighet	GV.RR
	Retningslinjer, prosesser og prosedyrer	GV.PO
	Tilsyn	GV.OV
	Risikostyring for forsyningskjeder innenfor cybersikkerhet	GV.SC
<b>Identifisere (ID)</b>	Forvaltning av eiendeler	ID.AM
	Risikovurdering	ID.RA
	Forbedring	ID.IM
<b>Beskytte (PR)</b>	Identitetsstyring, autentisering og tilgangskontroll	PR.AA
	Bevisshet og opplæring	PR.AT
	Datasikkerhet	PR.DS
	Plattformsikkerhet	PR.PS
	Motstandsdyktig teknologisk infrastruktur	PR.IR
<b>Oppdag (DE)</b>	Kontinuerlig overvåking	DE.CM
	Analyse av uønskede hendelser	DE.AE
<b>Reager (RS)</b>	Hendelseshåndtering	RS.MA
	Analyse av hendelser	RS.AN
	Rapportering og kommunikasjon ved håndtering av hendelser	RS.CO
	Håndtering av hendelser	RS.MI
<b>Gjenopprett (RC)</b>	Utførelse av gjenopprettingsplan for hendelser	RC.RP
	Kommunikasjon ved hendelsesgjenoppretting	RC.CO

Rammeverket Core, informative referanser og implementeringseksempler er tilgjengelige på [Rammeverket 2.0-nettstedet](#) og gjennom [Rammeverket 2.0 Reference Tool](#), som lar brukerne utforske dem og eksportere dem i menneske- og maskinlesbare formater. Rammeverket 2.0 Core er også tilgjengelig i et [eldre format](#) som ligner på Rammeverket 1.1.

**STYRE (GV):** Etablere, kommunisere og overvåke organisasjonens strategi, visjon og retningslinjer for styring av cybersikkerhetsrisiko

- **Organisatorisk kontekst (GV.OC):** Omstendighetene - oppdrag, forventninger fra interessenter og juridiske, regulatoriske og kontraktsmessige krav - som omgir organisasjonens beslutninger om cybersikkerhetsrisikostyring, er forstått
  - **GV.OC-01:** Organisasjonens oppdrag er forstått og informerer cybersikkerhetsrisikostyring
  - **GV.OC-02:** Interne og eksterne interessenter er fastsatt, og deres behov og forventninger når det gjelder cybersikkerhetsrisikostyring er forstått
  - **GV.OC-03:** Juridiske, forskriftsmessige og kontraktsmessige krav angående cybersikkerhet – inkludert personvern og borgerrettighetsforpliktelser – forstås og administreres
  - **GV.OC-04:** Kritiske mål, evner og tjenester som interessenter er avhengige av eller forventer av organisasjonen, bestemmes og kommuniseres
  - **GV.OC-05:** Resultater, evner og tjenester som organisasjonen er avhengig av, bestemmes og kommuniseres
- **Risikostyringsstrategi (GV.RM):** Organisasjonens prioriteringer, begrensninger, risikotoleranse og appetitterklæringer og forutsetninger etableres, kommuniseres og brukes til å støtte operasjonelle risikobeslutninger
  - **GV.RM-01:** Risikostyringsmål etableres og avtales av organisatoriske interessenter
  - **GV.RM-02:** Risikoappetitt og risikotoleranseerklæringer bestemmes, kommuniseres og vedlikeholdes
  - **GV.RM-03:** Styringsprosesser for virksomhetsrisiko inkluderer risikostyringsaktiviteter og resultater for cybersikkerhet
  - **GV.RM-04:** Strategisk retning som beskriver hensiktsmessige risikohåndteringsalternativer etableres og kommuniseres
  - **GV.RM-05:** Det etableres kommunikasjonslinjer på tvers av organisasjonen for cybersikkerhetsrisikoer, inkludert risiko fra leverandører og andre tredjeparter
  - **GV.RM-06:** En standardisert metode for å beregne, dokumentere, kategorisere og prioritere cybersikkerhetsrisiko etableres og kommuniseres
  - **GV.RM-07:** Strategiske muligheter (dvs. positive risikoer) identifiseres og inkluderes i organisatoriske diskusjoner om risiko i cybersikkerhet



- 
- **Roller, ansvar og myndighet (GV.RR):** Cybersikkerhetsroller, ansvar og myndigheter for å fremme ansvarlighet, ytelsesvurdering og kontinuerlig forbedring etableres og kommuniseres
    - **GV.RR-01:** Organisatorisk ledelse er pålagt og ansvarlig for cybersikkerhetsrisiko og fremmer en kultur som er risikobevist, etisk og kontinuerlig forbedring
    - **GV.RR-02:** Roller, ansvar og myndigheter knyttet til risikostyring av cybersikkerhet etableres, kommuniseres, forstås og håndheves
    - **GV.RR-03:** Tilstrekkelige ressurser allokeres i samsvar med strategi for risiko i cybersikkerhet, roller og ansvar og retningslinjer
    - **GV.RR-04:** Cybersikkerhet er inkludert i personalpraksis
- 
- **Retningslinjer, prosesser og prosedyrer (GV.PO):** Organisasjonens policyer, prosesser og prosedyrer for cybersikkerhet etableres, kommuniseres og håndheves
  - **GV.PO-01:** Retningslinjer, prosesser og prosedyrer for håndtering av cybersikkerhetsrisiko etableres basert på organisatorisk kontekst, strategi for risiko i cybersikkerhet og prioriteringer og kommuniseres og håndheves
  - **GV.PO-02:** Retningslinjer, prosesser og prosedyrer for håndtering av cybersikkerhetsrisikoer gjennomgås, oppdateres, kommuniseres og håndheves for å gjenspeile endringer i krav, trusler, teknologi og organisatorisk oppdrag
- 
- **Tilsyn (GV.OV):** Resultater av organisasjonens risikostyringsaktiviteter og ytelse for cybersikkerhet brukes til å informere, forbedre og justere risikostyringsstrategien
  - **GV.OV-01:** Risikostyringsstrategi-resultater for cybersikkerhet gjennomgås for å informere og justere strategi og retning
  - **GV.OV-02:** Risikostyrings-strategien for cybersikkerhet gjennomgås og justeres for å sikre dekning av organisatoriske krav og risikoer
  - **GV.OV-03:** Organisatorisk ytelse for risikostyring av cybersikkerhet måles og gjennomgås for å bekrefte og justere strategisk retning
- 
- **Risikostyring av cybersikkerhet i forsyningskjeden (GV.SC):** Prosessene for håndtering av risiko i cyber forsyningskjeder identifiseres, etableres, styres, overvåkes og forbedres av organisatoriske interessenter
  - **GV.SC-01:** Et risikostyrings-program, strategi, mål, retningslinjer og prosesser for cybersikkerhet er etablert og avtalt av organisatoriske interessenter
  - **GV.SC-02:** Cybersikkerhetsroller og ansvar for leverandører, kunder og partnere etableres, kommuniseres og koordineres internt og eksternt
  - **GV.SC-03:** Risikohåndtering i forsyningskjeder for cybersikkerhet er integrert i cybersikkerhet og bedriftens risikostyring, risikovurdering og forbedringsprosesser
  - **GV.SC-04:** Leverandører er kjent og prioritert etter kritikalitet



- **GV.SC-05:** Krav for å håndtere cybersikkerhetsrisiko i leverandørkjeder etableres, prioriteres og integreres i kontrakter og andre typer avtaler med leverandører og andre relevante tredjeparter
- **GV.SC-06:** Planlegging og aktsomhetsplikt utføres for å redusere risiko før det inngås formelle leverandør- eller andre tredjepartsforhold
- **GV.SC-07:** Risikoene som utgjøres av en leverandør, deres produkter og tjenester og andre tredjeparter identifiseres, registreres, prioriteres, vurderes, besvares og overvåkes i løpet av hele forholdet
- **GV.SC-08:** Relevante leverandører og andre tredjeparter er inkludert i hendelsesplanlegging, respons og gjenopprettingsaktiviteter
- **GV.SC-09:** Sikkerhetspraksis for forsyningskjeden er integrert i programmer for cybersikkerhet og programmer for styring av bedriftsrisiko, og ytelsen overvåkes gjennom hele livssyklusen til teknologiproduktet og tjenesten
- **GV.SC-10:** Risikostyringsplaner for cybersikkerhet i forsyningskjeden inneholder bestemmelser for aktiviteter som oppstår etter avslutning av en partnerskaps- eller serviceavtale

---

#### **IDENTIFISERE (ID):** Organisasjonens nåværende cybersikkerhetsrisiko er forstått

---

- **Kapitalforvaltning (ID.AM):** Eiendeler (f.eks. data, maskinvare, programvare, systemer, fasiliteter, tjenester, mennesker) som gjør det mulig for organisasjonen å oppnå forretningsformål, identifiseres og styres i samsvar med deres relative betydning for organisatoriske mål og for organisasjonen
  - **ID.AM-01:** Beholdninger av maskinvare som administreres av organisasjonen opprettholdes
  - **ID.AM-02:** Beholdninger av programvare, tjenester og systemer som administreres av organisasjonen opprettholdes
  - **ID.AM-03:** Representasjoner av organisasjonens autoriserte nettverkskommunikasjon og interne og eksterne nettverksdataflyter opprettholdes
  - **ID.AM-04:** Beholdning av tjenester levert av leverandører opprettholdes
  - **ID.AM-05:** Ressurser prioriteres basert på klassifisering, kritikalitet, ressurser og innvirkning på oppdraget
  - **ID.AM-07:** Databeholdninger og tilhørende metadata for angitte datatyper opprettholdes
  - **ID.AM-08:** Systemer, maskinvare, programvare og tjenester og data administreres gjennom hele livssyklusen
- **Risikovurdering (ID.RA):** Organisasjonen forstår cybersikkerhetsrisikoen for organisasjonen, eiendeler og individer

- **ID.RA-01:** Sårbarheter i ressurser identifiseres, valideres og registreres
  - **ID.RA-02:** Etterretning om cybertrusler mottas fra informasjonsdelingsfora og kilder
  - **ID.RA-03:** Interne og eksterne trusler mot organisasjonen identifiseres og registreres
  - **ID.RA-04:** Potensielle virkninger og sannsynlighet for at trusler utnytter sårbarheter identifiseres og registreres
  - **ID.RA-05:** Trusler, sårbarheter, sannsynlighet og innvirkning brukes til å bestemme naturlig risiko og informere risikoprioritering
  - **ID.RA-06:** Risikoresponser velges, , prioriteres, planlegges, spores og kommuniseres
  - **ID.RA-07:** Endringer og unntak håndteres, vurderes for risikopåvirkning, registreres og spores
  - **ID.RA-08:** Prosesser for mottak, analyse og svar på sårbarhetsavsløringer er etablert
  - **ID.RA-09:** Ektheten og integriteten til maskinvare og programvare vurderes før anskaffelse og bruk
  - **ID.RA-10:** Kritiske leverandører vurderes før oppkjøp
- 
- **Forbedring (ID.IM):** Forbedringer av organisatoriske risikostyringsprosesser, prosedyrer og aktiviteter for cybersikkerhet er identifisert på tvers av alle rammeverkets funksjoner
    - **ID.IM-01:** Evalueringer brukes for å identifisere forbedringer
    - **ID.IM-02:** Sikkerhetstester og øvelser, inkludert de som gjøres i koordinering med leverandører og relevante tredjeparter, gjennomføres for å identifisere forbedringer
    - **ID.IM-03:** Erfaringer under utførelse av operasjonelle prosesser, prosedyrer og aktiviteter brukes til å identifisere forbedringer
    - **ID.IM-04:** Cybersikkerhetsplaner som påvirker driften kommuniseres, vedlikeholdes og forbedres
- 

---

**BESKYTTE (PR):** Bruk av sikkerhetsmekanismer for å forhindre eller redusere cybersikkerhetsrisiko

---

- **Identitetsadministrasjon, autentisering og tilgangskontroll (PR.AA):** Tilgang til fysiske og logiske ressurser er begrenset til autoriserte brukere, tjenester og maskinvare, og administreres i samsvar med den vurderte risikoen for uautorisert tilgang
  - **PR.AA-01:** Identiteter og legitimasjon for autoriserte brukere, tjenester og maskinvare administreres av organisasjonen
  - **PR.AA-02:** Identiteter blir bekreftet og bundet til legitimasjon basert på interaksjonskonteksten
  - **PR.AA-03:** Brukere, tjenester og maskinvare blir autentisert
  - **PR.AA-04:** Identitetserklæringer beskyttes, formidles og verifiseres

- **PR.AA-05:** Tilgangstillatelser, rettigheter og autorisasjoner defineres i en policy, administreres, håndheves og gjennomgås, og innlemmer prinsippene om minste privilegium og separasjon av plikter
  - **PR.AA-06:** Fysisk tilgang til eiendeler styres, overvåkes og håndheves i samsvar med risiko
- 
- **Bevisstgjøring og opplæring (PR.AT):** Organisasjonens personell får bevissthet og opplæring i cybersikkerhet, slik at de kan utføre sine cybersikkerhetsrelaterte oppgaver
    - **PR.AT-01:** Brukerne får bevissthet og opplæring slik at de har kunnskap og ferdigheter til å utføre generelle oppgaver med sikkerhetsrisiko i tankene
    - **PR.AT-02:** Personer i spesialiserte roller får bevissthet og opplæring slik at de har kunnskap og ferdigheter til å utføre relevante oppgaver med sikkerhetsrisiko i tankene
- 
- **Datasikkerhet (PR.DS):** Data administreres i samsvar med organisasjonens risikostrategi for å beskytte konfidensialitet, integritet og tilgjengelighet av informasjon
    - **PR.DS-01:** Konfidensialitet, integritet og tilgjengelighet av data som er lagret er beskyttet
    - **PR.DS-02:** Konfidensialiteten, integriteten og tilgjengeligheten til data under transport er beskyttet
    - **PR.DS-10:** Konfidensialiteten, integriteten og tilgjengeligheten til data i bruk er beskyttet
    - **PR.DS-11:** Sikkerhetskopier av data opprettes, beskyttes, vedlikeholdes og testes
- 
- **Plattformsikkerhet (PR.PS):** Maskinvaren, programvaren (f.eks. fastvare, operativsystemer, applikasjoner) og tjenestene til fysiske og virtuelle plattformer administreres i samsvar med organisasjonens risikostrategi for å beskytte deres konfidensialitet, integritet og tilgjengelighet
    - **PR.PS-01:** Praksis for konfigurasjonsadministrasjon brukes
    - **PR.PS-02:** Programvare vedlikeholdes, erstattes og fjernes i samsvar med risiko
    - **PR.PS-03:** Maskinvare vedlikeholdes, erstattes og fjernes i forhold til risiko
    - **PR.PS-04:** Loggoppføringer skapes og gjøres tilgjengelig for kontinuerlig overvåking
    - **PR.PS-05:** Installasjon og kjøring av uautorisert programvare forhindres
    - **PR.PS-06:** Sikker praksis for programvareutvikling er integrert, og ytelsen overvåkes gjennom hele livssyklusen for programvareutvikling
- 
- **Motstandsdyktighet for teknologisk infrastruktur (PR.IR):** Sikkerhetsarkitekturer administreres med organisasjonens risikostrategi for å beskytte aktivas konfidensialitet, integritet og tilgjengelighet og organisatorisk motstandskraft
    - **PR.IR-01:** Nettverk og miljøer er beskyttet mot uautorisert digital tilgang og bruk
    - **PR.IR-02:** Organisasjonens teknologiske eiendeler er beskyttet mot miljøtrusler



- **PR.IR-03:** Mekanismer implementeres for å oppnå krav om motstandsdyktighet i normale og ugunstige situasjoner
  - **PR.IR-04:** Tilstrekkelig ressurskapasitet for å sikre at tilgjengeligheten opprettholdes
- 

---

#### **OPPDAG (DE):** Finne og analysere mulige cybersikkerhetsangrep og sikkerhetsbrudd

---

- **Kontinuerlig overvåking (DE.CM):** Eiendeler overvåkes for å finne uregelmessigheter, indikatorer på kompromiss og andre potensielt uønskede hendelser
    - **DE.CM-01:** Nettverk og nettverkstjenester overvåkes for å finne potensielt uønskede hendelser
    - **DE.CM-02:** Det fysiske miljøet overvåkes for å finne potensielt uønskede hendelser
    - **DE.CM-03:** Personellaktivitet og teknologibruk overvåkes for å finne potensielt uønskede hendelser
    - **DE.CM-06:** Aktiviteter og tjenester fra eksterne tjenesteleverandører overvåkes for å finne potensielt uønskede hendelser
    - **DE.CM-09:** Databehandling av maskinvare og programvare, kjørende miljøer og deres data overvåkes for å finne potensielt uønskede hendelser
  - **Analyse av Uønskede Hendelser (DE.AE):** Avvik, indikatorer på kompromiss og andre potensielt uønskede hendelser analyseres for å karakterisere hendelsene og oppdage cybersikkerhetshendelser
    - **DE.AE-02:** Potensielt uønskede hendelser analyseres for å bedre forstå tilknyttede aktiviteter
    - **DE.AE-03:** Informasjon er korrelert fra flere kilder
    - **DE.AE-04:** Estimert konsekvens og omfang av uønskede hendelser er forstått
    - **DE.AE-06:** Informasjon om uønskede hendelser gis til autorisert personell og verktøy
    - **DE.AE-07:** Etterretning om cybertrusler og annen kontekstuell informasjon er integrert i analysen
    - **DE.AE-08:** Hendelser erklæres når uønskede hendelser oppfyller de definerte hendelseskriteriene
-

---

**REAGER (RS):** Ta handling i forbindelse med en oppdaget cyber-sikkerhetshendelse

---

- **Hendelseshåndtering (RS.MA):** Svar på oppdagede cybersikkerhetshendelser administreres
    - **RS.MA-01:** Hendelsesrespons-planen utføres når en hendelse er erklært i koordinering med relevante tredjeparter
    - **RS.MA-02:** Hendelsesrapporter triageres og valideres
    - **RS.MA-03:** Hendelser kategoriseres og prioriteres
    - **RS.MA-04:** Hendelser eskaleres eller forhøyes etter behov
    - **RS.MA-05:** Kriteriene for å initiere hendelsesgjenoppretting anvendes
  - **Hendelsesanalyse (RS.AN):** Etterforskning utføres for å sikre effektiv respons og støtte undersøkelser og gjenoppretingsaktiviteter
    - **RS.AN-03:** Analyse utføres for å finne ut hva som har skjedd under en hendelse og den grunnleggende årsaken til hendelsen
    - **RS.AN-06:** Handlinger utført under en undersøkelse registreres og journalenes integritet og opprinnelse bevares
    - **RS.AN-07:** Hendelsesdata og metadata samles inn, og deres integritet og opprinnelse bevares
    - **RS.AN-08:** Hendelsens omfang estimeres og valideres
  - **Rapportering og kommunikasjon av hendelsesrespons (RS.CO):** Responsaktiviteter koordineres med interne og eksterne interessenter i henhold til lover, forskrifter eller retningslinjer
    - **RS.CO-02:** Interne og eksterne interessenter varsles om hendelser
    - **RS.CO-03:** Informasjon deles med utpekte interne og eksterne interessenter
  - **Hendelsesbegrensning (RS.MI):** Aktiviteter utføres for å forhindre utvidelse av en hendelse og redusere virkningene
    - **RS.MI-01:** Hendelser ivaretas
    - **RS.MI-02:** Hendelser håndteres
- 

---

**GJENOPPRETT (RC):** Gjenopprett ressurser og operasjoner som ble påvirket av en cybersikkerhetshendelse

---

- **Utførelse av plan for gjenoppretting av hendelser (RC.RP):** Gjenoppretingsaktiviteter utføres for å sikre operativ tilgjengelighet av systemer og tjenester som er berørt av hendelser
  - **RC.RP-01:** Gjenoppretingsdelen av hendelsesresponsplanen utføres når den er initiert fra hendelsesresponsprosessen

- **RC.RP-02:** Gjenopprettings-handlinger bestemmes, avgrenses, prioriteres og utføres
  - **RC.RP-03:** Integriteten til sikkerhetskopier og andre restaureringsmidler verifiseres før de brukes til restaurering
  - **RC.RP-04:** Kritiske oppdragsfunksjoner og risikostyring av cybersikkerhet vurderes for å etablere operasjonelle normer etter hendelsen
  - **RC.RP-05:** Integriteten til gjenopprettede eiendeler verifiseres, systemer og tjenester gjenopprettes, og normal driftsstatus bekreftes
  - **RC.RP-06:** Kriteriene for å bestemme slutten på hendelsesgjenoppretting brukes, og hendelsesrelatert dokumentasjon fylles ut
- 
- **Kommunikasjon under hendelsegjenoppretting (RC.CO):** Gjenopprettingsaktiviteter koordineres med interne og eksterne parter
    - **RC.CO-03:** Gjenopprettings-aktiviteter og fremdrift i gjenoppretting av operasjonelle evner kommuniseres til utpekte interne og eksterne interessenter
    - **RC.CO-04:** Offentlige oppdateringer om hendelses-gjenoppretting deles på riktig måte ved hjelp av godkjente metoder og meldinger
-



## Vedlegg B. Beskrivelser av Rammeverkets Nivåer

Tabell 3 beskriver rammeverkets nivåer som diskutert i seksjon 3.2. Nivåene karakteriserer omfanget av en organisasjons praksis for styring av cybersikkerhetsrisikoer (STYRE) og praksis for håndtering av cybersikkerhetsrisikoer (IDENTIFISER, BESKYTT, OPPDAG, REAGER og GJENOPPRETT).

**Tabell 2. Rammeverkets Nivåer**

Nivå	Styring av cybersikkerhetsrisiko	Håndtering av cybersikkerhetsrisiko
Nivå 1: Delvis	<p>Bruk av organisasjonens strategi for cybersikkerhetsrisiko håndteres på en tilfeldig måte.</p> <p>Prioritering er tilfeldig og ikke formelt basert på mål eller trussel miljø.</p>	<p>Det er begrenset bevissthet om cybersikkerhetsrisiko på organisatorisk nivå.</p> <p>Organisasjonen iverksetter cybersikkerhetsrisikostyring på en uregelmessig, sak-for-sak basis.</p> <p>Organisasjonen har kanskje ikke prosesser som muliggjør deling av cybersikkerhetsinformasjon internt i organisasjonen.</p> <p>Organisasjonen er generelt uvitende om cybersikkerhetsrisikoene knyttet til sine leverandører og produktene og tjenestene den anskaffer og bruker.</p>
Nivå 2: Risikoinformert	<p>Riskhåndteringspraksisene er godkjent av ledelsen, men er kanskje ikke etablert som organisasjonsomfattende retningslinjer.</p> <p>Prioritering av cybersikkerhetsaktiviteter og beskyttelsesbehov er direkte informert av organisasjonens risikomål, trusselmiljøet eller forretnings-/oppdragskrav.</p>	<p>Det er en bevissthet om cybersikkerhetsrisiko på organisasjonsnivå, men en organisasjonsomfattende tilnærming til håndtering av cybersikkerhetsrisiko er ikke etablert.</p> <p>Vurdering av cyberrisiko i organisatoriske mål og programmer kan forekomme på noen nivåer av organisasjonen, men ikke på alle. Vurdering av cyberrisiko for organisatoriske og eksterne eiendeler forekommer, men er vanligvis ikke gjentakende eller regelmessige.</p> <p>Cybersikkerhetsinformasjon deles innen organisasjonen på en uformell basis.</p> <p>Organisasjonen er klar over cybersikkerhetsrisikoene knyttet til sine leverandører og produktene og tjenestene den anskaffer og bruker, men den handler ikke konsekvent eller formelt som respons på disse risikoene.</p>
Nivå 3: Repeterbar	<p>Organisasjonens risikostyringspraksis er formelt godkjent og uttrykt som retningslinjer.</p>	<p>Det er en organisasjonsbred tilnærming til håndtering av cybersikkerhetsrisikoer.</p> <p>Det er etablert konsistente metoder for å respondere effektivt på endringer i risiko. Personalet besitter</p>

	<p>Retningslinjer, prosesser og prosedyrer basert på risikovurdering er definert, implementert som tiltenkt og gjennomgått.</p> <p>Organisasjonens cybersikkerhetspraksis oppdateres jevnlig basert på bruk av risikostyringsprosesser i lys av endringer i forretnings-/oppdragskrav, trusler og teknologisk landskap.</p>	<p>kunnskap og ferdigheter til å utføre sine oppnevnte roller og ansvar.</p> <p>Organisasjonen overvåker konsekvent og nøyaktig cybersikkerhetsrisikoer for eiendeler. Ledere innen cybersikkerhet og ikke-cybersikkerhet kommuniserer jevnlig angående cybersikkerhetsrisikoer. Toppledelsen sørger for at cybersikkerhet vurderes i alle driftslinjer i organisasjonen.</p> <p>Organisasjonens risikostrategi er informert av cybersikkerhetsrisikoene knyttet til sine leverandører og produktene og tjenestene den anskaffer og bruker. Personell handler formelt på disse risikoene gjennom mekanismer som skriftlige avtaler for å formidle grunnleggende krav, styringsstrukturer (f.eks. risikoråd), og policyimplementering og -overvåking. Disse handlingene gjennomføres konsekvent og som tiltenkt, og blir kontinuerlig overvåket og gjennomgått.</p>
<p>Nivå 4: Tilpasningsdyktig</p>	<p>Det er en organisasjonsomfattende tilnærming til håndtering av cybersikkerhetsrisikoer som bruker risikoinformerte retningslinjer, prosesser og prosedyrer for å håndtere mulige cybersikkerhetshendelser. Forholdet mellom cybersikkerhetsrisikoer og organisatoriske mål er tydelig forstått og vurderes når beslutninger tas. Ledere overvåker cybersikkerhetsrisikoer i samme kontekst som økonomiske og andre organisatoriske risikoer.</p> <p>Organisasjonsbudsjettet er basert på en forståelse av nåværende og forutsatte risikomiljø og risikotoleranse.</p> <p>Forretningsenheter implementerer ledelsens visjon og analyserer risiko på systemnivå i sammenheng med organisasjonens risikotoleranser.</p> <p>Cybersikkerhetsrisikohåndtering er en del av organisasjonskulturen. Den utvikler seg fra bevissthet om tidligere aktiviteter og kontinuerlig bevissthet om aktiviteter på organisasjonens systemer og nettverk.</p> <p>Organisasjonen kan raskt og effektivt tilpasse seg endringer i forretnings-/oppdragsmål i hvordan risiko nærmer seg og kommuniseres.</p>	<p>Organisasjonen tilpasser sine cybersikkerhetspraksiser basert på tidligere og nåværende cybersikkerhetsaktiviteter, inkludert lærdommer og prediktive indikatorer. Gjennom en kontinuerlig forbedringsprosess som inkorporerer avanserte cybersikkerhetsteknologier og praksiser, tilpasser organisasjonen seg aktivt til et stadig skiftende teknologisk landskap og responderer på en rask og effektiv måte på stadig mer avanserte trusler.</p> <p>Organisasjonen bruker sanntids- eller nær sanntidsinformasjon for å forstå og konsekvent handle på cybersikkerhetsrisikoene knyttet til sine leverandører og produktene og tjenestene den anskaffer og bruker.</p> <p>Cybersikkerhetsinformasjon deles kontinuerlig gjennom organisasjonen og med autoriserte tredjeparter.</p>

## Vedlegg C. Ordliste

### Rammeverk-kategori

En gruppe relaterte cybersikkerhetsresultater som samlet utgjør en CSF-funksjon.

### Fellesskapsprofiler i rammeverket

Et grunnlag av CSF-resultater som opprettes og publiseres for å ivareta felles interesser og mål blant flere organisasjoner. En fellesskapsprofil utvikles vanligvis for en bestemt sektor, undersektor, teknologi, trusseltype eller annet bruksområde. En organisasjon kan bruke en fellesskapsprofil som grunnlag for sin egen målprofil.

### Rammeverket-kjernen

En taksonomi av overordnede cybersikkerhetsresultater som kan hjelpe enhver organisasjon med å håndtere sine cybersikkerhetsrisikoer. Dens komponenter er en hierarki av funksjoner, kategorier og underkategorier som beskriver hvert resultat i detalj.

### Nåværende profil i Rammeverket

En del av en organisasjonsprofil som spesifiserer de kjerneutfallene som en organisasjon for øyeblikket oppnår (eller prøver å oppnå) og karakteriserer hvordan eller i hvilken grad hvert utfall oppnås.

### Rammeverket-funksjonen

Det høyeste nivået av organisasjon for cybersikkerhetsresultater. Der er seks funksjoner i Rammeverket: Styre, Identifisere, Beskytte, Oppdage, Reagere, Gjenopprette

### Eksempel på implementering av Rammeverket

En kortfattet, handlingsorientert, hypotetisk illustrasjon av en måte å bidra til å oppnå et kjerneutfall i Rammeverket

### Rammeverket-Informativ Referanse

En kartlegging som indikerer et forhold mellom et Rammeverket-kjerneutfall og en eksisterende standard, retningslinje, forskrift eller annet innhold.

### Rammeverket organisasjonsprofil

En mekanisme for å beskrive en organisasjons nåværende og/eller målrettede cybersikkerhetsstatus i forhold til Rammeverk-kjernens resultater.

### Rammeverket Hurtigstartsguide

En supplerende ressurs som gir kortfattet, handlingsrettet veiledning om spesifikke Rammeverksrelaterte emner.

### Rammeverket underkategori

En gruppe mer spesifikke resultater av tekniske og ledelsesmessige cybersikkerhetsaktiviteter som utgjør en CSF-kategori.

### Rammeverket Målprofil

En del av en organisasjonsprofil som spesifiserer de ønskede kjerneutfallene som en organisasjon har valgt og prioritert for å oppnå sine mål for cybersikkerhetsrisikostyring.

### Rammeverket Nivå

En karakterisering av grundigheten i en organisasjons praksis for styring og håndtering av cybersikkerhetsrisiko. Der er fire nivåer: Delvis (Nivå 1), Risikoinformert (Nivå 2), Gjentakende (Nivå 3), and Tilpassingsdyktig (Nivå 4).



Visse utstyr, instrumenter, programvare eller materialer, enten kommersielle eller ikke-kommersielle, er identifisert i dette dokumentet for å spesifisere den eksperimentelle prosedyren tilstrekkelig. En slik identifikasjon innebærer ikke anbefaling eller godkjenning av noen produkter eller tjenester fra NIST, og den innebærer heller ikke at de identifiserte materialene eller utstyret nødvendigvis er de beste tilgjengelige for formålet.

#### **NIST policyer for Teknisk Serie**

[Opphavsrett, Bruk og Lisensieringsuttalelser](#)

[NIST Technical Series Publication Identifier Syntax](#)

#### **Hvordan sitere denne NIST Teknisk Serie publikasjonen**

National Institute of Standards and Technology (2024) NIST rammeverk for cyber- og informasjonssikkerhet (CSF) 2.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 29 nor. <https://doi.org/10.6028/NIST.CSWP.29.nor>

#### **Kontaktinformasjon**

[cyberframework@nist.gov](mailto:cyberframework@nist.gov)

National Institute of Standards and Technology

Attn: Applied Cybersecurity Division, Information Technology Laboratory

100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Alle kommentarer kan etterspørres under Freedom of Information Act (FOIA).