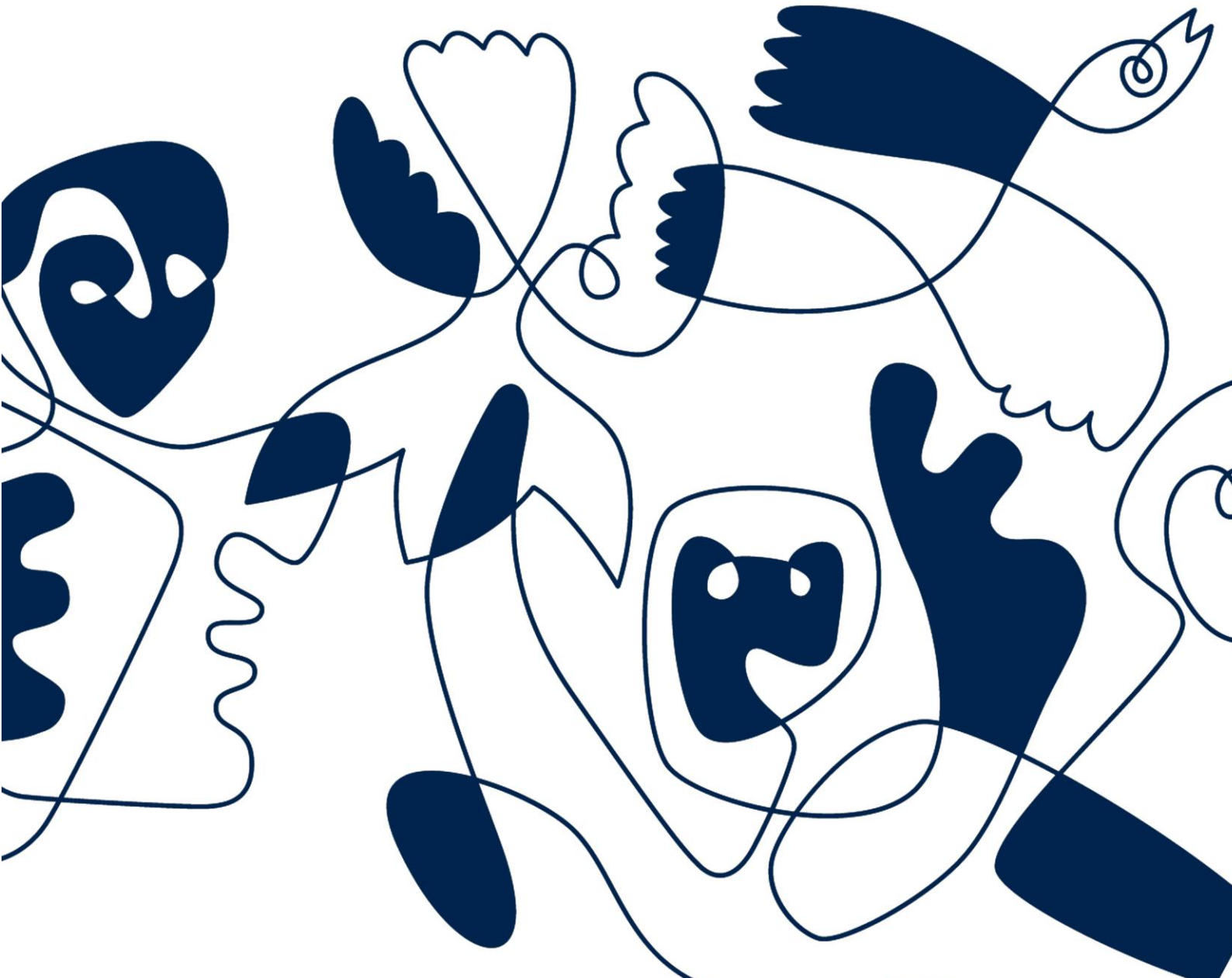
Statsforvalteren i Nordland

– virker til Nordlands beste

Evaluering av Øvelse Nordland 2021



Innhold

1.0 Innledning

Statsforvalteren i Nordland gjennomførte sin årlige krisehåndteringsøvelse i uke 4 i januar 2021. Øvelse Nordland er rettet mot kommunens øverste kriseledelse og har også vært gjennomført i 2016, 2017, 2018, 2019 og 2020.

Årets scenario var sammenfallende hendelser som bygget på pandemisituasjonen vi står i, og et dataangrep mot kommunens IKT systemer. Øvelsen ble gjennomført som en diskusjonsøvelse (table-top) med løpende innspill fra Statsforvalteren. 33 kommuner gjennomførte øvelsen. Ytterligere to kommuner var påmeldt, men måtte melde seg av kort tid før øvelsen grunnet håndtering av reelle hendelser.

2.0 Bakgrunn

Scenario for Øvelse Nordland har tidligere vært hentet ut av risiko- og sårbarhetsanalysen for Nordland fylke (FylkesROS Nordland).

I 2016 som diskusjonsøvelse med tema alvorlig voldhendelse i skole. I 2017 som spilløvelse med tema atomhendelse. I 2018 som diskusjonsøvelse med tema pandemi. I 2019 som diskusjonsøvelse med tema forurensning av drikkekilde, og i 2020 med diskusjonsøvelse rundt en storbrann på et fartøy plassert i sentrum av kommunen. Tilbakemeldingene fra kommunene på de foregående øvelsene har vært gode.

Årets tema er også inspirert av FylkesROS, men basert på faktiske hendelser i nyere tid.

Kommunene er gjennom forskrift for kommunal beredskapsplikt § 7 pålagt å øve kommunens overordnede beredskapsplan minimum annet hvert år. § 8 i samme forskrift pålegger kommunene en plikt til å evaluere øvelser og uønskede hendelser. Deltagelse og evaluering av denne øvelsen er dermed med på å oppfylle kommunens plikter etter lov og forskrift om kommunal beredskapsplikt.

3.0 Gjennomføring

3.1 Invitasjon

For å gi flest mulig kommuner mulighet til å delta ble det tilbudt to alternative øvingsdager, 26. og 28. januar 2021. Invitasjon til kommunene ble sendt ut 20. november 2020, etterfulgt av en påminnelse sendt 15. desember 2020. Det ble arrangert en ekstra øvelsesdag 4. februar for de som ikke kunne stille de planlagte dagene.

3.2 Deltagere

Tirsdag 26.01.21	Torsdag 28.01.21	Torsdag 04.01.21
Alstahaug	Bodø	Sortland
Andøy	Fauske	
Beiarn	Flakstad	
Bindal	Grane	
Brønnøy	Hamarøy	
Bø	Meløy	
Hadsel	Moskenes	
Hattfjelldal	Rana	
Lurøy	Saltdal	
Narvik	Sømna	
Vega	Øksnes	
Hemnes	Evenes	
Nesna	Leirfjord	
Røst	Rødøy	
Træna	Vestvågøy	
	Vevelstad	
	Værøy	

3.3 Øvingsmateriell

Alle kommuner fikk tilsendt øvingsdirektivet for øvelsen 19. januar 2021. Dette inneholdt praktisk informasjon om gjennomføring, scenariobeskrivelse og en del momenter til diskusjon under øvelsen. Hensikten med øvingsdirektivet var at deltagerne skulle få mulighet til å sette seg inn i scenario og problematikk på forhånd av gjennomføringen. På selve øvelsesdagen fikk deltakerkommunene tilsendt scenario og momentliste. Dette inneholdt gjentakelser av praktisk informasjon, og scenariobeskrivelser og en utvidet liste over diskusjonsmomenter.

3.4 Kompetanseløft

Den 21. januar 2021 ble det i forbindelse med øvelsen gjennomført to webinar for å øke kompetansen innenfor henholdsvis digital sikkerhet og bruken av krisehåndteringsverktøyet CIM.

For kompetanseøkning innenfor digital sikkerhet stilte Norsk Sikkerhetsmyndighet (NSM), Kommune-CSIRT, og Forening kommunal informasjonssikkerhet (KiNS) som foredragsholdere. Temaet for kompetansetimen var informasjonssikkerhet, situasjonsbildet, hendelseshåndtering og sikkerhetskultur. Målgruppen var kommunal kriseledelse, og det var omtrent 200 tilhørere på kurset. Tilbakemeldingen fra kommune var positive, og interessen for lignende kompetanseløft i fremtiden var stor.

Det andre webinaret var grunnleggende informasjon om CIM. Målgruppen var beredskapskoordinator i kommunene, spesielt de som ikke har brukt CIM mye tidligere. Det ble blant annet gått gjennom løsninger for loggføring, kontakter, meldinger, tiltakskort, rapporter og infotavler. Det var 83 tilhørere på dette webinaret. Statsforvalteren planlegger å gjennomføre flere slike samlinger om CIM, slik at brukerne får tilgang til et forum for erfaringsutveksling og kompetansebygging.

3.4 Gjennomføring på øvelsesdagen

Øvelsen ble gjennomført på følgende måte:

1. Varsling: Statsforvalteren sendte via DSB-CIM ut en varslingsepost til kommunenes beredskapsadresse samt ordfører, rådmann og beredskapskoordinator. Det ble også sendt til øvelsens kontaktpersoner. Kommuner uten egen beredskapsadresse fikk denne tilsendt postmottak. E-posten var satt opp med responsprofil slik at kommunene skulle kvittere på mottatt varsel via klikkbar lenke «melding mottatt». Ordfører, rådmann og beredskapskoordinator fikk i tillegg til epost også tilsendt SMS-varsel. Statsforvalteren sendte også e-poster til kontaktpersonene med oppdaterte varsel, informasjon om scenariet og fiktive tilbakemeldinger fra kommunale enheter under øvelsen.
2. Diskusjonsøvelse: Med bakgrunn i scenarioet og momentliste for diskusjon skulle kriseledelsen diskutere hvordan de ville håndtert situasjonen. Kriseledelsen skulle organisere seg selv og holde på så lenge de fant det formålstjenlig.
3. Evaluering: Evaluering av øvelsen skulle sendes til Statsforvalteren innen onsdag 29. januar 2021.

4.0 Scenario

4.1 Situasjon før øvelsen startet

Scenariet kjøres i reell tid. Det vil si at kommunene står i en pandemihåndtering, på valgt dato i januar 2021.

En uke før øvelsen ble flere kommuner i Troms og Finnmark, og i Oslo og Viken utsatt for dataangrep. Flere kommuneansattes personalopplysninger havnet på avveie, og skadeomfanget er fortsatt ikke kjent. I forbindelse med et pågående angrep, knyttet til innhenting av personopplysninger mot kommuner i Troms og Finnmark og Oslo og Viken, har NSM og Kommune-CSIRT sendt ut varsel til kommunene. Selv om det per nå ikke er kjent at flere kommuner har blitt angrepet, kan man ikke se bort fra at det vil kunne skje, og det anbefales at kommunene er ekstra observante og jobber forebyggende mot et mulig angrep.

4.2 Dreiebok og scenarioets utvikling

Under øvelsen sendte Statsforvalteren følgende innspill til kommunens kriseledelse:

09:00	Scenario med ny momentliste
Kommunene ble gitt noe tid før scenariet fikk innvirkning direkte på kommunen. Tanken bak dette var at kommunen skulle kunne bruke tid på å tenke på forebyggende tiltak og hvordan status på dette var i kommunen.	
09:20	Melding fra NRK
Kommunen fikk så et varsel om at personlig informasjon om ansatte var på avveie. Forskjellige typer informasjon var lekket (kontonummer, personnummer og innloggingsinformasjon) for å indikere at det ikke bare var ett system som var utsatt, og at innbruddet derfor kunne være omfattende	
09:30	Varsel fra fagorgan
Informasjon om angrepet og viruset fra fagorgan. Informasjonen var basert på et brev sendt i forbindelse med dataangrepet i Østre-Toten kort tid før øvelsen.	
09:40	Falsk epost # 1

Det ble så sendt e-post fra en falsk e-postadresse (sfnoovelse@gmail.com). Det ble brukt dårlig språk, og «Fylkesmannen» i stedet for «Statsforvalteren». Lenken som så ut til å gå til Fylkesmannens nettside ledet i stedet til skjema (Google Forms), der kommunene ble bedt om å fylle inn kontaktinformasjon om kriseledelsen. Også her ble det brukt dårlig språk, utdaterte/gale kommunelister, gale øvelsesdatoer osv.	
09:50	Råd fra Kripos
Kripos oppfordret kommunene om å være på vakt, blant annet mot ukjente/mistenkelige e-poster, og bruke tofaktor-autorisering.	
10:00	Oppdatert scenario - arkivansvarlig melder om løsepengevirus
Arkivansvarlig, rektor, leder på eldresenter og legevakten melder om at deres systemer var låste, og at de hadde fått krav om 15 millioner kroner i kryptovaluta.	
10:20	Mediehenvendelse
NRK ønsket svar på spørsmål om angrepet, omfanget, og hvordan det berører kommunen og innbyggerne.	
10:40	Statsforvalteren ber om situasjonsrapport
10:45	Falsk epost 2
Det ble så sendt en ny falsk e-post, denne med enda dårligere språk. Det ble bedt om at kriseledelsen fylte ut et nytt skjema, denne gang med kontonummer og koder, for å motta bonus som beste kommune.	
11:15	Frist situasjonsrapport
11:40	Datamaskiner og mobiltelefoner kan ikke benyttes
Kommunen fikk så en e-post om at angrepet er såpass omfattende at kommunens IT-systemer ikke kan benyttes, muligens så lenge som en uke.	
12:00	Øvelsen er over
Med påminnelse om evaluering.	

5.0 Målsetting og øvingsmomenter

5.1 Målsetting

Målsettingen med øvelsen var å øke deltakernes forståelse og evne til å håndtere en komplisert krisesituasjon gjennom åpen dialog og diskusjon. Målsettingen med øvelsen ble også illustrert med punkter:

Målsetting 1: Øke forståelsen for hvilke konsekvenser dataangrep kan medføre for kommunen.
Indikator: Opplever kriseledelsen at de har økt forståelse?
Målsetting 2: Øke deltakernes forståelse av eget ansvar og roller i kriseledelsen.
Indikator: Opplever deltakere at de kjenner egen og andres rolle bedre?
Målsetting 3: Øke kjennskap til, og øve bruk av egen beredskapsplan.
Indikator: Ble beredskapsplanen brukt under øvelsen?
Målsetting 4: Øke kjennskap til CIM

Indikator: Loggføring og rapportering til Statsforvalteren gjennom CIM.

5.2 Øvingsmomenter

Ved øvelsesstart ble det sendt ut en e-post gjennom CIM med scenarioet og noen øvingsmomenter for å igangsette diskusjon. Momentene var:

- Hva er trusselen?
- Hvilke risiko- og sårbarhetsreduserende tiltak har vi gjennomført/kan vi gjennomføre?
- Har vi en plan for dataangrep? Hva går den ut på? Når skal den iverksettes?
  - Kan vi løse dette selv? Hvem kan hjelpe? Når skal myndighetene varsles?
  - Kan vi be om hjelp fra nabokommuner? Kan de overta enkelte tjenester?
  - Hva gjør vi dersom dette blir langvarig?
- Har vi en plan for informasjon på avveie? Eller andre planer som kan benyttes for et slikt scenario?

5.3 Diskusjonspunkter

Det ble utformet en del punkter som skulle danne bakteppe for diskusjonene kommunene skulle gjennomføre. Disse punktene er også Statsforvalterens mulighet til å påvirke og sørge for at kommunene dekker de aspektene ved håndteringen som er ønskelig. Det ble i første omgang sendt ut en kortere liste med diskusjonspunkter som en del av øvingsdirektivet. Diskusjonspunktene var som følger:

- Hva er kommunens umiddelbare handling når det oppstår uønskede hendelser? Overordnet kriseledelse, sektor/etat?
- Hvilke rutiner/planer har kommunen for datasikkerhet, herunder vern av persondata og informasjonssikkerhet.
- Hvordan vil informasjonsbehovet hos egne ansatte og befolkningen håndteres?
- Hvordan vil en slik hendelse berøre kommunens oppgaver - helse og omsorg, barnehage, skole, teknisk?
- Er kommunens planverk godt nok for å håndtere denne typen hendelse? Trengs det oppdateringer? (Helhetlig ROS, overordnet beredskapsplan, planverk på sektornivå)
- Hvilke tiltak iverksettes? Hvordan informere om tiltakene?
- Hvordan er kommunens evne til å opprettholde normalfunksjon ved siden av krisehåndtering?

6.0 Sammendrag av kommunenes evaluering

Sammendraget av kommunenes evaluering presenteres her delt inn i hendelsens/krisens faser.

6.1 Initialfase

Generelt var kommunene godt forberedt til øvelsen ved blant annet å ha satt seg inn i øvelsesdirektivet, men også ved å ha deltatt på kompetanseløftet som ble arrangert en uke i forkant av øvelsen. Flere kommuner omtalte årets scenario som hensiktsmessig, men opplevde noen utfordringer knyttet til kunnskap og ressurser. I planleggingsfasen konkluderte flere at det var nødvendig å inkludere kommunens IKT avdeling for å ha best mulig forståelse for scenarioet. To kommuner meddelte at de raskt inkluderte IKT avd. da scenarioet krevde faglig kunnskap.

Varsling viste seg å være noe mer komplisert for noen kommuner når systemet deres sviktet. De med varslingssystemer som varsling24 og UMS opplevde ikke problemer med å få opplyst befolkningen. Kommuner som baserer seg på e-post og sosiale medier opplevde mer utfordring med å nå ut med informasjon. En digital hendelse er ofte svært omfattende og kan berøre sårbare grupper i samfunnet. Det er derfor svært viktig å nå ut med informasjon tidligst mulig.

6.2 Krisehåndtering og etterarbeid

Under øvelsen ble det sendt inn innspill fra Statsforvalteren. Flere kommuner meldte inn at innspillene bistod i å etablere gode diskusjoner i kriseledelsen. De «veiledet» når diskusjonen stod fast. Noen kommuner skrev at de opplevde innspillene som stressende for diskusjonen, hvor da noen viktige temaer ble avsluttet fortere enn ønsket. Færre innspill hadde vært mer givende.

Evalueringene tok for seg flere punkter som ble ansett som avgjørende for å kunne håndtere lignende hendelser i fremtiden. Det er her forsøkt å gi et samlet bilde av de viktigste punktene:

- IKT hendelser må håndteres med fagfolk, og kriseledelsen må etablere en oversikt over eksterne aktører som har spisskompetanse til å kunne bistå i krisehåndteringen.
- Kommunen må få på plass nødvendig planverk;
  - Hvilke tiltak som må iverksettes på hvilket tidspunkt (tiltakskort).
  - ROS-analyse og kriseplan: Herunder må det defineres hvilket ansvar de ulike avdelingene har, og hvilke roller kriseledelsen har under hendelseshåndteringen.
  - Kommunen må kartlegge hvilke oppgaver og tjenester som går inn under definisjonen kritisk samfunnsfunksjon, og som vil få konsekvenser av stor betydning om de mister tilgang til systemene sine.
- Etablere en god sikkerhetskultur i kommunens kriseledelse, men også generelt i organisasjonen.
- Stille krav til to—autentiseringssystem ved innlogging i kommunale digitale tjenester.
- Opprette et interkommunalt/ på tvers- samarbeid for å styrke kunnskap og ressurstilgang. (eks. IKT-Lofoten og Digitale Helgeland)
- Rutiner for mediehåndtering under krisehåndtering. Ha alternative mediekanaler for å kunne nå ut til flest mulig, raskest mulig med informasjon.

7.0 Statsforvalterens evaluering og oppfølgingspunkter

Kommunene ble varslet via e-post til beredskapsadresse, ordfører, rådmann og beredskapskoordinator, samt SMS til de tre sistnevnte. E-postene ble sendt ut med responsprofil for kvittering ved å trykke på lenken «melding mottatt». Over de tre dagene ble e-posten sendt til 111 mottakere, av disse kvitterte 93 på mottatt varsel (84 %). Minst en mottaker fra alle kommunene har bekreftet mottatt varsel. For Statsforvalteren er det svært viktig å vite at varsling fungerer og at informasjon når ut til de rette aktørene, dermed dobbelt varsling ved hjelp av e-post og SMS.

Det er vanskelig å forutse hvor belastende innspillene vil være, og hvor mye tid kommunene vil behøve for å diskutere problemstillingene. Dette vil nok også variere fra kommune til kommune. Statsforvalteren vil ta med i fremtidige øvelser at tid og innspill må være forenlig.

Under øvelsen ble det sendt ut to e-poster som skulle illustrere phishing. Avsenderadressen hadde likheter med Statsforvalterens øvelsese-post, men med noen synlige feil. Det var ikke indikert i øvingsdirektivet at andre epostadresser enn sfnoovelse@statsforvalteren.no skulle benyttes, eller at

det skulle innhentes informasjon gjennom slikt skjema. Intensjonen var å teste kriseledelsens evne til å registrere ukjente epostadresser. Flere kommuner trykte på lenken i e-posten, og fylte ut skjema. På det første skjemaet ble det sendt inn totalt 101 svar fra 20 kommuner. Det andre skjema var det ikke mulig å sende inn svar på. Flere kommuner oppdaget at e-postene ikke var ekte, og sendte spørsmål/rapport tilbake til Statsforvalteren. Flere kommuner poengterte i sin evaluering at dette var et kreativt trekk med mye læring.

8.0 Oppsummering

Generelt er Statsforvalteren fornøyd med at så mange kommuner tok seg tid til å øve i en svært krevende tid med krisehåndtering av korona. Oppsettet med kompetanseheving, diskusjonsøvelse med innspill og Phishing-eposter virket til å fungere godt. Intensjon var å løfte opp aktuelle og kjente problemstillinger innen digitale hendelser, samt skape en god diskusjon i kriseledelsen, noe vi anser som vellykket.

Kriseledelsene har i Øvelse Nordland 2021 kartlagt viktige elementer som må være til stede i kommunen for å etablere en akseptert risiko rundt digital sikkerhet. Øvelsen viser at det er svært komplekst å kunne ruste seg mot alt av digitale trusler, men man kan oppnå en aksept for hva som er «sikkert nok». Se tabell med samlet oversikt:

Identifiser:	*Skaff en oversikt over kritiske oppgaver og funksjoner i kommunen. Kartlegg hvilke risikoer som knyttes til oppgavene.*
Beskytt:	*Etabler en hensiktsmessig beskyttelse ovenfor oppgaver som trenger det.*
Oppdag:	*Etabler et system og en kultur i organisasjon som oppdager angrep og brudd i tide.*
Responder:	*Ha et planverk for å kunne respondere riktig og raskt.*
Normaliser:	*Ha planverk og ressurser til å gjenopprette en normalsituasjon etter et angrep.*