Sluttrapport

UH – SIKKERHETSSATSING 2019-2022

Denne fylles ut ved behandling.

Prosjektnummer	**Journalnummer**	
Behandlet dato: 28.10.2022	**Behandlet av / Prosjekteier:** Styringsgruppene for prosjektene: - Analysesenter og responsmiljø - Rådgivingstjenester og kompetanseheving	**Utarbeidet av** Bjørn Helge Kopperud
Beslutning: Godkjent		
Signatur ved godkjenning (prosjekteier): Tom Are Røtting		

Innhold

ENDRINGSLOGG

Versjon	Dato	Endring	Produsent	Godkjent
0.1	21.06.2022	Påstartet sluttrapport	Anders Lund og Maria Luces	
0.2	16.08.2022	Gjennomgang med POL på nytt utkast	Anders Lund, Maria Luces og Bjørn Helge Kopperud	
0.3	17.08.2022	Gjennomgang/revisjon	Bjørn Helge Kopperud	
0.4	23.08.2022	Kvalitetssikring og mindre justeringer	Anders Lund	
0.5	24.08.2022	Felles gjennomgang og revisjon	Bjørn Helge Kopperud, Maria Luces og Anders Lund	
0.6	30.08.2022	Justering av formuleringer og språk. Kvalitetssikring.	Julie Storlie og Tom A. Røtting	
0.7	02.09.2022	Justeringer etter kvalitetssikring	Bjørn Helge Kopperud	
0.8	06.09.2022	Gevinstrealisering og økonomi	Bjørn Helge Kopperud og Maria Luces	
0.9	07.09.2022	Formattering og formaliteter	Bjørn Helge Kopperud	
1.0	15.10.2022	Justeringer etter høringsrunde	Julie Storlie	

DISTRIBUSJONSLOGG

Versjon distribuert	Dato	Navn
0.5	24.08.2022	Julie Storlie, Roar Olsen, Tom A. Røtting
0.6	04.09.2022	Kristin Selvaag, HK-dir (samordning)
0.9	07.09.2022	Styringsgruppen og navngitte eksperter som er rådgivere for styringsgruppen.
1.0	19.10.2022	Styringsgruppen
1.0	DD.MM.ÅÅÅÅ	Kunnskapsdepartementet, Digitaliseringsstyret, Sikt.no

1. FORMÅL MED SLUTTRAPPORTEN

Formålet med sluttrapporten er intern og ekstern læring. Sluttrapporten dokumenterer erfaringer som er nyttige for fremtidige prosjekter og annen relevant informasjon som er relevant for de som skal drifte og vedlikeholde prosjektets produkter.

Sluttrapporten er et ledelsesprodukt som skal foreligge til beslutningspunkt 5 for å avslutte prosjektet og oppløse styringsgruppe og prosjektgruppe.

2. Oppsummering av prosjektet

2.1. Finansiering og mål

I Prop. 1 S (statsbudsjettet) for budsjettåret 2019 ble det satt av 17,5 millioner i årlig ramme til «program for informasjonssikkerhet i Universitets- og høgskolesektoren». Midlene ble av Kunnskapsdepartementet tildelt Unit for gjennomføring av et fireårig program for informasjonssikkerhet i UH-sektoren.

Styringsdokumentet for programmet ble vedtatt i Digitaliseringsstyret 11. april 2019, med følgende mål for arbeidet:

«Sektoren skal totalt sett forbedre sin evne til å forebygge, oppdage og håndtere trusler, og styringen med informasjonssikkerheten i sektoren skal under bedre kontroll. Dette skal samordnes bedre og gjøres mer helhetlig, og settes inn i en større nasjonal sammenheng. Den totale effekten av dette, er at arbeidet med informasjonssikkerhet i sektoren skal opp på et bedre nivå enn de nasjonale minstekravene.»

2.2. Sluttrapportens omfang

Sikkerhetssatsingen har omfattet tre leveranser:

1. Ny styringsmodell for informasjonssikkerhet og personvern (ansvarlig: Unit, HK-Dir fra 2022)
2. Analysesenter og responsmiljø (ansvarlig: Uninett, Sikt fra 2022)
3. Rådgivingstjenester og kompetanseheving (ansvarlig: Uninett, Sikt fra 2022)

Denne sluttrapporten tar for seg erfaringer og læringspunkter fra prosjekt nummer 2 og 3.

Sluttrapporten for prosjekt nummer 1 utarbeides av HK-dir og behandles i henhold til styringslinjene for dette prosjektet, senest innen utgangen av 2022.

Sluttrapporten for alle de tre prosjektene vil gjøres tilgjengelig som en del av porteføljestyringen av nasjonal digitaliseringsportefølje, som Sikt koordinerer.

2.3. Sammendrag av prosjektgjennomføringen

Organisering:
UH:Sikkerhetssatsing 2019-2022 ble fra start organisert som et program med tre prosjekter:

1. **Ny styringsmodell for informasjonssikkerhet og personvern**
   Denne delen av programmet skulle innføre en styringsmodell for informasjonssikkerhet i sektoren, basert på rammeverket ISO/IEC 27014:2013. Gjennom dette arbeidet skulle det også etableres en forvaltning av en slik styringsmodell, med tilhørende overordnet rapportering til Kunnskapsdepartementet.

2. **Analysesenter og responsmiljø**
   Forbedring av deteksjons- og analysekapasitet, og etablering av et helhetlig og felles analysesenter for cybersikkerhet i sektoren, var viktige mål med dette prosjektet. Uninett skulle ivareta rollen som responsmiljø for sektoren, i tråd med NSMs «Rammeverk for håndtering av IKT-sikkerhetshendelser». På den måten skulle man forbedre sektorens evne til å håndtere trusler gjennom bedre tilrettelegging og organisering.

3. **Rådgivingstjenester og kompetanseheving**
   Programmet skulle etablere rådgivingstjenester for implementering og helhetlig praktisering av etablerte ledelsessystem for informasjonssikkerhet, samt etablere et program for heving av kompetanse innenfor informasjonssikkerhet og personvern for lederen, forskeren, studenten og øvrige ansatte.

I tildelingsbrevet til Sikt ble oppdraget beskrevet med føring om at oppdraget skulle gjennomføres i samarbeid med sektoren, med deltakelse fra informasjonssikkerhetsmiljøene på Gjøvik ved NTNU og USIT ved UiO. I oppstarten av programmet (våren 2019) ble det opprettet et programstyre med representanter fra Unit (styreleder og programeier), Uninett (programleder og prosjektledelse), samt representanter fra kunnskaps- og helsesektoren; UiO, NTNU, NMBU, UiA, og NHN. Det ble nedsatt en prosjektgruppe per prosjekt, bestående av en prosjektleder og prosjektdeltakere fra Uninett, NTNU, UiO, Unit og NSD.

I mai 2020 besluttet programstyret å endre styringsformen fra program til prosjekt. Det ble da nedsatt separate styringsgrupper for prosjektene.

Økonomi:
Budsjettrammen for fire årsperioden på totalt MNOK 70 har vært fordelt med MNOK 50 til prosjektene som Uninett og senere Sikt fikk ansvaret for, og MNOK 20 til prosjektet som Unit og senere HK-Dir fikk ansvaret for.

Det er ventet at denne rammen ikke overstiges ved utgangen av 2022, etter at sluttføring av prosjektet og overlevering av prosjektets produkter til linjeorganisasjonen i Sikt er gjennomført.

Ressurser og fremdrift:
Gjennomføring av programmet har vært i henhold til de føringene som er gitt gjennom tildelingsbrevet fra Kunnskapsdepartementet og videre tildelingsbrev fra Unit til Uninett. I første del av programperioden ble ressursene prioritert til «Analysesenter og Responsmiljø», og ressursbruken til «Rådgivning og kompetanseheving» har gradvis økt i programperioden. I 2022 bidro resultatene fra disse prosjektene til at Cyber-sikkerhetssenter for forskning og utdanning ble vedtatt av Digitaliseringsstyret som en fellestjeneste i UH-sektoren.

Kvalitetssikring av prosjektet og leveranser:
Karabin AS ble i mars 2021 engasjert for å gjennomføre en uavhengig kvalitetssikring av arbeid, framdrift, fremtidig leveranse, samt generell styring av prosjektene og satsingsmidler. Hovedpunktene fra deres rapport er tatt med som en del av denne erfaringsrapporten.

Tjenestedesign, prototyping, pilotering og MVP har vært viktige bærebjelker i prosjektene. Disse metodene har vært viktig for å forstå og treffe brukerbehovene på best mulig måte.

3. OPPNÅELSE AV PROSJEKTETS MÅL

3.1. Virksomhetsmål

Programmet og prosjektenes overordnede mål har vært:

Sektoren skal totalt sett forbedre sin evne til å forebygge, oppdage og håndtere trusler, og styringen med informasjonssikkerheten i sektoren skal under bedre kontroll. Dette skal samordnes bedre og gjøres mer helhetlig, og settes inn i en større nasjonal sammenheng. Den totale effekten av dette er at arbeidet med informasjonssikkerhet i sektoren skal opp på et bedre nivå enn de nasjonale minstekravene.

3.2. Effektmål

Fem effektmål ble definert for sikkerhetssatsingen:

- Forbedre evnen til å forebygge, oppdage og håndtere trusler
- Bedre styring med informasjonssikkerheten i sektoren
- Bedre og mer helhetlig samordning
- Sette arbeidet inn i en større nasjonal sammenheng
- Bedre nivå på arbeidet enn de nasjonale minstekravene

«Nasjonale minstekrav» er summen av lovpålagte og regulatoriske krav som den enkelte virksomhet er underlagt. Kunnskapssektoren har betydelige informasjonsverdier og bør derfor heve nivået på styringen av informasjonssikkerheten til et nivå over minimumskravet.

Sikkerhetssatsingen har bidratt til oppnåelse av effektmålene. Ved å etablere tjenesten som én felles tjeneste bidrar satsingen til mer helhetlig samordning, og muliggjør bedre styring av informasjonssikkerheten i en nasjonal sammenheng. Dette vil også bidra til at arbeidet beveger seg i retning av de nasjonale minstekravene.

Satsingen har lagt til rette for å forbedre evnen til å forebygge, oppdage og håndtere trusler, og effektene fra dette målet vil i hovedsak realiseres av virksomhetene som tar i bruk tjenestene, etter at tjenestene er tatt i bruk.

I tillegg til realisering av de fem definerte effektmålene, har sikkerhetssatsingen bidratt til å øke attraktiviteten i arbeidsmarkedet. Ved at Cybersikkerhetssenteret er blitt en så tydelig satsing på sikkerhet i kunnskapssektoren, har vi underveis i programmet fått ansatt solid sikkerhetskompetanse. Videre fremover blir det også enklere å tiltrekke solid sikkerhetskompetanse i et stramt arbeidsmarked for denne type kompetanse.

3.3. Resultatmål

Gjennom styringsdokumentasjonen til programmet og prosjektene ble det vedtatt en strategi for hvordan gjennomføring skulle skje. Det ble vektlagt å komme fram til en kontinuerlig leveransemodell, hvor bruk av smidige prosesser, tjenestedesign, prototyping og MVP er foretrukne metoder. Trusselsituasjonen sektoren står ovenfor er kontinuerlig i endring og teknologiskifter skjer mye hurtigere i dag enn før. Resultatmålene for arbeidet har derfor endret seg underveis, og i mandat/styringsdokumentasjon har vi vært forsiktig med å låse oss for tidlig i langsiktige milepæler.

I arbeidet har vi også vært opptatt av å så tidlig som mulig finne en bærekraftig modell for kontinuerlige leveranser.

Prosjektets resultatmål	Grad av oppnåelse	Kommentar	Forankret hvor
Cybersikkerhetssenter for forskning og utdanning vedtatt som en fellestjeneste i sektoren med tilhørende tjenestekatalog	Oppnådd. I henhold til oppdrag og mandat/styrings-dokumentasjon («etableres et helhetlig og felles analysesenter for cybersikkerhet i sektoren»).	Arbeidet har vært svært tids- og ressurskrevende som følge av at virksomhetene i norsk UH-sektor har ulike behov og dermed divergerende ønsker om hvordan en fellestjeneste innen sikkerhet skulle innrettes.	Digitaliserings-styret
Rollen som «Sektorvist Responsmiljø» (SRM) utviklet og formalisert	Oppnådd I henhold til Unit sitt «Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren».	Formalisert av KD som Sikts ansvar fra og med 2022.	KD og Unit/HK-Dir
Etablert samhandlingsarena for erfarings- og kunnskapsutveksling om informasjonssikkerhet i sektoren	Oppnådd To fagfellesskap er etablert og/eller videreutviklet i programperioden. • Operative sikkerhetseksperter (IRT-community) • CISO-forum	Potensial for etablering av ytterligere fora: Forum for jurister knyttet til GDPR, Schrems II og andre aktuelle problemstillinger er diskutert, men så langt ikke realisert.	Sikt og HK-Dir
Bedret deteksjonsevne.	Delvis oppnådd. En første versjon er etablert, men videreføring forutsetter stabil og vedvarende finansiering. En rekke infrastrukturtiltak er gjennomført for å ha bedre evne til deteksjon av pågående trusler. En første versjon av en felles nasjonal delings- og beskyttelsesplattform for søk og registrering av kjente trusler tilgjengeliggjøres i løpet av 2022.	Data og erfaringsgrunnlag fra NTNU og UiO har vært avgjørende for å øke deteksjonsevnen i sektoren. Dette er ventet videreført ut over programperioden dersom rammebetingelsene tillater det.	Programstyret

4. PROSJEKTETS PRODUKTER

Tilskuddsbrev, styringsdokumentasjon og prosjektmandat har gitt mål og rammer for arbeidet. Det viktigste produktet som overleveres fra satsingen er «Cybersikkerhetssenter for forskning og utdanning», som er et direkte svar på dette. I tillegg har innføring av «Rammeverket for håndtering av alvorlige IKT-sikkerhetshendelser i UH-sektoren» og opprettelsen av en styringsmodell for arbeidet med informasjonssikkerhet (forvaltet av HK-Dir) gitt «sektorvist responsmiljø» et mandat og tydeliggjort styringslinjene.

Senteret vil styre hendelseshåndtering, forebyggende arbeid, analyse, rådgiving og kompetanseutvikling i sektor. Effekter skapes når flest mulig virksomheter er tilknyttet senteret, og ved å trekke på dyktige kompetansemiljø i sektoren i gjennomføring av arbeidet. Her er det fortsatt potensial for å hente ut mer, men gjennom de fire årene har det vært en endringsprosess og omlegging av eksisterende leveranser og pågående tiltak, hvor et cybersikkerhetssenter har bedre kapabiliteter og mer helhetlig tilnærming til fortsatt kontinuerlig leveranseutvikling.

Når sikkerhetssatsingen avsluttes i 2022 vil følgende tjenester videreføres gjennom arbeidet i Cybersikkerhetssenteret for forskning og utdanning, gruppert i tre tjenesteabonnementer:

- **Basisabonnement**
  Varsling ved hendelser i sektoren. Bistand ved alvorlige eller kritiske hendelser. Tilgang til nettverk av operative sikkerhetseksperter (IRT-community) og CISOer (CISO-forum) for utveksling av informasjon, erfaringer og kompetanse. Skjermet og sikker kommunikasjonskanal for deling av oppdatert trusselinformasjon, kjente sårbarheter og sikkerhetshendelser. Sikkerhetssertifikater.

- **Plussabonnement**
  Nettverkssensor som avdekker trusler og varsler om hendelser. Tilgang til nasjonal delings- og beskyttelsesplattform for søk og registrering av kjente trusler og sårbarheter (kommer i 2022). Automatisk blokkering av kjente trusler via etablerte sikkerhetsløsninger.

- **Totalabonnement**
  Tjeneste rettet mot mindre virksomheter der Cybersikkerhetssenter for forskning og utdanning kan levere en helhetlig portefølje av sikkerhetstjenester – både operativt og rådgivende.

- **Tilleggstjenester**
  En rekke viktige tilleggstjenester som ukentlig sårbarhetsscan, loggalanalyseverktøyet Humio, sektor- og institusjonsvise øvelser, rådgivning og kurs knyttet til virksomhetsledelse, risiko og samsvar

Ved overlevering fra prosjekt til forvaltning bør suksessfaktorer for å hente ut nytteverdien av Plussabonnementet (nettverkssensor) følges opp. Nettverksensor avdekker trusler og varsler for sektoren som helhet, og nytten henger sammen med antall institusjoner som bruker av tjenesten. For denne tjenesten har deler av BOTT et alternativt samarbeid, og det kan være hensiktsmessig å utarbeide et målbilde for nettverkene som helhet, og følge opp den videre utviklingen.

5. ØKONOMI

Prosjektenes påløpte kostnader, inkludert aktiviteter ut 2022, er tilnærmet lik rammen for prosjektet. Prosjektene har vært finansiert i form av tilskudd fra Unit/HK-Dir, gjennom årlige bevilgninger på 12,5 MNOK over fire år.

Økonomiske hovedtall frem til realiseringsfasen (BP5)	Godkjent budsjett	Prognose helår 2022
Prosjektkostnader	50 MNOK	51.7 MNOK

Budsjettramme og forbruk (pr juli 2022)

	2019	2020	2021	2022	2019-2022
Inntekter:	MNOK	MNOK	MNOK	MNOK	**MNOK**
Inntekter - bevilgning	12.5	12.5	14.2*	12.5	**51.7**
Kostnader:					
Utstyr/software	0.1	4.2	4.4	2.5	11.2
Konsulenttjenester	3.5	2.6	2.7	0.2	9.0
Reise- og møtekostnader	0.1	0.1	0.0	0.5	0.7
Timekostnader Uninett	5.6	10.0	8.3	6.9	30.8
Sum kostnader	**9.3**	**16.9**	**15.4**	**10.1**	**51.7**
Resultat	**3.2**	**-4.4**	**-1.2**	**2.4**	**0**

* Inkludert ekstra tilskudd fra Unit (MNOK 1.7) for gjennomføring av sårbarhets-scan for UH-institusjoner underlagt KD i mai/juni 2021.

Følgende leveranser har vært kostnadsdrivende i programperioden:

- Finansiering av Nasjonal klientdriftprosjektet
- Infrastruktur og programvare for data-/logganalyse
- Sårbarhets-scan

Per august 2022 gjenstår 5.9 millioner som i løpet av satsingsperioden skal gå til å:

- Forbedre deteksjonsevne og tilhørende eksisterende tjenestetilbud
- Styrke kompetansenettverkene IRT-community og CISO-forum
- Sikre finansiering for Cybersikkerhetssenteret for 2023 og videre
- Formelt avslutte sikkerhetssatsingen og sikre god overlevering fra prosjektet til linjen

Økonomistyringen av resterende satsingsmidler overføres til Sikt, og blir en del av porteføljestyringen. I sum skal arbeidet gå i økonomisk balanse ved årets slutt.

6. PROSJEKTETS FREMDRIFT

Prosjektene fremdriftsplaner har lagt til rette for smidig tilnærming innenfor rammene av prosjektmodellen
Styringsdokumentasjon og prosjektmandat har vært utformet med fremdriftsplan hvor det er definert et hensiktsmessig nivå og antall av milepæler, i kombinasjon med en mest mulig smidig gjennomføringsform. Fokus har vært på kort og mellomlang tidshorisont, slik at prosjektene har kunnet planlegge på en effektiv måte og utnytte muligheter og ny innsikt underveis.

Fremdriften har vært god, men påvirket av rollesammenblanding og organisasjonsendringer
Fremdriften i sikkerhetssatsingen har periodevis vært god, men har også vært preget av uklar rolleforståelse mellom Uninett og deres samarbeidspartnere. I tillegg har sammenslåing av virksomheter, nye styringsstrukturer og andre organisatoriske forhold påvirket fremdriften, spesielt siste halvår 2021 og første halvår 2022.

Tidlige avklaring om etablering av fellestjeneste var en suksessfaktor for etablering innenfor tidsrammen
Tidligere erfaring viser at man ofte starter for sent med å sikre vedvarende leveranser og finansiering også når satsings- og/eller programperioden er over. Uninett, med forankring i prosjektenes styringsgrupper, besluttet derfor tidlig – omtrent halvveis i perioden – at Cybersikkerhetssenteret måtte vedtas som en fellestjeneste i Digitaliseringsstyret. Dette tok mer enn et år å gjennomføre som følge av ulike behov hos virksomhetene i sektoren.

Satsingen har håndtert pandemien på en god måte
I perioden har samfunnet vært preget av pandemi og tilhørende hjemmekontor, men prosjektet har i stor grad tilrettelagt for digitale møter og arbeid, slik at dette i liten grad har påvirket fremdriften.

7. PROSJEKTETS BRUK AV POLITISKE PRINSIPPER OG FØRINGER

Tabellen under beskriver bruk av prinsipper og føringer.

Prinsipper for realisering av digitalisering	Den faktiske implementeringen i dette prosjektet
1. Sett brukeren i sentrum.	Prosjektene har i stor grad jobbet med etter prinsippet om brukeren i sentrum. Prosjektet har benyttet tjenestedesign, iterativ forbedring med utgangspunkt i «minimum viable product»/pilotering, dialog med representanter fra sektoren i dette arbeidet. Opprettelse av ny styringsmodell i sektoren og faktisk gjennomføring av kontinuerlig tilstands- og risikovurdering av det helhetlige arbeidet bygger også opp under dette prinsippet.
2. Tenk stort, start smått gjennom smidig utvikling. Prototyping og utprøving foran utredning. Bruk tverrfaglige team i størst mulig grad.	Prosjektet har jobbet etter smidige prinsipper herunder prinsippet om å «utprøve fremfor å utrede». Kompetanse og erfaringen med smidig er ulik i sektoren, og interessenter har av og til hatt forventninger om mer tradisjonell fossefalls-metodikk med større leveranser basert på mer utredning. Erfaringen fra dette er at felles forståelse for både mål og metode kan påvirke effektivitet.
3. Data lagres kun én gang og skal gjøres tilgjengelige for gjenbruk.	Sentral logganalyseplattform og bruk av «API» har vært viktig rettesnor i arbeidet. I arbeid med deling av trusselinformasjon er også prinsippet med tilgangsstyring vært viktig, slik at tilgjengeliggjøring og gjenbruk kan styres og kontrolleres.
4. Bygg inn sikkerhet og personvern i løsningene.	Et absolutt prinsipp i arbeid med produkter og leveranser i satsingen. Tillitt ligger mye til grunn for arbeidet, og uten innebygd sikkerhet og personvern har man ikke dette.
5. Sikre kontroll på tilgang til data og ressurser.	Også et absolutt prinsipp i arbeidet. Hvem som skal ha tilgang til hvilken informasjon må være under kontroll for å både ha tillitt og kunne skjøtte rollen som cybersikkerhetssenter og sektorvist responsmiljø.
6. Sky først: Når det ikke foreligger spesielle hindringer for å ta i bruk skytjenester, og slike tjenester gir den mest hensiktsmessige og kostnadseffektive løsningen, bør offentlig sektor velge slike tjenester.	Dette har i gjennomføring også vært vurdert ved en rekke anledninger, og vil være det framover også. Dette gjelder både ved etablering av infrastruktur, men også i vurderinger av leveranser fra markedet. Det er også et faktum at stadig større andel av informasjonsverdier som skal sikres ligger i skyløsninger, og man må derfor se sikkerhetsmekanismer opp mot sky-plattformer.
7. Offentlig sektor skal i utgangspunktet ikke gjøre selv det som markedet kan gjøre bedre og mer effektivt	Fellestjeneste Cybersikkerhetssenteret benytter både hyllevareprodukter som kan anskaffes, samt egenutviklede komponenter der det ikke er gode/kosteffektive produkter i markedet.

8. EVALUERING AV PROSJEKTET OG LÆRINGSPUNKTER

8.1. Organisering og roller

Sikkerhetssatsingen ble initiert av et tildelingsbrev fra Kunnskapsdepartementet til Unit, som igjen delegerte ansvaret for gjennomføringen av to av prosjektene til Uninett med tilhørende midler. Oppdraget ble gitt med en forutsetning om at NTNU og Universitetet i Oslo skulle delta i prosjektgjennomføringen.

Tydelighet om organisering og ansvar kan være en suksessfaktor for samarbeid
Samarbeidet mellom Uninett, NTNU og UiO har vært utfordrende på styringsnivå og operativt nivå i sikkerhetssatsingen. En av utfordringene har vært at NTNU og Universitetet i Oslo har roller som samarbeidspartnere, underleverandører og kunder til sikkerhetstjenester levert av Uninett/Sikt. Det har i store deler av satsingsperioden vært ulike oppfatninger av hvilken rolle NTNU og UiO skal ha i arbeidet, og i hvor stor grad de skulle ha innflytelse i styringen av satsingen.

Eksempler på utfordringer har vært:

- Uenighet om teknologivalg
- Ønske fra NTNU og UiO om å være mer delaktig i utviklingen av sluttproduktet
- Uavklart rapporteringsformat/detaljnivå for økonomirapporteringen (beskrevet som separat tema)
- Uenighet om prosjektets mandat/oppdrag og hvorvidt sektorvist responsmiljø var omfattet av tilskuddsbrev og styringsdokument

Samarbeidet og rollesammenblanding skapte forsinkelser gjennomgående, og spesielt utfordringer knyttet til fremtidig finansiering og konsumering av tjenester. Digitaliseringsstyrets vedtak i april 2022, bidro til å lande en omforent løsning for videre arbeid. Prosessen viste at samstyringsmodellen om fellestjenester kan gi beslutninger, men også har et forbedringspotensial. Evalueringen fra sikkerhetssatsingen vil benyttes som læring ved etablering av de nye samstyringsmodellen.

Et annet læringspunkt er at tydelighet om ansvar og myndighet ved tildeling av oppdrag kan være en forutsetning for god fremdrift og samarbeidsklima. Dette gjelder særlig premisser for organisering, som bør være avklart i etatsstyringen, og ligge som føring for prosjektets mandater og roller.

Hvis samarbeidsutfordringer oppstår på styrende nivå i fremtiden, kan et læringspunkt være at interessent-/samarbeidsrisiko bør risiko- og tiltaksstyres med ryddige og relevante skaleringsveier.

Tidlig og tydelig forventningsavklaring om rapportering kunne påvirket tilfredsheten med økonomistyringen
Et gjentakende diskusjonspunkt i sikkerhetssatsingen har vært transparens knyttet til regnskap og budsjett. Dette er forsøkt ivaretatt i underlag til styringsgrupper og Digitaliseringsstyret, men dette har ikke vært tilstrekkelig detaljert for alle. For å sørge innfrielse av forventninger kunne prosjektet avklart forventninger tidligere og på en tydeligere måte. Bedre tydelighet om roller og ansvar både på styringsgruppenivå og i prosjektene kunne også bidratt til bedre innfrielse av forventninger om rapporteringen. Ønske om innsyn i mer detaljerte økonomirapporter og timeføring bør normalt kunne løses med skalering og/eller justeringer i prosjektets controller-funksjon.

Digitaliseringsstyret har tilført verdi gjennom beslutningsmyndighet om innføring av fellestjenester
Prosjektenes styringsgrupper hadde tett oppfølging av aktivitetene i prosjektet i store deler av satsingsperioden, men etter hvert som satsingen realiserte tjenester ble Digitaliseringsstyret en viktig premissgiver for varig forvaltning av disse. På den måten ivaretok Digitaliseringsstyret den viktige

samarbeids- og samstyringsrollen når universitetene og høgskolene gjensidig forpliktet seg til en videreføring av felles sikkerhetsarbeid gjennom etableringen av Cybersikkehetssenteret. Digitaliseringsstyret vil være en kontinuitetsbærer for det videre sikkerhetsarbeidet, og bidra til oppfølging gjennom den årlige tilstandsrapporten for handlingsplanen som HK-Dir. har ansvaret for.

Både styringsgruppene og Digitaliseringsstyret hadde stor verdi og ga viktig bidrag under utvikling av tjenestene og operasjonaliseringen av Cybersikkerhetssenteret.

Prosjektorganisering ga mer effektive beslutningsprosesser enn programorganisering
Styringen av prosjektet ble endret underveis i perioden, fra programstyre til to styringsgrupper for hvert sitt prosjekt. Dette ble gjort for å kunne gi mer støtte til og tettere oppfølging av prosjektene. Effekten av endret organisering ble positiv, gjennom mer effektive beslutninger og bedre fremdrift.

8.2. Ressurser

Tydelige avtaler kunne gitt bedre forutsigbarhet for allokeringen av ressurser
Allokering av ressurser på tvers av samarbeidende virksomheter har vært utfordrende. Årsaken har vært at arbeidet med sikkerhetssatsingen kommer i tillegg til eksisterende arbeidsoppgaver. Det er et betydelig behov for sikkerhetskompetanse både lokalt og sentralt, noe som har gjort både planlegging og prioritering utfordrende. Tydeligere avtaler knyttet til ressursuttak og forventede leveranser ville trolig ha gjort utfordringen noe enklere å håndtere, og er et viktig læringspunkt.

Organiseringen og styringslinjene har medført ressursbruk til rapportering
Det er brukt betydelig tid på rapportering i programperioden til et stort antall aktører og interessenter. Både ledelse og styre i egen virksomhet (Uninett), oppdragsgivere (Unit og Kunnskapsdepartementet), og grupperinger i samstyringsmodellen (Digitaliseringsstyre, Fagutvalg, Tjenesteråd, UH-IT mv.) forventet ulike former for rapportering. Rapporteringsmengde kan med fordel reduseres i fremtidige program/satsinger.

8.3. Beslutningsprosesser

Transparens og tilbakemeldinger om høringer og beslutningsprosesser kan påvirke beslutningskvalitet
Digitaliseringsstyrets rolle om etablering av fellestjenester, betalingsmodell og inngåelse av økonomiske forpliktelser kunne vært tydeliggjort ovenfor Styringsgruppen. UiO og NTNU har gitt innspill om at prosessen for involvering og rådføring i forkant av beslutninger i Digitaliseringsstyret burde vært bedre. Et annet forbedringsområde er behandlingen av resultater fra innsiktsarbeidet. Forbedringene gjelder både i hvordan innspillene ivaretas i anbefalinger og hvordan de involverte får tilbakemeldingen på prosess og utfall.

8.4. Samarbeidet fremover

Enighet om å styrke sikkerheten i kunnskapssektoren og godt samarbeid med ressurspersoner har bidratt til gode produkter
Til tross for samarbeidsutfordringene har alle involverte virksomheter et felles ønske om å styrke sikkerheten i norsk kunnskapssektor, og at samarbeid er avgjørende for å få til dette. Nettopp denne felles forståelsen og det vedvarende gode samarbeidet med enkeltpersoner på konkrete problemstillinger, er årsaken til at sikkerhetssatsingen kan vise til gode resultater i form av en fellestjeneste som alle solidarisk skal konsumere og finansiere.

Godt kommunikasjonsarbeid med en bred interessentgruppe har bidratt til styrket oppslutning for samarbeidet på sikkerhetsområdet

Når det gjelder forankring i sektoren, utover styringsgruppen og prosjektgruppen, har det vært lagt ned betydelig arbeid til formidling av målbilde, fremdrift og leveranser i ulike fora. I tillegg til styringsgruppene og oppdragsgiverne har satsingens referansegruppe, Digitaliseringsstyret, fagutvalg for informasjonssikkerhet, tjenesteråd for IMD og informasjonssikkerhet, UH-IT, IRT-teamene og CISO-forum fått mer eller mindre jevnlige oppdateringer om det pågående arbeidet i sikkerhetssatsingen. Tilbakemeldingene har jevnt over vært positive, og det er bred enighet i sektoren om at et samarbeid innen sikkerhetsområdet er viktig.

8.5. Gevinstrealisering

Sikkerhetssatsingen bidrar til realisering av digitaliseringsstrategien for offentlig sektor og strategien for bærekraft og like muligheter. Satsingen bidrar også til sektorspesifikke strategier herunder; strategi for digitalisering i høyere utdanning og forskning, strategi for kvalitetsutvikling i skolen i lys av fagfornyelsen, strategi for desentralisert og fleksibel utdanning og strategi for tilgjengeliggjøring og deling av forskningsdata.

Sikkerhetssatsingen påvirker direkte strategioppnåelsen av digitaliseringsstrategien og kan betraktes som en forutsetning for de sektorspesifikke strategiene. Av direkte bidrag fra satsingen er følgende mål i digitaliseringsstrategien relevante:

1. «Offentlig sektor digitaliseres på en åpen, inkluderende og tillitvekkende måte»
   Beskrivelse av bidrag: God sikkerhetsstyring bidrar til tillit og forebygger mot angrep og skader. Ved å styre sikkerheten som en fellestjeneste kan forebyggende arbeid og risiko styres mer helhetlig, datadrevet og faktabasert. Det muliggjør strategisk arbeid og kommunikasjon for involvering og åpenhet

2. «Flere oppgaver løses digitalt, og som sammenhengende tjenester».
   Beskrivelse av bidrag: Sikkerhet kan sees på som et økosystem, hvor hvert ledd har avhengigheter til det øvrige systemet. Ved å etablere en helhetlig tjeneste for sikkerhet som alle benytter, kan data fangstes og deles i hele økosystemet, og dermed blir det mulig bygge sammenhengende tjenester for datadeling. på en mer sikker måte.

3. «Offentlig sektor utnytter potensialet i deling og bruk av data til å lage -brukervennlige tjenester, og for å bidra til verdiskapning for næringslivet».
   Beskrivelse av bidrag: Både innhenting, strukturering og deling av sensitive data forutsetter god sikkerhet. Strukturert og helhetlig tilnærming til sikkerhet skaper tillit, og er dermed også en forutsetning for samarbeid både i relasjoner og mellom systemer.

4. «Kommunale og statlige virksomheter henter gevinster fra digitalisering på en systematisert måte»
   Beskrivelse av bidrag: Et enhetlig og strukturert system for overvåking, rapportering, kompetansebygging, hendelseshåndtering og beredskap for sikkerhet muliggjør gevinstoppfølging på en systematisk måte på sektornivå.

I tillegg til målene i digitaliseringsstrategien, påvirker satsingen innsatsfaktorene ved å tilrettelegge for samhandling, mer effektiv ressursbruk og økt sikkerhet. Cybersikkerhetssenter for forskning og utdanning tilbyr både ekspertkompetanse for rådgivning, og fora for erfaringsutvikling mellom institusjonene, og påvirker dermed innsatsfaktoren om at «offentlig sektor skal samhandle bedre om digitale tjenester og effektivisere ressursbruken gjennom styrket samordning på tvers av forvaltningsnivåer og sektorer, og systematisk uthenting av gevinster fra digitalisering». En annen innsatsfaktor hvor sikkerhetssatsingen er sentral, er «nasjonal digital samhandling og tjenesteutvikling, fellesløsninger og felles arkitekturer, skal etableres i et helhetlig og overordnet styrt og koordinert

økosystem». Sikkerhetssatsingen er helhetlig i sin utforming både fra et styringsperspektiv og teknisk. Det nasjonale forskningsnettet er koblet til internasjonale nett, og systematisk sikkerhetsarbeid er en forutsetning for at samarbeidet internasjonalt kan videreføres.

Gevinstene fra sikkerhetssatsingen vil realiseres av den enkelte virksomhet i universitets- og høgskolesektoren, og fra kunnskapssektoren som helhet. Som en del av arbeidet med revidert samstyringsmodell for sektoren, er gevinstoppfølging av handlingsplanen til vurdering. Handlingsplanen inkluderer sikkerhet som et satsingsområde og Cybersikkerhetssenteret kan bidra til en mer felles og datadrevet gevinstoppfølging for sikkerhet. Det videre arbeidet med gevinstoppfølging kan bli koordinert med samstyringsmodellen.

Selv om sikkerhetssatsingen har lykkes med å etablere en felles og brukerfinansiert tjeneste, er ytterligere finansiering fra rammesettere en forutsetning for videre arbeidet og skalering. Under etableringen av satsingen er trusselbildet nasjonalt og internasjonalt endret, og betydningen av sikkerhet økt. Det pågår blant annet dialog med departementet for å vurdere alternativer og finne løsninger for videre finansiering.

8.6. Hovedpunkter fra ekstern kvalitetssikring

Den eksterne uavhengige kvalitetssikringen (utført av Karabin AS) identifiserte gode leveranser og tilfredsstillende prosjektstyring. Etablering av Cybersikkerhetssenteret allerede halvveis i prosjektperioden vitnet om god gjennomføringskraft i prosjektarbeidet samtidig som det ville danne en viktig plattform for kommende leveranser. Rapporten pekte imidlertid på behovet for å styrke gevinstrealisering, rapportering og kommunikasjon i prosjektene. Karabin pekte også på at oppmerksomheten omkring risikostyring i prosjektene burde ha vært løftet og i større grad inkludert i styringsgruppens behandling. Dette tar vi med oss som læringspunkter.

8.7. Styringsgruppens godkjenning av sluttrapporten

Styringsgruppen har gitt sine innspill gjennom høring av sluttrapporten. Alle styringsgruppens medlemmer, med unntak av Universitetet i Oslo, stiller seg bak sluttrapportens innhold. Vesentlige innspill fra styringsgruppen er innarbeidet i siste versjon av rapporten.

Universitetet i Oslo sin tilbakemelding er at de ikke har kunnskapsgrunnlag til å uttale seg om sluttrapporten, og er uenig i eller ikke tilfreds med teknologivalg, prosjektets styringsdokumenter, organisering, økonomistyring, sporbarhet i prosesser og beslutninger, herunder prismodellen for tjenesten.

For å sikre hensiktsmessig ressursbruk og bidra til et konstruktivt samarbeid fremover, er Styringsgruppen likevel enige om å godkjenne sluttrapporten.

9. VEDLEGG

Vedlegg 1. Tilskuddsbrev 2019 fra Unit

Vedlegg 2. Styringsdokumentasjon for UH Sikkerhetssatsing 2019-2022

Vedlegg 3. Prosjektmandat Analysesenter og Responsmiljø

Vedlegg 4. Prosjektmandat Rådgivningstjenester og Kompetanseheving

Vedlegg 5. Rapport fra ekstern kvalitetssikring (Karabin AS)

Vedlegg 1
Tilskuddsbrev 2019

Statsbudsjettet 2019 kap. 280 post 72 - tilskuddsbrev til UNINETT AS

1. Innledning

På bakgrunn av Stortingets behandling av statsbudsjettet for 2019 sender Unit – Direktoratet for IKT og fellestjenester (Unit) tilskuddsbrev til UNINETT AS (UNINETT). Tilskuddsbrevet følger opp Stortingets budsjettvedtak og forutsetninger. Brevet viser også hvilke vilkår som Unit stiller og som virksomheten aksepterer ved å ta i bruk midlene. Eventuelle endringer eller ytterligere tilskudd blir formidlet gjennom supplerende tilskuddsbrev i løpet av året.

2. Mål for 2019

Kunnskapsdepartementet har fastsatt følgende overordnede mål for tilskuddet til UNINETT over kap. 280 post 51, jf. Prop. 1 S (2018–2019):

UNINETT skal utvikle et landsomfattende datanett og tilby avanserte tjenester for utdanning, forskning, formidling, forvaltning og utdanning, i samspill med internasjonale forskningsnett i Europa og verden ellers.

3. BUDSJETT FOR 2019

Stortinget har vedtatt statsbudsjettet for 2019, jf. Innst. 12 S (2018–2019) og Prop. 1 S (2018–2019). Midlene omtalt nedenfor tildeles med dette til UNINETT AS. Midlene utbetales til UNINETTs arbeidskonto 4200 40 67953.

3.1 Budsjettvedtak kap. 280 post 72

Unit gir med dette tilsagn om 26 345 000 kroner i driftstilskudd til UNINETT for 2019.

3.2 Budsjettvedtak kap. 280 post 01

Unit gir med dette også tilsagn om 12 500 000 kroner for gjennomføring av et prosjekt for informasjonssikkerhet i universitets- og høyskolesektoren til UNINETT for 2019. Dette er i utgangspunktet et fireårig prosjekt.

3.3 Vilkår for disponering av tilskuddet

Den primære målgruppen for aktiviteten til UNINETT skal være universiteter, høyskoler og forskningsinstitusjoner. Selskapet kan tilby tjenester til andre institusjoner og brukere dersom alternative leverandører ikke finnes, og det er til nytte for den primære målgruppen.

Forskningsnettet, som UNINETT tilbyr sine målgrupper, er knyttet sammen med andre akademiske forskningsnett over hele verden. UNINETT skal tilby kostnadseffektive kommunikasjonstjenester av minst like høy kvalitet som andre tilbydere i det internasjonale akademiske miljøet. Videre skal UNINETT bidra til å fremme forskning innenfor sitt område og delta i samarbeid med nasjonale og internasjonale nettoperatører der dette kan være aktuelt.

Målet skal være at UNINETT tilbyr et forskningsnett som muliggjør minst 1 gigabit fram til den enkelte arbeidsplass, og 10 gigabitkapasitet til miljøer med ekstra behov. Tilskuddet skal videre bidra til selskapets arbeid for å fremme bruk av åpne internasjonale standarder innenfor datakommunikasjon for å øke muligheten for akademisk samhandling på tvers av landegrensene.

UNINETT skal sørge for samtrafikk mellom nasjonale og internasjonale tjenesteoperatører som er aktuelle for den primære målgruppen. Selskapet skal tilby operative nettjenester primært til forsknings- og høyere utdanningsinstitusjoner for å nå målene, og skal kunne gjøre dette i egen regi. Der hvor aktuelle nettjenester kan skaffes til lavere kostnader fra kommersielle underleverandører, skal normalt slike benyttes. I motsatt fall kan UNINETT selv tilby tjenester. En tilstrekkelig andel av tilskuddet skal brukes til investeringer, ny funksjonalitet og ekstra kapasitet i forskningsnettet. Nyinvesteringene skal være forankret i den nasjonale porteføljestyringen og handlingsplanen for realisering av Kunnskapsdepartementets digitaliseringsstrategi.

UNINETT skal satse på infrastruktur, mellomvare og data samt overvåking av nett og tjenester, herunder informasjonssikkerhet. UNINETT skal bistå Unit med faglige utredninger og rådgivning innen sine fagområder.

Deler av tilskuddet til UNINETT kan brukes til utviklingsprosjekter utover forskningsnettet som skal være forankret i den nasjonale porteføljestyringen og handlingsplanen for realisering av Kunnskapsdepartementets digitaliseringsstrategi. Et allerede identifisert utviklingsprosjekt er at UNINETT,i samarbeide med sektoren og Unit, skal etablere et felles produkt for identitets- og tilgangsstyring (IAM). Deltakelse i nasjonale og internasjonale utviklingsprosjekter skal sikre at målgruppen på sikt fortsatt kan tilbys høy internasjonal kvalitet.

Kunnskapsdepartementet har i digitaliseringsstrategien for universitets- og høyskolesektoren lagt vekt på at universitetene og høyskolene har et bevisst forhold til informasjonssikkerheten som en kritisk suksessfaktor. Departementet har lagt til grunn at institusjonene i arbeidet med digitalisering har en egen interesse i å ha bedre informasjonssikkerhet enn de nasjonale minstekravene. Kunnskapsdepartementet gir tilsagn om 17,5 mill. kroner til Unit for en årlig satsing innen informasjonssikkerhet i universitets- og høyskolesektoren. Av disse gis tilsagn om 12,5 mill. kroner til Uninett og et prosjekt for styrket informasjonssikkerhet og etablering av sektorens analysesenter for cybersikkerhet. Målsettingen er blant annet å forbedre evnen til å forebygge, oppdage og håndtere trusler, og inkludere tiltak som bedre analyseverktøy, tilbud om rådgivingstjenester og kompetanseheving. UNINETT skal i samarbeid med sektoren etablere et prosjekt for å realisere målene, med deltagelse fra informasjonssikkerhetsmiljøene på Gjøvik (NTNU) og USIT ved UiO. Unit vil på oppdrag fra Kunnskapsdepartementet styrke styringen av informasjonssikkerhet i sektoren gjennom å etablere roller i tråd med beskrivelsene i rammeverket ISO/IEC 27014:2013[1]. De øvrige 5 mill. kroner skal finansiere etablering og forvaltning av disse oppgavene og rollene i Unit. UNINETT kan få tildelt enkelte oppgaver knyttet til operasjonalisering av oppgavene i dette rammeverket. UNINETT CERT skal ivareta oppgaven med å være et sektorvist responsmiljø slik dette er beskrevet i rammeverket og det skal utarbeides en arbeidsdeling og et løpende samarbeid mellom Unit og UNINETT i håndteringen av IKT-sikkerhetshendelser. Arbeidet med gjennomføringen av rammeverket handler i stor grad om å koordinere og forbedre sektorens etablerte rutiner og kapasitet for hendelseshåndtering samt å sette dette inn i en større nasjonal sammenheng.

Tilskuddene tildeles UNINETT og skal ikke overføres videre til datterselskaper.

Unit forutsetter at selskapet driver kostnadseffektivt og har kostnadsbasert prising av tjenestene. Unit forutsetter at det er en god intern kontroll i virksomheten, herunder intern kontroll knyttet til informasjonssikkerhet.

[1] ISO/IEC 27014:2013: Information technology — Security techniques — Governance of information security. Dette er en standard på overordnet nivå som beskriver anbefalte konsepter, prinsipper og prosessser for styring av informasjonssikkerhet.

3.4 Kontroll

Unit og Riksrevisjonen kan kontrollere at midlene blir brukt etter forutsetningene, jf. bevilgningsreglementet § 10 annet ledd og lov om Riksrevisjonen § 12. Unit kan kreve tilskuddet helt eller delvis tilbakebetalt dersom det ikke benyttes i samsvar med forutsetningene.

4. RAPPORTERING

UNINETT skal **innen 01. mars 2019** sende Unit en rapport om bruken av de tildelte midlene, resultater og måloppnåelse for 2018. Rapporten skal inneholde omtale av aktivitetene UNINETT har gjennomført, og av kvaliteten til leverte tjenester. Det skal også gis en omtale av selskapets økonomi, herunder en oversikt over eventuelle større investeringer. Det skal videre bekreftes at tilskuddet er benyttet i samsvar med forutsetningene i tilskuddsbrevet.

Økonomirapportering skal skje i samsvar med bestemmelsene i regnskapsloven og god regnskapsskikk. Årsregnskap og styrets årsberetning for 2018 skal sendes Unit innen **15. april 2019**.

Rapport, årsregnskap og årsberetning sendes til postmottak@unit.no.

5. SØKNAD OM STATSTILSKUDD for 2020

UNINETT må innen **20. oktober 2019** sende Unit en søknad om behov for statstilskudd i 2021. Foreløpig budsjett for 2020 skal legges ved søknaden. For søknad om tilskudd til særskilte tiltak må det gis en kort redegjørelse og begrunnelse, og kostnadene må tallfestes. Søknaden sendes til postmottak@unit.no.

Med hilsen

Roar Olsen
direktør

Agnete Sidselrud
seksjonssjef

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer

Kopi

Kunnskapsdepartementet

Riksrevisjonen

Vedlegg 2

STYRINGSDOKUMENTASJON FOR UH SIKKERHETSSATSNING 2019-2022

STYRINGSDOKUMENTASJON FOR UH SIKKERHETSSATSNING 2019-2022

Programleder Anders Lund, Uninett	Programeier Sigurd Eriksson, Unit

ENDRINGSLOGG

Versjon	Dato	Endring	Produsent	Godkjent
0.1	15.03.2019	Første versjon opprettet	Anders Lund	
0.8	22.03.2019	Ferdig utkast	Anders Lund	
1.0	25.04.2019	Oppdatert med siste deltakerliste i Programstyre	Anders Lund	Digitaliseringsstyre/Programstyre

Innhold

1. INNLEDNING

Programmet «UH Sikkerhetssatsning 2019-2022» skal gå over fire år. I forkant av etableringen har nivået på informasjonssikkerhet i universitets- og høyskolesektoren vært et diskusjonstema mellom Kunnskapsdepartementet, Uninett og sektoren. Det har også blitt gjennomført en ekstern vurdering av arbeidet med informasjonssikkerhet i Uninett, knyttet til Uninett CERT, Sekretariatet for informasjonssikkerhet og Forskningsnettet. I 2017 publiserte departementet «Digitaliseringsstrategien for universitets- og høyskolesektoren 2017-2021» og i 2018 ble Unit opprettet. Dette konkretiserte arbeidet og en sentral finansiering for perioden kom på plass.

Digitaliseringsstrategien for universitets- og høyskolesektoren 2017-2021 inneholder følgende tiltak:

> ***5.4.10 En målrettet styrking av informasjonssikkerheten***
> *Kunnskapsdepartementet har overordnet ansvar for informasjonssikkerheten i UH-sektoren og vil fortsette å stille tydelige krav til institusjonene, og følge opp disse kravene gjennom styring og tilsyn. Disse kravene bygger på nasjonale regler og føringer og må forstås som minstekrav til informasjonssikkerhet. Departementet legger vekt på at UH-institusjonene har et bevisst forhold til informasjonssikkerheten som en kritisk suksessfaktor for egne digitaliseringsstrategier og strategiske satsinger. Universitetene og høyskolene er kunnskapsvirksomheter hvor forvaltning og foredling av informasjon/data er en del av kjernevirksomheten. Å videreutvikle denne kjernevirksomheten gjennom en strategisk satsing på digitalisering innebærer også at institusjonene må ha et aktivt forhold til styringen av informasjonssikkerheten, og ha en egen strategisk interesse i å løfte denne høyere enn de nasjonale minstekravene.*

I Prop. 1 S (statsbudsjettet) for budsjettåret 2019 er det satt av 17,5 millioner for å gi dette tiltaket konkret innhold:

> *Regjeringa foreslår 17,5 mill. kroner til eit program for informasjonstryggleik i universitets- og høgskolesektoren. Evalueringar har peikt på veikskapar ved tryggleiken i forskingsnettet og utfordringar med å få på plass tilstrekkeleg styring av informasjonstryggleiken i sektoren.*

Midlene er forslått gitt til Unit, men det er påpekt at disse midlene også kan anvendes til å gi Uninett tilskudd. Noe mer detaljering rundt forventet innhold i prosjektet er gitt i kap. 281 post 01:

> *Kunnskapsdepartementet foreslår å løyve 17,5 mill. kroner årleg til UNIT til eit program for informasjonstryggleik i universitets- og høgskolesektoren. Dette er i utgangspunktet eit fireårig program. Programmet skal mellom anna forbetre evna til å førebygge, oppdage og handtere truslar mot forskingsnettet, og inkludere tiltak som betre analyseverktøy og kompetanseheving.*

Unit er nå ansvarlig for eierstyringen av Uninett, og har gjennom tildelingsbrev for 2019 satt rammer for Uninetts del av programmet:

> *Kunnskapsdepartementet har i digitaliseringsstrategien for universitets- og høyskolesektoren lagt vekt på at universitetene og høyskolene har et bevisst forhold til informasjonssikkerheten som en kritisk suksessfaktor. Departementet har lagt til grunn at institusjonene i arbeidet med digitalisering har en egen interesse i å ha bedre informasjonssikkerhet enn de nasjonale minstekravene. Kunnskapsdepartementet gir tilsagn om 17,5 mill. kroner til Unit for en årlig satsing innen informasjonssikkerhet i universitets- og høyskolesektoren. Av disse gis tilsagn om 12,5 mill. kroner til Uninett og et prosjekt for styrket informasjonssikkerhet og etablering av sektorens analysesenter for cybersikkerhet. Målsettingen er blant annet å forbedre evnen til å forebygge, oppdage og håndtere trusler, og inkludere tiltak som bedre analyseverktøy, tilbud om rådgivingstjenester og*

kompetanseheving. UNINETT skal i samarbeid med sektoren etablere et prosjekt for å realisere målene, med deltagelse fra informasjonssikkerhetsmiljøene på Gjøvik (NTNU) og USIT ved UiO. Unit vil på oppdrag fra Kunnskapsdepartementet styrke styringen av informasjonssikkerhet i sektoren gjennom å etablere roller i tråd med beskrivelsene i rammeverket ISO/IEC 27014:2013. De øvrige 5 mill. kroner skal finansiere etablering og forvaltning av disse oppgavene og rollene i Unit. UNINETT kan få tildelt enkelte oppgaver knyttet til operasjonalisering av oppgavene i dette rammeverket. UNINETT CERT skal ivareta oppgaven med å være et sektorvist responsmiljø slik dette er beskrevet i rammeverket og det skal utarbeides en arbeidsdeling og et løpende samarbeid mellom Unit og UNINETT i håndteringen av IKT-sikkerhetshendelser. Arbeidet med gjennomføringen av rammeverket handler i stor grad om å koordinere og forbedre sektorens etablerte rutiner og kapasitet for hendelseshåndtering samt å sette dette inn i en større nasjonal sammenheng.

2. MÅL

I forarbeid, fram til satsningen ble vedtatt av departementet, er det pekt på flere områder som bør inngå i et program for økt satsning på informasjonssikkerhet i UH-sektoren. Dette har også vært drøftet og forankret i «Fagutvalg for informasjonssikkerhet», samt i «Prioriteringsrådet for nett og nettnære tjenester». Prop. 1S og tildelingsbrev støtter opp under disse forslagene, og i dette framkommer flere målsetninger med programmet.

Sektoren skal totalt sett forbedre sin evne til å forebygge, oppdage og håndtere trusler, og styringen med informasjonssikkerheten i sektoren skal under bedre kontroll. Dette skal samordnes bedre og gjøres mer helhetlig, og settes inn i en større nasjonal sammenheng. Den totale effekten av dette er at arbeidet med informasjonssikkerhet i sektoren skal opp på et bedre nivå enn de nasjonale minstekravene.

Tydeliggjøring av ansvar og roller vil også inngå som et mål med programmet. Gjennom implementering av styringsmodellen vil det utarbeides arbeidsdeling og et løpende samarbeid mellom Unit og Uninett i håndteringen av IKT-sikkerhetshendelser.

3. LEVERANSER

Programmet vil gruppere arbeidet i tre hovedområder:

1. Ny styringsmodell for informasjonssikkerhet og personvern
2. Analysesenter og responsmiljø
3. Rådgivingstjenester og kompetanseheving

Ny styringsmodell for informasjonssikkerhet og personvern (Ansvarlig: Unit)
Denne delen av programmet vil implementere en styringsmodell for informasjonssikkerhet i sektoren, basert på rammeverket ISO/IEC 27014:2013. Gjennom dette arbeidet vil det også etableres en forvaltning av en slik styringsmodell, med tilhørende overordnet rapportering til Kunnskapsdepartementet.

Analysesenter og responsmiljø (Ansvarlig: Uninett)
Deteksjons- og analysekapasitet skal forbedres, og det skal etableres et helhetlig og felles analysesenter for cybersikkerhet i sektoren. Uninett skal ivareta rollen som sektorvist responsmiljø, i tråd med NSMs «Rammeverk for håndtering av IKT-sikkerhetshendelser», og forbedre sektorens evne til å håndtere trusler. Både gjennom bedre tilrettelegging og organisering.

Rådgivingstjenester og kompetanseheving (Ansvarlig: Uninett)
Programmet skal etablere rådgivingstjenester for implementering og helhetlig praktisering av etablerte ledelsessystem for informasjonssikkerhet, samt etablere et program for heving av kompetanse innenfor informasjonssikkerhet og personvern for lederen, forskeren, studenten og øvrige ansatte.

4. RAMMEBETINGELSER

Digitaliseringsstrategien for universitets- og høyskolesektoren 2017-2021 er tydelig på behovet for en målrettet styrking av informasjonssikkerheten i UH-sektoren, og føringer for gjennomføring er gitt gjennom tildelingsbrev til Unit og Uninett. Rammene for innholdet er også satt av «Fagutvalg for informasjonssikkerhet» og nedfelt i foreslått handlingsplan som går til Digitaliseringsstyret for godkjenning.

Gjennom tildelingsbrev fra Kunnskapsdepartementet til Unit, og videre i tildelingsbrev fra Unit til Uninett, kan programmet få styringssignaler. I etableringen tas det utgangspunkt i at programmet vil ha en årlig ramme på 17,5 millioner, med varighet fire år, fastlagt i årets tildelingsbrev.

Programmet eies av Unit, med programledelse hos Uninett.

I de delene av programmet hvor Uninett har ansvar er det pekt på at gjennomføring skal skje med deltagelse fra informasjonssikkerhetsmiljøene på Gjøvik (NTNU) og USIT ved UiO.

5. AVGRENSNINGER OG AVHENGIGHETER

I oppstart av programmet er det naturlig å vektlegge prosjektene «Ny styringsmodell» og «Analysesenter og responsmiljø». Det vil gjennom arbeid med implementasjon av styringsmodell i Unit bli en tydeliggjøring av roller og ansvar, som vil være med på avgrensning av omfang. Kartlegging og rapportering i dette arbeidet vil også være viktig innspill når prioritering og mer målrettet rådgivingstjenester og kompetanseheving i sektoren skal etableres.

Programmet kan ikke ta ansvar for gjennomføring av oppgaver som virksomhetene selv er juridisk ansvarlige for, men programmet skal i størst mulig grad tilby målrettede tjenester som gir gevinster og tilrettelegge i større grad for at virksomhetene kan bedre utføre oppgaver de er ansvarlige for.

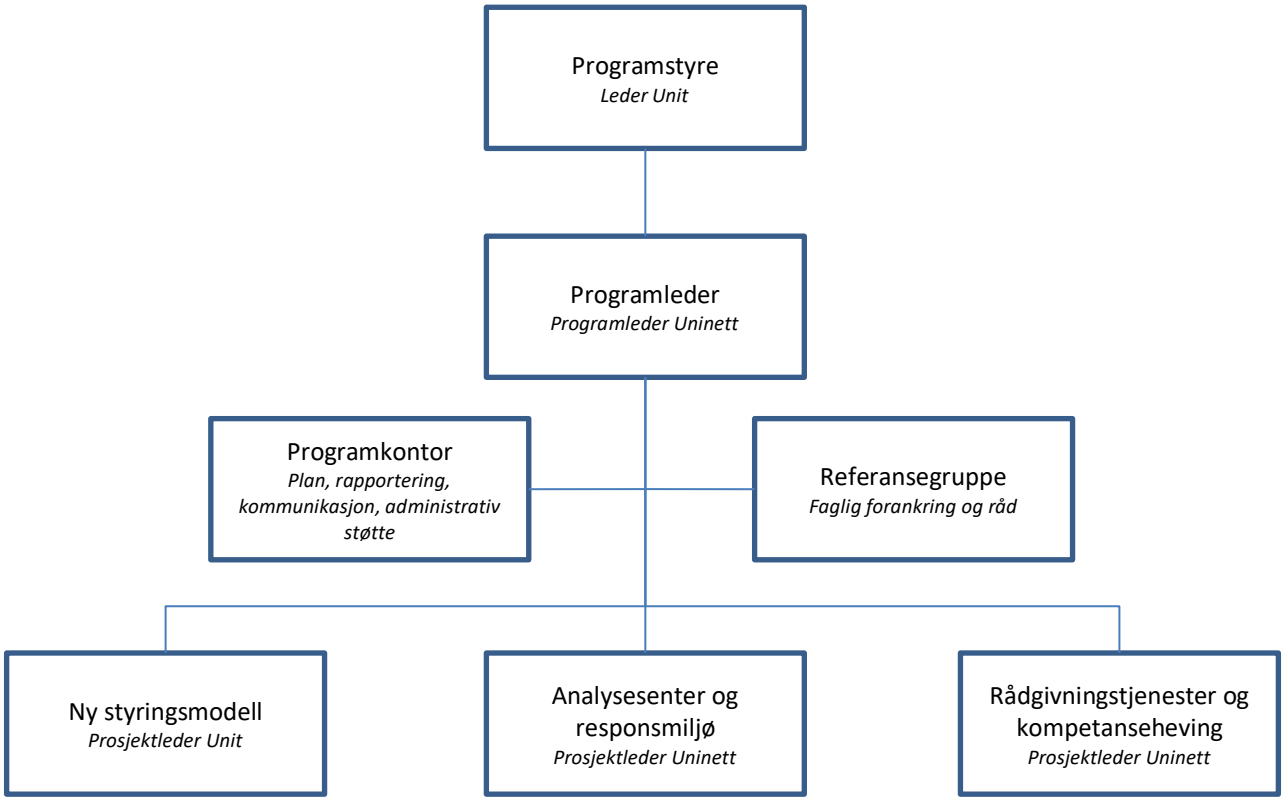
6. INTERESSENTER

Gjennomføringen av programmet skal skje i tråd med de føringene som er gitt gjennom tildelingsbrev fra Kunnskapsdepartementet, og videre i tildelingsbrev til Uninett fra Unit. Disse gir målsetninger for programmet hvor hele universitets- og høyskolesektoren er involvert, og mer spesifikt pekes det på et samarbeid med UiO og NTNU. Forankring i sektoren er viktig, både på innhold og faktisk gevinstrealisering. Deltakelse i programstyre og framtidig referansegruppe (eller flere referansegrupper om dette er hensiktsmessig) må gjenspeile dette, samtidig er det viktig å bygge på allerede eksisterende fora i sektoren:

- **Fagutvalg for informasjonssikkerhet**
  Inngår i den strategiske styringsmodellen Unit har etablert i sektoren, og skal bidra til brukermedvirkning.
- **Prioriteringsråd for nett og nettnære tjenester**
  Etablert av Uninett for å sikre brukermedvirkning på tjenesteporteføljen Uninett har.
- **UH-IT**
  Samarbeidsorgan mellom de største institusjonene i sektoren rundt IT (IT-ledere).

God kommunikasjon rundt programmet er en viktig premiss for å realisere målene. Det vil derfor være nødvendig å sette av egne ressurser til et slikt arbeid, og i den sammenhengen utarbeide mer detaljerte planer og strategi for en helhetlig kommunikasjon.

7. ORGANISERING, ROLLER OG ANSVAR



Programstyre består av:

- Sigurd Eriksson, Ass. direktør og Avdelingsdirektør i Unit (Programeier, Leder programstyre)
- Tom Røtting, Adm. direktør i Uninett
- Lars Oftedal, IT-direktør ved UiO
- Håkon Alstad, IT-sjef ved NTNU
- Jostein Jensen, Direktør for sikkerhet ved NHN
- Lars Atle Holm, Direktør ved NMBU
- Anette Thorkildsen Osaland, CISO ved UiA
- Hildegunn Vada, Avdelingsdirektør ved Uninett

8. PROGRAMMETS USIKKERHETER

På et overordnet nivå i programmet er det et sett med risikoer som kan bidra til usikkerhet. Tabellen nedenfor viser noen slike, men det vil gjennom prosjektene i programmet ytterligere tydeliggjøres risikomatriser som er mer spesifikke.

Risiko	Håndtering av risiko
Ressurspersoner nedprioriterer oppgaver i programmet til fordel for daglige operative gjøremål.	Programstyre med eierskap til ressursuttak, samt tydelige bestillinger rundt omfang av oppgaver. Anvendelse av markedet for innleie.
Manglende utbredelse av leveranser gjennom programmet.	God kommunikasjon og informasjon rundt nye tjenester. God forankring i sektoren for arbeidet som gjøres. Synliggjøring av gevinster av fellesløsninger, i samarbeid med premissleverandører.
Organisering som program kan hindre en smidig utviklings- og leveransemodell.	Programstyret har kontinuerlig bevissthet rundt dette og legger til rette for og anerkjenner prototyping, MVP (Minimum Viable Product) og Design Thinking som metodikk.

Manglende enighet og forankring blant interessenter fører til forsinkelser og begrensninger	Programstyre med beslutningsmyndighet. Bruke nyopprettede styringsmodeller (på utsiden av programmet) for eventuelle beslutninger som krever dette.
Forsinkede leveranser i deler av programmet påvirker leveranser i andre prosjekter.	Identifisere og fokusere på avhengigheter i og utenfor programmet, tydeliggjøre roller og ansvar i programmet og eksterne leveranser.
Programmet blir for fragmentert og gir for utydelig helhetsverdi for sektoren.	Utarbeide veikart/handlingsplan som omhander hele programmet. Forankre innholdet hos viktige interessenter.

9. TIDSPLAN OG MILEPÆLER

Programmet vil basere seg på en mest mulig smidig gjennomføring, med fokus på kontinuerlige leveranser og realisering av tjenester/innhold som gir merverdi for sektoren. Dette betyr at planlegging og innhold for leveranser vil ha et fokus på kort og mellomlang tidshorisont. Prosjektene i programmet vil detaljere dette mer, mens overordnet i programmet vil en hovedleveranse være et veikart/handlingsplan (sommeren 2019) for programmets periode. Denne må kunne revideres jevnlig, i tråd med føringer gitt av Programstyre og de styringssignaler som gis av departementet og Unit gjennom tildelingsbrev.

10. BUDSJETT OG FINANSIERING

Programmets finansiering er å anse som investeringsmidler for å forbedre håndtering og kontroll med informasjonssikkerheten i sektoren. Investeringen er årlig på 17,5 millioner. Totalt 70 millioner over fire år. Arbeidet med ny styringsmodell for informasjonssikkerhet og personvern vil basere seg på omlag 28,5% av disse investeringsmidlene, mens det resterende vil gå til arbeidet med analysesenter, respons, rådgiving og kompetanseheving. Her kan eventuelt departementet og/eller Unit komme med endrede styringssignaler, men dette er rammene som er gitt i utgangspunktet.

I programmet er det viktig å forsøke å holde de administrative kostnadene nede, samtidig som disse i størst mulig grad holdes innenfor de prosjektene hvor de tilhører. På en slik måte at administrasjon av selve programmet holdes nede på et minimum og størst mulig effekt av investeringene går til gevinstrealisering.

Gjennom programmet må de enkelte prosjektene utarbeide betalingsmodeller og finansieringsmodeller for den løpende håndteringen av tjenester og leveranser som etableres.

11. STRATEGI FOR GJENNOMFØRING

I programmet er det, som tidligere nevnt, naturlig å fokusere på «ny styringsmodell» og «analyse og respons» i oppstart av programmet. Dette har også vært avklart med sektoren, både i Fagutvalg for informasjonssikkerhet og i Prioriteringsråd for nett og nettnære systemer. Denne typen forankring er viktig i gjennomføringen av programmet, og for gevinstrealiseringens del en nødvendighet.

For konkrete arbeidsoppgaver og milepæler i programmets prosjekter må det tas stilling til:

- Anvendelse av markedet, som i endel sammenhenger kan gi hurtigere leveranser og bedre håndtere svingninger i etterspørsel
- Forsøke å bygge på sektorens samlede kompetanse ved gjennomføring
- Se til internasjonalt og nasjonalt samarbeid for å finne synergier, gjenbruk av løsninger og erfaringer
- Ved gjennomføring vurdere hva det er viktig å bygge internt i sektoren av kapasitet, og dermed hvilken kjernekompetanse sektoren selv bør besitte opp mot markedsleveranser

Programmets forskjellige prosjekter må tilrettelegge for at leveranser kan utvikles og leveres på en smidig måte. Det er viktig med en kontinuerlig leveransemodell, hvor fortløpende forbedringer kan

inngå. Gjennom å tilrettelegge for smidige leveranser, der Design Thinking, prototyping og MVP er viktige bærebjelker, vil man treffe brukerbehovene på best mulig måte, samtidig som programmet leverer kontinuerlig verdi.

12. KRITISKE SUKSESSFAKTORER

Programmet er forventet å heve nivået på arbeidet med informasjonssikkerhet i sektoren. Det vil derfor være en forutsetning at programmet løpende leverer konkrete verdiøkende tjenester til sektoren og at disse får en utbredelse i sektoren. Et slikt samspill krever god informasjon og kommunikasjon rundt leveransene i programmet, samt god brukermedvirkning og forankring.

Tidligere erfaring tyder på at sektoren har et varierende nivå på arbeidet med informasjonssikkerhet. Det vil i programmet være viktig å løfte de som er på et lavt nivå, samtidig som de institusjonene som i dag allerede har et sterkt fokus på slikt arbeid opplever at programmet bidrar til merverdi.

Visjonen er at arbeidet med informasjonssikkerhet i sektoren skal opp på et bedre nivå enn de nasjonale minstekravene. Konkretisering av minstekrav, og bedre indikatorer som kan tydeliggjøre at sektoren er på riktig vei, vil kunne bidra til dette.

Vedlegg 3

Prosjektmandat

Analysesenter og responsmiljø

PROSJEKTMANDAT FOR

PROSJEKTET «ANALYSESENTER OG RESPONSMILJØ»

INNENFOR PROGRAMMET
«UH SIKKERHETSSATSING 2019-2022»

UNINETT PROSJEKTNUMMER: U1210017

Programleder Anders Lund, Uninett	Programeier Sigurd Eriksson, Unit

Prosjektleder Maria Luces, Uninett	Prosjekteier Tom Røtting, Uninett

ENDRINGSLOGG

Versjon	Dato	Endring	Produsent	Godkjent
0.1	10.04.19	Første versjon opprettet	AL	
0.2	14.05.19	Første utkast	AL, ML, LES	
0.8	24.05.19	Andre utkast	AL, ML, LES	
1.0	17.06.19	Siste versjon – vedtatt i programstyret	AL, ML, LES	Programstyre

1. BAKGRUNN

Prosjektet «Analysesenter og responsmiljø» er organisert som et prosjekt under det fireårige programmet «UH Sikkerhetssatsing 2019-2022», tildelt av Kunnskapsdepartement (KD) til Unit[1]. Sikkerhetssatsingen er tiltak med bakgrunn i «Digitaliseringsstrategien for UH-sektoren 2017-2021». Mandatet for programmet[2] er forankret og vedtatt i Digitaliseringsstyret. Overordnet mål for programmet er å forbedre sektorens evne til å forebygge, oppdage og håndtere trusler og iverksette tiltak som skal forbedre analyseverktøy, rådgivningstjenester og kompetanseheving innen informasjonssikkerhet og personvern.

Uninett har fått tildelt midler fra Unit for å lede arbeidet, i tett samarbeid med sektoren, for å realisere målene, og bidra til å styrke informasjonssikkerhet.

Frem til sikkerhetssatsingen ble vedtatt av KD ble det diskutert flere områder som burde inngå i et arbeid for forbedret informasjonssikkerhet i UH-sektoren. Flere av områdene er drøftet og forankret i «Fagutvalg for informasjonssikkerhet» og i «Prioriteringsrådet for nett og nettnære tjenester»:

- Helhetlig og felles deteksjons- og analysekapasitet.
- Forbedret evne til å håndtere sikkerhetstrusler i sektoren i tråd med NSMs rammeverk for hendelseshåndtering.
- Rådgivningstjenester innenfor informasjonssikkerhet til sektoren.
- Kompetanseheving innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og andre brukere i sektoren.

Dette har ledet frem til at den nevnte Sikkerhetssatsingen organiseres som et program med tre hovedprosjekter:

1. Ny styringsmodell for informasjonssikkerhet og personvern
2. Analysesenter og responsmiljø
3. Rådgivingstjenester og kompetanseheving

Dette dokumentet beskriver mandatet for prosjektet «Analysesenter og responsmiljø».

1 Tildelingsbrev fra Kunnskapsdepartement til Unit_ref.nr. 18/4768, datert 19.12.18
2 Programmandat – Styringsdokumentasjon for UH sikkerhetssatsing 2019-2022 (styrevedtatt i Digitaliseringsstyret - 11.04.19, Oslo)

2. MÅL, HOVEDINNHOLD OG FORVENTEDE RESULTATER

Prosjektet "Analysesenter og responsmiljø" skal:

1. Forbedre deteksjons-, analyse- og responskapasiteten i UH-sektoren.

2. Etablere sektorens analysesenter for cybersikkerhet (teknisk tilrettelegging og støtteverktøy, bemanning, organisasjonsutvikling, rutiner, etc.), i tett samarbeid med sektorens etablerte sikkerhetsmiljøer.

3. Forbedre sektorens evne til å håndtere trusler.

4. Utvikle og innføre felles sikkerhetstjenester for sektoren, innen deteksjon, analyse og respons. Tjenestene må sikre bærekraftige finansieringsmodeller som gir tilstrekkelige ressurser, også etter at satsingen er over.

Arbeidet i prosjektet skal utføres i tett samarbeid med sektoren, og med konkret deltagelse fra informasjonssikkerhetsmiljøene på NTNU og UiO. Prosjektet skal ha fokus på kontinuerlige og smidige leveranser, hyppige delleveranser av nye og forbedrede sikkerhetstjenester.

Uninett, som sektorCERT og ansvarlig for forskningsnettet og andre fellestjenester i UH-sektoren, har et særskilt ansvar for å ha gode systemer og rutiner for egen beredskap rundt deteksjon og analyse av IKT-hendelser. Dette påpekes i strategier, rammeverk og retningslinjer fra blant annet regjeringen og NSM, og inngår også som beste praksis i generelt sikkerhetsarbeid.

I samarbeid med NTNU og UiO vil prosjektet i 2019 starte etableringen av en sentral plattform for håndtering av data til analyseformål. God samhandling mellom den sentrale plattformen og allerede eksisterende analysekapasitet ved UiO og NTNU vil være en viktig suksessfaktor for etableringen av et felles analysesenter for cybersikkerhet som kommer alle institusjoner i sektoren til gode.

Prosjektet skal der det er mulig og hensiktsmessig benytte eksisterende verktøy og infrastruktur i utviklingsarbeidet. Prosjektet skal vurdere anvendelse av markedet, som i en del sammenhenger kan gi hurtigere leveranser og bedre håndtere svingninger i etterspørsel.

3. ANGREPSVINKEL OG METODE FOR GJENNOMFØRING – OMFANG AV ARBEIDET

Gjennomføringen av prosjektet «Analysesenter og responsmiljø» skal skje i tråd med de føringene som er gitt gjennom tildelingsbrev fra KD, og videre i tildelingsbrevet fra Unit til Uninett. Prosjektet skal gjennomføres i tett samarbeid mellom Uninett, UiO/USIT og NTNU/Gjøvik.

Prosjektet skal i størst mulig grad benytte bestepraksis-metodikk. Prosjektet planlegger å benytte smidig metodikk og tjenestedesign («design thinking») for utvikling av nye tjenester, for å sikre brukermedvirkning og for å tilføre raskest mulig verdi for kunder og brukere.

Prosjektveiviseren, som er Difis anbefalte prosjektmodell for styring av digitaliseringsprosjekter i offentlige virksomheter, skal brukes som styringsmodell for prosjektet.

I konseptfasen skal prosjektet utarbeide et veikart som viser prioriterte tiltak og aktiviteter for prosjektperioden (2019-2022). Veikartet vil være utgangspunkt for planlegging av arbeidsomfang og ressursbehov i prosjektet.

Unit har nylig foretatt en risiko- og tilstandsvurdering for sektoren på oppdrag fra KD. Denne, og tilsvarende trusselvurderinger i sektoren, vil kunne gi relevante innspill til etablering av veikartet og prioriteringen av aktivitetene i prosjektet.

4. HOVEDAKTIVITETER OG MILEPÆLSPLAN

4.1. Hovedaktiviteter for første prosjektår (2019)

I 2019 planlegger vi i prosjektet å igangsette følgende aktiviteter:

1. DNS brannmur levert som en fellestjeneste i UH-sektoren, hvor grunnlag for sperringer også inkluderer data levert av NTNU og UiO.
2. Starte etablering av en sentral plattform for håndtering av data til analyseformål.
3. Avklaring av juridisk problemstillinger knyttet til deling av data i sektoren, som grunnlag for etablering av et helhetlig og felles deteksjons- og analysesenter.
4. Legge til rette for bedre kommunikasjon mellom de operative sikkerhetsmiljøene i sektoren, slik at dialog kan foregå fortløpende og i sann tid rundt aktuelle hendelser.
5. Distribuering av trusselvurderinger, utarbeidet av NTNU, gjennom sektorens kontaktnett av IRTer (Incident Response Team).

Hovedaktivitet	JAN	FEB	MAR	APR	MAI	JUN	JUL	AUG	SEP	OKT	NOV	DES
DNS brannmur tjeneste - Pilotfase												
DNS brannmur etablert som fellestjeneste												
Utarbeidelse av veikart for prosjektet												
Sektorens trusselvurdering												
Etablere sentral plattform for håndtering av data til analyseformål												
Nytt kommunikasjonsverktøy («Sikker chat») mellom operative sikkerhetsmiljø i sektoren												
Avklaring juridiske ramme for datahåndtering i sektoren												

4.2. Milepæler

Som beskrevet tidligere i dokumentet skal prosjektet benytte smidige metoder for systemutvikling, med vektlegging av fleksibilitet og hyppige delleveranser. Prosjektgruppen er i gang med kartlegging og prioritering av aktivitetene (veikartarbeid).

Milepælsplanen for prosjektet blir etablert etter at arbeidet med veikartet er fullført.

4.3. Konsekvenser for drift og forvaltning

De fleste av tjenestene som prosjektet skal levere krever allokering av tekniske ressurser for både utvikling, drift og vedlikehold. Tjenestene som utvikles i prosjektet overleveres som fellestjenester for sektoren, med egne betalingsmodeller og forvaltning. Denne prosessen kan være tids- og ressurskrevende og bør planlegges inn i tjenesteutviklingen.

En sentral plattform for håndtering av data til analyseformål er en levende plattform under konstant utvikling, med behov for hyppige oppgradering og gode sikrings-, drifts- og vedlikeholdsrutiner. Dette medfører behov for allokering og rekruttering av spisskompetanse for de konkrete arbeidsoppgavene. I tillegg til tekniske ressurser, er det viktig å ha tilgang til juridisk kompetanse for etablering av dekkende og entydige databehandleravtaler mellom partene.

Robuste driftsmiljøer, god rådgivning og organisasjonsutvikling vil være avgjørende for å møte stadige økende krav til sikker drift av viktige sikkerhetstjenester knyttet til myndighetenes strategier for digital sikkerhet.

5. ORGANISERING

Prosjektet er organisert i et kjerneteam bestående av sentrale ressurser fra NTNU, UiO og Uninett.

Prosjektleder rapporterer direkte til programleder for sikkerhetssatsingen.

Prosjektet skal organisere aktiviteter og delleveranser på en hensiktsmessig måte. Team og samarbeidsgrupperinger etableres ut fra behov for ressurser, kompetanse, fremdrift, samhandling.

Tabellen under viser deltakere i kjerneteamet:

Navn	Rolle i prosjektet	Periode	Spesifikke arbeids- og ansvarsområder
Maria Luces - Uninett	Prosjektleder	2019-2022	Prosjekt- og prosessledelse
Rune Sydskjør - Uninett	Fagansvarlig Uninett	2019-2022	
Stian Husemoen – NTNU Seksjonsleder digital sikkerhet	Fagansvarlig NTNU	2019-2022	
Espen Grøndahl - UiO IT Sikkerhetssjef	Fagansvarlig UiO	2019-2022	

Interessentgruppen og andre samarbeidspartnere for programmet er kartlagt gjennom en interessentanalyse.

6. BUDSJETT

6.1. Finansiering

Kunnskapsdepartementet har gitt tilsagn om 17,5 mill. kroner årlig til Unit for etablering og gjennomføring av programmet for økt sikkerhetssatsing i UH-sektoren i fire år. Av disse er det gitt tilsagn om 12,5 mill. kroner til Uninett for å rigge og lede prosjektet som skal implementere de nødvendige tiltak for å styrke informasjonssikkerhet bla etablering av sektorens analysesenter for cybersikkerhet, rådgivingstjenester og kompetanseheving inne informasjonssikkerhet og personvern. De øvrige 5 mill. kroner skal finansiere etablering og forvaltning av oppgavene og rollene i Unit.

12,5 mill. kroner tildelt Uninett fordeles mellom de to prosjektene som Uninett er ansvarlig for; «Analysesenter og responsmiljø» og «Rådgivningstjenester og kompetanseheving».

Prosjekt	**Tilskudd** (MNOK pr år)
Ny styringsmodell (Unit)	**5,0**
Analysesenter og responsmiljø (Uninett)	**12,5**
Rådgivningstjenester og kompetanseheving (Uninett)	
Totalt årlig tilskudd	**17,5**

I tabellen under vises et grovt estimat over foreslått fordeling av tilskuddet mellom prosjektene.

Budsjett	**2019**	**2020**	**2021**	**2022**
Programadministrasjon	1	0,5	0,5	1
Analysesenter og responsmiljø	**10**	**7**	**7**	**7,5**
Rådgivningstjenester og kompetanseheving	1,5	5	5	4
Totalt tilskudd (NMOK)	**12,5**	**12,5**	**12,5**	**12,5**

Et mer detaljert budsjett for prosjektet blir utarbeidet etter at veikartet for prosjektet er skissert ferdig. Prosjektet er basert på smidig metodikk og dermed er kostnadsfordelingen over år og mellom de to prosjektene som Uninett står ansvarlig for basert på et grovt estimat.

6.2. Planlagt forbruk

Prosjektet pådrar seg følgende kostnader:

- Egen ressursinnsats
- Konsulent (programstøtte) og annen innleie
- Reise- og møtekostnader
- Lisenser, hardware og andre direktekostnader

De to første prosjektårene er det estimert et timeforbruk på omtrent 5 årsverk, hvor tekniske ressurser utgjør den største andelen i arbeidet med system- og tjenesteutvikling. Arbeidsinnsatsen fra NTNU og UiO er estimert til 1 årsverk fra hver for hvert av de to første prosjektårene. Arbeidsomfanget og ressursbehovet knyttet til de ulike arbeidspakkene blir definert gjennom arbeidet med veikartet for prosjektet.

7. KRITISKE SUKSESSFAKTORER / RISIKOER

Suksessfaktor	Risikoreduserende tiltak
Konkretisering og riktig prioritering av leveransene i prosjektet i tråd med målsetninger og brukerbehov	Grundig planleggings- og veikartarbeid prioriteres, med involvering av tekniske ressurser hos Uninett og samarbeidspartnere. Veikartet forankres hos prosjektgruppen og godkjennes av Programstyret.
Tilgang på tilstrekkelige ressurser	God ressursplanlegging mht veikartet for leveransene og arbeidsomfang. Sette i gang rekruttering av kompetansen om nødvendig.
Tilfredsstillende fremdrift i prosjektet	God planlegging av delleveranser og aktivitetene som inngår i utviklingsløpet for hver tjeneste. Jevnlig statusrapportering i prosjektet.
Tydelig roller og ansvarfordeling i prosjektet	Tydelig prosjektmandat og styringsdokumentasjon. Sikre felles forståelse blant prosjektdeltakere.
Sikre forankring av prosjektet hos interessentgruppen	Involvering og jevnlig informasjon til premissgivere og andre relevante interessenter.
Tillit og godt samarbeid blant deltakere i prosjektet	Åpen og hensynsfull kommunikasjon. Klare ansvarsforhold og gode rutiner for informasjonsformidling.

8. PROSJEKTSTYRING

Prosjektet rapporterer til Programstyret i forbindelse med styremøtene som er planlagt å avholdes fire ganger per år. Minimums rapportering skal innebære en rapportering på fremdrift, kvalitet og økonomi. Rapportering utover denne minimumsrapportering kan avtales ved behandling av prosjektbeskrivelsen.

Programlederen deltar på styremøtene i tillegg til medlemmene i programstyret, med ansvar for rapportering om status på de tre prosjektene som programmet består i.

Prosjektet skal ha hyppigere rapportering og kontinuerlig dialog med programlederen, minst to ganger i måned.

Prosjektgruppen og samarbeidspartnere skal avtale hyppige status- og arbeidsmøter basert på organisering av arbeidet innen hver arbeidspakke.

Prosjektdokumentene skal lagres på programportalen opprettet på MS Sharepoint hos Uninett. Det benyttes samhandlingsverktøy (O365) der prosjektgruppen får tilgang til relevant prosjektinformasjon.

Vedlegg 4

Prosjektmandat

Rådgivningstjenester og kompetanseheving

PROSJEKTMANDAT FOR

PROSJEKTET «RÅDGIVNINGSTJENESTER OG KOMPETANSEHEVING»

INNENFOR PROGRAMMET «UH SIKKERHETSSATSING 2019-2022»

UNINETT PROSJEKTNUMMER: U1210018

Programleder Anders Lund, Uninett	Programeier Sigurd Eriksson, Unit

Prosjektleder TBA	Prosjekteier Tom Røtting, Uninett

ENDRINGSLOGG

Versjon	Dato	Endring	Produsent	Godkjent
0.1	05.09.19		ML	
0.2	09.09.19	Endringer ifm prosjektomfang	ML	
0.3	22.09.19	Revidert ihht kommentarer fra AL, RSN, TG og ØE	ML	
0.9	23.09.19	Siste justeringer før gjennomgang i Programstyre	ML	AL
0.9.1	03.10.19	Endringer ihht innspill fra Unit	ML, RSN	
0.9.1.1	17.10.19	Tekstlige justeringer under “Relevante tjenester” (pkt. 2 og 3)	RSN	
0.9.2	04.11.19	Endringer etter presentasjon i fagutvalget (okt) og innspill fra SE.	ML, RSN	
1.0	08.11.19	Siste versjon – vedtatt i programstyret	ML, RSN	Programstyre

1. BAKGRUNN

Prosjektet «Rådgivningstjenester og Kompetanseheving» er et av de tre hovedprosjektene definert under programmet «UH Sikkerhetssatsingen 2019-2022». Sikkerhetssatsingen er et tiltak med bakgrunn i «Digitaliseringsstrategien for UH-sektoren 2017-2021» fra Kunnskapsdepartementet (KD)[1].

Midler over statsbudsjettet er tildelt Unit og programmet skal gå over fire år. Av disse har Unit gjort videre tildeling til Uninett for å gjennomføre større deler av programmet. Programmet er organisert i tre hovedprosjekter, hvor Uninett har fått ansvaret for å lede to av dem:

1. Ny styringsmodell for informasjonssikkerhet og personvern (ledes av Unit)
2. Analysesenter og Responsmiljø (ledes av Uninett)
3. Rådgivingstjenester og Kompetanseheving (ledes av Uninett)

Dette dokumentet beskriver mandatet for prosjektet «Rådgivningstjenester og Kompetanseheving». Prosjektet skal utrede og anbefale hvilke tjenester som skal bidra til at institusjonene får mulighet til å bedre nivået på informasjonssikkerhet og personvern. Prosjektet skal videre foreslå en organisering og leveransemodell for hvordan disse tjenestene skal leveres til sektoren.

Mandatet for prosjektet understøttes av hovedanbefalingene som trekkes fram i tilstandsrapporten utgitt av Unit (2019)[2]. Som en del av Sikkerhetssatsingen, gjennomførte Unit kartleggingsmøter med de 21 statlig eide universitetene og høgskolene. Hensikten med kartleggingen er å få oversikt over omfanget av og systematikken i deres arbeid med informasjonssikkerhet og personvern. Rapporten kommer med klare anbefalinger på institusjonsnivå om å prioritere tiltak for kompetanseheving innenfor informasjonssikkerhet i alle virksomhetsområder og etablere en konsulent- og rådgivningstjenester for informasjonssikkerhet og personvern som kan bistå sektoren.

2. MÅL, HOVEDINNHOLD OG FORVENTEDE RESULTATER

Sikkerhetsløftet i kunnskapssektoren skal skje både gjennom forebyggende tiltak, videreutvikling og styrkning av den operative sikkerheten og sikkerhetskulturen generelt i sektoren.

Prosjektet skal etablere rådgivingstjenester for implementering og helhetlig praktisering av etablerte ledelsessystem for informasjonssikkerhet. Det skal etableres nødvendige tiltak for å heve kompetansen innenfor informasjonssikkerhet og personvern for ledere, forskere, studenter og øvrige ansatte.

[1] Tildelingsbrev fra Kunnskapsdepartement til Unit_ref.nr. 18/4768, datert 19.12.18

[2] Unit (2019): Tilstandsvurdering av informasjonssikkerhet og personvern blant de statlig eide universitetene og høgskolene

Prosjektet skal ta for seg organisering, mulighetsrom og utfordringer knyttet til sikkerhetsrådgivning i sektoren.

Prosjektet «Rådgivningstjenester og Kompetanseheving» skal konkret:

1. Etablere en fellesfunksjon i sektoren med ansvar for overordnet koordinering av rådgivningstjenester, og som bistår sektoren innen informasjonssikkerhet og personvern.
2. Kartlegge eksisterende kompetanse som kan tilgjengeliggjøres i sektoren og identifisere eksisterende tiltak for kompetanseheving som det kan være hensiktsmessig å bygge videre på. Dette skal bygge videre på allerede gjennomført kartleggingsarbeid i sektoren, for eksempel gjennomført risikovurdering (tilstandsrapporten, se under).
3. Iverksette nye tiltak for å heve kompetanse på institusjonsnivå innen informasjonssikkerhet og personvern i tråd med kartleggingen.
4. Vurdere hensiktsmessige samhandlingsarenaer for å skape forankring, brukerinvolvering, drøfting av løsninger, etc.
5. Vurdere hvordan prosjektet best mulig kan hjelpe institusjonene i arbeidet med kultur- og holdningsskapende arbeid innenfor informasjonssikkerhet og personvern

Prosjektet skal totalt sett bidra til å oppnå hovedmålet med programmet - å forbedre sektorens evne til å forebygge, oppdage og håndtere sikkerhetstrusler. Prosjektet skal i lag med de andre to prosjektene i satsingen bidra til å løfte informasjonssikkerheten i sektoren på et høyere nivå enn de nasjonale minstekravene.

Prosjektet vil benytte tilstands- og risikovurderingen som leveres av Unit hvert år for å gjøre justeringer på hvilke tjenester som bør prioriteres.

3. ANGREPSVINKEL OG METODE FOR GJENNOMFØRING – OMFANG AV ARBEIDET

Prosjektet skal i størst mulig grad benytte bestepraksis-metodikk. Prosjektet skal benytte smidig metodikk og tjenestedesign («design thinking») for utvikling av nye rådgivningstjenester og tiltak for kompetanseheving. Konkrete leveranser i prosjektet løftes etter hvert ut av programmet. Dette krever at prosjektet etablerer bærekraftige betalingsmodeller som sikrer at disse tjenester kan være selvbærende.
Pilotering og mest mulig kundeinvolvering skal benyttes.

Begge prosjektene ledet av Uninett gjennomføres i samarbeid med sikkerhetsmiljøene fra NTNU og UiO. Prosjektene skal samkjøres hvor det er hensiktsmessig, for å dra mest mulig nytte av synergien som finnes i arbeidet med utvikling av nye fellestjenester innen informasjonssikkerhet, rådgivning og kompetanseheving. Unit vil delta i prosjektet for å koordinere og sikre at behovene som er identifisert blir dekket i anbefalte løsninger, og vurdere hvordan de ulike miljøene best kan benyttes for å dekke behovene for rådgivningstjenester.

I tillegg til erfaringer fra tilstands- og risikovurderingen fra Unit skal man også gjennom prosjektet «Analysesenter og Responsmiljø» identifisere behov for tiltak innen kompetanseheving og rådgivningstjenester.

Arbeidet med kartlegging av rådgivningstjenester og tiltak for kompetanseheving vil falle inn under to fagområder:

- Operativ IKT[3]-sikkerhet og IRT[4] relatert (teknisk og operativ orientert)
  Målgruppe: Sikkerhetsmiljø/responsteam (IRT)
  Formål: Tiltakene skal bidra til å styrke kompetanse og øke evne til å effektivt håndtere sikkerhetshendelser lokalt på institusjonsnivå

- Informasjonssikkerhet og personvern (rettet mot administrasjon og ledelse)
  Målgruppe: Ledelse, ansatte og studenter
  Formål: Tiltakene skal bidra til å etablere felles metodikk og systemer for å bedre effekten av ledelsessystemer, internkontroll og rapportering på informasjonssikkerhet og personvern, som en integrert del av institusjonenes visksomhetsstyring.

Erfaringer og resultater fra tidligere arbeid i Sekretariatet for informasjonssikkerhet, etablert av Kunnskapsdepartementet og lagt til Uninett (2013-2018), danner et godt utgangspunkt for prosjektet.

Sekretariatet leverte følgende tjenester og tiltak til sektoren:

- Rammeverk og metodikk
- Risiko- og sårbarhetsvurderinger
- Sikkerhetskulturbygging
- Maler og informasjonsmateriell
- Internasjonalt samarbeid
- Drift av sikkerhetsforum
- Egne websider med informasjon

Sekretariatet dekket også leveranser innenfor bla. bistand til kontinuitets- og beredskapsplaner, revisjoner, bistand ved ledelsens gjennomgang, informasjon om trusselbildet og utvikling av dette.

4. HOVEDAKTIVITETER OG MILEPÆLSPLAN

4.1. Hovedaktiviteter for prosjektet

Prosjektet skal i første omgang kartlegge og prioritere arbeidspakkene og aktivitetene for perioden 2019-2020, med utgangspunkt i behovene som finnes i sektoren, slik beskrevet ovenfor. Behovs- og kompetansekartlegging er et utgangspunkt for å etablere veikartet for prosjektet.Følgende aktiviteter prioriteres for tidsrammen 2019-2020 (foreløpig plan):

[3] IKT = Informasjons- og KommunikasjonsTeknologi
[4] IRT = Incident Respons Team

Hovedaktivitet	NOV	DES	JAN	FEB	MAR	ABR	MAI	JUN	JUL	AUG	SEP	OKT	NOV
– Behovskartlegging													
Prioritering og etablering av tjenester													
Pilotering													
Evaluering													

Prosjektet anser følgende tjenester som relevant for sektoren, med bakgrunn i erfaringer fra Uninett gjennom Sekretariatarbeid (2013-2018) og hovedanbefalinger fra tilstandsrapporten utgitt av Unit (2019):

1) Revisjon og videreutvikling av ledelsessystem for informasjonssikkerhet: Bistå institusjonene med revisjoner av informasjonssikkerhet og personvern, og komme med forslag til nødvendige tiltak på bakgrunn av revisjoner. Omfatter vurdering av prosesser, organisering, sikkerhetstiltak og bruk av partnere og leverandører.

2) Risiko- og sårbarhetsvurdering (ROS): Bistand og kompetanseheving (kursing, gjennomføring og rapportskriving) for å bidra til at institusjonene gjennomfører regelmessige risikovurderinger. Risikovurderinger er et nødvendig grunnlag for alt forebyggende sikkerhetsarbeid, og er lovpålagt når det gjelder personopplysninger.

3) Bistand på institusjonsnivå for å skaffe oversikt over informasjonsverdier og klassifisering av informasjon (i forhold til f.eks. kritikalitet, sensitivitet, oppbevaringsperiode og avhending), inkludert digitale systemer og tjenester, slik anbefalt i tilstandsrapporten fra Unit (2019).

4) Styrke sikkerhetskompetanse lokalt på institusjonsnivå basert på det arbeidet som Uninett bidrar til. De fleste UH-institusjonene har gjennomført kurs hos Uninett om hvordan man etablerer og driver et responsteam («IRT-kurs»). Prosjektet skal vurdere behovet for oppfølging, oppfriskning og påfyll i sektoren, med spesielt fokus på interne rutiner for rapportering, avviks- og hendelseshåndtering. Dette inkluderer å innlemme en eksisterende IRT-funksjon i ledelsessystem.

5) Kontinuitets- og Beredskapsplan (KBP) for IT-infrastruktur: Bistå institusjonene i planlegging for gjenopprettelsen av normal drift i etterkant av alvorlige sikkerhetshendelser. Bidra til utarbeidelse, revisjon og testing av slike planer. «Kontinuitetsplanlegging» er påpekt som et anbefalt tiltak på institusjonsnivå i tilstandsrapporten fra Unit (2019).

6) Bistand til å utvikle og gjennomføre beredskapsøvelser på IKT - området. Tiltaket er spesifikk nevnt i årets tildelingsbrev fra KD/Unit.

4.2. Milepæler

Milepælsplanen for prosjektet blir mer detaljert etter arbeidet med veikartet er fullført. Tabellen under viser milepælene definert for 2019-2020.

	Beskrivelse	Ferdig dato	Godkjennes av
M0	Prosjektmandat godkjent	Nov 2019	Programstyre
M1	Behovskartlegging for prosjektet utført og godkjent	Feb 2020	Programstyre
M2	Prioritering og etablering av tjenester igangsatt	Mars 2020	
M3	Oppstart pilotering av tjenester	Mai 2020	

4.3. Konsekvenser for drift og forvaltning

Nye fellestjenester innen rådgivning og kompetanseheving for informasjonssikkerhet og personvern krever spesiell kompetanse og en robust organisasjon som holder informasjon, kompetanse og kursmaterialet oppdatert til enhver tid.

Kunnskapsdepartementets sektorvise responsmiljø; Uninett CERT og organisasjonen som prosjektet skal etablere som en faglig sentral rådgivningsenhet for sektoren må styrkes og bemannes i forhold til det reelle behovet for å klare å ivareta både vanlig drift og operative sikkerhetsoppgaver og forespørselen om sikkerhetsrådgivning fra sektoren.

5. ORGANISERING

Tabellen under viser deltakere i kjerneteamet:

Navn	Organisasjon/rolle	Rolle i prosjektet
TBA	Uninett Prosjektleder	Prosjektleder
Øyvind Eilertsen	Uninett Seniorrådgiver Sikkerhet	Seniorrådgiver
Tor Gjerde	Uninett Seniorrådgiver Sikkerhet	Seniorrådgiver
Nyansatt Seniorrådgiver	Uninett Seniorrådgiver Sikkerhet	Seniorrådgiver
NSD (TBA)		
Unit (TBA)		
Sektor representant (TBA)		

Kompetansemiljøet som finnes i Unit for informasjonssikkerhet og i NSD for personvern generelt vil trekkes inn i kjerneteamet.

Prosjektet skal etablere en referansegruppe som gjenspeiler bredden i sektoren. Det anbefales at referansegruppen skal bidra aktivt.

Interessentgruppen og andre samarbeidspartnere for programmet er kartlagt gjennom egen interessentanalyse.
Programstyret er premissgiveren for prosjektet. Referansegruppen etablert for prosjektet «Analysesenter og Responsmiljø» vil kunne gi verdifull input for de delene av prosjektet som omhandler operative og tekniske aspekter. Utover denne gruppen er det naturlig å involvere Fagutvalget for informasjonssikkerhet.

6. BUDSJETT

6.1. Finansiering

Kunnskapsdepartementet har gitt tilsagn om 17,5 mill. kroner årlig til Unit for etablering og gjennomføring av programmet for økt sikkerhetssatsing i UH-sektoren i fire år. Av disse er det gitt tilsagn om 12,5 mill. kroner til Uninett for å etablere og lede prosjektene som skal implementere nødvendige tiltak for å styrke informasjonssikkerheten, bl.a. etablering av sektorens analysesenter for cybersikkerhet, rådgivingstjenester og kompetanseheving innen informasjonssikkerhet og personvern. De øvrige 5 mill. kroner skal finansiere etablering og forvaltning av oppgavene og rollene i Unit.

12,5 mill. kroner tildelt Uninett fordeles mellom de to prosjektene som Uninett er ansvarlig for; «Analysesenter og responsmiljø» og «Rådgivningstjenester og Kompetanseheving».

Prosjekt	**Tilskudd** (MNOK pr år)
Ny styringsmodell (Unit)	**5,0**
Analysesenter og responsmiljø (Uninett)	**12,5**
Rådgivningstjenester og kompetanseheving (Uninett)	
Totalt årlig tilskudd	**17,5**

I tabellen under vises et grovt estimat over foreslått fordeling av tilskuddet mellom prosjektene.

Budsjett	**2019**	**2020**	**2021**	**2022**
Programadministrasjon	1	0,5	0,5	1
Analysesenter og Responsmiljø	10	8	7	7,5
Rådgivningstjenester og Kompetanseheving	**1,5**	**4**	**5**	**4**
Totalt tilskudd (NMOK)	**12,5**	**12,5**	**12,5**	**12,5**

Et mer detaljert budsjett for prosjektet blir utarbeidet etter at veikartet for prosjektet er skissert ferdig. Prosjektet er basert på smidig metodikk. Dermed er kostnadsfordelingen over år og mellom de to prosjektene som Uninett leder basert på et grovt estimat.

6.2. Planlagt forbruk

Prosjektet pådrar seg følgende kostnader: Egen ressursinnsats, konsulent og annen innleie, reise- og møtekostnader, samt arbeidsressurs fra samarbeidspartnere og andre direktekostnader.

De to første prosjektårene er det estimert et timeforbruk i underlag av 3 årsverk. Estimatet for timeforbruk innebærer fagpersoner fra både Uninett og eksterne fra samarbeidspartnere i prosjektet. Arbeidsomfanget og ressursbehovet for tidsrammen 2019-2020 blir først definert gjennom arbeidet med behovskartlegging i prosjektet.

7. KRITISKE SUKSESSFAKTORER / RISIKO

Suksessfaktor	Risikoreduserende tiltak
Konkretisering og riktig prioritering av leveransene i prosjektet i tråd med målsetninger og brukerbehov	Grundig planleggings- og veikartarbeid prioriteres, med involvering av ressurser hos Uninett og samarbeidspartnere. Veikartet for prosjektet forankres hos prosjektgruppen og godkjennes av Programstyret.
Tilgang på tilstrekkelige ressurser og spesialkompetansen	God ressursplanlegging mht veikartet. Inkludert innleie eller evt rekruttering av spesialkompetanse om nødvendig.
Tilfredsstillende fremdrift i prosjektet	God planlegging av delleveranser og aktivitetene ihht veikartet. Jevnlig statusrapportering i prosjektet for kjerneteamet og overfor Programstyret.
Tydelig roller og ansvarfordeling i prosjektet	Tydelig prosjektmandat og styringsdokumentasjon. Sikre felles forståelse blant prosjektdeltakere.
Sikre forankring av prosjektet hos interessentgruppen	Involvering og jevnlig informasjon til premissgivere og andre relevante interessenter.
Tillit og godt samarbeid blant deltakere i prosjektet	Åpen og hensynsfull kommunikasjon. Klare ansvarsforhold og gode rutiner for informasjonsformidling.

8. PROSJEKTSTYRING

Prosjektet rapporterer til Programstyret i forbindelse med styremøtene som er planlagt å avholdes minst fire ganger i året, på samme linje som de andre delprosjektene som inngår i satsingen. Minimumsrapportering skal innebære fremdrift, leveranser og økonomi. Rapportering utover denne minimumsrapportering kan avtales ved behandling av prosjektbeskrivelsen.

Programlederen deltar på styremøtene i tillegg til medlemmene i programstyret, med ansvar for rapportering om status på de tre prosjektene som programmet består i. Prosjektlederne kan også delta ved behov for statusrapportering.

Prosjektet skal ha hyppigere rapportering og kontinuerlig dialog med programlederen, minst to ganger i måned.

Prosjektgruppen og samarbeidspartnere skal avtale hyppige arbeids- og statusmøter basert på organisering av arbeidet iht veikartet for prosjektet.

Prosjektdokumentene skal lagres på programportalen opprettet på MS Sharepoint hos Uninett. Det benyttes samhandlingsverktøy (O365) der prosjektgruppen får tilgang til relevant prosjektinformasjon.

Vedlegg 5

Kvalitetssikring (ekstern revisjon) av Sikkerhetssatsing 2019-2022

UNINETT

Kvalitetssikring (ekstern revisjon) av Sikkerhetssatsing 2019-2022

Oslo, 15.03.2021

karabin

Kvalitetssikringens formål har vært å avdekke i hvilken grad prosjektarbeidet utført i perioden 2019-2020 og leveranseplan for resterende prosjektperiode 2021-2022 svarer på oppdraget og forventninger fra oppdragsgiveren; Unit (på vegne av Kunnskapsdepartementet).

Espen Andresen
Partner i Karabin AS

Frederik Westerberg
Manager i Karabin AS

0

Prosjektrammer

Bakgrunn og formål

Kunnskapsdepartementet har i digitaliseringsstrategien for universitets- og høyskolesektoren lagt vekt på at universitetene og høyskolene har et selvstendig og bevisst forhold til informasjonssikkerhet, herunder personvern, som en kritisk suksessfaktor for egne digitaliseringsstrategier og strategiske satsinger. Unit har en sentral rolle i at dette legges til grunn på sektornivå. I strategien har Kunnskapsdepartementet også fremhevet at det vil styrke styring av informasjonssikkerheten på sektornivå gjennom et tydeligere rammeverk.

Kunnskapsdepartementet har gitt et tilsagn om 17,5 mill. kroner til Unit for en årlig satsing innen informasjonssikkerhet i universitets- og høyskolesektoren i perioden 2019-2022. Av disse gis tilsagn om 12,5 mill. kroner til Uninett og prosjektene «Analysesenter og responsmiljø» *(heretter forkortet til A&R)* og «Rådgivingstjenester og kompetanseheving» *(heretter forkortet til R&K).* Målsettingen er blant annet å forbedre evnen til å forebygge, oppdage og håndtere trusler, og inkludere tiltak som bedre analyseverktøy, tilbud om rådgivingstjenester og kompetanseheving. De øvrige 5 mill. kroner skal finansiere etablering og forvaltning av disse oppgavene og rollene i Unit.

På oppdrag fra Uninett som prosjekteier har Karabin AS gjennomført en uavhengig kvalitetssikring av arbeid, framdrift, fremtidig leveranseplan, samt generell styring av prosjektene og satsingsmidler. Kvalitetssikringen er forventet å vurdere:

- Forventningene fra Unit (og ev. Kunnskapsdepartement) knyttet til sluttleveransen i prosjektene
- Framdrift opp mot forbruk av midler
- Risikoelementer som kan evt. hindre framdrift og oppnåelse av sluttleveranse
- Konkrete anbefalinger, forbedringspunkter og forebyggende tiltak knyttet til risikoelementer avdekket i prosjektene

Beskrivelse av prosjektene

Prosjektene ***«Analysesenter og responsmiljø»*** og ***«Rådgivningstjenester og kompetanseheving»*** inngår i programmet *UH Sikkerhetssatsningen 2019-2022* under UNIT, og er en del av digitaliseringsstrategien for UH sektoren 2019-2022 under Kunnskapsdepartementet. Formålet med prosjektene er beskrevet i tildelingsbrevene til UNI og Uninett og er forankret i programmandatet for UH Sikkerhetssatsningen og prosjektmandatene for de enkelte prosjekter.

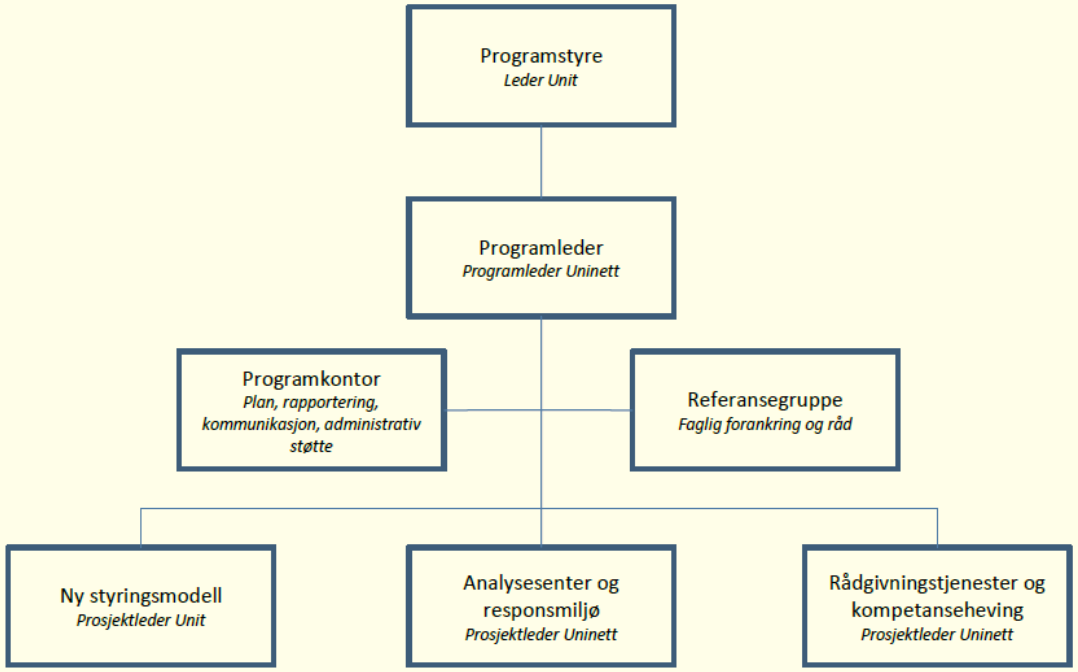
Prosjektenes målsetting defineres i programmandatet, slik:

1. *Prosjektet «Analysesenter og responsmiljø»: Deteksjons- og analysekapasitet skal forbedres, og det skal etableres et helhetlig og felles analysesenter for cybersikkerhet i sektoren. Uninett skal ivareta rollen som sektorvist responsmiljø, i tråd med NSMs «Rammeverk for håndtering av IKT-sikkerhetshendelser», og forbedre sektorens evne til å håndtere trusler.*

2. *Prosjektet «Rådgivningstjenester og kompetanseheving»: Etablere rådgivningstjenester for implementering og helhetlig praktisering av etablerte ledelsessystem for informasjonssikkerhet, samt etablere et program for heving av kompetanse innenfor informasjonssikkerhet og personvern for lederen, forskeren, studenten og øvrige ansatte.*

Gjennom to års prosjektarbeid har ressursinnsatsen i prosjektene vært innrettet mot ett overordnet mål: Etablering av "Cybersikkerhetssenteret for forskning og utdanning" som en fellestjeneste i sektoren ved utgangen av 2021. Et felles Cybersikkerhetssenter vil kunne tilby sektoren sikkerhets- og rådgivningstjenester spesielt tilpasset kunnskapsektoren; bla. sektorspesifikt trusselbilde, datalagring, analyse, deteksjon, hendelseshåndtering, kompetanseheving og sikkerhetsrådgivning.

Uninett blir i perioden 2019-2022 årlig tildelt 12,5 MNOK til prosjektene.



Programstyre består av:

- Sigurd Eriksson, Ass. direktør og Avdelingsdirektør i Unit (Programeier, Leder programstyre)
- Tom Røtting, Adm. direktør i Uninett
- Lars Oftedal, IT-direktør ved UiO
- Håkon Alstad, IT-sjef ved NTNU
- Jostein Jensen, Direktør for sikkerhet ved NHN
- Lars Atle Holm, Direktør ved NMBU
- Anette Thorkildsen Osaland, CISO ved UiA
- Hildegunn Vada, Avdelingsdirektør ved Uninett

1

Forutsetninger og Avgrensninger

Forutsetninger og avgrensninger

Kvalitetssikringen dekker prosjektene

- *Analysesenter og responsmiljø (A&R)*
- *Rådgivningstjenester og kompetanseheving (R&K)*

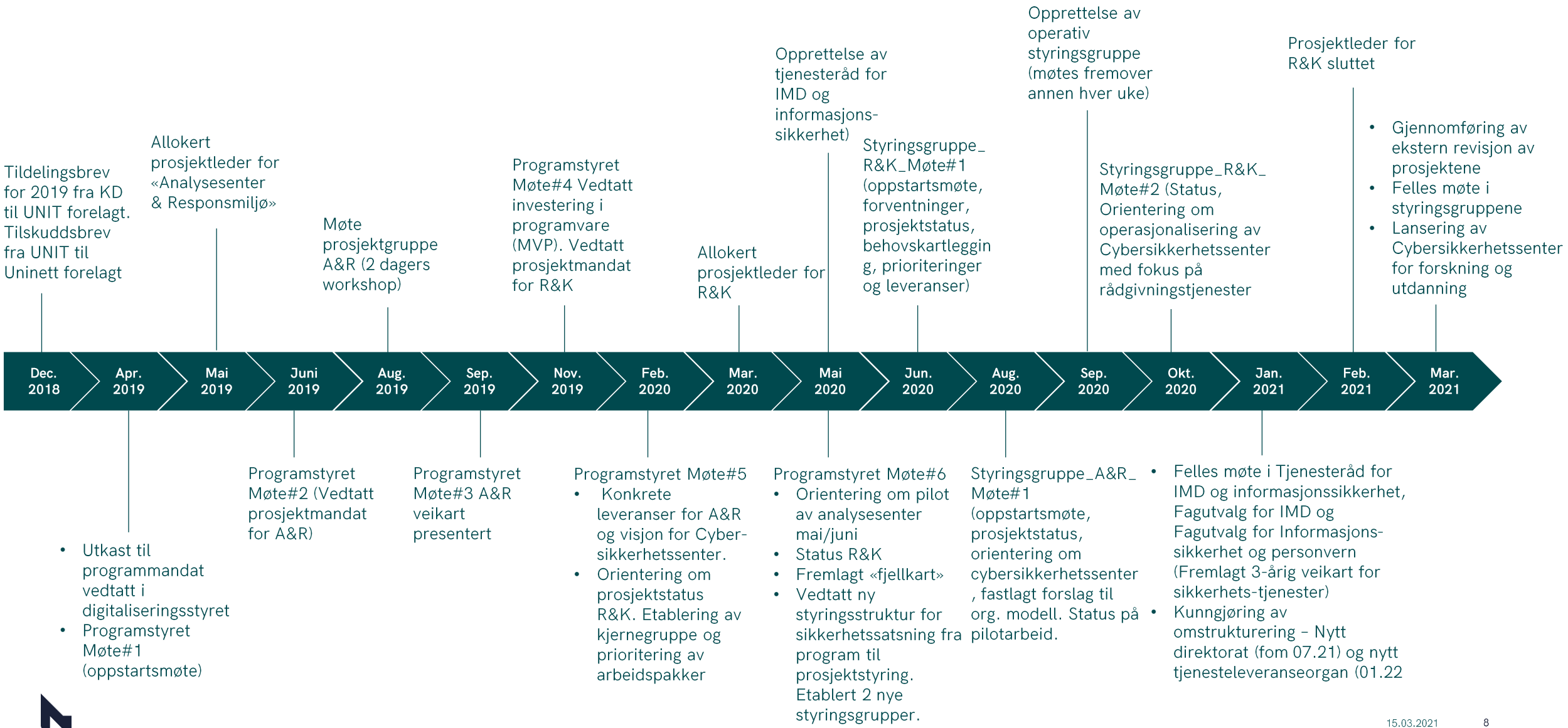
Men med følgende avgrensninger:

- Gjennomgangen dekker kun sammenhengen mellom mandater og utførelse. Bakgrunnen for mandater er ikke vurdert.
- Prosjektet Ny styringsmodell for informasjonssikkerhet og personvern var en del av programmet for sikkerhetssatsing, men er ivaretatt av Unit. Vi har i liten grad fått innsikt i dette prosjektet og dets innvirkning på de andre prosjektene.
- Interessentmiljøet er analysert ut fra intervjuer med nøkkelpersonell i og utenfor prosjektet. Hele interessentbildet er ikke belyst.
- Vi har ikke hatt tilstrekkelig godt grunnlag til å si noe kvalifisert i vurderingen av fremdrift opp mot forbruk av midler ettersom vi i liten grad har hatt innsikt i prosjektets leveranser

Kvalitetssikringen baserer seg på informasjon fra et fåtall intervjuer avtalt med oppdragsgiver og innsyn i relevant og tilgjengeliggjort dokumentasjon. Rapporten reflekterer vår vurdering av denne informasjonen. Vi har i noen grad forsøkt å avdekke om all relevant informasjon er mottatt, men kan ikke avskrive muligheten for at annet relevant materiale skulle vært er mottatt. De observasjoner og tilhørende anbefalinger som er gitt i denne rapporten forutsetter at informasjonen vi har mottatt er korrekt og at vi har snakket med et representativt utvalg nøkkelpersoner.

Anbefalingene i rapporten er basert på det arbeidet som er utført under kvalitetssikringen. Oppdragsgiver må selv vurdere om anbefalingene er velegnede og om tiltak kan implementeres på en kostnadseffektiv måte.

Tidsperiode vurdert

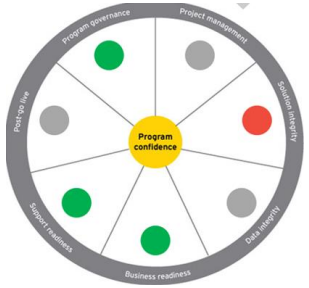


2

Arbeidsmetode og angrepsvinkel

Arbeidsmetode og angrepsvinkel

1

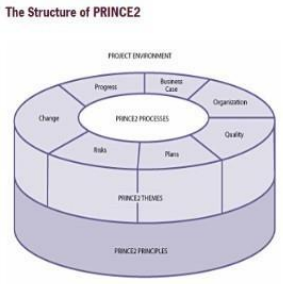


Karabin
I arbeidet med kvalitetssikringen har Karabin hatt referanse til rammeverket *Building confidence in IT programs*

2

Uninett
Modell for prosjektstyring i DIFI (prosjektveiviseren), samt smidig metodikk og tjenestedesign (design thinking)

3



Ledende praksis
PRINCE2, ITIL

Angrepsvinkel

- For å sikre en mest mulig hensiktsmessig tilnærming til kvalitetssikringsoppdraget er vår angrepsvinkel basert på anerkjent metode og relevante rammeverk
- Disse komponentene er særlig vektlagt i denne rapporten:

1. Omfang og mandat
2. Gevinstrealisering
3. Planlegging og budsjettering
4. Prosjektstyring

Metode

- Gjennomgangen er gjort i perioden primo mars – medio mars 2021
- Kvalitetssikringen baserer seg på intervjuer med identifisert nøkkelpersonell i prosjektet, samt gjennomgang av dokumenter som er tilgjengeliggjort for oss
- Det vises til vedlegg for detaljert oversikt over gjennomførte intervjuer og grunnlagsdokumenter

Angrepsvinkel – Symboler og forklaring av score

Symbolene representerer vår subjektive oppfatning av situasjonen, og er ikke en garanti for den reelle godhet på de etablerte styrings- og kontrolltiltakene. Det er alltid en risiko for at forhold som kunne ha medført en annen konklusjon ikke har vært vurdert.

Forklaring av fargekoder

5 **Ledende -** Etablert styring og kontroll (rammeverk, etterlevelse og ledelse) vurderes som, og i samsvar med, "ledende praksis". Det er etablert effektive og hensiktsmessige styrings- og kontrollsystemer, og tilfredsstillende etterlevelse.

4 **Kvaliteten er tilstrekkelig -** Etablert styring og kontroll vurderes som tilstrekkelig. Det er ikke avdekket kritiske forhold som ikke er håndtert på en tilfredsstillende måte. Det kan likevel være områder som kan forbedres og effektiviseres.

3 **Kvaliteten bør forbedres** - Etablert styring og kontroll bør forbedres da enkelte risikoer ikke er håndtert på en tilfredsstillende måte. Det er avdekket enkelte svakheter knyttet til etablert rammeverk, etterlevelse og/eller ledelse.

2 **Kvaliteten må forbedres** - Styring og kontroll må forbedres på vesentlige områder. Enkelte vesentlige risikoer er ikke håndtert på en tilfredsstillende måte, noe som kan medføre tap, kontraktsbrudd, negativt omdømme, eller andre vesentlige konsekvenser.

1 **Vesentlige svakheter** - Det er avdekket vesentlige svakheter i rammeverket og/eller kritiske mangler knyttet til etterlevelse. Kritiske risikoer og/eller eksterne lovkrav er ikke håndtert på en akseptabel måte, noe som kan medføre vesentlige tap, kontraktsbrudd, negativt omdømme, eller andre vesentlige konsekvenser.

Prioritering av anbefalingsforslag

! **Kritisk** - Anbefaling som vurderes som kritisk og hvor tiltak må implementeres som følge av lovbrudd eller (systematisk) manglende etterlevelse av sentrale interne retningslinjer

Høy **Anbefaling med Høy Prioritet** - Anbefaling som vurderes som vesentlig for å sikre måloppnåelse (strategi, drift, rapportering og compliance), og for å sikre tilstrekkelig håndtering av vesentlige risikoer

Medium **Anbefaling med Medium Prioritet** - Anbefaling som vil kunne bidra til bedre måloppnåelse ,og som bør implementeres for å sikre en bedre risikohåndtering

Lav **Anbefaling med Lav Prioritet** - Anbefaling som antas å kunne forenkle eller forbedre dagens prosess

3

Overordnet vurdering

Oppsummering

I hvilken grad prosjektarbeidet utført i perioden 2019-2020 og leveranseplan for resterende prosjektperiode 2021-2022 svarer på oppdraget og forventninger fra oppdragsgiveren er utfordrende å kvalifisere ettersom både målbilde, leveranser og gevinster er vagt beskrevet i de opprinnelige styringsdokumentene slik vi ser det. I prosjektperioden er dette i begrenset grad konkretisert eller utdypet og gjør det utfordrende for prosjektene å kommunisere effektivt omkring leveranser, fremdrift og gevinster.

Vi har funnet flere tegn på gode leveranser og på god prosjektstyring. Den kommende etableringen av et senter for cybersikkerhet allerede halvveis i prosjektperioden vitner om god gjennomføringskraft i prosjektarbeidet samtidig som det danner en viktig plattform for kommende leveranser, operasjonalisering og gevinstrealisering.

Samtidig ser vi særlig et behov for å styrke gevinstrealisering, rapportering og kommunikasjon i prosjektene. Oppmerksomheten omkring risikostyring i prosjektene bør løftes og i større grad inkludere styringsgruppens behandling. Etableringen av ulike fora og arbeidsgrupper har bidratt til å heve kvaliteten i leveransene og sikret god kommunikasjon med enkelte interessentgrupper. Systematisk kommunikasjon bør ivaretas også overfor andre grupper av interessenter.

Omfang, mandat & tilnærming

Prosjektene opererer innenfor et komplekst fagfelt, der det stilles krav fra flere sider. Forankring og til en vis grad formalisering skal ikke bare skje i prosjektstyrene, men også i fagråd, hos Unit og i KD, samt hos Digitaliseringsstyret. Dette til tross, vi forventet i større grad å kunne følge leveranser, fremdrift og endring av disse opp mot mandat. For oss fremstår disse sammenhengene som noe uklare. Difi's prosjektveiviser og smidig utvikling er valgt som tilnærming, men vi fant en del avvik fra anbefalingene i disse rammeverkene. Ut fra intervjuene kan vi konstatere at innholdet i prosjektene vurderes som høyst relevant og innenfor mandat.

Gevinstrealisering

Prosjektenes gevinster er i liten grad belyst ved prosjektstart, men er i noen grad belyst senere i prosjektene. Etter det vi kan se er det ikke forsøkt å tallfeste gevinster og vi finner lite dokumentasjon i prosjektene forbundet med gevinstrealisering. For oss ser det ut som om prosjektene ikke har et aktivt forhold til gevinstrealisering og at det vil være en styrke for prosjektene at dette etableres, gjerne basert på Difis prosjektveiviser eller liknende rammeverk. De utførte intervjuer bekrefter dette bildet.

Planlegging og budsjettering

Vi opplever at planleggingsaktiviteter stort sett er ivaretatt på et overordnet nivå men at det i liten grad er sammenheng mellom budsjett, planverk og fremdriftsrapportering. Vi har sett at til tross for at prosjektene har endret innhold underveis og at arbeidspakker endrer tidsfrister er det ikke reflektert som avvik. Vi har registret at både styringsgruppen i programmet og senere prosjektstyringsgruppene har utfordret planverket i prosjektene. I tillegg har de ved flere anledning bedt om utdypende rapportering på økonomi. Etter vår oppfatning er den økonomiske oppfølgning for overordnet og for periodisk.

Prosjektstyring

Usikkerhet ser ut til å være håndtert gjennom etableringen av risikoregistre med tilhørende malverk. Det er et positivt tiltak, som forhåpentlig har gitt gode føringer for det operative arbeidet. Imidlertid ser vi små tegn på at risikoregistrene er kommunisert og fulgt opp på styringsgruppenivå. Vi opplever videre at rapportering og oppfølgning av planer, status og fremdrift bør styrkes. Prosjektene har etablert ulike råd, samt to styringsgrupper – en overordnet styringsgruppe og en operativ styringsgruppe – for å sikre forankring og kvalitet i leveransene. Både våre intervjuer og en del av det mottatte materialet tyder på at det har fungert etter hensikten. Etter vår oppfatning kan det se ut som om de ulike rådene også har blitt brukt som kommunikasjons-fora og at det kan forklare noe av den manglende kommunikasjon til styringsgruppene. I tillegg har en periodevis utfordrende tilgang på ressurser utvilsomt hemmet formaliseringen og dokumentasjon.

4

Detaljering per område

Omfang, mandat & tilnærming (1/2)

Score 3

I dette avsnittet har vi vurdert prosjektenes omfang, hvorvidt de er innenfor mandat og om den valgte tilnærming til prosjektstyring er overholdt.

Prosjektene opererer innenfor et komplekst fagfelt, der det stilles krav fra flere sider. Forankring og til en vis grad formalisering skal ikke bare skje i prosjektstyrene, men også i fagråd, hos Unit og i KD, samt hos Digitaliseringsstyret. Dette til tross, vi forventet i større grad å kunne følge leveranser, fremdrift og endring av disse opp mot mandat. For oss fremstår disse sammenhengene som noe uklare. Difi's prosjektveiviser og smidig utvikling er valgt som tilnærming, men vi fant en del avvik fra anbefalingene i disse rammeverkene. Ut fra intervjuene kan vi konstatere at innholdet i prosjektene vurderes som høyst relevant og innenfor mandat.

Kilde	Tema	Observasjon	Forslag til tiltak
Program & prosjekt-mandat, tildelings brev, intervjuer	Omfang & mandat	Prosjektene tar utgangspunkt i sikkerhetssatsningen som har sitt utgangspunkt i digitaliseringsstrategien under KD. Prosjektmandatene er utarbeidet av Uninett på denne bakgrunn. Dette har vist seg å være krevende ettersom bestillingen som ble gitt fra Unit og ultimativt KD er ganske bred og gir rom for tolkning. Vi har fått opplyst at Unit mottok prosjektmidler først i desember 2018 og at tildelingsbrevet til Uninett kom enda senere. Dette skal ha bidratt til at det var krevende å få til en god og strukturert mobilisering av prosjektene tidlig i 2019. Vi mener dette kan forklare noen av de forhold som prosjektene har måttet håndtere i prosjektperioden. Til dette bildet kommer at det ene prosjektet startet opp før programmandatet ble etablert, for deretter å bli forankret på nytt i et prosjektmandat.	ingen
Program & prosjekt-mandat Styrings-doku-menter og intervjuer	Tilnær-ming og løpende opp-følging	Tilnærmingen som er benyttet i prosjektene er beskrevet i mandatene for programmet og senere i mandatene til prosjektene. Metodemessig er det valgt en tilnærming som støtter seg på Difis prosjektveiviser, smidig metodikk og tjenestedesign. Dette mener vi er hensiktsmessig og støttes også av de intervjuede som peker på at tilnærmingen har bidratt til gode leveranser og sikker fremdrift. Etter vår oppfatning er imidlertid dokumentasjon og rapportering av leveranser og fremdrift utilstrekkelig. Vår vurdering er at leveransene i prosjektene i liten grad er synliggjort eller forsøkt konkretisert i de styringsdokumentene vi har hatt innsyn i. Mandatene beskriver ambisjoner og forventede resultater, men uten at dette følges opp og konkretiseres ytterligere i planverket vi har hatt tilgjengelig. Det er etablert et knippe arbeidspakker per prosjekt. Disse gir en viss grad av innsikt i hvilke komponenter som inngår, ettersom de inneholder en listing av nøkkelaktiviteter. Utfordringene i at det ikke foreligger fullverdige leveransebeskrivelser er at det kan bidra til å skapes distanse og at det blir krevende å kommunisere i prosjektet, mellom prosjektene og fremfor alt til interessentene i sektoren.	Se nedenfor

Omfang, mandat & tilnærming (2/2)

Kilde	Tema	Observasjon	Forslag til tiltak
Program & prosjekt-mandat Styrings-doku-menter og intervjuer	Tilnær-ming og løpende opp-følging	De intervjuede har påpekt at prosjektene gjennomføres innenfor et fagfelt der landskapet endrer seg raskt. Dette i kombinasjon med smidig tilnærming oppgis også som en del av forklaringen på at det ikke foreligger fullverdige leveransebeskrivelser. Det kan vi forstå, men det bør etter vår oppfatning ikke frita prosjektene fra å synliggjøre fremdrift mot mandat, ei heller fra ansvaret fra å beskrive leveranser på en måte som utfyller eller tydeliggjør prosjektenes mandater. Kombinasjon av waterfall og smidig tilnærming er prinsipielt god gitt prosjektets egenart. Det må imidlertid poengteres at dette ikke fritar prosjektledelsen fra det ansvaret som knytter seg til å etablere robuste mål, planer, arbeidsfordeling og oppfølging så langt det er mulig.	Vi vil normalt anbefale å definere prosjektleveransene som et sett av komponenter i et overordnet målbilde. Hver av leveransene bør beskrives så detaljert det lar seg gjøre, gjerne beskrevet i et perspektiv der de viktigste interessentene er i varetatt.
Program-mandat og prosjekt-mandater	«Ny styrings-modell»	Forholdet til prosjektet «Ny Styringsmodell» er usikkert. Vi har hatt lite innsyn i styringsdokumentene for dette prosjektet og følgelig er det vanskelig å se hvordan avhengighetene fra dette prosjektet skal utnyttes i gjennomføringen av «Analysesenter og responsmiljø» og «Rådgivning og kompetanseheving». I intervjuene har vi fått innblikk i at det eksisterer synergier mellom prosjektene, men vi finner altså ikke støtte for at dette er ivaretatt. Vi har oppfattet at «Ny Styringsmodell» er i en implementeringsfase. I den forbindelse fremstår det som uklart for oss hvordan oppfølgingen av implementeringsarbeidet ivaretas, slik at effektene kan realiseres og slik at erfaringspunkter og læring ivaretas i prosjektene «Analysesenter og responsmiljø» og «Rådgivning og kompetanseheving».	Vi anbefaler at prosjektene tydeliggjør føringene i den nye styringsmodellen og konkretisere betydningen for prosjektenes governance
Program-mandat og prosjekt-mandater	Organi-sering	Etableringen av rådene Fagutvalg, Prioriteringsråd og UH-IT er gode grep som sikrer støtte ved behov for eskalering eller beslutninger innenfor angitt mandat. Mandatet for disse rådene er ikke tydelig definert for oss, men vi legger til grunn at etablering av rådene er avklart med og godkjent av programledelsen. Vi opplever bruken av utvalg og råd hensiktsmessig og naturlig ettersom de ordinære styringslinjene i Unit ikke har kapasitet eller kompetanse til å kunne gi prosjektet den støtte som har vært nødvendig innenfor relativt tekniske og detaljerte problemstillinger. Vi har ikke hatt tilgang til referater eller annen dokumentasjon fra vurderingene som er gjort i utvalg og rådsmøter og kan derfor ikke vurdere kvaliteten. Prosjektene er organisert med en operativ styringsgruppe i tillegg til den overordnede styringsgruppe. Denne organisering ser vi både fordeler og mulige utfordringer i, hvilket beskrives nærmere i avsnittet rundt prosjektstyring.	ingen

Planlegging og budsjettering (1/2)

Score 3

I dette avsnittet har vi vurdert hvorvidt prosjektene er planlagt og fulgt opp i tilstrekkelig grad. I vurderingen har vi sett på mål, planverk og oppfølging av aktiviteter, fremdrift og leveranser. I tillegg har vi sett på budsjett og i hvilken grad dette følges opp og hvordan dette korresponderer med reelt timeforbruk.

Vi opplever at planleggingsaktiviteter stort sett er ivaretatt på et overordnet nivå men at det i liten grad er sammenheng mellom budsjett, planverk og fremdriftsrapportering. Vi har sett at til tross for at prosjektene har endret innhold underveis og at arbeidspakker endrer tidsfrister er det ikke reflektert som avvik. Vi har registret at både styringsgruppen i programmet og senere prosjektstyringsgruppene har utfordret planverket i prosjektene. I tillegg har de ved flere anledning bedt om utdypende rapportering på økonomi. Etter vår oppfatning er den økonomiske oppfølgning for overordnet og for periodisk.

Kilde	Tema	Observasjon	Forslag til tiltak
Plan-doku-menter	Malverk og planer	Det mottatte materialet gir ingen tydelige holdepunkter for å kunne å ta stilling til om prosjektene fremdriftsmessig er innenfor den planlagte tidsrammen. Oppfølgingen av fremdrift på arbeidspakkene og datosetting for ferdigstillelse av disse vurderes ikke som tilstrekkelig og vi har funnet eksempler på at tidsfrister for de enkelte arbeidspakker er justert, uten at det er kommentert som avvik. Det er benyttet ulike verktøy og maler i planleggingen. Det medfører at det er krevende å få oversikt eller aggregere informasjon for sentral prosjektledelse eler programledelse. For eksempel har prosjektet Analysesenter og Responsmiljø ulik planverk fra Rådgivningstjeneste og kompetanseheving. Av den dokumentasjonen vi har hatt innsyn i fremstår planverket til Analysesenter og Responsmiljø som svært overordnet og med liten mulighet til å følge aktiviteter eller se avhengigheter. Planverket for Rådgivningstjeneste og kompetanseheving på den annen side inneholder i større grad beskrivelser av nøkkelaktiviteter og fremdriftsplan på ukenivå. Vi vil for øvrig nevne at begge sett av planer fremstår som uferdige og/eller ikke ajourført i tillegg til at de ikke inneholder reflekterer et planperspektiv ut over 2020. I det materialet vi har hatt tilgang til kan vi ikke se at det eksisterer fullverdig plandokumenter for disse prosjektene for 2021 og 2022.	Vi anbefaler å prioritere arbeidet knyttet til å ajourføre prosjekt-, og milepælsplaner, herunder leveranseplaner, fremdriftsplaner, aktivitetsplaner, ressursplaner og budsjett
Beste praksis	Budsjett-ering og avsetning	Vi har ikke identifisert retningslinjer for estimering og bruk av risikoavsetning i prosjektene. Føringene knyttet til å anvende smidig tilnærming i prosjektene vil naturlig skjerpe kravene for økonomioppføling ettersom metodikken innebærer en større frihetsgrad knyttet til løsningsutarbeidelsen enn den tradisjonelle waterfall-tilnærmingen. Vi vil hevde at frihetsgraden i smidig også representerer større usikkerhet i utfallsrommet og derfor vil kreve noe større risikoavsetning i budsjettene.	Prosjektledelsen bør vurdere etablere prosesser og rutiner som gjelder for estimering og bruk av risikoavsetninger. Kommunikasjonen bør også fokusere på årsaken til valgte prosesser for å sikre forståelse.

Planlegging og budsjettering (2/2)

Kilde	Tema	Observasjon	Forslag til tiltak
Plan-dokumenter, budsjett, rapportering og intervjuer	Budsjettering og økonomioppfølging	Budsjettoppfølgingen viser et underforbruk i 2019 og et overforbruk i 2020 som samlet sett gir et overforbruk på ca. 10% mot tildelt ramme for 2019 og 2020. Vi har ikke mottatt informasjon om budsjettsituasjonen så langt i 2021. Vi har ikke hatt tilgang til informasjon som tilsier at de årlige tildelingene er periodisert eller fordelt mellom prosjektene gjennom året. Det er vanskelig å se at det drives løpende økonomisk oppfølgning i prosjektene. Prosjektstyrene har ved flere anledninger bedt om status og utdypning av prosjektenes økonomi. I de tilfeller der det er rapportert på økonomi til styringsgruppene er det ikke gitt noen forklaring på hvorfor man har disponert som man har gjort og hva som ligger til grunn. Dette bekreftes i intervjuer.	Vi vil anbefale å øke oppmerksomheten omkring produktiviteten i prosjektene. Produktivitet måles ved å dele opptjent tid (earned value) på faktisk tid (actual value). Opptjent tid (earned value) er differansen mellom planlagt tid (baseline) og gjenstående tid (estimated time to completion – ETC).

Gevinstrealisering

Score 2

I dette avsnittet har vi vurdert hvordan det er jobbet med gevinstrealisering. Vi ser blant annet på om det er forsøkt å estimere gevinster ved prosjektstart, i hvilken grad de er tallfestet og hvilke tiltak det gjøres for å sikre gevinster.

Prosjektenes gevinster er i liten grad belyst ved prosjektstart, men er i noen grad belyst senere i prosjektene. Etter det vi kan se er det ikke forsøkt å tallfeste gevinster og vi finner lite dokumentasjon i prosjektene forbundet med gevinstrealisering. For oss ser det ut som om prosjektene ikke har et aktivt forhold til gevinstrealisering og at det vil være en styrke for prosjektene at dette etableres, gjerne basert på Difis prosjektveiviser eller liknende rammeverk. De utførte intervjuer bekrefter dette bildet.

Kilde	Tema	Observasjon	Forslag til tiltak
Intervjuer	Fremtidig gevinstrealisering	Allerede halvveis i prosjektperioden evner prosjektene å etablere et operativt cybersikkerhetssenter. Vi har god tro på at en slik forsert operasjonalisering vil gi et godt grunnlag for arbeidet med gevinstrealisering. Det vil gi data, retning og kunnskap som igjen vil kunne fungere som input til de mer langsiktige gevinstene fra prosjektene.	
Styringsdokumenter og intervjuer	Dokumentasjon av gevinster og gevinstoppfølging	Programmet/prosjektene har etter det vi kan se ikke arbeidet metodisk med gevinstrealisering og det foreligger verken et «business case», gevinstkart eller effektmål for initiativene, utover det som angis i prosjektmandatene. Selv om gevinstene og effektene kan være åpenbare for prosjektdeltakerne og prosjektenes nøkkelinteressenter, er det vår oppfatning at initiativet som helhet ville vært tjent med en mer strukturert tilnærming til gevinstrealisering slik at prosjekteier og linjeledelsen lettere vil kunne følge opp og sikre at gevinstene realiseres i etterkant av prosjektet. Dette ville kunne bidra til å synliggjøre resultater og effekter av programmet i tråd med departementets ambisjon. Gevinstrealisering som begrep er ikke gitt et innhold som prosjektorganisasjonen er fortrolig med. Dette er godt synlig i identifiserings-, planleggings-, gjennomførings- og dokumentasjonsfasen av prosjektene. Særlig i gevinstplanleggingsfasen er det et potensiale for å konkretisere målsettinger og tydeliggjøre ambisjoner med hensyn til gevinstuttak. Eierskapet til gevinstrealisering virker å være svak. Rolle og ansvarsforhold er ikke tydeliggjort og operasjonalisering av dette er så langt vi kan se ikke gjennomført. Ledelsesoppfølgingen blir tilfeldig ettersom det ikke eksisterer en systematikk for måling og oppfølging av gevinster.	Uavhengig av hvilke formelle krav prosjektene er underlagt, bør ledelsen sikre at gevinster identifiseres, estimeres og rapporteres som en del av periodiske gjennomganger av programmets gevinster. Dette er viktig for å kunne godtgjøre ressursbruken og synliggjøre effektene av et godt gjennomført prosjekt.
Styringsdokumenter og intervjuer	Best practice	Difi og andre anerkjente rammeverk, eksempelvis «*Managing benefits*», anbefaler at det jobbes kontinuerlig med gevinstrealisering gjennom prosjektet. Utover dette er det en anbefaling å utarbeide en oversikt over forventede gevinster i begynnelsen av prosjektet med forsøk på tallfestelse, utprøving og måling. Gevinstrealisering kommenteres via begrepene mål og effekter i prosjektmandatene, og det å kople dem opp mot digitaliseringsstrategien for UH sektoren og de føringer som er gitt i tildelingsbrevet. Gevinstene beskrives, men det gjøres ikke forsøk på å tallfeste eller i særlig grad angi hvordan prosjektene skal jobbe med gevinstrealisering. I prosjektet A&R er det jobbet med å fastlegge gevinstene per arbeidspakke, men det angis ikke hvordan man skal sikre at de blir oppnådd eller om de kan gjøres målbare. De utførte intervjues bekrefter og forsterker dette bildet.	I arbeidet med gevinstrealisering bør man i høyere grad forsøke å støtte seg opp av rammeverk som Difis prosjektveiviser eller Managing benefits.

Prosjektstyring (1/2)

Score 3

I dette avsnittet har vi vurdert ulike sider av prosjektstyringen i prosjektene. Vi har blant annet vurdert styring og kontroll, risikostyring, kommunikasjon og interessenthåndtering.

Usikkerhet ser ut til å være håndtert gjennom etableringen av risikoregistre med tilhørende malverk. Det er et positivt tiltak, som forhåpentlig har gitt gode føringer for det operative arbeidet. Imidlertid ser vi små tegn på at risikoregistrene er kommunisert og fulgt opp på styringsgruppenivå. Vi opplever videre at rapportering og oppfølgning av planer, status og fremdrift bør styrkes. Prosjektene har etablert ulike råd, samt to styringsgrupper – en overordnet styringsgruppe og en operativ styringsgruppe – for å sikre forankring og kvalitet i leveransene. Både våre intervjuer og en del av det mottatte materialet tyder på at det har fungert etter hensikten. Etter vår oppfatning kan se det ut som om de ulike rådene også har blitt brukt som kommunikasjons-fora og at det kan forklare noe av den manglende kommunikasjon til prosjektstyrene. I tillegg har en periodevis utfordrende tilgang på ressurser utvilsomt hemmet formaliseringen og dokumentasjon.

Kilde	Tema	Observasjon	Forslag til tiltak
Prosjekt-rapporter og inter-vjuer	Risiko-styring	Kvalitet i rapporteringen knyttet usikkerhet er kanskje noe av det viktigste i beslutningsgrunnlaget for styringsgruppen og det bør derfor vektlegges å gi løpende god informasjon både om usikkerhet, utfallsrom og de handlinger som skal kontrollere risiko i prosjektene. Denne informasjonen bør vedlikeholdes og følges opp, alle helst gjennom en åpen dialog i styringsgruppene. Det er påregnelig at usikkerheten endres gjennom prosjektforløpet og at kontrolltiltak løpende må tilpasses. God risikostyring i prosjekter bidrar til å redusere kontrollgapet gjennom prosjektforløpet. Det er en styrke for prosjektene at det er etablert et risikoregister og tilhørende malverk for risikostyring. Imidlertid er det en svakhet at løpende rapportering av risiko til programstyret ikke ser ut til å være ivaretatt. For oss ser det ut til at første rapportering av prosjektrisiko til styringsgruppe for prosjektet Rådgivning og Kompetanse har vært i juni 2020 og for prosjekt Analysesenter og Responsmiljø i august 2020. Det er et pluss at det er sammenfall i malverket for risiko i prosjektene. Det bidrar til enklere kommunikasjon omkring usikkerhet og potensielt enklere aggregering av risiko for prosjektene. Det bør imidlertid påpekes at risikorapporteringen i liten grad viser spor av utvikling over tid, slik at det er transparens mht når en risiko ble rapportert, hvilket tiltak som ble iverksatt, hvem som ble gjort ansvarlig for tiltaket og frist for utførelse. Videre er det en svakhet at risikomatrisen bygger på omtrentlige angivelser av sannsynlighet og konsekvens. Det gis liten støtte for vurdering av graden av sannsynlighet og utfallsrom dersom usikkerheten inntreffer.	Vi anbefaler Uninett å ajourføre malverk samt utarbeide retningslinjer for risikostyring i prosjektene. Dette vil bidra til en er enhetlig tilnærming og gi styringsgruppene et bedre utgangspunkt for god styring og kontroll. Vi anbefaler Uninett å tydelig kommunisere forventninger og krav til prosjektledere, prosjektdeltakere og styringsgruppemedlemmer om etterlevelse av fastsatte retningslinjer. Det bør etableres en felles forståelse for konsekvenser ved manglende etterlevelse. Vi anbefaler at Uninett vurderer risikorapporteringen til styringsgruppene for å forbedre overordnet styringsinformasjon. Både hyppighet, innhold og formål bør vurderes. Vi anbefaler at Uninett tilstreber transparens i vurderingene som gjøres i konsolidering og aggregering av risiko, men slik at prosjektdeltakerne og andre interessenter kjenner seg igjen.

Prosjektstyring (2/2)

Kilde	Tema	Observasjon	Forslag til tiltak
Inter-vjuer	Rappor-tering, planer og priori-tering	Intervjuede uttrykker tillit til prosjektledelsen og til at prosjektene har evnet å gjøre riktige prioriteringer. Samtidig etterlyses det en høyere frekvens i statusrapporteringene. Flere intervjuede opplever det som utfordrende å skulle uttale seg om status i prosjektene og/eller om graden av fremdrift, risiko, avhengigheter mellom prosjekter eller øvrige initiativer. Vi observerer at det er godt rom for en større grad av involvering og diskusjon i styringsgruppene. Engasjementet for det er absolutt er til stede, men styringsgruppene opplever i for liten grad at de blir rådspurt.	ingen
Styrings -doku-menter og inter-vjuer	Organi-sering og ressurser	Begge prosjektene er etablert med en overordnet styringsgruppe og en operativ styringsgruppe. Innad i Uninett utrykkes det tilfredshet med modellen og det poengteres at det sikrer tett koordinering med de samarbeidende parter og fremdrift i prosjektene. På den annen side krever modellen løpende og tett koordinering slik at avstanden mellom den overordnede styringsgruppen og det arbeide som utføres ikke blir for stor. En tettere koordinering kan imidlertid bidra til bedre ressursbruk av både interne og eksterne ressurser. Ut fra det mottatte materiale og det vi kan lese av styrerapportene ser det ut til at det i perioder har vært utfordringer på ressurssiden. Det gjelder både for ledelsen av prosjektene i den operative del internt og eksternt. For de operative ressursene kommer deres daglige virke foran prosjektene, noe som kan skape utfordringer for kapasiteten i prosjektene.	Vi anbefaler å beholde nåværende organisering, men forsøke å øke støtten til prosjektledelse og hvis mulig i det operative arbeid.
Styrings -doku-menter og inter-vjuer	Kommu-nikasjon	Kommunikasjon fra prosjektarbeidet er ivaretatt på ulike måter. Det er etablert ulike fora som både er rådspurt og involvert i gjennomføringen. Fagutvalg, prioriteringsråd og UH-IT samt Tjenesteråd er etablert. Vi har ikke informasjon om hvorvidt det er dedikerte ressurser på kommunikasjon eller om det finnes særskilte planer for kommunikasjon og/eller interessenthåndtering. Normalt vil vi forvente at dette i større grad var synliggjort som del av dokumentets styringsdokumenter. Foruten fremlagt «Fjellkart», som vi før øvrig oppfatter som et meget godt initiativ, har vi i liten grad sett planlagte aktiviteter for å sikre en løpende kommunikasjon til grupper av interessenter utenfor prosjektenes sfære. Det er for eksempel ikke planlagt denne typen aktiviteter i «Analysesenter og responsmiljø».	Vi opplever at det er mye positivt å fortelle om prosjektene og leveransene. Vi anbefaler derfor at denne informasjonen blir distribuert til de relevante interessenter og at den samtidig fungerer som et verktøy for forankring for veien fremover.

5

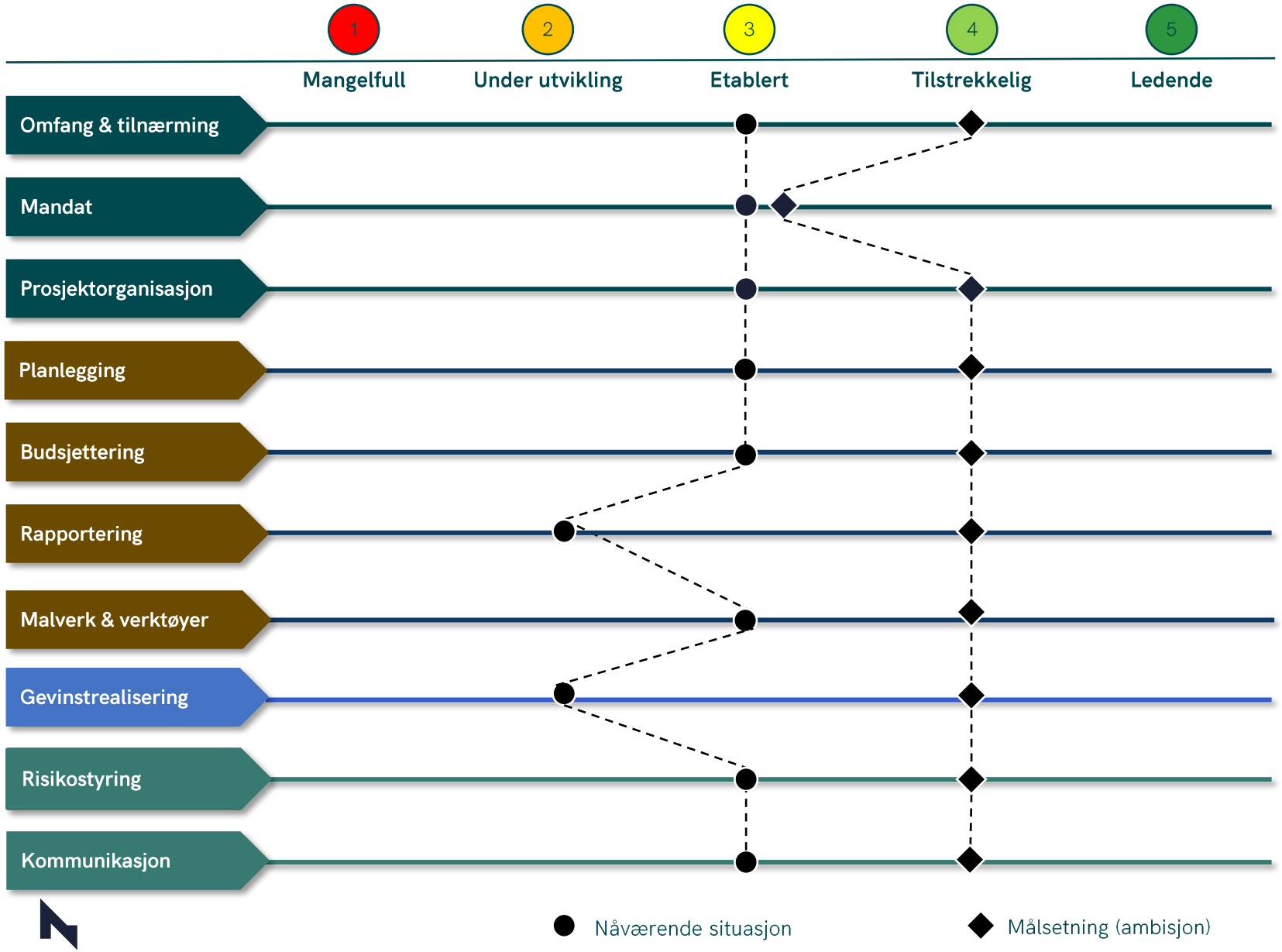
Forbedringstiltak

Forbedringsforslag oppsummert

Høy	**Anbefaling med Høy Prioritet** - Anbefaling som vurderes som vesentlig for å sikre måloppnåelse (strategi, drift, rapportering og compliance), og for å sikre tilstrekkelig håndtering av vesentlige risikoer
Medium	**Anbefaling med Medium Prioritet** - Anbefaling som vil kunne bidra til bedre måloppnåelse ,og som bør implementeres for å sikre en bedre risikohåndtering
Lav	**Anbefaling med Lav Prioritet** - Anbefaling som antas å kunne forenkle eller forbedre dagens prosess

Område	Anbefaling	Prioritet
Omfang, mandat & tilnærming	Vi vil normalt anbefale å definere prosjektleveransene som et sett av komponenter i et overordnet målbilde. Hver av leveransene bør beskrives så detaljert det lar seg gjøre, gjerne beskrevet i et perspektiv der de viktigste interessentene er i varetatt.	Medium
	Vi anbefaler at prosjektene tydeliggjør føringene i den nye styringsmodellen og konkretisere betydningen for prosjektenes governance	Medium
Plan-legging & budsje-ttering	Vi anbefaler å prioritere arbeidet knyttet til å ajourføre prosjekt-, og milepælsplaner, herunder leveranseplaner, fremdriftsplaner, aktivitetsplaner, ressursplaner og budsjett	Høy
	Prosjektledelsen bør vurdere etablere prosesser og rutiner som gjelder for estimering og bruk av risikoavsetninger. Kommunikasjonen bør også fokusere på årsaken til valgte prosesser for å sikre forståelse.	Medium
	Vi vil anbefale å øke oppmerksomheten omkring produktiviteten i prosjektene. Produktivitet måles ved å dele opptjent tid (earned value) på faktisk tid (actual value). Opptjent tid (earned value) er differansen mellom planlagt tid (baseline) og gjenstående tid (estimated time to completion – ETC).	Høy
Gevinst-realisering	Uavhengig av hvilke formelle krav prosjektene er underlagt, bør ledelsen sikre at gevinster identifiseres, estimeres og rapporteres som en del av periodiske gjennomganger av programmets gevinster. Dette er viktig for å kunne godtgjøre ressursbruken og synliggjøre effektene av et godt gjennomført prosjekt.	Høy
	I arbeidet med gevinstrealisering bør man i høyere grad forsøke å støtte seg opp av rammeverk som Difis prosjektveiviser eller Managing benefits.	Medium
Prosjekt-styring	Vi anbefaler Uninett å ajourføre malverk samt utarbeide retningslinjer for risikostyring i prosjektene. Dette vil bidra til en er enhetlig tilnærming og gi styringsgruppene et bedre utgangspunkt for god styring og kontroll. Vi anbefaler Uninett å tydelig kommunisere forventninger og krav til prosjektledere, prosjektdeltakere og styringsgruppemedlemmer om etterlevelse av fastsatte retningslinjer. Det bør etableres en felles forståelse for konsekvenser ved manglende etterlevelse. Vi anbefaler at Uninett vurderer risikorapporteringen til styringsgruppene for å forbedre overordnet styringsinformasjon. Både hyppighet, innhold og formål bør vurderes. Vi anbefaler at Uninett tilstreber transparens i vurderingene som gjøres i konsolidering og aggregering av risiko, men slik at prosjektdeltakerne og andre interessenter kjenner seg igjen.	Høy
	Vi anbefaler å beholde nåværende organisering, men forsøke å øke støtten til prosjektledelse og hvis mulig i det operative arbeid.	Medium
	Vi opplever at det er mye positivt å fortelle om prosjektene og leveransene. Vi anbefaler derfor at denne informasjonen blir distribuert til de relevante interessenter og at den samtidig fungerer som et verktøy for forankring for veien fremad	Medium

Forslag til ambisjonsnivå for forbedring av kvalitet



Vurdering av kvalitet og modenhet

5	**Ledende -** Etablert styring og kontroll (rammeverk, etterlevelse og ledelse) vurderes som, og i samsvar med, "ledende praksis". Det er etablert effektive og hensiktsmessige styrings- og kontrollsystemer, og tilfredsstillende etterlevelse.
4	**Kvaliteten er tilstrekkelig -** Etablert styring og kontroll vurderes som tilstrekkelig. Det er ikke avdekket kritiske forhold som ikke er håndtert på en tilfredsstillende måte. Det kan likevel være områder som kan forbedres og effektiviseres.
3	**Kvaliteten bør forbedres** - Etablert styring og kontroll bør forbedres da enkelte risikoer ikke er håndtert på en tilfredsstillende måte. Det er avdekket enkelte svakheter knyttet til etablert rammeverk, etterlevelse og/eller ledelse.
2	**Kvaliteten må forbedres** - Styring og kontroll må forbedres på vesentlige områder. Enkelte vesentlige risikoer er ikke håndtert på en tilfredsstillende måte, noe som kan medføre tap, kontraktsbrudd, negativt omdømme, eller andre vesentlige konsekvenser.
1	**Vesentlige svakheter** - Det er avdekket vesentlige svakheter i rammeverket og/eller kritiske mangler knyttet til etterlevelse. Kritiske risikoer og/eller eksterne lovkrav er ikke håndtert på en akseptabel måte, noe som kan medføre vesentlige tap, kontraktsbrudd, negativt omdømme, eller andre vesentlige konsekvenser.

Vedlegg

Oversikt over mottatt materiale og intervjues

Intervjuer:

Den tilgjengelige periode for analyse og intervjuer har bevirket at vi kun har utført 3 intervjuer. Dette skyldes både tidsmangel hos oss og de folk vi hadde utsett som relevante for intervjuer. Optimalt sett hadde vi gjerne utført flere intervjuer for å oppnå en brede forståelse og en mer samlet tilbakemelding fra hele interessentgruppen.

11/3-2021, Sigurd Eriksson (UNIT): Leder for programstyre
11/3-2021, Tom Røtting (Uninett): Leder av styringsgruppe
10/3-2021, Ove Brusegaard (NMBU): Medlem av styret i prosjektet Rådgivning & kompetanse.

Avholdte møter:

2/3-2021, Oppstartsmøte, deltakere: Anders Lund,
Maria Carolina Luces Barreat, Espen Andresen, Frederik Westerberg

5/3-2021, Oppfølgingsmøte, deltakere: Anders Lund,
Maria Carolina Luces Barreat, Espen Andresen, Frederik Westerberg

12/3-2021, Gjennomgang av sluttrapport, deltakere: Anders Lund,
Maria Carolina Luces Barreat, Espen Andresen, Frederik Westerberg

Mottatt materiale på teams

Alt materiale til kvalitetssikringen er mottatt på teams kanalen *Ekstern revisjon – Sikkerhetssatsing 2019-2022.* Vi har i noen grad forsøkt å avdekke om alt relevant informasjon er mottatt, men kan ikke uttale oss om hvorvidt det finnes annet relevant materiale

- Oppdragsbeskrivelse
  - Offisiell beskrivelse av oppdraget
- Prosjektrammer:
  - Tilskuddsbrev
  - Tildelingsbrev
  - Programmandat
  - Prosjektmandater
- Programstyre – Saksunderlag & Referat:
  - Styrepresentasjoner
  - Underlag til styrepresentasjoner
  - Referat fra styremøter
- Styringsgrupper – Saksunderlag & Referat:
  - Styrepresentasjoner for begge prosjektene
  - Underlag til styrepresentasjoner for begge prosjektene
  - Referat fra styremøter for begge prosjektene
- Statusrapporter:
  - Aktivitetsrapporter til Unit
  - Statusrapporter for begge prosjektene for 2021
- Risikostyring
  - Risikoregister for begge prosjektene
- Tidslinje:
  - Overordnet tidslinje for programmet og prosjektene
- Økonomistyring:
  - Regneark for budsjett prognose og oppfølgning av programmet og prosjektene
- Diverse prosjektstyring:
  - Regneark inneholdende arbeidspakker og oppfølging av disse for begge prosjektene

Kontakter:

Partner
Espen.Andresen@karabin.no
+47 913 33 436

Manager
Frederik.Westerberg@karabin.no
+47 401 91 564