BRUK AV STANDARDISERINGSARBEID I ROS

For standardiseringsutvalget

Tor Indstøy, NHN

norskhelsenett

Hørt i NHN og e-helse (minner fra 2019).

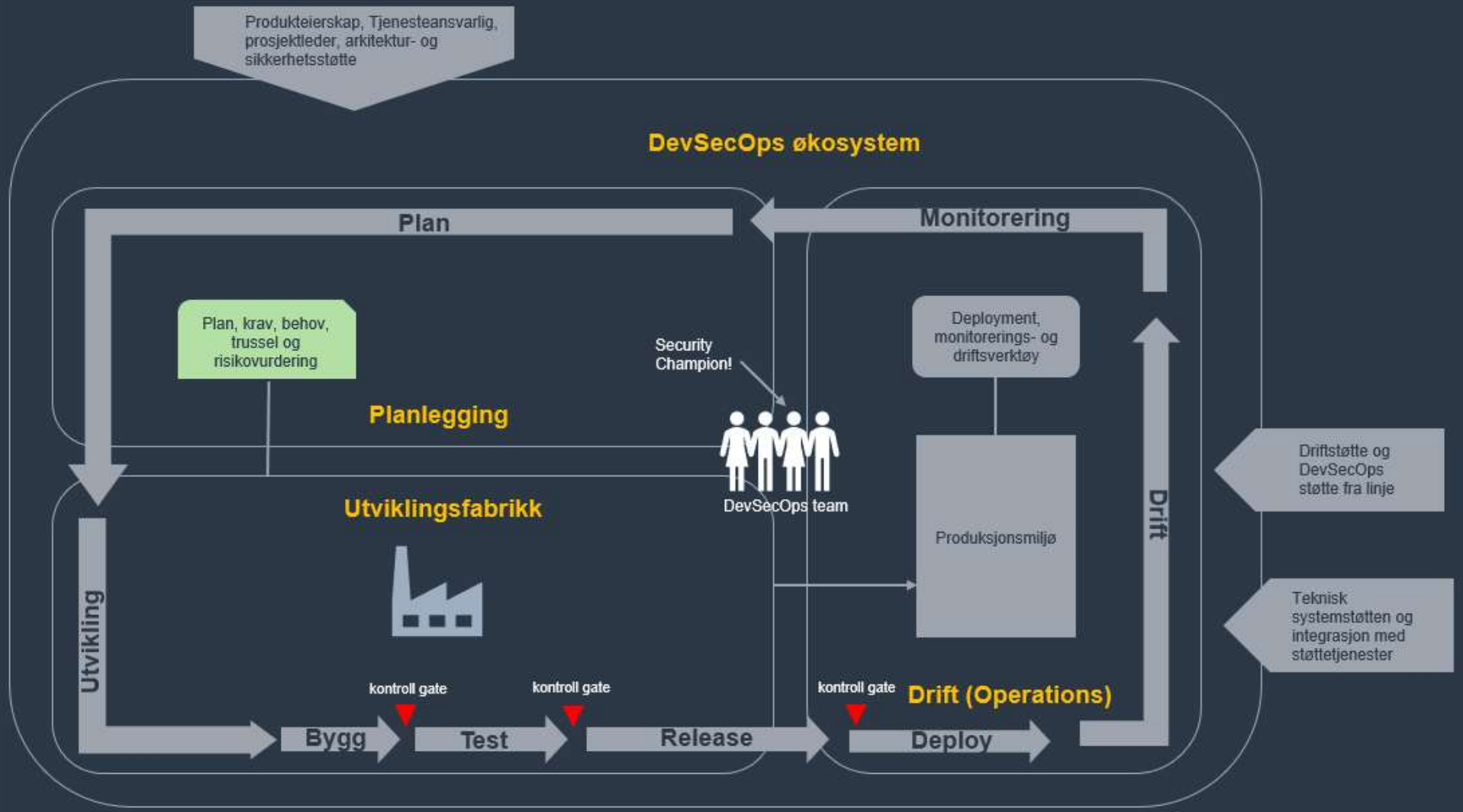
«jeg har 200 risikovurderinger, men er ikke sikker på om jeg får bedre sikkerhet av dette»

«vi har sikkert 10 vurderinger av sesjonshåndtering»

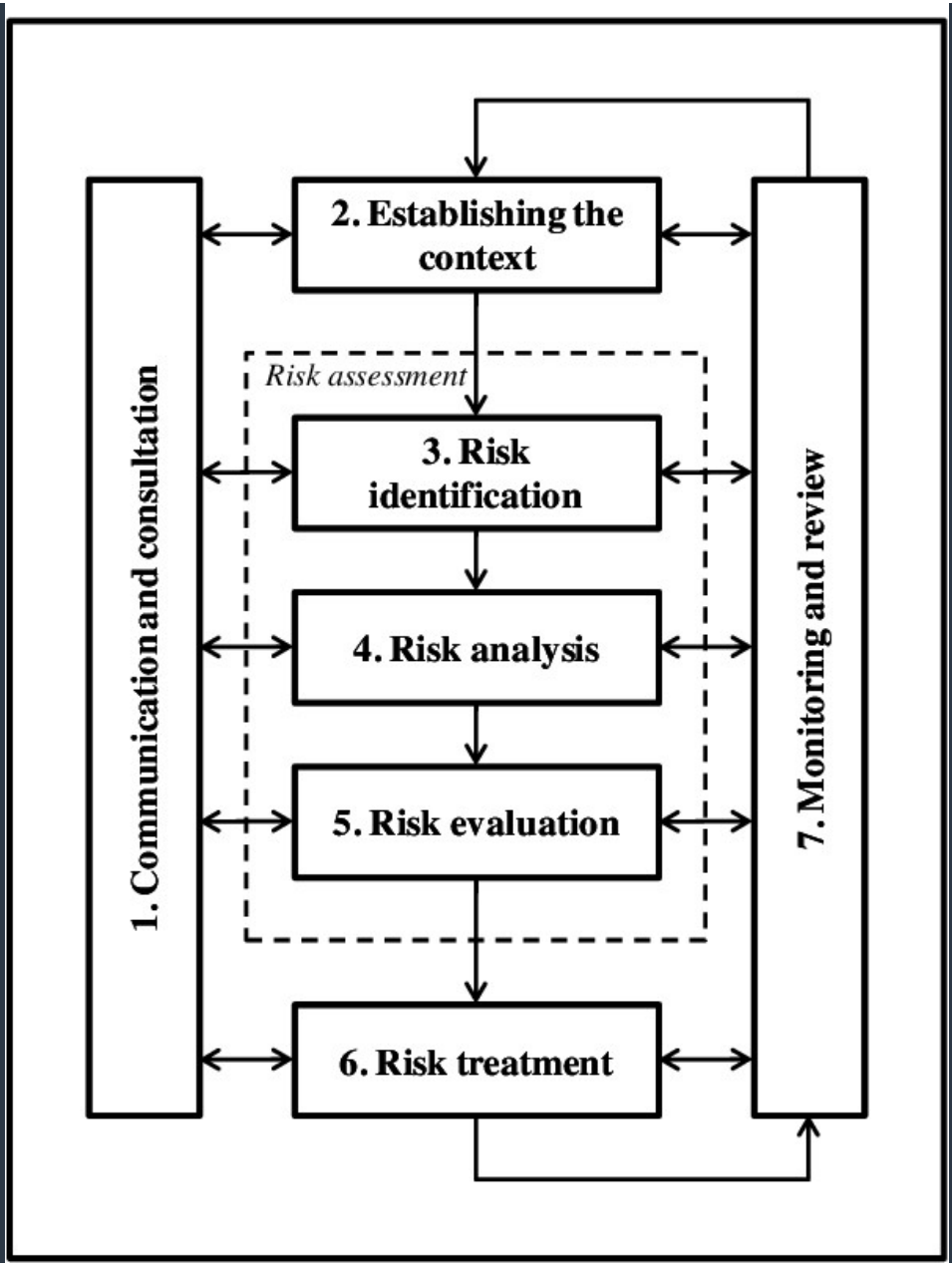
«kan vi lage en ROS som har større fokus på løsningens funksjonalitet?»

«må ROS’en ta så lang tid?»

Helsenorges økosystem



ISO 31000


2. Establishing the context
Risk assessment
3. Risk identification
4. Risk analysis
5. Risk evaluation
6. Risk treatment
1. Communication and consultation
7. Monitoring and review

RoS og Scenario analyser

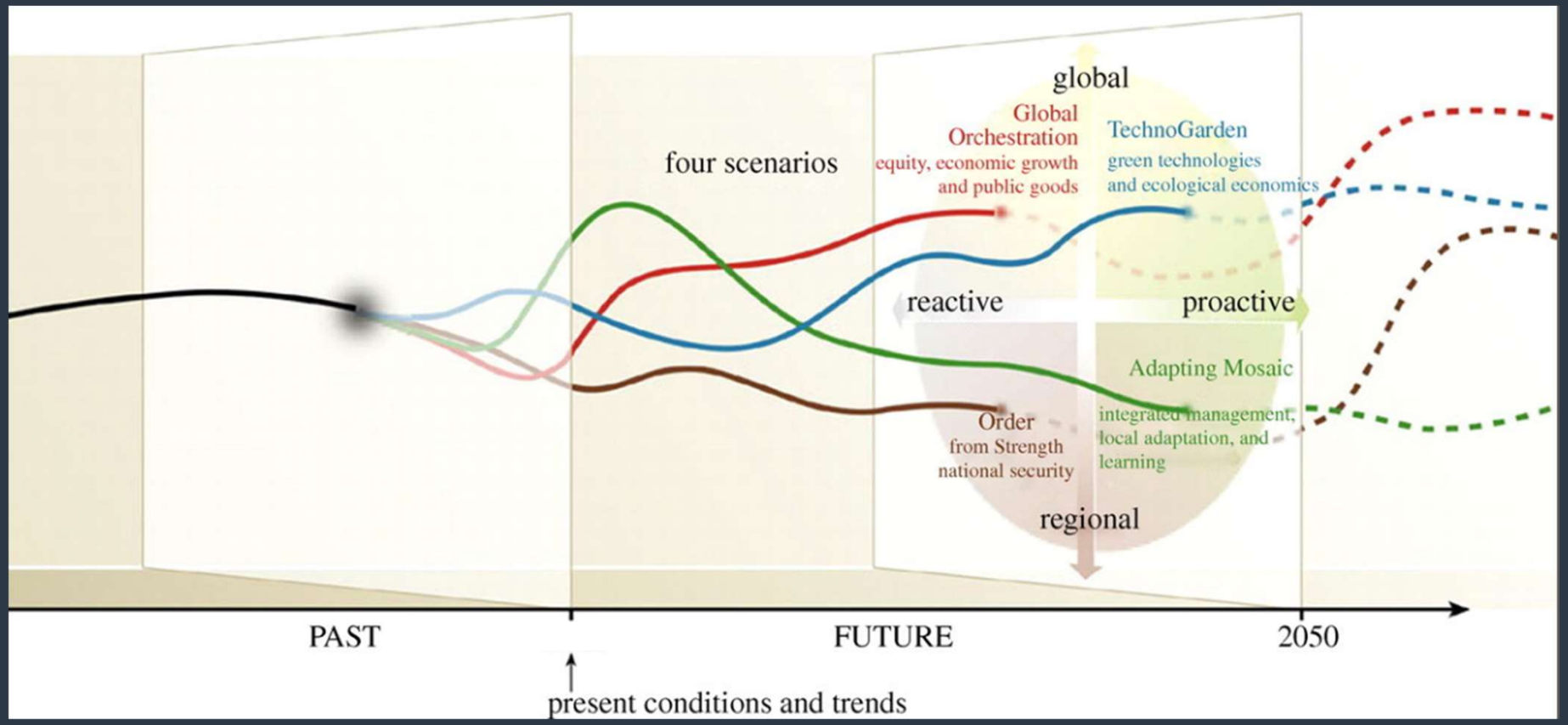
- Scenarios are hypothetical sequences of events constructed for the purpose of focusing attention on causal processes and decision-points. They answer two kinds of questions:

(1) Precisely how might some hypothetical situation come about, step by step? And

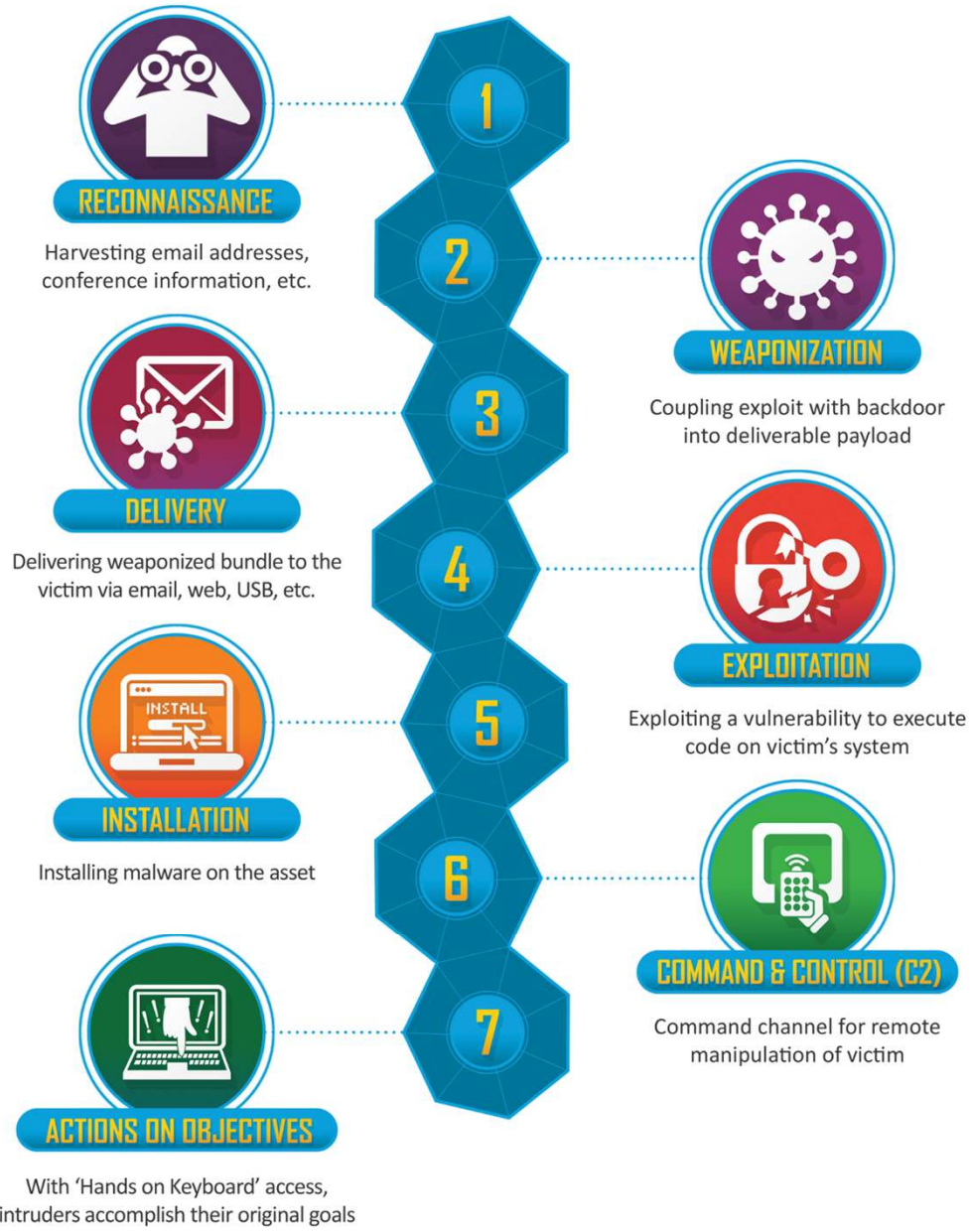
(2) What alternative exist, for each actor, at each step, preventing, diverting, or facilitating the process.

Kahn and Wiener, 1967

Nåtid og (*nær*) fremtid



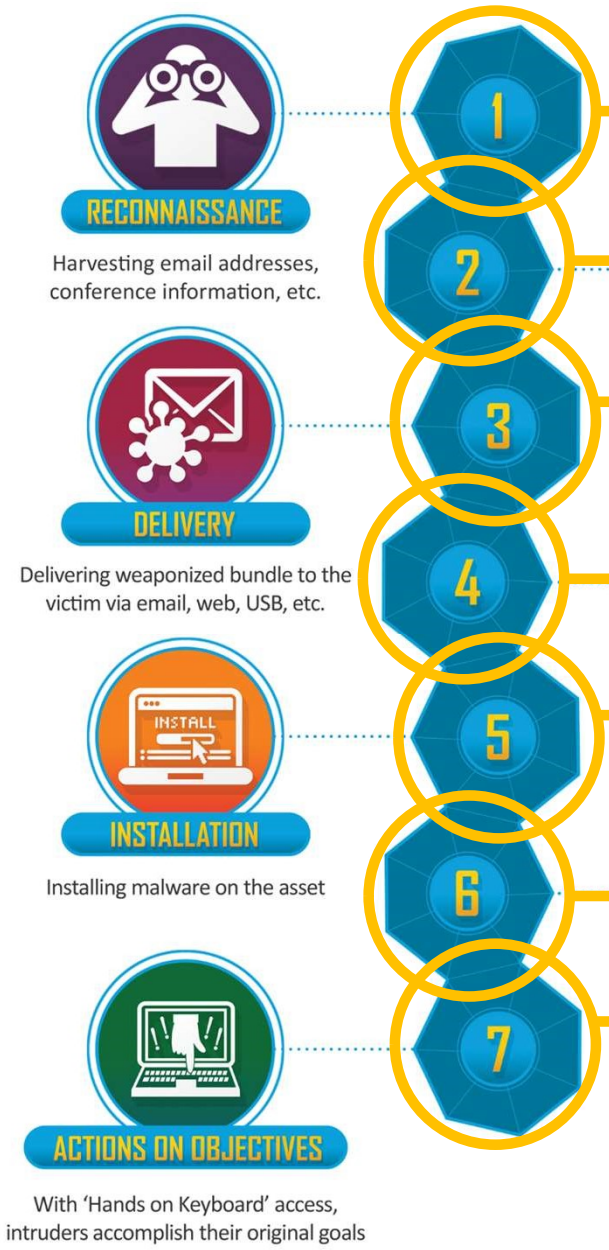
Kilde: Carpenter et al. (2005).



what is the

CYBER KILL CHAIN?

The cyber kill chain, created by Lockheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.



A: HelseCERT ser etter lekkede epost
B: Dark Web søk etter leverandørel

A: Utvikling av opensource verktøy
B: Sårbarhetsscannere
C: Pentests

A: Deteksjon av innbruddsforsøk, API, webfront
B: Phishing, deteksjon varsling av ansatte
C: Drive by infeksjoner

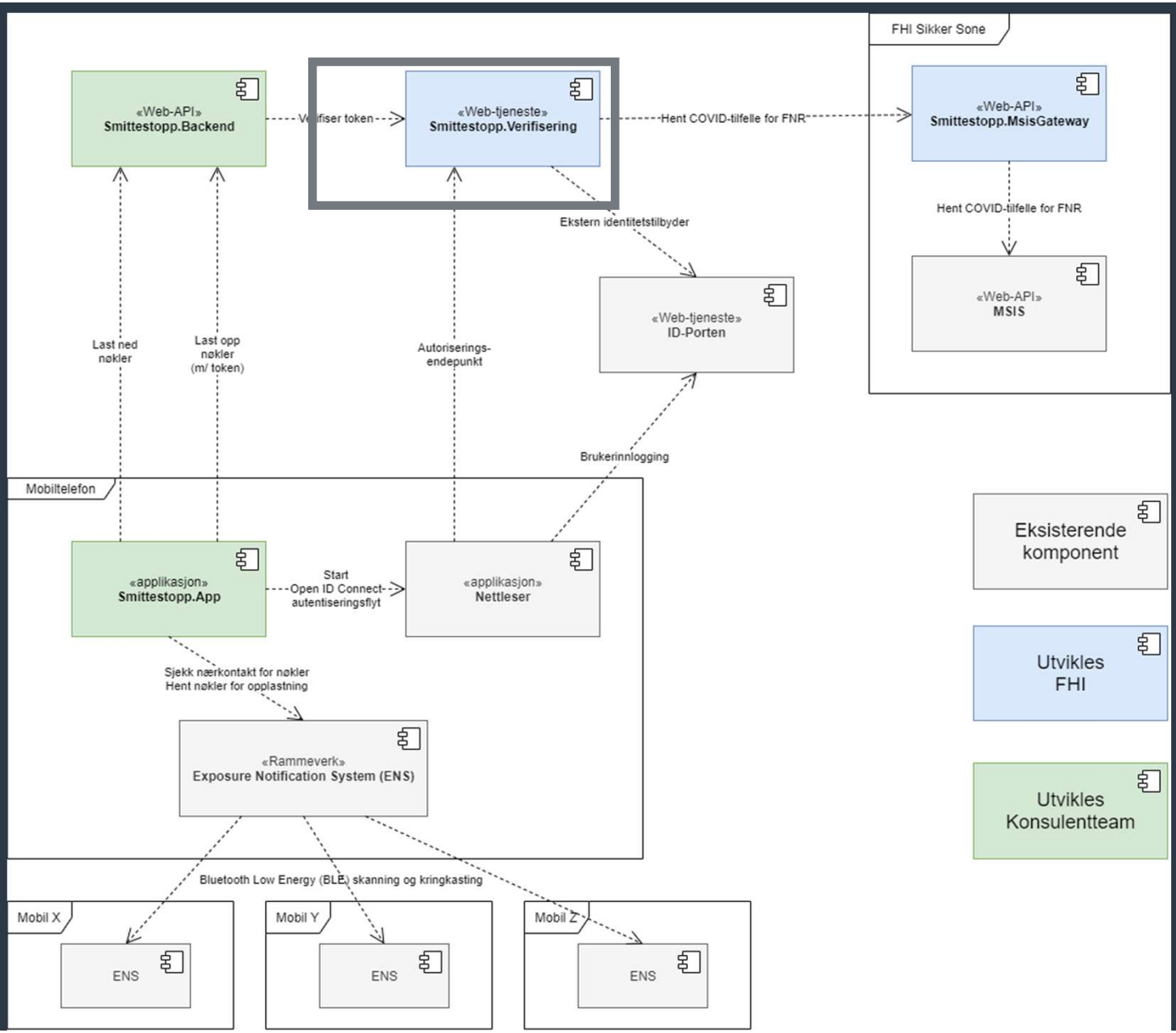
A: Sårbarheter
B: Input validering
C: Tjenester ikke autonome

A: Kode eksekveres på klient
B: Anomali, AV, SOC, loganalyse
C: Bruker varsler

A: Utgående kommunikasjon (SOC)
B: Deteksjon av kjente IP'er
C: Bruk av «allow list» på servere

A: Datalekkasje systemer
B: Ikke normale leseaktiviteter på sensitivt innhold
C: Tilgangskontroll

A: HelseCERT ser etter lekkede epost
B: Dark Web søk
A: Utvikling av opensource verktøy
B: Sårbarhetsscannere
C: Pentests
A: Deteksjon av innbruddsforsøk, API, webfront
B: Phishing, deteksjon varsling av ansatte
C: Drive by infeksjoner
A: Sårbarheter
B: Input validering
C: Tjenester ikke autonome
D: Innebygd personvern
A: Kode eksekveres på klient
B: Anomali, AV, SOC, loganalyse
C: Bruker varsler
A: Utgående kommunikasjon (SOC)
B: Deteksjon av kjente IP'er
C: Bruk av «allow list» på servere
A: Datalekkasje systemer
B: Ikke normale leseaktiviteter på sensitivt innhold
C: Tilgangskontroll


FHI Sikker Sone
«Web-API»
Smittestopp.Backend
Verifiser token
«Web-tjeneste»
Smittestopp.Verifisering
Hent COVID-tilfelle for FNR
«Web-API»
Smittestopp.MsisGateway
Hent COVID-tilfelle for FNR
«Web-API»
MSIS
Ekstern identitetstilbyder
«Web-tjeneste»
ID-Porten
Last ned nøkler
Last opp nøkler (m/ token)
Autoriserings-endepunkt
Brukerinnlogging
Mobiltelefon
«applikasjon»
Smittestopp.App
Start Open ID Connect-autentiseringsflyt
«applikasjon»
Nettleser
Sjekk nærkontakt for nøkler
Hent nøkler for opplastning
«Rammeverk»
Exposure Notification System (ENS)
Bluetooth Low Energy (BLE) skanning og kringkasting
Mobil X
ENS
Mobil Y
ENS
Mobil Z
ENS
Eksisterende komponent
Utvikles FHI
Utvikles Konsulentteam

Smittestopp status 25. januar

658.300 nedlastninger

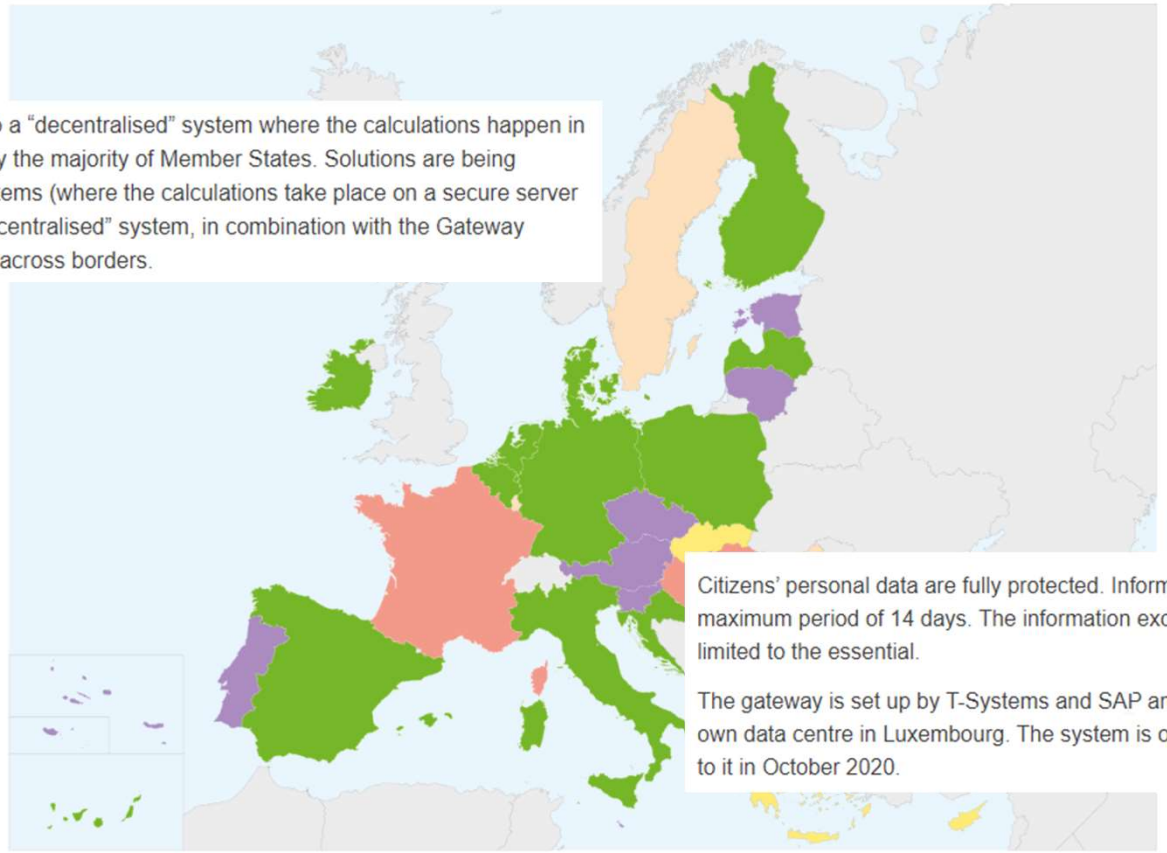
655 har meldt seg smittet

Oppdaterte tall på https://www.fhi.no/om/smittestopp/nokkeltall-fra-smittestopp/

Hva betyr endringen for oss?

https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic_en

Currently, this service works according to a "decentralised" system where the calculations happen in the user's app. This has been adopted by the majority of Member States. Solutions are being analysed to include the "centralized" systems (where the calculations take place on a secure server of the national health authority). This "decentralised" system, in combination with the Gateway Services enables these apps to be used across borders.



Citizens' personal data are fully protected. Information will only be stored in the gateway for a maximum period of 14 days. The information exchanged is fully pseudonymised, encrypted and limited to the essential.

The gateway is set up by T-Systems and SAP and the server itself is hosted in the Commission's own data centre in Luxembourg. The system is operational and the first national apps are connected to it in October 2020.

6.9 Tabell for vurdering av usikkerhet

Ettersom dette prosjektet er etablert på svært kort tid og inneholder stor grad av usikkerhet benyttes følgende skala for usikkerhetsvurdering i RoS-analysen og speiler på grad av bevis som er lagt frem. Skalaen definerer *kunnskapsstyrken* bak vurderingene som beskrives og tallfestes (epistemic uncertainty), og ikke iboende «naturgitt» usikkerhet til risikohendelse og dens årsakssammenheng og konsekvensrom (aleatory uncertainty).

Usikkerhets-beskrivelse	Grad av usikkerhet (konfidensintervaller)	Baysian probability [1](%)	IPCC skala[2]	Legal standard of proof
INGEN	10 (Helt sikkert)	100-99	Virtually certain	Virtually certain
	9	90-99	Very likely	Clear and convincing evidence
LAV	8	80-90		Clear showcase
	7	67-80	Likely	Substantial and credible evidence
	6	50-67	Medium likelihood	Preponderance of the evidence
MIDDELS	5	33-50		Clear indication
	4	20-33		Probably cause, reasonable belief
	3	10-20	Unlikely	Reasonable indication
HØY	2	1-10		Reasonable
	1	<1	Very unlikely	Inchoate hunch, fanciful conjecture
	0 (Helt usikkert)	0		Insufficient even to support a hunch or conjecture

Scenarier og tiltak

Bruk av appen oppfattes som obligatorisk og mange føler seg presset til å ta appen i bruk.

Norske myndigheter oppfordrer til nedlastning og bruk av appen, men presiserer at det er på frivillig basis. Andre offentlige organer, serveringssteder, butikker o.l., både i Norge og i utlandet, innfører krav og bevis på bruk av smittesporingsapper for å gi adgang/servering eller lignende. Kravene innføres på lik linje med at det tidligere har vært krav om registrering før servering på enkelte plasser.

Dette fører til at brukeren ikke opplever reell frivillighet, da det kontinuerlig kreves bevis på bruk av smittesporingsapplikasjon for å komme gjennom hverdagen, eksempelvis handle på butikken, delta på aktiviteter eller møte på arbeidsplassen. Brukere på reise/ tilreisende til Norge opplever heller ikke reell frivillighet fra myndigheter i EU da bruk av appen blir satt som et krav for økt mobilitet på tvers av grenser.

Konsekvensen av dette er misnøye blant brukerne og negative medieoppslag. Videre oppstår det en splittelse i befolkningen der noen nekter å bruke Smittestopp-appen. Utbredelsen av appen vil dermed reduseres, og virkningen av Smittestopp i sporingsarbeidet reduseres også. Nytteverdien av deling av smittesporingsdata på tvers av grenser i EU svekkes også betydelig med mindre utbredelse. Nytten ved digital smittesporing generelt og tillit til norske myndigheter vil svekkes.

Bruk av appen oppfattes som obligatorisk og mange føler seg presset til å ta appen i bruk.

A) Tydelig kommunikasjonsplan som fokuserer på frivillighetsaspektet ved applikasjonen og at den ikke skal benyttes som adgangskort til aktiviteter/steder.

B) Informasjonsdeling mellom EU-land for å sikre at formålet til smittesporingsapplikasjoner ikke blir utnyttet. Opprettholde god kommunikasjon og samlet strategi mellom EU-land.

Trusselaktør misbruker Smittestopp appen til å påvirke arrangement gjennom å tvinge en gruppe nordmenn i karantene/testing for å påvirke f.eks. et arrangement.

Trusselaktør ønsker å påvirke en kategori av nordmenns bevegelsesmønster for å videre påvirke utfallet av et arrangement. Over tid kartlegger trusselaktøren en gruppe mennesker som skal påvirkes til et ondsinnet formål. Gjennom diverse sosiale medier, åpne forum eller andre tilgjengelige kilder søker trusselaktøren informasjon som vil sette den i stand til å identifisere menneskene som skal påvirkes. Aktøren benytter seg av mulighetsrommet EU-Gateway åpner opp for og velger enten å bli smittet i Norge eller i sitt eget hjemland, tester seg og får positivt resultat. Aktøren sørger for enten i forkant eller etterkant å påtvinge nærkontakt med de i målgruppen sin og nærkontaktene blir varslet om at de har vært i kontakt med en smittet og må teste/gå i karantene.

Aktøren kan dermed påvirke f.eks.:

- planlagte demonstrasjoner,
- valg,
- viktige møter,
- forsamlinger,
- konkurrenter innen forskjellige bransjer, eller
- befolkningens tillit til myndighetens tiltak og deres effekt, både i Norge og EU-land.

Trusselaktør misbruker Smittestopp appen til å påvirke arrangement gjennom å tvinge en gruppe nordmenn i karantene/testing for å påvirke f.eks. et arrangement.

A. Autentisering av bruker for å laste opp diagnosenøkler.

B. Kontinuerlig trusselmonitorering for å identifisere nye trusselaktører og detektere mulige angrep.

C. Monitorering etter ikke-normale mønstre i brukeratferd og bevegelser.

D. Blokkere enkeltindivider som misbruker Smittestopp-appen. For å muliggjøre dette må man kunne detektere mønstre for å identifisere og stenge ute misbrukende enkeltbrukere. Det kan gjøres gjennom bruk og lagring av logger i en kort periode (14 dager), slik at mønstre kan detekteres. En avveining mellom dataminimering og håndteringsmulighet av misbruk må gjøres i forkant av denne beslutningen.

E. Etablere system for deling av trusseletterretning mellom EU-land.

Nedlastningstallet på smittesporingsapplikasjoner i EU-land er lav.

Nedlastningstallet på smittesporingsapplikasjoner i EU-land er lav. Dette resulterer i liten nytteverdi for digitalt smittesporingssamarbeid. Dette gjelder både innenlands og for sporingsarbeidet på tvers av grenser. Lav utbredelse av applikasjonene resulterer i høyere press på manuell smittesporing. Applikasjonen skaper en falsk trygghet hos brukere, og applikasjonene blir tatt ned og fjernet fra smittesporingsarbeidet på grunn av lav utbredelse.

Nedlastningstallet på smittesporingsapplikasjoner i EU-land er lav.

A. Kommunikasjonsmekanisme mellom medlemslandene som sikrer åpenhet og oppdaterte oppdateringer om endringer i hvert lands system.
B. Etablere en felles kommunkasjonskampanje i medlemsland.
C. Kontinuerlig utbedring av funksjonalitet.
D. Fremheve viktigheten av å bruke appen under pressekonferanser. Få politikere og fagpersoner til å nevne appen som et essensielt verktøy i smittesporingsarbeidet.

	Tittel	Trussel	Beste praksis	Etterlevelse basert på eksisterende tiltak. I henhold til beste praksis Tiltak eksisterer, men er ikke effektivt	Vurdering før ytterligere tiltak			Ytterligere tiltak (Føres inn i tiltaksliste)	Vurdering etter tiltak			Risikoeier H: Hovedansvarlig U: Utførende K: Konsulteres
R-1-6	Lav smittesporing og økt smitte blant innvandrere.	Norske myndigheter har fått kritikk[3] for å ikke nå ut med viktig informasjon om smitte og smittevernstiltak til innvandringsgrupper, noe som har ført til langvarig og økende Covid-19 smitte mange steder. Personer født utenfor Norge er overrepresentert blant de med påvist smitte og sykehusinnleggelser relatert til Covid-19. Mennesker som bor i Norge, men som i liten grad benytter seg av norske media, kan oppfatte det som svært utfordrende å oppdrive tilstrekkelig informasjon om Smittestopp. Dette gjelder både personer som bor fast i Norge, og personer som er i Norge for en periode. Med bakgrunn i den manglende informasjonen om smitte og smittevernstiltak, men spesielt rundt Smittestopp-appen, kan antallet nedlastinger blant visse innvandrermiljøer være lavt, fordi de ikke har fått informasjon om hvordan eller hvorfor dette skal gjøres. Dette kan føre til at den digitale smittesporing blant innvandrermiljøer med høy smitte ikke bidrar like effektivt inn i smittesporingsarbeidet. Dette kan på sikt få en negativ påvirkning på smittespredningen og smittesporingen i samfunnet generelt. EU Gateway koblingen kan føre til forvirring blant Europeere i Norge ved manglende informasjon om hvilket land sin app som bør brukes i hvilket tilfelle.	A) Ihht "Nasjonal Beredskapsplan Pandemisk Influensa"[4] skal det utarbeide en tydelig kommunikasjonsplan, som inkluderer: • Analysere det store bildet • Definere overordnet kommunikasjonsmål for Smittestopp • Definere kommunikasjonsmål per målgruppe • Definere passende kommunikasjonskanaler per målgruppe • Utarbeide hovedbudskapet • Utarbeide en tidslinje med nøkkelaktiviteter • Utvikle en trinnvis prosess som vil bli fulgt for å nå målet • Implementere planen • Gjennomføre revisjon av planen for å identifisere eventuelle forbedringsområder (hva fungerer, hva fungerer ikke) B) I henhold til DSB sine anbefalinger for god krisekommunikasjon[5] og "Nasjonal Beredskapsplan Pandemisk Influensa"[6] bør planen følge en		3	3	HØY	A), B) og C) FHI styrker kommunikasjonsevnen og iverksetter en mer målrettet og mer proaktiv kommunikasjonsstrategi for å forsikre at all relevant informasjon om pandemien og applikasjonen er lett tilgjengelig, på flere språk og kommuniseres via relevante interesseorganisasjoner slik at det også når de mest utsatte målgruppene.	1	2	MIDDELS	A) H: FHI, U: FHI/Dinamo, K: FHI, I: FHI B) H: FHI, U: FHI/Dinamo, K: FHI, I: FHI C) H: FHI, U: FHI/Hdir, K: Dinamo, I: FHI

Stående ROS | Scenarios | Tiltak | Arkitektur

Avgrensning: Alle | Kategori: Alle | Område: Alle | Kilde: Alle

Etterlevelse

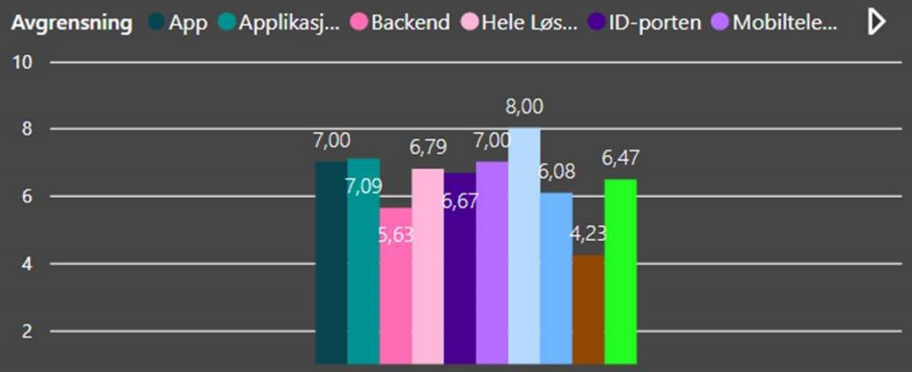
62%

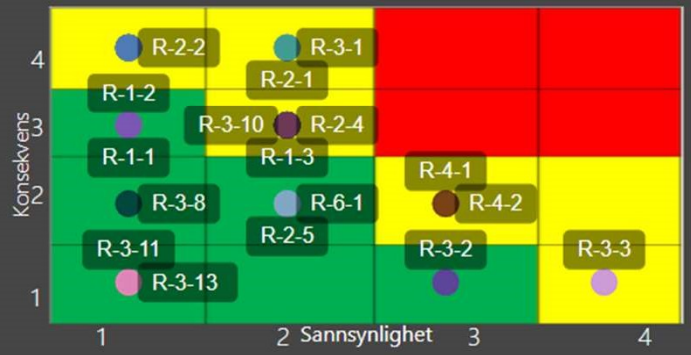
Etterlevelse
(etter beste praksis)

Usikkerhet

5,00

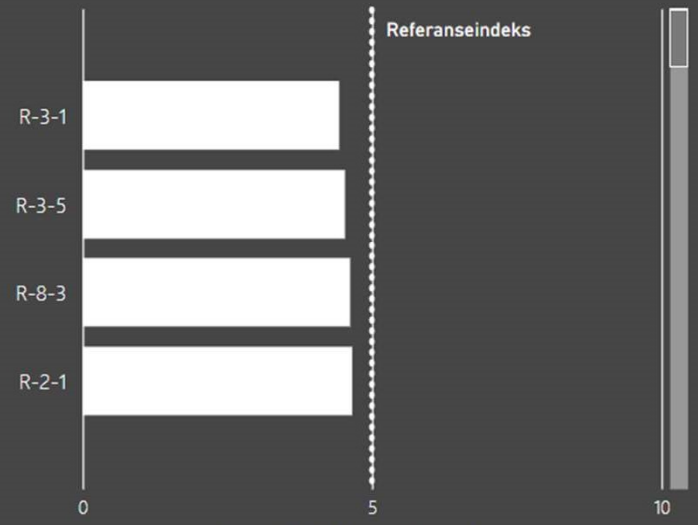
Gjennomsnittlig etterlevelse per avgrensning



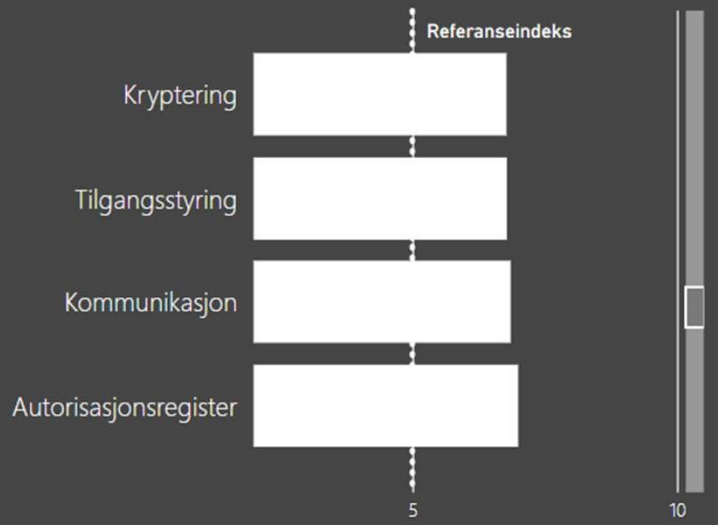


ID	Scenario
R-1-1	Misbruk av formålet med Smittestopp.
R-1-2	Formålets omfang øker til å inkludere eksempelvis andre offentlige organers bruk som ikke er i tråd med det originale formålet.
R-1-3	Mistillit til smittesporings applikasjoner resulterer i at en stor andel av befolkningen ikke tar i bruk appen.
R-2-1	Trusselaktører korrumperer diagnosenøkler ved å kompromittere backendløsningen til Smittestopp appen.
R-2-2	Person med tilgang til backendløsningen utnytter sin rolle og korrumperer data i backend.

Gjennomsnittlig etterlevelse per scenario



Gjennomsnittlig etterlevelse per kategori



Stående ROS Scenarios Tiltak **Arkitektur**

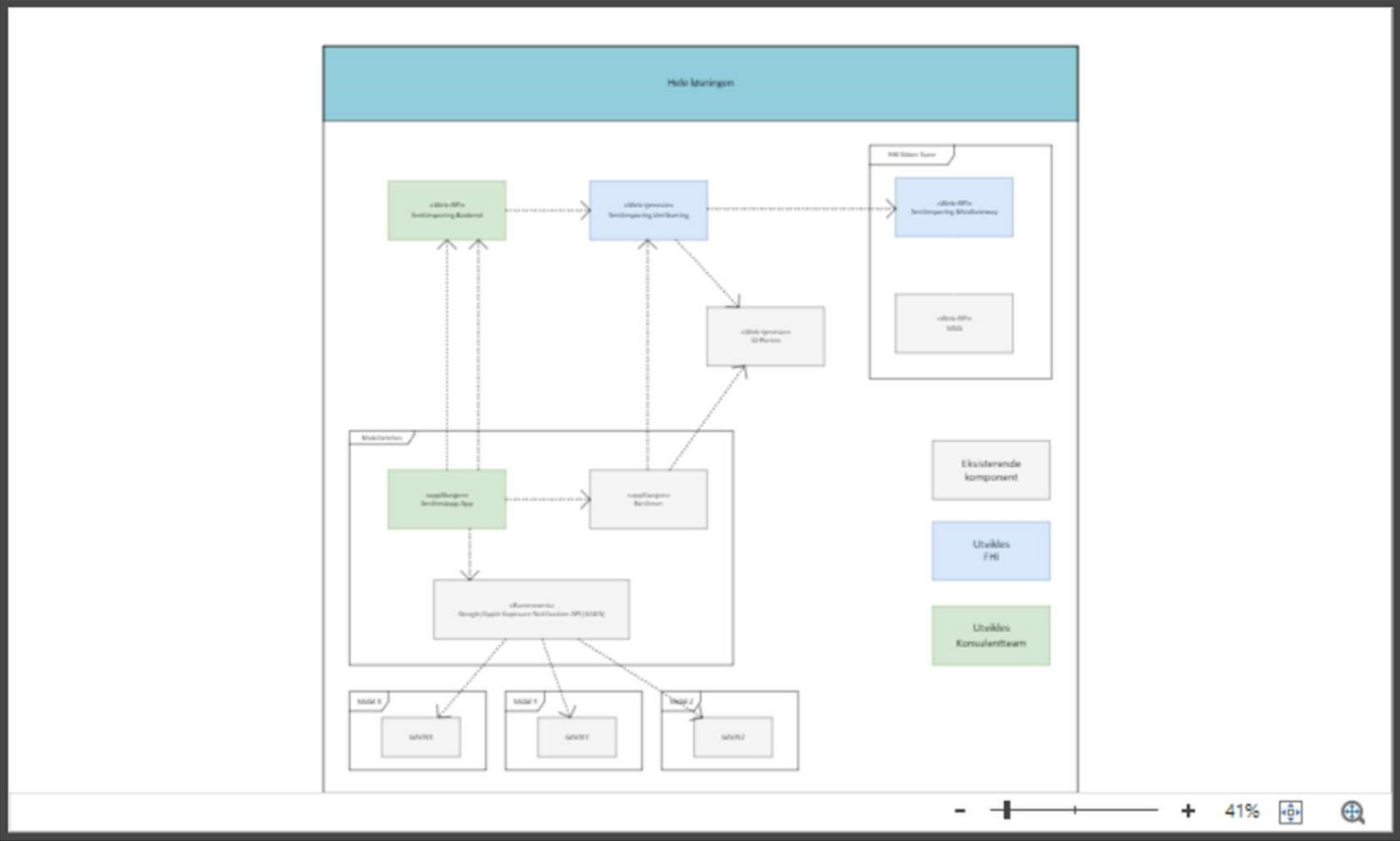
Område: Alle

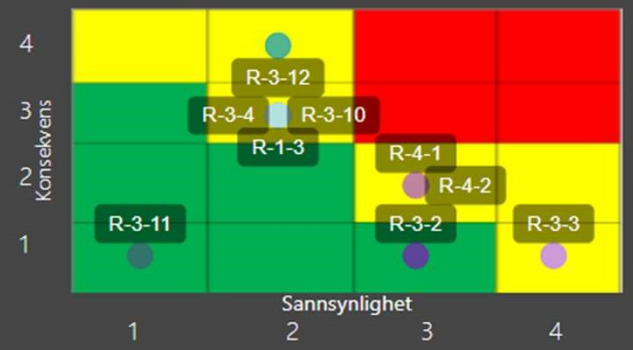
Kategori: Alle

Etterlevelse 6,24

Usikkerhet 5,00

Velg komponent





Scenarioer tilknyttet komponent

VariantID	Scenario
R-1-1	Misbruk av formålet med Smittestopp.
R-1-2	Formålets omfang øker til å inkludere eksempelvis andre offentlige organers bruk som ikke er i tråd med det originale formålet.
R-1-3	Mistillit til smittesporings applikasjoner resulterer i at en stor andel av befolkningen ikke tar i bruk appen.
R-2-1	Trusselaktører korrumperer diagnosenøkler ved å kompromittere backendløsningen til Smittestopp appen.
R-2-2	Person med tilgang til backendløsningen utnytter sin rolle og korrumperer data i backend.
R-2-3	Tilsiktet eller utilsiktet overføring av personopplysninger lagret i backend, ut av EU/EØS uten ytterligere tiltak, fører til