Deloitte.

Forvaltningsrevisjon av beredskap| Bergen kommune

Delrapport om cyberberedskap

September 2023

Forvaltningsrevisjon av beredskap -
delrapport om cyberberedskap

September 2023

Rapporten er utarbeidet for Bergen
kommune av Deloitte AS.

Deloitte AS
Postboks 6013 Postterminalen, 5892
Bergen
tlf: 55 21 81 00
www.deloitte.no

Sammendrag

Dette er første delrapport i et forvaltningsrevisjonsprosjekt om beredskap i Bergen kommune. Delrapporten omhandler cyberberedskap ved angrep som rammer kommunens saks- og arkivsystem Bk360. Prosjektet ble bestilt av kontrollutvalget i Bergen kommune i møte den 18. januar 2023 sak 10/23.

Forvaltningsrevisjonen består av fire delrapporter. I denne delrapporten er formålet å undersøke om kommunen er tilstrekkelig forberedt til å håndtere en situasjon der kommunens saks- og arkivsystem Bk360 rammes av et cyberangrep som gjør skade på arkivet og hindrer tilgang til systemet over en lengre periode.

I undersøkelsen er det gjennomført analyse av planer og rutiner, intervju med seks personer som er involvert i eller har ansvar for informasjonssikkerhet i ulike deler av kommunen. Oppdraget er gjennomført i tidsrommet februar til september 2023.

Kommunens tiltak for å forebygge cyberhendelser som kan ramme Bk360

Rolle og ansvarsbeskrivelser er utarbeidet for rollene innen informasjonssikkerhet og personvern i kommunen

Bergen kommune har utarbeidet gode og utfyllende rolle- og ansvarsbeskrivelse for rollene innen informasjonssikkerhet og personvern i kommunen, men det er Deloittes vurdering at det bør være enklere å finne frem til hvem som innehar de ulike rollene i organisasjonen. Ved å gjøre det enklere å finne frem til hvem som innehar ulike roller blir det tydelig hvem som har ansvar for spesifikke oppgaver og ansvarsområder innen informasjonssikkerhet og personvern. Dette vil også gjøre det enklere å finne frem til hvem som innehar hvilken beslutningsmyndighet og hvem som er ansvarlig for ulike aspekter av systemadministrasjon, brukerstøtte osv.

Roller og ansvarsbeskrivelse er utarbeidet i kommunens beredskapsplanverk

Undersøkelsen viser at det er tydelig hvilke roller som kan fatte beslutning på ulike nivå ved en hendelse. I kommunens planverk er det utarbeidet tydelige rollebeskrivelser for ledere med beslutningsmyndighet på ulike nivåer.

Det er etablert en egen vaktordning for ivaretagelse av krav til vakthold for å respondere på IKT-hendelser hele døgnet. Deloitte mener imidlertid at det vil være hensiktsmessig at eksisterende vaktordning også inkluderes i seksjon for digitalisering og innovasjon sin temaspesifikke beredskapsplan for informasjonssikkerhet og personvern.

For å ivareta døgnkontinuerlig drift (24/7) av ulike driftstjenester utenom ordinær arbeidstid, har kommunen etablert en egen vaktordning for personvern og informasjonssikkerhet. Vaktordningen består av et vaktlag som skal håndtere eventuelle hendelser innen personvern og informasjonssikkerhet som oppstår. Deloitte mener at vaktlagets oppgaver og ansvar bør fremgå i form av en rollebeskrivelse i kommunens beredskapsplanverk. Dette er viktig for å sikre hvilke oppgaver som skal gjennomføres nå og at varsling og håndtering av hendelsen blir effektiv. Rollebeskrivelsen bør også omtale hvordan vaktlaget skal håndtere hendelser i samspill med den øvrige beredskapsorganisasjonen.

Bergen kommune har ikke tilstrekkelig oversikt over konsekvensene ved bortfall av Bk360 eller andre virksomhetskritiske systemer, ettersom nødvendige analyser ikke er gjennomført.

Kommunen har ikke tilstrekkelig oversikt over konsekvensene ved bortfall av Bk360 eller andre virksomhetskritiske systemer. Dette er fordi kommunen ikke har gjennomført en Business Impact Analysis (BIA). Resultatene av en BIA vil gi viktig informasjon som kan brukes til å utforme en effektiv IKT-beredskapsplan og sikkerhetsstrategi. Ved å ha en klar forståelse av virkningen og konsekvensene av potensielle IKT-hendelser, kan organisasjonen utvikle passende gjenopprettingsstrategier, sikkerhetskontroller og beredskapstiltak for å sikre at de er i stand til å håndtere og respondere på uforutsette hendelser på en effektiv måte.

Kommunens planer for hvordan berørte deler av kommunens virksomhet skal opprettholdes ved bortfall av Bk360

Det overordnede beredskapsplanverket, herunder temaspesifikk beredskapsplan for svikt i informasjonssikkerhet og overordnet beredskapsplan – administrativ del, er godt utarbeidet. Planverket er strukturert på en slik måte at det kommer tydelig frem hvem som innehar beslutningsmyndighet på ulike nivå.

Samtidig er det risiko for at beredskapsplanverket ikke er tilstrekkelig kjent i beredskapsorganisasjonen i seksjon for digitalisering og innovasjon (SDI), spesielt på lavere nivå. Dette kan medfører en risiko for manglende forberedelser, manglende koordinering mellom de ulike nivåene, tap av verdifull tid i varsling og umiddelbar respons, sviktende og uklar ansvarsfordeling og utilstrekkelig opplæring og trening av beredskapsorganisasjonen.

Bergen kommune har et tilfredsstillende regime for klassifisering av alvorlighetsgrad for ulike cyberhendelser som kan inntreffe. Samtidig kan det være uheldig at det i klassifisering av hendelser brukes ulik skala i ulike deler av organisasjonen, ettersom dette kan føre til misforståelser og utydelig kommunikasjon mellom de ulike nivåene i organisasjonen.

Bergen kommune har planer for gjenoppretting etter en hendelse, men planene bør være mer spesifikke

Til tross for at det er utarbeidet en oversikt over akseptabel nedetid for Bk360 i det digitale beredskapsplanverket og katastrofegjenopprettingsplanene, finnes det ingen systemspesifikke planer for gjenoppretting av enkeltsystem. Akseptabel nedetid defineres gjennom en konsekvensvurdering av ulike kjerneprosesser. En konsekvensvurdering av ulike kjerneprosesser blir vanligvis dekket av en Business Impact analysis (BIA), noe som mangler i kommunen. Det er derfor ukjent hva som ligger til grunn for vurderingen av konsekvens og akseptabel nedetid på under en time for BK360.

Det digitale beredskapsplanverket i kommunen vil kunne ivareta gjenopprettingen på en god måte, men kan etter Deloittes vurdering likevel forbedres. Grunnen til dette er at Bergen kommune har ikke full oversikt over hvordan en hendelse som berører BK360 vil påvirke driften av kommunen. Ved å utarbeide en Business Impact Analysis (BIA) vil man få en økt forståelse av de ulike konsekvensene og man vil kunne ta informerte og gode beslutninger i hendelseshåndteringen og gjenopprettingen basert på et godt informasjonsgrunnlag. I forlengelse av dette anbefaler Deloitte at det utarbeides systemspesifikke planer for å ivareta gjenopprettingen på en god måte. Dette vil sikre en trinnvis og tilpasset veiledning som vil bidra til en effektiv og rask gjenoppretting. Dagens digitale beredskapsverk dekker ikke dette behovet og fremstår som for generelle.

Kommunens primære kommunikasjonsløsning er ikke tydelig

Bergen kommune har etter Deloittes vurdering gode kommunikasjonskanaler som skal benyttes i forbindelse med hendelser. Krisehåndteringsverktøyet RAVYN sikrer et felles verktøy for distribuering av kommunikasjon og samhandling blant de som er involvert i hendelseshåndteringen på overordnet nivå. Deloitte vil samtidig fremheve at RAYVN er et krisehåndteringsverktøy som primært benyttes på strategisk nivå. På operasjonelt og taktisk nivå (det vil si seksjon for digitalisering og innovasjon, SDI) og på de ulike driftsenhetene, er ikke RAYVN etablert som primært verktøy for hendelseshåndtering, men også her er det etablert gode prosesser for når og hvem som skal varsler internt og eksternt.

Deloitte mener imidlertid at det er en risiko for at det ikke er en felles forståelse for hva som er primærløsning for kommunikasjon ved en hendelse som tar ned IT-systemene. Grunnen til dette er at det ikke er samsvar mellom de kommunikasjonsløsningene som benyttes av den kommunale kriseledelsen og de løsningene som planverket slår fast at skal benyttes på lavere nivå (operasjonelt og taktisk nivå). I en innledende fase av håndteringen av en cyberhendelse er det viktig å opprette kommunikasjon slik at man raskt får koordinert responsen. Når det er uklart hvilke kommunikasjonsløsninger som skal benyttes, gir det en økt risiko for at den innledende responsen blir forsinket.

Bergen kommune har mangelfulle avtaler med tredjeparter for å ivareta hendelseshåndteringen

I kommunens eksisterende beredskapsplanverk blir det henvist til et Incident Response Team (IRT), selv om dette per dags dato ikke inngår i kommunens beredskap. Å henvise til ikke-eksisterende ressurser skaper falsk trygghet. Konsekvensen av dette er at man i en hendelse kan risikere å belage seg på ressurser som i realiteten ikke er tilgjengelige. Dette fører til en økt risiko for at hendelsen ikke blir løst så effektivt som den potensielt kunne ha blitt.

Deloitte kan heller ikke se at det er utarbeidet spesifikke avtaler med leverandøren av Bk360 for å sikre seg bistand i håndtering av hendelser. Dette kan bidra til å sikre rask respons, tydelig ansvarsfordeling, kontinuerlig forbedring og effektiv hendelseshåndtering.

Kommunens etterleving av egne rutiner for gjennomføring av øvelser og test av beredskapsplanverk

Kommunen gjennomførte øvelser i 2014 og i 2022 som rettet oppmerksomheten mot svikt i informasjonssikkerhet. Kommunens rutiner legger imidlertid opp til at dette skal gjennomføres årlig. Deloitte mener derfor at Bergen kommune ikke etterlever kravene til opplæring og øving av personell i henhold til beskrivelse i eget beredskapsplanverk.

At det ikke blir gjennomført øvelser der de ulike rollene som inngår i SDI sitt eget beredskapsplanverk blir testet, fører dessuten til risiko for manglende forberedelse til og dermed redusert effektivitet i hendelseshåndteringen. Det kan videre gi risiko for sviktende samhandling på ulike nivå og manglende oppdatering og verifisering av eget planverk basert på læring fra øvelsene.

Basert på funn og vurderinger i undersøkelsen kommer Deloitte med noen anbefalinger til kommunen i kapittel 6 i rapporten.

Innhold

Figurer

Tabeller

1 Innledning

1.1 Bakgrunn

Dette er en av fire delrapporter i et forvaltningsrevisjonsprosjekt om beredskap i Bergen kommune. Delrapporten omhandler cyberberedskap ved angrep som rammer kommunens saks- og arkivsystem Bk360. De andre delrapportene i prosjektet vil omhandle beredskap knyttet til radioaktiv forurensning som påvirker kommunens tjenesteytende arbeid, pågående livstruende vold (PLIVO) som rammer skolene og vedlikehold av tilfluktsrom. Prosjektet ble bestilt av kontrollutvalget i Bergen kommune i møte den 18. januar 2023 sak 10/23.

1.2 Formål

Beredskap er definert som planlagte og forberedte tiltak som gjør oss i stand til å håndtere hendelser og redusere konsekvenser av det inntrufne (Meld. St. 10 – Risiko i et trygt samfunn, s. 22). Kommunal beredskap innebærer å ha oppdaterte planverk, prosedyrer og samarbeidsrutiner som gir klare føringer og instrukser om hva kommunen skal gjøre dersom en krise inntreffer. Beredskap innebærer også ha tilstrekkelig med materiell og ressurser som kan bidra til å håndtere hendelser som inntreffer.

I Bergen kommune er det utarbeidet en overordnet risiko- og sårbarhetsanalyse (ROS-analyse)[1] som skal beskrive overordnet risiko for Bergen. ROS-analysen kartlegger hvilke uønskede hendelser som kan inntreffe i kommunen og vurderer sannsynlighet for at disse hendelsene inntreffer og hvordan de i så fall kan påvirke kommunen. ROS-sanalysen skal legges til grunn for kommunens arbeid med samfunnssikkerhet og beredskap.

I dette prosjektet er det tatt utgangspunkt i tre mulige hendelser identifisert i ROS-analysen for Bergen for å undersøke om kommunens beredskapsarbeid er tilfredsstillende. I denne delrapporten er formålet å undersøke om kommunen er tilstrekkelig forberedt til å håndtere følgende mulige hendelse:

1 H-24 Svikt i informasjonssikkerhet:

> Svikt i informasjonssikkerhet kan være at informasjon kommer på avveier, blir endret eller utilgjengelig. Svikt kan oppstå ulike steder i nettverksinfrastrukturen og IKT systemene. Innbyggere eller samfunn vil ikke alltid bli direkte berørt, men følgehendelser kan føre til redusert eller bortfall av en forventet tjeneste.
>
> *Vi ser på følgende mulige hendelse: Kommunens saks- og arkivsystem Bk360 rammes av[2] et cyberangrep som gjør skade på arkivet og hindrer tilgang til systemet over en lengre periode*.

1.3 Problemstillinger

Denne delrapporten omhandler følgende problemstilling med underproblemstillinger:

Har Bergen kommune etablert tilstrekkelig beredskap for følgende mulige hendelse: Kommunens saks- og arkivsystem Bk360 utsettes for et cyberangrep som gjør skade på arkivet og hindrer tilgang til systemet over en lengre periode. Under dette:

a) Har kommunen identifisert tiltak for å forebygge cyberhendelser som kan ramme Bk360 og iverksatt disse?
b) Har kommunen tilfredsstillende planer for hvordan berørte deler av kommunens virksomhet skal opprettholdes ved bortfall av Bk360?
c) Har kommunen øvd på å håndtere en cyberhendelse som kan ramme Bk360?

---

1 Bergen-ROS-2020-Bergen-en-trygg-by-for-fremtiden-Rapport-fra-arbeidsprosessen-med-revisjon-av-helhetlig-risiko-og-sabarhetsanalyse-for-Bergen-docx (5).PDF

2 Opprinnelig formulering var «utsettes for». Endret til «rammes av» for å få frem at et cybrangrep ikke nødvendigvis er rettet direkte mot Bk360, men mot kommunen slik at Bk360 rammes.

1.4 Avgrensning

Deloitte har lagt vekt på utvalgte kontroller og krav som er definert i Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet. Dette er i tråd med Bergen kommunes egen Temaplan for informasjonssikkerhet og personvern der kommunen forplikter seg til å følge NSM sine grunnprinsipper, sammen med kommunens vedtatte rammeverk for risikostyring.

1.5 Metode

Oppdraget er utført i samsvar med gjeldende standard for forvaltningsrevisjon (RSK 001) og kvalitetssikret i samsvar med kravene til kvalitetssikring i Deloitte Policy Manual (DPM).

Oppdraget er gjennomført i tidsrommet februar 2023 til juni 2023.

1.5.1 Dokumentanalyse

Informasjon om Bergen kommune sitt styringssystem for personvern og informasjonssikkerhet og dokumentasjon på etterlevelse av interne rutiner, regelverk mm. blitt samlet inn og analysert. Innsamlet dokumentasjon har blitt vurdert opp mot revisjonskriteriene. Dokumentanalysen har blitt gjennomført løpende, slik at også dokumenter som har blitt utarbeidet under prosjektperioden har blitt analysert.

1.5.2 Intervju

For å få supplerende informasjon til de skriftlige kildene, har Deloitte intervjuet utvalgte personer i Bergen kommune som er involvert i eller har ansvar for informasjonssikkerhet i ulike deler av organisasjonen. Deloitte har intervjuet totalt seks personer.

1.5.3 Verifiseringsprosesser

Oppsummering av intervju er sendt til de som er intervjuet for verifisering og det er informasjon fra de verifiserte intervjureferatene som er benyttet i rapporten.

Datadelen av rapporten er sendt til kommunen for verifisering, og rapportens datadeler er justert på bakgrunn av tilbakemeldinger. Byrådens høringsuttalelse er lagt ved rapporten i vedlegg 1.

1.6 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal bli vurdert opp mot. Kriteriene er utledet fra autoritative kilder i samsvar med kravene i gjeldende standard for forvaltningsrevisjon. I dette prosjektet er revisjonskriteriene i hovedsak hentet fra Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet. Kriteriene er nærmere presentert innledningsvis under hvert tema, og i vedlegg 2.

2 Om Bk360, organisering og styring av informasjonssikkerheten i kommunen

2.1 Saks- og arkivsystemet Bk360

Bk360 er Bergen kommunes løsning for administrativ og politisk saksbehandling og arkivering. I tillegg til at Bk360 benyttes til behandling av interne saker og dokumenter, publiseres det offentlig journal, politiske saker og dokumenter til kommuneportalen gjennom Bk360. Bk360 er organisert med arkiv for de ulike sakene og fagspesifikke spesialarkiv som deles mellom flere enheter. I tillegg finnes spesialarkiv for enkelte avdelinger eller fagområder.

Hensikten med Bk360 er å sikre samhandling og felles rutiner for journalføring, lagring og gjenfinning av informasjon. Dette sikrer igjen at informasjon forvaltes i tråd med regelverket og blir arkivert for ettertiden. Det gjelder særlig for journal- og arkivpliktig dokumentasjon som er resultat av en saksbehandling. Fra kommunen blir det vist til at BK360 skal sikre etterlevelse av lovverk som arkivlov, forvaltningslov og offentlighetsloven med forskrifter.

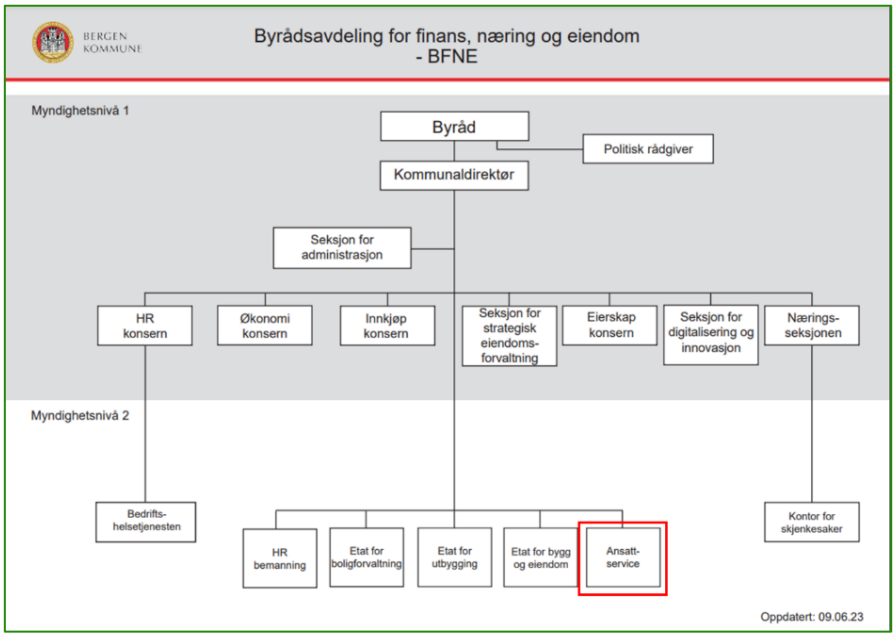
2.2 Organisering

Bk360 er driftet og forvaltet av Ansattservice i byrådsavdelingen for finans, næring og eiendom (BFNE)[3]. Bk360 er en del av Bergen kommunes datasenter og underlagt de til enhver tid gjeldende krav og retningslinjer for etablering, drift og forvaltning av IKT-systemer i kommunen. Det er Ansattservice som har all konfigurasjonsstyring[4] og kontroll med datasenter med tilhørende infrastruktur. Figuren under viser organiseringen av byrådsavdeling for finans, næring og eiendom.

[3] https://allmenningen.bergen.kommune.no/styringsdokument/SD-18-1125

[4] Prosessen med å identifisere, organisere og kontrollerer konfigurasjonen av IT-systemer, inkludert maskinvare, programvare, nettverk og relaterte komponenter.

Figur 1 Organisering av Byrådsavdeling for finans, næring og eiendom - BFNE



2.3 Styringssystem for personvern og informasjonssikkerhet

Bergen kommune har etablert et styringssystem for personvern og informasjonssikkerhet[5] for å sikre en systematisk måte å planlegge, gjennomføre, evaluere og korriger arbeidet som gjøres i kommunen innen personvern og informasjonssikkerhet. Bakgrunnen for dette er å sikre at krav fastsatt i lover, forskrifter og interne prosedyrer og reglement etterleves.

Et styringssystem består av et dokumenthierarki og deles inn i styrende, gjennomførende og kontrollerende dokumenter. I Bergen kommune består styringssystemet for personvern og informasjonssikkerhet av et reglement med tilhørende prosedyrer. Figuren under gir en oversikt over styringssystemet i kommunen:

Figur 2 Oppbygning av styringssystem for personvern og informasjonssikkerhet[6]

Dokumentkategori	Dokument	Forklaring	Eksempel på dokumenter
Styrende dokumenter	Reglement	Stiller krav og fastsetter plikter for ulike roller	Reglement for digitalisering og IKT i Bergen kommune Temaplan for informasjonssikkerhet og personvern i Bergen kommune Overordnet beredskapsplan for Bergen kommune – Administrativ del

[5] https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/personvern-og-informasjonssikkerhet/styringssystem-for-personvern-og-informasjonssikkerhet
[6] https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/personvern-og-informasjonssikkerhet/styringssystem-for-personvern-og-informasjonssikkerhet

			Temaspesifikk beredskapsplan for svikt i informasjonssikkerhet
Gjennomførende dokumenter	Prosedyrer	Prosedyrer, verdivurdering og klassifisering av informasjon og informasjonssikkerhet	Overordnet prosedyre for verdivurdering/risiko og konsekvensvurdering og klassifisering av informasjon og informasjonssikkerhet
			Styringsavtale for digitalisering- og IKT tjenester i Bergen kommune
Øvrige	Øvrige	Inneholder alle IKT Driftstjenesteavtaler og liste over fleste IT-tjenester og fagsystemer som er i bruk i kommunen i dag	Tjenestekatalog
Øvrige	Øvrige	Oppdage risikoer og tilhørende tiltak, og for å prioritere ressurser på best mulig måte	Risiko- og sårbarhetsanalyse BK360

I vedlegg 3 gir vi nærmere informasjon om de ulike styrende dokumentene i kommunens styringssystem for personvern og informasjonssikkerhet.

3 Identifisering av forebyggende tiltak for cyberhendelser

3.1 Problemstilling

I dette kapittelet vil vi svare på følgende problemstilling med underproblemstilling:

Har Bergen kommune etablert tilstrekkelig beredskap for følgende mulige hendelse: Kommunens saks- og arkivsystem Bk360 utsettes for et cyberangrep som gjør skade på arkivet og hindrer tilgang til systemet over en lengre periode. Under dette:

- *Har kommunen identifisert tiltak for å forebygge cyberhendelser som kan ramme Bk360 og iverksatt disse?*

3.2 Revisjonskriterier

Når det skjer alvorlige uønskede hendelser som ikke effektivt nok kan håndteres i den ordinære driften, mobiliserer beredskapsorganisasjonen for å håndtere dem. Beredskapsorganisasjonen benytter beredskapsplanene som støtte i sitt arbeid for å forhindre at farehendelser får utvikle seg til uønskede hendelser eller for å redusere konsekvensene av uønskede hendelser som har oppstått.

En viktig del av beredskapen og hendelseshåndteringen i kommunen er tydelige rolle- og ansvarsbeskrivelser for involvert personell. Dette vil bidra til effektivt samarbeid og koordinering på alle nivå. Det vil også bidra til rask respons ved at de ulike rollene vet hva som skal gjøres og hvilke oppgaver den enkelte er ansvarlig for. I tillegg bidrar det til effektiv kommunikasjon gjennom tydelige kommunikasjonslinjer.

Når hendelsen først inntreffer er det viktig at kommunen også har analysert potensielle konsekvenser for virksomheten og på forhånd vurdert hvilke prosesser som blir berørt og hvordan kommunen skal prioritere mellom ulike funksjoner og prosesser som er viktig og kritisk for å opprettholde kommunens drift.

Deloitte har lagt vekt på utvalgte kontroller og krav som er definert i Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for IKT-sikkerhet. Dette er i tråd med Bergen kommune sin egen Temaplan for informasjonssikkerhet og personvern der kommunen forplikter seg til å følge NSM sine grunnprinsipper, sammen med kommunens vedtatte rammeverk for risikostyring. Basert på krav i NSMs grunnprinsipper for IKT-sikkerhet har Deloitte utledet følgende revisjonskriterier knyttet til problemstillingen som undersøkes i dette kapitlet:

Kommunen skal:

- Utarbeide rolle- og ansvarsbeskrivelse for personell som skal involveres i hendelseshåndteringen jf NSMs grunnprinsipper for IKT-sikkerhet nr 102
- Kartlegge omfang og påvirkning på forretningsprosessene[7] jf NSMs grunnprinsipper for IKT-sikkerhet nr 109

3.3 Datagrunnlag

3.3.1 Rolle og ansvarsbeskrivelser for personell med sentrale oppgaver

Det fremkommer av Bergen kommune sitt styringssystem for personvern og informasjonssikkerhet[8] at det er utarbeidet rolle- og ansvarsbeskrivelser for personell med sentrale oppgave, som for eksempel IT-sjef,

[7] I vår sammenheng viser dette til prosesser som er viktige og kritiske for å opprettholde kommunens drift
[8] https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/personvern-og-informasjonssikkerhet/styringssystem-for-personvern-og-informasjonssikkerhet

applikasjonsansvarlig mm. Byrådsavdeling for finans, næring og eiendom (BFNE) - seksjon for administrasjon har utarbeidet de ulike rollekortene og i dag er følgende roller beskrevet i eget rollekort:

- Personvern og informasjonssikkerhetskoordinator
- Systemeier
- Systemkoordinator
- Prosjekteier
- Prosjektleder
- Digitaliseringskoordinator
- IKT-koordinator
- Behandlingsansvarlig

Rollebeskrivelsene skal sørge for likere utførelse av rollene og tydeliggjøre ansvar og grensesnitt mellom roller internt i byrådsavdelingen og mellom byrådsavdelingene og de sentrale IKT- og digitaliseringsmiljøene. Formålet med rollekortene er tydelige avklaringer om oppgaver, ansvar og myndighet slik at viktige oppgaver ikke nedprioriteres.

Samtlige roller gis en kort beskrivelse, hvilke ansvar og fullmakt den enkelte roller har, samt krav til kompetanse. I tillegg er følgende beskrevet for den enkelte rolle:

- Styring og forvaltning av konsern- og fagsystem
- Data- og informasjonsforvaltning
- Personvern og informasjonssikkerhet
- Portefølje, prosjekt - og programstyring
- Virksomhetsarkitektur
- Samstyring

3.3.2 Kommunens rolle- og ansvarsbeskrivelse for personell som skal involveres i hendelseshåndteringen

Rolle og ansvarsbeskrivelser for ledere med beslutningsansvar på ulike nivåer

I kommunens overordnede beredskapsplan – administrativ del går det frem at beredskapsorganisasjonen i Bergen kommune består av tre nivåer som har ulike ansvarsområder og oppgaver:

Strategisk nivå representerer kommunes øverste politiske og administrative ledelse, forsterket med sentrale faglige støttefunksjoner. Det strategiske nivå skal primært ivareta kommunens overordnede interesser, herunder sikre driftskontinuitet og ivareta kommunens tillit og omdømme.

Operasjonelt nivå er en støtteenhet til det strategiske nivået ved svært alvorlige, store eller komplekse beredskapssituasjoner som rammer kommunen eller bysamfunnet.

Taktisk nivå er den kommunale resultatenhet som er rammet av en beredskapshendelse eller de representanter og ressurser kommunen disponerer på ett eller flere innsatssteder.

Videre fremkommer det av Seksjon for digitalisering og innovasjon sin beredskapsplan – *temaspesifikk beredskapsplan for svikt i informasjonssikkerhet* hvilke ledere som har hvilket ansvar når det gjelder beslutningsansvar på ulike nivå. Dette beskrives i planverkets ulike funksjonskort til samtlige roller i beredskapsorganisasjonen og følgende roller er beskrevet:

- Stabsleder
- Administrativ støtte i informasjonssikkerhetsstab
- Nestleder/stedfortreder
- Systemeier
- Fagleder
- Liaison
- Andre funksjoner i informasjonssikkerhetsstaben

Samtlige roller har definerte ansvarsområder, beskrivelse av tildelt myndighet og viktige arbeidsoppgaver. I tillegg beskrives viktige interne ressurser den ulike rollen kan mobilisere og disponere, viktige eksterne samarbeidspartnere rollen bør koordinere med, hvem som skal varsles, samt hvem som er stedfortreder til den enkelte rolle.

Det finnes ikke en samlet oversikt over hvem som innehar de ulike rollene innen informasjonssikkerhet og personvern i kommunen. Fra kommunen blir det opplyst at det de ulike rollene fremgår slik:

- Rollene systemeier og systemkoordinator er navngitt i kommunens systemoversikt.
- Prosjekteier og prosjektleder er navngitt i kommunens prosjektstyringsløsning, BkProsjekt.
- Behandlingsansvarlig fremgår av behandlingsprotokoll, og dels i risikomodulen i BkStyring.
- Kommunaldirektør fremgår av kommunens organisasjonskart og fullmaktstruktur.
- Rollene digitaliseringskoordinator, personvern- og informasjonssikkerhetskoordinator (PISK) og IKT-koordinator fremgår i samstyringsmodellen forvaltet av digitaliseringssekretariatet SDI.

Beredskapsvakter som er tilgjengelig utenom normal arbeidstid og i ferieperioder
I kommunens overordnede prosedyre for verdivurdering og klassifisering av informasjon og informasjonssystemer stilles det krav til etablering av vaktordning ved klassifisering av systemer på «høy» eller «kritisk» nivå. Bk360 er klassifisert som et driftsnivå 3-system i kommunen og er vurdert som et virksomhetskritisk system i Byrådsavdeling for finans, næring og eiendom (BFNE). Dette innebærer *at systemer som brukes hele døgnet, eller utover ordinær arbeidstid, har behov for utvidet applikasjonsdrift og oppetid (24/7). Det innebærer også en vaktordning utenfor arbeidstid*[9].

Også i tjenesteavtalevedlegg[10] Bk360 sak- og arkivsystem[11], intern sone stilles det krav til etablering av en vaktordning. Av intervju går det fram at det er etablert en egen vaktordning for ivaretagelse av krav i prosedyre for informasjon og informasjonssikkerhet og tjenesteavtalevedlegget.

Vaktordningen har som grunntanke å opprettholde driftstjenester utenom ordinær arbeidstid (24/7). Tjenesten inngås avtalemessig for et fagsystem og det implementeres utvidet overvåking gjennom tekniske verktøy. Definerte avvik i fagsystemet eller hendelser, blir automatisk sendt via SMS til vaktlag, som påbegynner feilsøking straks innenfor de pålagte responstider. Som hovedregel vil utrykning bli iverksatt av automatiske alarmer fra de ulike overvåkings-løsningene.

3.3.3 Kommunens analyse av virksomhetskritiske effekter

Det fremkommer av *Temaplan for informasjonssikkerhet og personvern: 2021-2025 i Bergen kommune* at det skal gjennomføres en Business Impact Analysis (BIA) og at det er informasjonsansvarlig i hver virksomhet eller enhet som er ansvarlig for gjennomføringen. Det er deres rolle å koordinere og utføre BIA-prosessen innenfor sine ansvarsområder.

Informasjonsansvarlige er vanligvis ansatte som har ansvar for informasjonssikkerhet og personvern i den aktuelle virksomheten eller enheten. Deres oppgave er å identifisere og vurdere konsekvensene av potensielle IKT-hendelser på virksomhetens drift og prioritere tiltak for å sikre kontinuitet og beskyttelse av informasjon og persondata.

En Business Impact Analysis (BIA) er en prosess og analyse som brukes til å identifisere og vurdere de ulike forretningsprosessene og funksjonene som er kritisk for kommunen, samt avhengigheter av ulike IKT-systemer. Formålet med en BIA er å forstå de økonomiske, operasjonelle og omdømmemessige konsekvensene en organisasjon kan møte ved for eksempel en IKT-relaterte hendelser.

I intervju bekreftes det at det ikke er gjennomført en egen vurdering av kritikalitet på Bk360 slik det er beskrevet i en BIA, og hvordan et eventuelt bortfall av systemet vil kunne påvirke de øvrige prosessene som er viktige for

[9] https://bergen.extend.no/cgi-bin/document.pl?pid=bergen&DocumentID=8617
[10] Et tjenestevedlegg er en spesifikk type dokument som brukes i forbindelse med levering av IKT-tjenester. Dette dokumentet inneholder detaljert informasjon om tjenesten som skal leveres, inkludert tekniske spesifikasjoner, arbeidsomfang, tidsrammer og eventuelle kostnader
[11] https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/systemer-tilganger-og-passord/sla

kommunens drift (forretningsprosessene) er usikkert. Dette medfører at det i dag knyttes høy usikkerhet til hvordan et bortfall av Bk360 vil påvirke de ulike forretningsprosessene i kommune på samtlige nivå.

For å tilrettelegge for utarbeidelse av BIA i de ulike enhetene har seksjon for digitalisering og innovasjon utarbeidet en mal for vurdering av kritikalitet for informasjonssystemer og digitale løsninger. Malen er trinnvis inndelt i kritikalitet og består av en rekke påstander i tabellform. Ved bekreftelse på en eller flere påstander vurderes systemet som med kritikalitet *kritisk*, *høy*, *middels* eller *lav*.

Det fremkommer av intervjuene at denne malen ikke er tatt i bruk per i dag. Det fremkommer ikke av intervjuene hvordan seksjon for digitalisering og innovasjon (SDI) eventuelt vil å ta i bruk eksisterende mal i de ulike byrådsavdelingene og etatene. I forbindelse med verifisering av rapporten opplyser kommunen at det er startet et eget prosjekt i regi av SDI for systemkritikalitet, der prosedyre og mal skal implementeres i hele kommunen (alle byrådsavdelinger). Prosjektet har fått godkjent mandat og startet i august 2023. Plan for ferdigstillelse blir opplyst å være første kvartal 2024.

3.4 Vurdering

3.4.1 Rolle og ansvarsbeskrivelser innen informasjonssikkerhet og personvern

Det er Deloittes vurdering at Bergen kommune kun delvis har identifisert tiltak for å forebygge cyberhendelser som kan ramme Bk360 og iverksatt disse.

Bergen kommune har utarbeidet gode og utfyllende rolle- og ansvarsbeskrivelse for rollene innen informasjonssikkerhet og personvern i kommunen, men det er Deloittes vurdering at det bør være enklere å finne frem til hvem som innehar de ulike rollene i organisasjonen. Ved å gjøre det enklere å finne frem til hvem som innehar ulike roller blir det tydelig hvem som har ansvar for spesifikke oppgaver og ansvarsområder innen informasjonssikkerhet og personvern. Dette vil også gjøre det enklere å finne frem til hvem som innehar hvilken beslutningsmyndighet og hvem som er ansvarlig for ulike aspekter av systemadministrasjon, brukerstøtte osv.

3.4.2 Roller og ansvarsbeskrivelse er utarbeidet i kommunen beredskapsplanverk

Det er Deloitte sin vurdering at det er tydelig hvilke roller som kan fatte beslutning på ulike nivå ved en hendelse. I kommunens overordnede beredskapsplanverk – administrativ del og SDI sin temaspesifikke beredskapsplan for svikt i informasjonssikkerhet er det utarbeidet tydelige rollebeskrivelse for ledere med beslutningsansvar på ulike nivåer.

For å ivareta døgnkontinuerlig drift (24/7) av ulike driftstjenester utenom ordinær arbeidstid, har kommunen etablert en egen vaktordning for personvern og informasjonssikkerhet. Vaktordningen består av et vaktlag som skal håndtere eventuelle hendelser innen personvern og informasjonssikkerhet som oppstår. Deloitte mener at vaktlagets oppgaver og ansvar bør fremgå i form av en rollebeskrivelse i kommunens beredskapsplanverk. Dette er viktig for å sikre hvilke oppgaver som skal gjennomføres nå og at varsling og håndtering av hendelsen blir effektiv. Rollebeskrivelsen bør også omtale hvordan vaktlaget skal håndtere hendelser i samspill med den øvrige beredskapsorganisasjonen.

3.4.3 Bergen kommune har ikke tilstrekkelig oversikt over konsekvensene ved bortfall av Bk360 eller andre virksomhetskritiske systemer, ettersom nødvendige analyser ikke er gjennomført.

Det er Deloittes vurdering at kommunen ikke har tilstrekkelig oversikt over konsekvensene ved bortfall av Bk360 eller andre virksomhetskritiske systemer. Dette er fordi kommunen ikke har gjennomført en Business Impact Analysis (BIA). Resultatene av en BIA vil gi viktig informasjon som kan brukes til å utforme en effektiv IKT-beredskapsplan og sikkerhetsstrategi. Ved å ha en klar forståelse av virkningen og konsekvensene av potensielle IKT-hendelser, kan organisasjonen utvikle passende gjenopprettingsstrategier, sikkerhetskontroller og beredskapstiltak for å sikre at de er i stand til å håndtere og respondere på uforutsette hendelser på en effektiv måte.

Oppsummert har Bergen kommune bare delvis identifisert tilstrekkelig med forebyggende tiltak for å forebygge cyberhendelser som kan ramme Bk360 og iverksatt disse. Dette er fordi kommunen ikke har gjennomført nødvendige analyser som gir oversikt over konsekvensene for viktige prosesser i kommunen ved bortfall av Bk360.

Revisjonskriterium	Oppfyllelse av kriteriet
Utarbeide rolle- og ansvarsbeskrivelser	
Kartlegge omfang og påvirkning på forretningsprosessene	

4 Planer for opprettholdelse av virksomheten ved bortfall av Bk360

4.1 Problemstilling

I dette kapittelet vil vi svare på følgende problemstilling med underproblemstillinger:

Har Bergen kommune etablert tilstrekkelig beredskap for følgende mulige hendelse: Kommunens saks- og arkivsystem Bk360 utsettes for et cyberangrep som gjør skade på arkivet og hindrer tilgang til systemet over en lengre periode. Under dette:

- *Har kommunen tilfredsstillende planer for hvordan berørte deler av kommunens virksomhet skal opprettholdes ved bortfall av Bk360?*

4.2 Revisjonskriterier

Basert på krav i NSMs grunnprinsipper for IKT-sikkerhet har Deloitte utledet følgende revisjonskriterier knyttet til problemstillingen som undersøkes i dette kapitlet.

Kommunen skal:

- Etablere et planverk for hendelseshåndtering jf. NSMs grunnprinsipper for IKT-sikkerhet nr100
- Iverksette gjenopprettingsplan i løpet av, eller i etterkant av hendelsen jf. NSMs grunnprinsipper for IKT-sikkerhet nr112
- Fastsette hvilke kommunikasjonskanaler som skal benyttes i forbindelse med hendelser jf NSMs grunnprinsipper for IKT-sikkerhet nr104
- Utarbeide avtaler med relevante tredjeparter jf. NSMs grunnprinsipper for IKT-sikkerhet nr103

4.3 Datagrunnlag

4.3.1 Planverk for hendelseshåndtering

Klassifiseringsregime for hendelser og grenseverdier for å aktivere krisestab

I planer for håndtering av hendelser er det vanlig å klassifisere ulike typer hendelser for å tydeliggjøre hvilken respons de skal møtes med. Det fremkommer av Seksjon for digitalisering og innovasjon (SDI) sin temaspesifikke beredskapsplan for svikt i informasjonssikkerhet at det er utarbeidet en egen klassifisering for hendelser og grenseverdier for å aktivere krisestab når det gjelder hendelser knyttet til svikt i informasjonssikkerheten. Tabellen under viser vurdering av alvorlighetsgrad basert på konfidensialitet, integritet og tilgjengelighet. Kolonnen «konfidensialitet» beskriver graden av beskyttelse av sensitive og konfidensielle data mot uautorisert tilgang, kolonnen «integritet» beskriver i hvilken grad nøyaktighet, pålitelighet og fullstendighet av data og systemer er opprettholdt, mens «tilgjengelighet ansatt» handler om tilgang til data for ansatte i kommunen når det er behov for det.

Figur 3 Klassifisering av hendelser

Nivå	Konfidensialitet	Integritet	Tilgjengelighet-ansatt
1	Enkelte ansatte i Bergen kommune får tilgang til åpen informasjon de ikke har tjenstlig behov for.	Mindre avvik eller mangler i registrert informasjon, men ikke skadepotensial for kommunen eller tredjepart.	Ubetydelig nedetid eller utilgjengelighet av data.

2	Grupper av ansatte i Bergen kommune eller eksterne får tilgang til åpen informasjon som ikke er offentliggjort.	Mindre avvik eller mangler i registrert informasjon, men lavt skadepotensial for kommunen eller tredjepart. Moderat kvalitetsavvik.	Overskridelse av akseptabel nedetid for systemet. Enkelte ansatte blir mindre hindret i å utføre daglige arbeidsoppgaver i en kort periode.
3	Uvedkommende får tilgang til intern informasjon, men offentliggjøring av informasjon har lavt skadepotensiale. Mulig kritikk fra tilsynsorganer.	Feil eller mangler i registrert informasjon eller styringsdata kan føre til skade for kommunen eller tredjepart. Moderat kvalitetsavvik.	Overskridelse av akseptabel nedetid for systemet. Flere ansatte blir mindre hindret i å utføre daglige arbeidsoppgaver i en kort periode.
4	Uvedkommende får tilgang til intern eller sikker informasjon som kan misbrukes til skade for kommunen, samfunnet eller tredjeparter. Brudd på/avvik fra lov/forskrift. Kritikk fra tilsynsorganer, varsel om mulige sanksjoner. Potensielt erstatningsansvar overfor tredjeparter.	Feil eller mangler i registrert informasjon eller styringsdata kan gi alvorlig skadevirkning for kommune, samfunn eller tredjepart. Brudd på/avvik fra lov/forskrift. Kritikk fra tilsynsorganer, varsel om mulige sanksjoner. Potensielt erstatningsansvar overfor tredjeparter.	Alvorlig overskridelse av akseptabel nedetid for system eller prosess. Mange ansatte blir hindret i å utføre viktige arbeidsoppgaver i en kort periode, eller flere ansatte blir hindret i en lang periode. Viktige historiske data kan gjenskapes etter hendelsen. Midlertidig tap av styring og kontroll.
5	Omfattende lekkasje av sikker informasjon som kan misbrukes til alvorlig skade for kommunen, samfunnet eller tredjeparter. Alvorlig brudd på/avvik fra lov og forskrift. Sanksjoner fra tilsynsorganer. Erstatningsansvar overfor tredjeparter.	Feil eller mangler i registrert informasjon eller styringsdata kan gi svært alvorlig skadevirkning for kommune, samfunn eller tredjepart. Alvorlige brudd på/avvik fra lov og forskrift. Sanksjoner fra tilsynsorganer. Erstatningsansvar overfor tredjepart.	Svært alvorlig overskridelse av akseptabel nedetid for system eller prosess. Mange ansatte blir hindret i å utføre viktige arbeidsoppgaver i en lang periode. Tidskritiske arbeidsoppgaver kan ikke utføres. Viktige historiske data går tapt. Langvarig tap av styring og kontroll.

I henhold til Seksjon for digitalisering og innovasjon (SDI) sin temaspesifikke beredskapsplan skal hendelser på nivå 1 og 2 håndteres av Ansattservice. Ved hendelser på nivå 3 eller høyere vil direktør for seksjon for digitalisering og innovasjon (SDI), eller stedfortreder, vurdere om hele eller deler av informasjonssikkerhetsstaben skal mobiliseres. Denne vurderingen gjøres i samspill med kommunens vaktgående kriseledelse.

I det digitale beredskapsplanverket som er utarbeidet for Ansattservice er også alvorlighetsgraden beskrevet. Også her er hendelsene klassifisert fra nivå 1 – 5, der 5 utgjør den hendelsen med størst konsekvens. Alvorlighetsgraden bestemmes av den innledende analysen der teknikere og relevante avdelingsledere i Ansattservice gjør en

innledende vurdering av hendelsen for å fastslå omfanget av hendelsen, hendelseskategori og alvorlighetsgrad. Denne innledende analyse (ofte kalt «triage») skal bidra til valg av responsstrategi og teamsammensetning.

4.3.2 Digitalt beredskapsplanverk

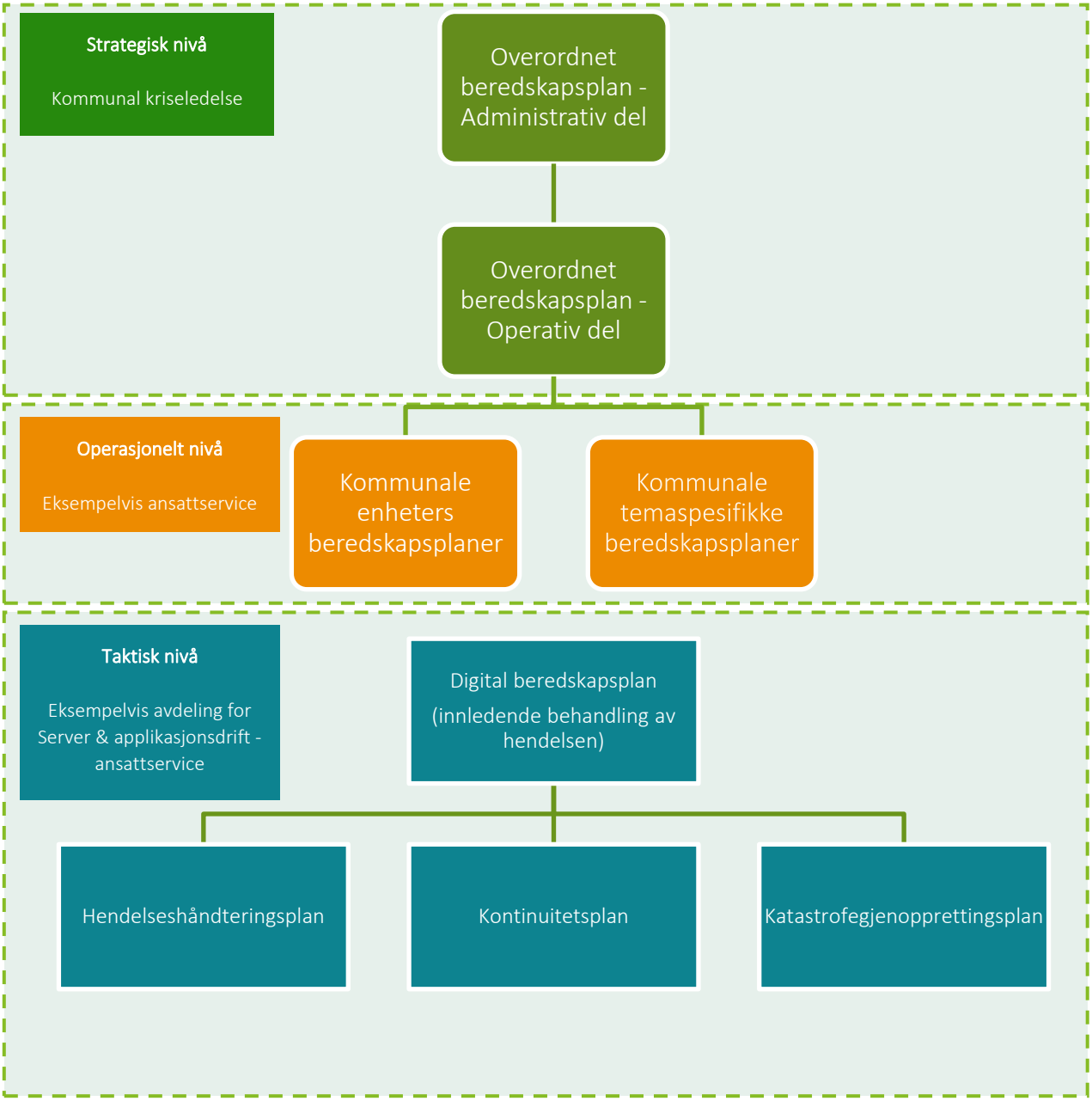
Den digitale beredskapsplan for Ansattservice skal være utgangspunktet for behandling og håndtering av alle IT-relaterte hendelser i Ansattservice. Dette skal bidra til å sikre og etablere en effektiv prosess for valg av planverk for videre håndtering og består i dag av tre ulike planverk.

- Hendelseshåndteringsplan
- Kontinuitetsplan
- Katastrofegjenopprettingsplan

Det er ledelsen i Ansattservice som beslutter om planen(e) skal iverksetter ved en hendelse.

Det er utarbeidet et eget veiledningsdokument som beskriver de enkelte planene i detalj.

Figur 4 Digitalt beredskapsplanverk - overordnet struktur[12]



[12] Se vedlegg 6 for utfyllende forklaring av de ulike beredskapsplanene

Det foreligger ulike aktiveringskriterier for hendelseshåndtering, - kontinuitets, - og katastrofegjenopprettingsplanene. Den innledende behandlingen av hendelsen skal sikre effektiv håndtering basert på de ulike planene. De ulike aktiveringskriteriene er som vist under:

Figur 5 Aktiveringskriterier digital beredskapsplan

Hendelseshåndteringsplan	• Det foreligger indikasjoner på at det er en villet ondsinnet handling bak hendelsen
Kontinuitetsplan	• Hendelsen indikerer at IT-systemer med driftsnivå 2 eller 3 vil være nede for mer enn akseptabel nedetid (RTO - Recovery Time Objective[13]) • Flere sammenhengende IT-systemer uavhengig av driftsnivå er nede uten at det foreligger en opplagt feil eller løsning på feil
Gjenopprettingsplan	• Det er forhold som tilsier at en katastrofe er nær forestående og produksjonsmiljøet med kritiske IT-systemer trolig vil gå ned. • Dersom produksjonsmiljøet er nede og katastrofen har ført til nedetid på kritiske IT-systemer

4.3.3 Planer for gjenoppretting i forbindelse med hendelser

Som en del av det digitale beredskapsplanverket er det utarbeidet katastrofegjenopprettingsplan. Planen har hovedfokus på å håndtere katastrofer som hindrer tilgang til IT-systemer fra primærlokasjon[14]. Dette kan eksempelvis være forårsaket av ulike eksterne og interne årsaker som naturkatastrofer, brann, menneskelige feil eller sabotasje.

Planen skal sikre kontinuitet ved hendelser som fører til bortfall av normal driftsløsning. Målet med planen er:

- Å redusere betydelige avvik fra normaltilstand
- Å minimere omfanget av betydelige driftsforstyrrelser og potensielle skader
- Å minimerer økonomiske konsekvenser av betydelige driftsforstyrrelser
- Å etablere strukturerte prosedyrer for alternativ drift før katastrofer oppstår

IT-system som inngår i løsningen, er delt inn i kategorier og skal gjenopprettes i følgende sekvens:

Figur 6 IT-systemer som inkluderes i katastrofegjenopprettingsløsningen

Sekvens	Kategori	Akseptabel nedetid	Tidsestimat gjenopprettingstid
1	Infrastruktur	1 time	1 time
2	Systemer på driftsnivå 3[15]	< 1 time	1 time

[13] Akseptabel nedetid (RTO-Recovery Time Objective) defineres som tidspunktet hvor de negative konsekvensene av et avbrudd blir uakseptable for Bergen kommune. IT-systemene må gjenopprettes innen predefinert RTO. Det fremkommer ikke av dokumentasjonen hvordan Bergen kommune har kommet frem til denne konklusjonen.

[14] En primærlokasjon for informasjons- og kommunikasjonsteknologi (IKT) refererer til den fysiske plasseringen der en organisasjon eller virksomhet plasserer sine viktigste IT-infrastrukturer og datasystemer. Dette kan inkludere servere, datalagring, nettverksutstyr og annen kritisk teknologi som er avgjørende for organisasjonens drift. For Bergen kommune er primærlokasjon Spelhaugen i Fyllingsdalen.

[15] BK360 blir opplyst å være et system på driftsnivå 3. Som nevnt i fotnote 11 er denne vurderingen ikke dokumentert. For systemer med kritisk eller høy kritikalitet, skal høyeste driftsnivå (3) velges der løsningen driftes av Ansattservice.

3	Systemer på driftsnivå 2	< 1 time innen normal arbeidstid	1 time innen normal arbeidstid
4	Systemer med driftsnivå 1	Ingen krav	Ved kapasitet innenfor normal arbeidstid

Planen gir videre en overordnet beskrivelse av de ulike fasene for gjenoppretting, fordelt på fire faser.

Figur 7 Overordnet beskrivelse av fasene

Fase I: Inkluderer umiddelbar varsling, utførelse og testing av flytting av applikasjon fra produksjonslokasjon til katastrofegjenopprettingslokasjon for å utføre fullkapasitets IT-operasjoner

Fase II: Inkluderer alle aktivitetene som må utføres for å påse at katastrofegjenopprettingsløsningen fungerer som den skal, på nivå med drift fra primærlokasjon.

Fase III: Inkluderer alle aktivitetene som må utføres for å tilbakeføre drift til primærlokasjon.

Fase IV: Inkluderer deaktivering av planverket og gjennomgang av læringspunkt.

4.3.4 Kommunikasjonskanaler som skal benyttes i forbindelse med hendelser.

Plan for intern og ekstern kommunikasjon rundt hendelser

I intervju blir det opplyst at Bergen kommune har besluttet å benytte seg av RAYVN som kommunens krisehåndteringsverktøy. RAYVN er designet for å hjelpe organisasjoner med å håndtere og koordinere krisesituasjoner. Verktøyet gir en sentralisert plattform for å samle og dele viktig informasjon, kommunisere med berørte parter og administrere oppfølging av hendelser. RAYVN skal muliggjøre sanntidsoppdateringer om situasjonen, gi teammedlemmer mulighet til å dele oppgaver og ansvar, og få et helhetlig bilde av krisesituasjonen. Deloitte får opplyst at automatiserte varslinger, geografisk kartlegging, tidsstyring og dokumenthåndtering, gjør at RAYVN kan hjelpe organisasjoner med å ta raskere beslutninger, redusere responsresponstiden og opprettholde kontroll over kritiske hendelser.

I intervju bekreftes det at RAYVN ble benyttet i forbindelse med gjennomføring av forrige øvelse som hadde fokus på IKT-hendelser i 2022. Erfaringen fra denne øvelsen gjorde at seksjon for digitalisering og innovasjon (SDI) ser det som formålstjenlig å benytte seg av RAYVN også ved fremtidige hendelser.

Også i Ansattservice sitt digitale beredskapsplanverk, inkludert hendelseshåndtering, - kontinuitets, - og katastrofegjenopprettingsplan, er kommunikasjonskanaler i forbindelse med hendelser beskrevet.

Det fremkommer av seksjon for digitalisering og innovasjon (SDI) sin temaspesifikke beredskapsplan for svikt i informasjonssikkerhet at det er utarbeidet planer for intern og ekstern kommunikasjon rundt hendelser. Det fremkommer samtidig av intervju at beredskapsplanverket og tilhørende kommunikasjonsplan ikke er tilstrekkelig kjent i Seksjon for digitalisering og innovasjon (SDI). I beredskapsplanverket er det etablert en

kommunikasjonsmatrise som gir en detaljert oversikt over interne og eksterne kontaktpunkt og kommunikasjonskanaler. Det fremkommer likevel ikke av kommunikasjonsmatrisen hvilke alternative kommunikasjonskanaler som kan benyttes ved en hendelse, dersom det skulle være behov for dette.

Samtidig bekreftes det i intervju og av overordnet beredskapsplan for Bergen kommune-administrativ del, at samfunnssikkerhetens hus besitter alternative kommunikasjonsmidler som kan benyttes ved behov. Dette er kommunikasjonsmidler (nødnett og mobiltelefon) som kan tas i bruk ved mobilisering av kommunal kriseledelse og involvering av Samvirkevakten. Dette gjelder både internt blant de ansatte, men også eksternt ut mot publikum. I intervju blir det opplyst at kommunikasjonsmidler som benyttes i forbindelse med en hendelse varierer basert på størrelsen. Seksjon for digitalisering og innovasjon (SDI) har flere ulike alternativer avhengig av om det skal kommuniseres internt eller eksternt. De har for eksempel mulighet til å publisere informasjon på Allmenningen eller som SMS-varsling til alle ansatte. Ved behov for å informere publikum, så eksisterer det også en mulighet for adressebasert varsling via Vaktsentralen.

I seksjon for digitalisering og innovasjon sin temaspesifikke beredskapsplan for svikt i informasjonssikkerhet, vedlegg 3, finnes det også en telefonliste for interne og eksterne personer som er aktuelle å kontakte. Listen inkluderer også e-postadresser.

4.3.5 Avtaler for å sikre effektiv hendelseshåndtering

Styringsavtale for digitalisering- og IKT-tjenester i Bergen kommune

Formålet med en styringsavtale er å etablere en klar og strukturert ramme for samarbeidet mellom ulike parter eller enheter innenfor en organisasjon når det gjelder levering, drift og styring av IT-tjenester. En styringsavtale bidrar til å sikre at alle involverte parter forstår sine roller og ansvar, samt at forventningene til tjenestekvalitet, ytelse og oppfølging er definert på en måte som er akseptabel for alle.

Det er utarbeidet en egen stryringsavtale for digitaliserings- og IKT-tjenester i Bergen kommune. Nåværende IKT-driftstjenesteavtale er under avvikling som del av endret organisering og ansvar innenfor Digitalisering og IKT. Etter opprettelsen av en egen etat, Ansattservice, er driftsansvaret for tjenester en del av styringsavtalen med de ulike tjenesteansvarlige. Med tjenesteansvarlig menes en person eller en rolle som har ansvar for administrering, drift og kvalitetssikring av en eller flere IT-tjenester innenfor en organisasjon. Denne rollen innebærer vanligvis å sørge for at de ulike IT-tjenestene fungerer på en pålitelig måte, oppfyller brukerbehov og er i tråd med organisasjonens mål og strategier. Formålet med avtalen er å definere ansvar og sette rammer for de digitaliserings- og IKT tjenester som utvikles, forvaltes og leveres av Ansattservice på vegne av tjenesteområdeeier[16], eksempelvis Bk360.

Tjenestekatalog

Formålet med en tjenestekatalog er å gi organisasjonens brukere og interessenter en strukturert og lettforståelig oversikt over de ulike IT-tjenestene som tilbys. Tjenestekatalogen fungerer som en sentral informasjonskilde som beskriver de tilgjengelige tjenestene, deres egenskaper, bruksområder, priser (hvis relevant) og eventuelle retningslinjer for bruk.

Ansattservice er ansvarlig for drift av de fleste IT-tjenester og fagsystemer som er i bruk i kommunen i dag, inkludert tjenestekatalogen. Per i dag består tjenestekatalogen av totalt 12 ulike tjenestebilag som beskriver teknisk infrastruktur, driftskonsept, IKT-styring mm.

Et tjenestebilag (SLA – Service Level Agreement) er et vedlegg til IKT-driftsavtalen og beskriver i detalj hvilke tjenester som skal leveres rundt systemet som oppetid, vakttjenester med mer. Det skal utarbeides tjenestebilag for systemer og tjenester som benytter kommunens infrastruktur for å sikre formelle strukturer rundt fordeling av oppgaver, vakttjenester avhengig av system/løsning, og forventet nede- oppetid. I Temaplanen[17] stilles det krav til SLA for alle systemer og tjenester som benytter kommunens infrastruktur, herunder også Bk360.

[16] En person eller en rolle som har ansvar for forvaltningen, koordineringen og styringen av en spesifikk tjeneste eller tjenesteområde innenfor en organisasjon eller bedrifts IKT-struktur.

[17] Se figur 2 eller vedlegg for nærmere beskrivelse.

Deloitte har gjennomgått SLA for BK360 med TietoEvry. Bk360 baserer seg på TietoEvry sitt system Public 360[18], med tilpasninger for Bergen kommune. Avtalen med TietoEvry inneholder ikke detaljer knyttet til hvordan leverandør skal bistå i en eventuell hendelse. En slik avtale inneholder vanligvis et krav til leverandør med å bistå i hendelseshåndteringen, for eksempel med bruk av et Digital forensic team/Incident response team (IRT). Et slikt team består av en gruppe fagpersoner som er ansvarlige for å håndtere og respondere på sikkerhetshendelser i en organisasjon[19].

I temaspesifikk beredskapsplan for svikt i informasjonssikkerhet - umiddelbare aksjoner fremkommer det at kommunen kan varsle et Digital forensic team/Incident response team (IRT) ved behov. Kommunen har imidlertid ikke tilgang til et incident response team (IRT) gjennom eksisterende avtaler.

4.4 Vurdering

Beredskapsplanverket legger til rette for å ivareta hendelseshåndteringen på en god måte, men det er risiko for at beredskapsplanverket ikke er tilstrekkelig kjent i organisasjonen. Det er Deloittes vurdering at det overordnede beredskapsplanverket, herunder temaspesifikk beredskapsplan for svikt i informasjonssikkerhet og overordnet beredskapsplan – administrativ del er godt utarbeidet og vil ivareta hendelseshåndteringen på en god måte. Planverket er strukturert på en slik måte at det kommer tydelig frem hvem som innehar beslutningsmyndighet på ulike nivå.

Det er samtidig Deloittes vurdering at det er risiko for at beredskapsplanverket ikke er tilstrekkelig kjent i organisasjonen, spesielt på lavere nivå. Dette kan medfører en risiko for manglende forberedelser, manglende koordinering mellom de ulike nivåene, tap av verdifull tid i varsling og umiddelbar respons, sviktende og uklar ansvarsfordeling og utilstrekkelig opplæring og trening av beredskapsorganisasjonen.

Videre er det Deloitte sin vurdering at Bergen kommune har et tilfredsstillende regime for klassifisering av ulike hendelser. Samtidig kan det være uheldig at det i klassifisering av hendelser brukes ulik skala. I seksjon for digitalisering og innovasjon er nivå 1 og 2 hendelser klassifisert som de mest alvorligste, mens det i Ansattservice sitt digitale beredskapsplanverk er nivå 5 som innehar høyest grad av alvorlighet. Beskrivelsen av de ulike nivåene er heller ikke sammenfallende. Deloitte mener dette kan føre til misforståelser og utydelig kommunikasjon mellom de ulike nivåene i organisasjonen.

4.4.1 Bergen kommune har planer for gjenoppretting etter en hendelse, men planene kan være mer spesifikke

Til tross for at det er utarbeidet en oversikt over akseptabel nedetid (RTO) (se figur 5 – IT-systemer som inkluderes i katastrofegjenopprettingsløsningen) for Bk360 i det digitale beredskapsplanverket og katastrofegjenopprettingsplanene, finnes det ingen systemspesifikke planer for gjenoppretting av enkeltsystem Akseptabel nedetid defineres gjennom en konsekvensvurdering av ulike kjerneprosesser i Bergen kommune. En konsekvensvurdering av ulike kjerneprosesser blir vanligvis dekket av en Business Impact analysis (BIA), noe som mangler i kommunen. Som tidligere pekt på så fremkommer det ikke av dokumentasjonen at dette er gjennomført. Det er derfor ukjent hva som ligger til grunn for vurderingen av konsekvens og akseptabel nedetid på under en time for BK360.

Det digitale beredskapsplanverket i kommunen vil kunne ivareta gjenopprettingen på en god måte, men kan etter Deloittes vurdering likevel forbedres. Grunnen til dette er at Bergen kommune har ikke full oversikt over hvordan en hendelse som berører BK360 vil påvirke driften av kommunen. Ved å utarbeide en Business Impact Analysis (BIA) vil man få en økt forståelse av de ulike konsekvensene og man vil kunne ta informerte og gode beslutninger i hendelseshåndteringen og gjenopprettingen basert på et godt informasjonsgrunnlag. I forlengelse av dette anbefaler Deloitte at det utarbeides systemspesifikke planer for å ivareta gjenopprettingen på en god måte. Dette

[18] Public 360 er en programvareløsning utviklet av TietoEVRY. Løsningen er designet for å hjelpe offentlige organisasjoner og virksomheter med å administrere dokumenter, saksbehandling, arkivering og informasjonsforvaltning på en effektiv måte. Public 360 er et såkalt sak- og arkivsystem som er spesielt tilrettelagt for behovene til offentlig sektor.

[19] Teamet er ofte spesialtrent og utstyrt for å reagere raskt og effektivt på ulike typer hendelser, for eksempel datainnbrudd, virusangrep, systemsvikt eller andre uønskede hendelser som kan true organisasjonens informasjonssikkerhet. å identifisere, analysere, isolere og løse sikkerhetshendelser, og implementere passende tiltak for å begrense skade, gjenopprette systemer og minimere fremtidig risiko. Incident Response Teamet samarbeider også med relevante interessenter, som interne avdelinger, leverandører, rettshåndhevelse og eksterne sikkerhetsorganisasjoner, for å håndtere hendelsene på en koordinert og samordnet måte.

vil sikre en trinnvis og tilpasset veiledning som vil bidra til en effektiv og rask gjenoppretting. Dagens digitale beredskapsverk dekker ikke dette behovet og fremstår som for generelle.

4.4.2 Kommunens primære kommunikasjonsløsning er ikke tydelig

Bergen kommune har gode kommunikasjonskanaler som skal benyttes i forbindelse med hendelser. Krisehåndteringsverktøyet RAVYN sikrer et felles verktøy for distribuering av kommunikasjon og samhandling blant de som er involvert i hendelseshåndteringen på overordnet nivå. Deloitte vil samtidig fremheve at RAYVN er et krisehåndteringsverktøy som primært benyttes på strategisk nivå. På operasjonelt og taktisk nivå (se figur 3 – digitalt beredskapsplanverk – overordnet struktur), det vil si Seksjon for digitalisering og innovasjon (SDI) og på de ulike driftsenhetene, er ikke RAYVN etablert som primært verktøy for hendelseshåndtering, men også her er det etablert gode prosesser for når og hvem som skal varsler internt og eksternt.

Deloitte mener imidlertid at det er en risiko for at det ikke er en felles forståelse for hva som er primærløsning for kommunikasjon ved en hendelse som tar ned IT-systemene. Grunnen til dette er at det ikke er samsvar mellom de kommunikasjonsløsningene som benyttes av den kommunale kriseledelsen og de løsningene som planverket slår fast at skal benyttes på lavere nivå (operasjonelt og taktisk nivå). I en innledende fase av hendelseshåndteringen er det viktig å opprette kommunikasjon slik at man raskt får koordinert responsen. Når det er uklart hvilke kommunikasjonsløsninger som skal benyttes er det en økt risiko for at den innledende responsen blir forsinket.

4.4.3 Bergen kommune har mangelfulle avtaler med tredjeparter for å ivareta hendelseshåndteringen

Det er Deloittes vurdering av selv om det i eksisterende beredskapsplanverk henvises til et Incident Response Team (IRT) så er dette noe som per dags dato ikke inngår i kommunens beredskap. Å henvise til ikke-eksisterende ressurser skaper falsk trygghet. Konsekvensen av dette er at man i en hendelse belager seg på ressurser som i realiteten ikke er tilgjengelig. Dette fører til en økt risiko for at hendelsen ikke blir løst så effektivt som den potensielt kunne ha blitt.

Deloitte kan heller ikke se at det er utarbeidet spesifikke avtaler med leverandøren av Bk360 for å sikre seg bistand i håndtering av hendelser. Dette kan bidra til å sikre rask respons, tydelig ansvarsfordeling, kontinuerlig forbedring og effektiv hendelseshåndtering.

Revisjonskriterium	Oppfyllelse av kriteriet
Etabler et planverk for hendelseshåndtering	
Iverksett gjenopprettingsplan i løpet av, eller i etterkant av hendelsen	
Fastsett hvilke kommunikasjonskanaler som skal benyttes i forbindelse med hendelser.	
Utarbeid avtaler med relevante tredjeparter	

5 Har kommunen øvd på å håndtere en cyberhendelse som kan ramme Bk360?

5.1 Problemstilling

I dette kapittelet vil vi svare på følgende problemstilling med underproblemstilling:

Har Bergen kommune etablert tilstrekkelig beredskap for følgende mulige hendelse: Kommunens saks- og arkivsystem Bk360 utsettes for et cyberangrep som gjør skade på arkivet og hindrer tilgang til systemet over en lengre periode. Under dette:

- *Har kommunen øvd på å håndtere en cyberhendelse som kan ramme Bk360?*

5.2 Revisjonskriterier

Basert på krav i NSMs grunnprinsipper har Deloitte utledet følgende revisjonskriterier knyttet til problemstillingen som undersøkes i dette kapitlet:

Kommunen skal:

- Teste og øve jevnlig på planer slik at disse er godt innøvd jf NSMs grunnprinsipper for IKT-sikkerhet nr105

5.3 Datagrunnlag

5.3.1 Opplæring og øving av personell i henhold til beskrivelse i planverk

Krav og prosedyrer

I overordnede beredskapsplanverket for Bergen kommune – Administrativ del, er det utarbeidet krav til testing og øving minimum en gang i året. Videre fremgår det av beredskapsplanverket at de ulike byrådsavdelingene og resultatenhetsledere er ansvarlig for å gjennomføre nødvendige øvings- og opplæringsaktiviteter for de funksjonene som beskrives i eget planverk.

Dette reflekteres også i det digitale beredskapsplanverket for Ansattservice hvor det stilles det krav til øvelser på behandling av IT-sikkerhetshendelser i kommunen og at disse skal gjennomføres jevnlig, og minimum årlig. Hensikten med øvelser er å teste flere deler av beredskapsplanverket, fra den digitale beredskapsplanen til underliggende planer som hendelseshåndtering-, kontinuitet-, og katastrofegjenopprettingsplan. Det er IT sikkerhetsansvarlig som er ansvarlig for å sikre at nødvendige øvelser gjennomføres.

Det fremkommer ikke av oversendt dokumentasjon at det er definerte krav til testing og øving av planverk og personell i seksjon for digitalisering og innovasjon (SDI). Rollene, som beskrevet i T*emaspesifikk beredskapsplan for svikt i informasjonssikkerhet*, har ingen krav til trening og øving utover det som er spesifisert i overordnet beredskapsplanverk.

Bergen kommune stiller krav til seg selv om å gjennomføre årlige øvelser av beredskapsplanverket. Det er imidlertid ikke etablert prosedyrer som sikrer jevnlig opplæring og øving av personell i henhold til beskrivelsen i beredskapsplanverket.

5.3.2 Test og øving av planverk

Det fremkommer av intervju at de siste gjennomførte øvelsene innen svikt i informasjonssikkerhet ble gjennomført i 2014 og 2022. Hensikten med øvelsene var opplæring av personell og roller slik de beskrevet i temaspesifikk beredskapsplan for svikt i informasjonssikkerhet.[20]

I intervju blir det pekt på at det er usikkerhet knyttet til rutiner og retningslinjer for frekvens på gjennomførelse av øvelser. Det gjelder for samtlige nivå i kommunen, selv om det er beskrevet i både i overordnet beredskapsplanverk i Bergen kommune og i digitalt beredskapsplanverk i Ansattservice med hvilken frekvens øvelsene skal gjennomføres (minimum en gang i året).

5.4 Vurdering

5.4.1 Kommunen har gjennomført to relevante øvelser, men etterleving av egne rutiner for gjennomføring av øvelser og test av beredskapsplanverk er mangelfull

Deloitte mener at Bergen kommune ikke etterlever kravene til opplæring og øving av personell i henhold til beskrivelse i eget beredskapsplanverk. Kommunen gjennomførte øvelser i 2014 og i 2022 som rettet oppmerksomheten mot svikt i informasjonssikkerhet, men kommunens rutiner legger opp til at dette skal gjennomføres årlig.

Det er Deloittes vurdering at manglende gjennomføring av øvelser knyttet til de ulike rollene som inngår i SDI sitt eget beredskapsplanverk, dessuten fører til risiko for manglende forberedelse til og dermed redusert effektivitet i hendelseshåndteringen. Det kan videre gi risiko for sviktende samhandling på ulike nivå og manglende oppdatering og verifisering av eget planverk basert på læring fra øvelsene.

Revisjonskriterium	Oppfyllelse av kriteriet
Jevnlig øvelser for test av planverk	

[20] Deloitte har verken gjennom oversendt dokumentasjon og i intervju blitt fremvist noe skriftlig dokumentasjon på at øvelsen er gjennomført og at øvelsen er fulgt opp i ettertid.

6 Konklusjon og anbefalinger

Undersøkelsen viser at Bergen kommune i hovedsak ivaretar beredskapen knyttet til cyberhendelser på en tilfredsstillende måte. Det er likevel identifisert områder som bør følges opp for å sikre en fullt ut tilfredsstillende beredskap på dette området.

Kommunen har bare delvis identifisert tiltak for å forebygge cyberhendelser som kan ramme Bk360 og iverksatt disse.

- Bergen kommune har utarbeidet gode og utfyllende rolle- og ansvarsbeskrivelse for rollene innen informasjonssikkerhet og personvern i kommunen, men det er Deloittes vurdering at det bør være enklere å finne frem til hvem som innehar de ulike rollene i organisasjonen.
- For å ivareta døgnkontinuerlig drift (24/7) av ulike driftstjenester utenom ordinær arbeidstid, har kommunen etablert en egen vaktordning for personvern og informasjonssikkerhet. Vaktordningen består av et vaktlag som skal håndtere eventuelle hendelser innen personvern og informasjonssikkerhet som oppstår. Deloitte mener at vaktlagets oppgaver og ansvar bør fremgå i form av en rollebeskrivelse i kommunens beredskapsplanverk. Dette er viktig for å sikre hvilke oppgaver som skal gjennomføres nå og at varsling og håndtering av hendelsen blir effektiv. Rollebeskrivelsen bør også omtale hvordan vaktlaget skal håndtere hendelser i samspill med den øvrige beredskapsorganisasjonen.
- Bergen kommune har ikke tilstrekkelig oversikt over konsekvensene ved bortfall av Bk360 eller andre virksomhetskritiske systemer. Kommunen har ikke gjennomført en Business Impact Analysis (BIA). En slik analyse kunne gitt kommunen en klar forståelse av virkningen og konsekvensene av potensielle IKT-hendelser, og ville gitt et godt grunnlag for å utvikle passende gjenopprettingsstrategier, sikkerhetskontroller og beredskapstiltak.

Beredskapsplanverket er godt utarbeidet og legger i hovedsak til rette for god hendelseshåndteringen.

- Planverket er strukturert på en slik måte at det kommer tydelig frem hvem som innehar beslutningsmyndighet på ulike nivå. Det er likevel uheldig at planverket ikke er tilstrekkelig kjent hos alle i beredskapsorganisasjonen i seksjon for digitalisering og innovasjon (SDI).
- Bergen kommune har et tilfredsstillende regime for klassifisering av ulike hendelser basert på alvorlighetsgrad. Men bruk av ulik skala i ulike deler av organisasjonen kan føre til misforståelser og utydelig kommunikasjon mellom de ulike nivåene i organisasjonen.
- Det digitale beredskapsplanverket i kommunen vil kunne ivareta gjenopprettingen etter cyberhendelser på en god måte, men kan etter Deloittes vurdering likevel forbedres ved å utarbeide en Business Impact Analysis (BIA). Da vil kommunen kunne få på plass blant annet systemspesifikke planer for å sikre raskest mulig gjenoppretting av enkeltsystem.
- Bergen kommune har gode kommunikasjonskanaler som skal benyttes i forbindelse med hendelser. Deloitte mener samtidig at det er en risiko for at det ikke er en felles forståelse for hva som er primærløsning for kommunikasjon ved en hendelse som tar ned IT-systemene. Grunnen til dette er at det ikke er samsvar mellom de kommunikasjonsløsningene som benyttes av den kommunale kriseledelsen, og de løsningene som planverket slår fast at skal benyttes på lavere nivå (operasjonelt og taktisk nivå
- Selv om det i eksisterende beredskapsplanverk henvises til et Incident Response Team (IRT) så er dette noe som per dags dato ikke inngår i kommunens beredskap. Å henvise til ikke-eksisterende ressurser skaper falsk trygghet. Deloitte kan heller ikke se at det er utarbeidet spesifikke avtaler med leverandøren av Bk360 (TietoEVRY) for å sikre seg bistand i håndtering av hendelser.

Kommunen etterlever ikke egne rutiner for gjennomføring av øvelser og test av beredskapsplanverk

- Deloitte mener at Bergen kommune ikke etterlever kravene til opplæring og øving av personell i henhold til beskrivelse i eget beredskapsplanverk. Kommunen gjennomførte øvelser i 2014 og i 2022 som rettet oppmerksomheten mot svikt i informasjonssikkerhet, men kommunens rutiner legger opp til at dette skal gjennomføres årlig.
- Det er Deloittes vurdering at manglende gjennomføring av øvelser knyttet til de ulike rollene som inngår i SDI sitt eget beredskapsplanverk, dessuten fører til risiko for manglende forberedelse til og dermed redusert effektivitet i hendelseshåndteringen. Det kan videre gi risiko for sviktende samhandling på ulike nivå og manglende oppdatering og verifisering av eget planverk basert på læring fra øvelsene.

Basert på funn og vurderinger i undersøkelsen anbefaler Deloitte at Bergen kommune setter i verk følgende tiltak:

1. Sikre en samlet oversikt over hvem som innehar ulike roller og ansvar innen informasjonssikkerhet og personvern i kommunen.
2. Inkluderer eksisterende vaktordning i seksjon for digitalisering og innovasjon sin temaspesifikke beredskapsplan for informasjonssikkerhet og personvern.
3. Utarbeide en Business Impact analysis for virksomheten
4. Sørge for at beredskapsplanverket er tilstrekkelig kjent hos alle i beredskapsorganisasjonen i seksjon for digitalisering og innovasjon (SDI).
5. Sikre at det det benyttes samme skala for klassifisering av hendelser på alle nivå
6. Utarbeide systemspesifikke planer for å sikre raskest mulig gjenoppretting av enkeltsystem med bakgrunn i en BIA.
7. Tydeliggjøre hvilken kommunikasjonsløsning som skal benyttes på samtlige nivå i hendelseshåndteringen.
8. Sikre at informasjon om ressurser som skal inngå i hendelseshåndteringen er oppdatert.
9. Sikre jevnlig trening og øving av beredskapsplanverket for IKT-hendelser.

Vedlegg 1: Høringsuttalelse

BERGEN KOMMUNE | *Digitalisering og innovasjon konsern*

Administrativ sak

Vår referanse: 2023/232282-2
Saksbehandler: Hedda Høyer
Dato: 21. september 2023

Unntatt offentlighet: Offl § 5

Høringssvar Forvaltningsrevisjon - Delrapport om cyberberedskap

Hva saken gjelder:

Byrådsavdeling for finans, næring og eiendom har mottatt høringsutkast til delrapport om cyberberedskap i Bergen kommune. Kommunaldirektøren gir med dette sin høringsuttalelse. Vi kjenner oss overordnet igjen i problemstillingene som Deloitte beskriver, og det legges i uttalelsen vekt på å utdype det pågående arbeidet med digital beredskap og tilhørende ansvarsfordeling. Avslutningsvis vil vi kommentere noen av tiltakene som Deloitte foreslår i rapporten.

1. Om høringsuttalelsen

Dette er den første av fire delrapporter i et forvaltningsrevisjonsprosjekt om beredskap i Bergen kommune. Delrapporten skal undersøke om kommunen er tilstrekkelig forberedt til å håndtere en situasjon der kommunens saks- og arkivsystem Bk360 rammes av et cyberangrep som gjør skade på arkivet og hindrer tilgang til systemet over en lengre periode. Arbeidet har omfattet å:

- Vurdere kommunens tiltak for å forebygge cyberhendelser som kan ramme Bk360
- Planer for hvordan berørte deler av kommunens virksomhet skal opprettholdes ved bortfall av Bk360
- Kommunens etterleving av egne rutiner for gjennomføring av øvelser og test av beredskapsplanverk

Basert på funn og vurderinger i undersøkelsen kommer Deloitte med noen anbefalinger til kommunens videre arbeid innen cyberberedskap i rapportens kapittel 6.

2. Arbeidet med digitalisering og digital beredskap i Bergen kommune

De siste årene har Bergen kommune arbeidet med å etablere roller, rammeverk og rutiner knyttet til forvaltning av kommunens systemportefølje. Som en del av dette arbeidet har rollebeskrivelser blitt utarbeidet for å synliggjøre ansvar knyttet til det enkelte system, både når det gjelder vurderinger av risiko og sårbarhet, personvernkonsekvenser og kritikalitet. Dette arbeidet er en forutsetning for at hendelser som oppstår kan håndteres effektivt i organisasjonen. Kommunens digitaliseringsstrategi forutsetter at personvern og informasjonssikkerhet er innebygd i tjenesteutvikling, drift og forvaltning av felles IT-løsninger, i tråd med målene i nasjonal strategi for digital sikkerhet. Samtidig bidrar samhandling på tvers av byrådsavdelinger, kommuner og forvaltningsnivåer til høyere kompleksitet i kommunens systemarkitektur. Jo lengre og mer komplekse de digitale tjenestekjedene blir, desto høyere krav stiller det til systemforvaltningen.

Seksjon for digitalisering og innovasjon (SDI) har konsernansvar på digitaliseringsområdet, og har i kraft av dette ansvaret for å sette de krav og standarder som er nødvendig for at Bergen kommune kan ha tilfredsstillende kontroll på systemporteføljen. Som en del av konsernansvaret skal SDI tilgjengeliggjøre metoder og verktøy som gjør det mulig for resten av organisasjonen å utøve sitt ansvar knyttet til IT-systemene. Bystyret har vedtatt en egen Temaplan for informasjonssikkerhet og personvern som inneholder prioriterte tiltak på området.

Kommunens styringssystem for personvern og informasjonssikkerhet forvaltes av SDI. Styringssystemet skal sikre at arbeidet knyttet til personvern og informasjonssikkerhet i kommunen planlegges, gjennomføres og kontinuerlig forbedres på en systematisk måte. Som støtte har seksjonen utarbeidet rollebeskrivelser for personell med sentrale oppgaver.

SDI har i senere tid gjennomgått og revidert sin egen beredskapsplan - temaspesifikk beredskapsplan for svikt i informasjonssikkerhet. Som en del av arbeidet er planen gjennomgått med alle ansatte på seksjonen. Personell med spesifikke roller i beredskapen har hatt egne gjennomganger av rollene og har gjennomført en beredskapsøvelse for å øve på anvendelse av planverket.

Systemeierskapet til kommunens saks- og arkivløsning Bk360 ligger hos SDI, mens Ansattservice har den operative drift og forvaltning av systemet, i tillegg til forvaltningen av en rekke andre sentrale IT-systemer i kommunen. Ansattservice drifter også kommunens digitale infrastruktur. Ansattservice er en egen etat på Byrådsavdeling for finans, næring og eiendom. Den digitale beredskapsplan for Ansattservice skal være utgangspunktet for behandling og håndtering av alle IT-relaterte hendelser som Ansattservice har ansvaret for. Dette bidrar til å sikre og etablere en effektiv prosess for videre håndtering.

Høsten 2023 har SDI startet en rekke aktiviteter som er ventet å bidra ytterligere til å bedre oversikt og kontroll på risiko i kommunens systemportefølje med tilhørende integrasjoner. Arbeidet omfatter blant annet implementering av forbedret rammeverk for kritikalitetsvurderinger for IT-systemer, og inkludert gjennomføring av nye vurderinger. Arbeidet vil gi en samlet oversikt over oppdaterte kritikalitet på tvers av hele systemporteføljen og legge til rette for en bedre oversikt over konsekvenser ved eventuelle hendelser.

Det pågår også et arbeid for å samle og etablere kapasitet og kompetanse innen IT-sikkerhet i et senter for digital sikkerhet. Senteret skal levere en rekke tjenester og kapabiliteter knyttet til blant annet hendelseshåndtering, sårbarhetsstyring, deteksjon og kompetanse, og er et prioritert tiltak i kommunens Temaplan for informasjonssikkerhet og personvern.

3. Vurdering av anbefalinger

Forvaltningsrevisjonsrapporten viser at det er rom for forbedring når det gjelder Bergen kommunes beredskap knyttet til hendelser som medfører at kommunens saks- og arkivsystem er utilgjengelig over en lengre periode. Vi kjenner oss i stor grad igjen i observasjonene som Deloitte har gjort.

Vi anerkjenner at virkingene av en eventuell hendelse som gjør Bk360 utilgjengelig over en lengre periode ennå ikke er tilstrekkelig kartlagt og beskrevet for hele kommunen. Hvordan den enkelte tjeneste påvirkes vil antagelig variere mye, og påvirkes både av tjenestens art, hvordan den enkelte tjenesteeier har valgt å bruke Bk360, og i hvor stor grad den enkelte tjenesteeier eller etat har etablert lokale kontinuitetsplaner som sikrer tjenesteleveransene hvis saks- og arkivsystemet er utilgjengelig.

Deloitte viser i sin rapport til at kommunen har et godt beredskapsplanverk, men at det ikke er like enkelt å dokumentere etterlevelsen av planverket. Årlige beredskapsøvelser inngår i SDIs årshjul og etterlevelsen vil følges nøye opp fremover.

Etableringen av senteret for digital sikkerhet vil gjøre det tydeligere hvordan operativ hendelseshåndtering skal foregå i praksis og hvilke ressurser som skal bidra ved eventuelle hendelser og avvik.

Med hilsen,

Tor Corneliussen – Kommunaldirektør for finans, næring og eiendom

Dokumentet er godkjent elektronisk.

Vedlegg 2: Revisjonskriterier

Krav i lov og forskrift

Overordnet om kommunens beredskapsplikt

Kommunens plikter knyttet til sivilt beredskap er fastsatt i Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven), og konkretisert i Forskrift om kommunal beredskapsplikt. Bestemmelsene om kommunal beredskapsplikt retter seg mot å utvikle en beredskap for uønskede hendelser som utfordrer kommunen. Av § 1 i Forskrift om kommunal beredskapsplikt går det frem at:

Kommunen skal jobbe systematisk og helhetlig med samfunnssikkerhetsarbeidet på tvers av sektorer i kommunen, med sikte på å redusere risiko for tap av liv eller skade på helse, miljø og materielle verdier.

Overordnet beredskapsplan

Av §15 i sivilbeskyttelsesloven går det videre frem at kommunen skal utarbeide en beredskapsplan som bygger på risiko- og sårbarhetsanalysen i §14, og som skal revideres årlig. Beredskapsplanen skal inneholde en oversikt over hvilke tiltak kommunen har forberedt for å håndtere uønskede hendelse. Som et minimum skal planen inneholde:

(..) en plan for kommunens kriseledelse, varslingslister, ressursoversikt, evakueringsplan og plan for informasjon til befolkningen og media.

Av § 4 i Forskrift om kommunal beredskapsplikt går det frem at kommunens overordnede beredskapsplan skal samordne og integrere øvrige beredskapsplaner i kommunen.

Forskrift om kommunal beredskapsplikt stiller krav til øvelser og opplæring i forbindelse med beredskap. Av § 7 i forskriften går det frem at kommunens overordnede beredskapsplan skal øves hvert annet år, og scenarioene for øvelsene bør hentes fra kommunens helhetlige ROS. Videre stiller §7 i forskriften krav om at kommunen har et system for opplæring som sikrer at ansatte som er tiltenkt en rolle i kommunens krisehåndtering har tilstrekkelige kvalifikasjoner.

NSMs grunnprinsipper for IKT-sikkerhet v2.0

NSMs grunnprinsipper for IKT-sikkerhet er et sett med anbefalinger for hvordan virksomheter kan sikre sine informasjonssystemer. Hvilke anbefalinger som er relevante vil variere fra virksomhet til virksomhet. For store virksomheter vil de fleste tiltakene være relevante, mens mindre virksomheter i større grad må prioritere.[21]

Deloitte har valgt å legge vekt på utvalgte prinsipper i denne revisjonen. De aktuelle prinsippene er gjengitt i de aktuelle kapitlene der de er benyttet som revisjonskriterium.

[21] 2020-07-03 - Støtteprodukter NSMs grunnprinsipper for IKT-sikkerhet.xlsx (live.com)

Vedlegg 3: Nærmere om kommunens styrende dokumenter på IKT området

6.1 Styring av informasjonssikkerheten i Bergen kommune

Med styrende dokumenter mener vi dokumenter som legger føringer for kommunen på ulike områder innen informasjonssikkerhet og personvern som kommunen skal forholde seg til. De styrende dokumentene godkjennes av ledelsen og det er ledelsen som stiller krav til gjennomføring av de ulike prosedyrene i dokumentet.

Under gjengir vi hovedinnholdet i disse styrende dokumentene og beskriver hvordan kommunen skal ivareta digitaliseringen i tråd med eget styringssystem for personvern og informasjonssikkerhet.

6.1.1 Reglement for digitalisering og IKT i Bergen kommune

Et særlig sentralt styrende dokument er reglement for digitalisering og IKT i Bergen kommune[22]. Reglementet gir en oversikt over hvordan digitalisering og IKT er regulert og operasjonalisert i kommunen. Det inneholder også krav som gjelder for ulike fagområder og hvilke roller som har et særlig ansvar for å overholde kravene. Reglementet består av ni ulike fagområder og til hvert av fagområdene gis det en kort forklaring til fagområdets innhold som vist i tabellen under.

Tabell 1 Reglement for digitalisering og IKT - Bergen kommune

	Fagområde	Forklaring	Ansvarlige roller
1.	Systemforvaltning	Med systemforvaltning menes ansvar og aktiviteter knyttet til anskaffelse, forvaltning, drift, videreutvikling og systemadministrasjon av IKT-systemer.	Kommunaldirektør/behandlingsvarlig Systemeier Systemkoordinator
2.	Informasjonsforvaltning	Digitaliseringsdirektoratet legger til grunn at informasjonsforvaltning innebærer et helhetlig syn på aktiviteter og verktøy for å sikre best mulig kvalitet, utnyttelse og sikring av informasjon i en virksomhet.	Kommunaldirektør Systemeier Ansattservice
3.	Sikker og stabil drift og infrastruktur	Kravene knyttet til digital drift og infrastruktur skal sikre at kommunens drift av systemer og løsninger er både sikker og stabil når nye systemer eller tjenester	Systemeier Systemkoordinator

[22] https://allmenningen.bergen.kommune.no/styringsdokument/SD-21-25

		etableres i kommunens infrastruktur	
4.	Avtaleforvaltning innenfor digitalisering og IKT	Avtaleforvaltning og oppfølging av leverandør er sentralt for å sikre at Bergen kommune har en hensiktsmessig portefølje av IKT-systemer og løsninger.	Kommunaldirektør Behandlingsansvarlig Systemeier Prosjekteier Resultatsenhetsleder
5.	Porteføljestyring	Porteføljestyring skal sikre at digitaliseringsarbeidet i kommunen er i tråd med strategier, planer og føringer på området. Det stilles derfor krav til hvordan digitaliseringsprosjekter skal gjennomføres og hvordan prosjektene skal rapportere til porteføljen.	Kommunaldirektør Resultatsenhetsleder Systemeier Prosjekteier Behandlingsansvarlig (hvis databaseansvarlig)
6.	Prosjekt- og programstyring	Bergen kommunes prosjektmetodikk er beskrevet i Prosjekthåndboken. Prosjekthåndboken er førende for alle digitaliseringsprosjekter og er tilgjengelig på Allmenningen, i BkKvalitet og i BkProsjekt.	Prosjekteier
7.	Virksomhetsarkitektur	Virksomhetsarkitektur handler om hvordan kommunen er organisert, hvordan arbeidsprosesser er satt sammen og hvordan IT-løsninger utnyttes slik at man sikrer gode brukeropplevelser, effektivisering og digitalisering på tvers.	Prosjekteier Resultatsenhetsleder Digitaliseringsrådet Prosjektleder
8.	Brukeropplevelse og universell utforming	Kommunens digitale løsninger skal være så brukervennlige at de er et naturlig førstevalg for ansatte, innbyggere og næringsliv. For å få det til må løsningene være brukervennlige for alle, og brukerne må føle seg trygge og ivaretatt i de digitale flatene.	Kommunaldirektør Systemeier

9.	Innovasjon og bærekraft	Innovasjon og fokus på bærekraft krever at kommunen utvikler kultur, kompetanse, ledelse og nye samarbeidsformer.	Resultatsenhetsleder Prosjekteiere
10.	Samstyring	Tilrettelegge for gode samhandlingsprosesser som støtter målet om mest mulig helhetlig digitalisering og IKT i Bergen kommune er det etablert flere samhandlingsfora. Det er etablert totalt seks ulike samhandlingsfora.	SD Ansattservice

6.1.2 Temaplan for informasjonssikkerhet og personvern

Temaplan for informasjonssikkerhet og personvern:2021-2025 har som *formål å legge til rette for at kommunen bedre kan lykkes med å få på plass egnede organisatoriske og tekniske tiltak som gir tilstrekkelig informasjonssikkerhet*. Temaplanen må ses i sammenheng med overnevnte reglement for digitalisering og IKT. Temaplanen ble behandlet i Bergen bystyre 24.03.2021 sak 92/32 og planen skal danne grunnlag for prioritering av kommunens innsats på områdene informasjonssikkerhet og personvern.

Temaplanen gir en introduksjon til de ulike fagområdene innen informasjonssikkerhet og personvern i Bergen kommune, samt en beskrivelse av dagens situasjon. Den omhandler videre omtale av organisering av personvern og informasjonssikkerhet, samarbeid mellom lokale, regionale og nasjonale aktører på informasjonssikkerhetsområdet, samt infrastruktur og forvaltning av fagsystem for informasjonssikkerhet. Temaplanen inneholder også en oversikt over aktuelle tiltak som skal bidra til bedre personvern og informasjonssikkerhet med tilhørende et kostnadsestimat.

I Temaplanen forplikter Bergen kommune seg til å følge Nasjonal sikkerhetsmyndighets (NSM) grunnprinsipper for informasjonssikkerhet, sammen med kommunenes vedtatte rammeverk for risikostyring. NSM sine grunnprinsipper hviler på fire pilarer eller kategorier. Tabellen under gir oversikt over pilarene med tilhørende grunnprinsipper:

Tabell 2 Temaplan for informasjonssikkerhet og personvern:2021-2025[23]

Kategori/Pilar	Grunnprinsipp
1. Identifisere og kartlegge	• Kartlegge styringsstruktur, leveranser og understøttende systemer • Kartlegge enheter og programvare • Kartlegge brukere og behov for tilgang
2. Beskytte og opprettholde	• Ivareta sikkerhet i anskaffelser- og utviklingsprosesser • Etablere en sikker IKT-arkitektur • Ivareta en sikker konfigurasjon • Beskytte virksomhetens nettverk • Kontroller dataflyt • Ha kontroll på identiteter og tilganger

[23] https://bergen.extend.no/cgi-bin/document.pl?pid=bergen&DocumentID=11508

		• Beskytte data i ro og i transitt • Beskytte e-post og nettleser • Etabler evne til gjenoppretting av data • Integrer sikkerhet i prosess for endringshåndtering
3.	Oppdage	• Oppdag og fjern kjente sårbarheter og trusler • Etabler sikkerhetsovervåkning • Gjennomfør inntrengingstester
4.	Håndtere og gjenopprette	• Forbered virksomheten på håndtering av hendelser • Vurder og klassifiser hendelser • Kontroller og håndter hendelser • Evaluer og lær av hendelser

6.1.3 Overordnet beredskapsplan for Bergen kommune – Administrativ del

Den overordnede *beredskapsplanen for Bergen kommune - administrativ del,* er et strategisk dokument som legger rammeverket for all beredskapshåndtering i kommunen, inkludert IKT-hendelser. Planen tar sikte på å sikre en effektiv respons, beskyttelse av befolkningen og håndtering av kriser eller katastrofer som kan oppstå.

Den overordnede beredskapsplanen for Bergen kommune - administrativ del, gir et helhetlig rammeverk for å håndtere kriser og katastrofer. Den hensyntar identifiserte risikoer og sårbarheter, organiserer beredskapsarbeidet, beskriver beredskapsplaner og tiltak, og legger vekt på opplæring, kommunikasjon og evaluering. Gjennom implementeringen av denne planen kan Bergen kommune bedre beskytte sine innbyggere og samfunnets viktige funksjoner under ekstraordinære forhold.

Planen gir en oversikt over ansvarlige aktører og deres roller i beredskapshåndteringen. Videre blir organiseringen av beredskapsarbeidet beskrevet. Dette inkluderer beredskapsorganisasjonens struktur og deres ansvarsområder. Det blir også gitt en oversikt over tilgjengelige beredskapsressurser og hvordan koordineringen av innsatsen skal foregå.

Beredskapsplaner og tiltak er utarbeidet for ulike scenarier, slik som naturkatastrofer, pandemier og terrorhendelser. Planene inneholder spesifikke tiltak og prosedyrer for håndtering av ulike typer kriser. Videre er koordineringen med eksterne aktører, som politi, brannvesen og helsevesen, også inkludert i planen.

Opplæring og øvelser er viktige komponenter i det å forberede seg til å håndtere hendelser. Beredskapsplanen inkluderer tiltak for å sikre at beredskapsorganisasjonen er godt forberedt. Det blir beskrevet opplæringstiltak for beredskapsorganisasjonen, samt planlegging og gjennomføring av jevnlige beredskapsøvelser for å teste responskapasiteten og samhandlingen.

Kommunikasjon og informasjon blir også vektlagt i planen. Det blir utarbeidet en strategi for intern og ekstern kommunikasjon under kriser, samt etablert informasjonskanaler og retningslinjer for krisekommunikasjon.

Planen legger også vekt på evaluering og revisjon. Det blir etablert prosesser for å evaluere beredskapshåndteringen etter en krisehendelse, samt revisjon og oppdatering av beredskapsplanen basert på erfaringer og endringer i risikobildet.

6.1.4 Temaspesifikk beredskapsplan for svikt i informasjonssikkerhet

Seksjon for digitalisering og innovasjon (SDI) har utarbeidet en egen temaspesifikk beredskapsplan for svikt i informasjonssikkerhet. Denne planen er en temaspesifikk beredskapsplan på operasjonelt nivå som skal være utgangspunktet for behandling og håndtering av hendelser knyttet til svikt i informasjonssikkerhet i kommunen. Det er direktør for SDI som er stabsleder for informasjonssikkerhetsstaben og beslutter når hele eller deler av stab skal mobiliseres.

Dersom kommunens kriseledelse (KKL) mobiliseres, vil Direktør SDI fylle funksjonen som fagleder i denne, vedkommende erstattes da av stedfortreder. I en slik situasjon vil det deretter følge umiddelbar varsling som skal sørge for at varsling gjennomføres til enheter som er relevante for hendelsen, basert på alvorlighetsgrad (fem nivåer for alvorlighet er definert) . Videre følger umiddelbare aksjoner for å begrense skade. Dette kan for eksempel være å påse at eventuelle fysiske lokasjoner blir sikret eller påse at sjenerende informasjon blir fjernet fra nettsted eller lignende.

Det er også en egen mobilisering- og kommunikasjonsplan ved hendelser som innebærer svikt i informasjonssikkerhet. Denne er delt opp i en strategisk, operasjonell og taktisk plan. Den viser også til ekstern kommunikasjon. Mobilisering- og kommunikasjonsplan inneholder ulike funksjonskort til samtlige roller i beredskapsorganisasjonen. Tabellen under viser hvilke roller det foreligger funksjonskort for:

Tabell 3 Roller og ansvar i temaspesifikk beredskapsplan for svikt i informasjonssikkerhet

Rolle	Ansvarsområde (forkortet)	Tildelt myndighet (forkortet)
Stabsleder	Stabsleder for Informasjonssikkerhetsstab og leder stabens behandling og håndtering av hendelser knyttet til svikt i informasjonssikkerhet i kommunen.	Delegert myndighet til å mobilisere Informasjonssikkerhetsstab når det vurderes som nødvendig.
Administrativ støtte i informasjonssikkerhetsstab	Stabsleders loggfører og dokumenterer stabens beredskapshåndtering.	Myndighet tilsvarer de fullmakter du besitter i ditt daglige arbeid ved enheten.
Nestleder/stedfortreder	Rådgiver for Stabsleder	Myndighet tilsvarer de fullmakter du besitter i ditt daglige arbeid ved enheten.
Systemeier	Ansvarlig for å forvalte og drifte systemet, herunder og kjenne systemets risikonivå og sikringstiltak.	Myndighet tilsvarer de fullmakter du besitter i ditt daglige arbeid ved enheten.
Fagleder	Ansvarlig for å gi faglige råd innenfor eget ansvarsområde til Stabsleder.	Myndighet tilsvarer de fullmakter du besitter i ditt daglige arbeid ved enheten.
Liaison	Bindeledd mellom Informasjonssikkerhetsstab og enheten du er sendt til.	Myndighet for øvrig i en beredskapssituasjon tildeles av Stabsleder i den enkelte situasjon.
Andre funksjoner i informasjonssikkerhetsstaben	Bistår Stabsleder i beredskapshåndteringen, slik Stabsleder beslutter at er hensiktsmessig.	Myndighet for øvrig i en beredskapssituasjon tildeles av Stabsleder i den enkelte situasjon.

Samtlige roller har definerte ansvarsområder, beskrivelse av tildelt myndighet og viktige arbeidsoppgaver. I tillegg beskrives viktige interne ressurser den ulike rollen kan mobilisere og disponere, viktige eksterne samarbeidspartnere rollen bør koordinere med, hvem som skal varsles, samt hvem som er stedfortreder til den enkelte rolle.

I tillegg er det utarbeidet aksjonskort for både mobilisering og demobilisering. Aksjonskort for mobilisering benyttes når informasjonssikkerhetsstab skal mobiliseres og bruk av aksjonskortet besluttes av Stabsleder. På samme måte benyttes aksjonskort for demobilisering når Stabsleder har besluttet å demobilisere informasjonssikkerhetsstaben etter en hendelse.

Til slutt i beredskapsplanverket er det utarbeidet tre vedlegg:

- Vedlegg 1 – Aksjonskort Risk assessment personopplysninger
- Vedlegg 2 – MAL situasjonsrapport
- Vedlegg 3 – Telefonliste

6.1.5 Gjennomførende dokumenter

Gjennomførenede dokumenter i Bergen kommune sitt styringssystem for personvern og informasjonssikkerhet retter seg i all hovedsak mot de ansatte. Her stilles det mer detaljerte krav som alle ansatt må etterleve i utførelsen av sine arbeidsoppgaver.

Overordnet prosedyre for verdivurdering og klassifisering av informasjon og informasjonssikkerhet
Det er utarbeidet en prosedyre for verdivurdering og klassifisering av informasjon og informasjonssystemer i kommune. Formålet med denne prosedyren er å etablere en oversikt over viktig informasjon og informasjonssystemer med den hensikt å ha en oversikt over hvilke systemer som er kritiske for kommunen. Denne prosedyren er forankret i *reglement for personvern og informasjonssikkerhet*. Når et system er klassifisert til «høy» eller «kritisk» i henhold til tabellen under, følger det av prosedyren at det skal settes krav for å ivareta systemets konfidensialitet, integritet og tilgjengelighet. Dette innebærer blant annet at det settes krav til krav til

- risiko- og sårbarhetsanalyse
- tekniske og organisatoriske tiltak som eksempelvis døgnbemanning, tekniske løsninger for å oppdage og respondere på sikkerhetsbrudd og etablering av vaktordning,
- kontinuitets- og beredskapsplan for hvordan kommunen skal prioritere og gjennomføre reetablering av ett eller flere systemer, herunder prioritering mellom systemer og tjenester.

Tabell 4 Klassifisering av informasjonssystemer[24]

Klasse/område	Tilgjengelighet	Konfidensialitet	Integritet
Kritisk	Systemet understøtter funksjoner og tjenester som er tidskritiske for kommunen i en krisesituasjon	Eksponering av informasjon i systemet vil være ødeleggende for funksjoner og tjenester som er kritisk for kommunen i en krisesituasjon	Feil eller mangler i opplysninger vil være ødeleggende for funksjoner og tjenester som er kritisk for kommunen i en krisesituasjon
Høy	Systemet understøtter funksjoner og tjenester som er tidskritisk for kommunens daglige drift	Eksponering av informasjon i systemet vil være ødeleggende for funksjoner og tjenester som er kritisk for kommunens daglige drift	Feil eller mangler i opplysninger vil være ødeleggende for funksjoner og tjenester som er kritisk for kommunens daglige drift
Middels	Systemet understøtter funksjoner og tjenester som	Eksponering av informasjon i systemet vil kunne være skade kommunens	Feil eller mangler i opplysninger vil kunne skade kommunens

[24] https://bergen.extend.no/cgi-bin/document.pl?pid=bergen&DocumentID=8617

	er viktige for kommunen, men ikke tidskritisk	funksjoner og tjenester i daglig drift	funksjoner og tjenester i daglig drift
Lav	Systemet understøtter ikke funksjoner og tjenester som er tidskritiske for kommunens daglige drift	Eksponering av informasjon i systemet vil ikke påvirke kommunens funksjoner og tjenester i daglig drift	Feil eller mangler i opplysninger vil ikke påvirke kommunens funksjoner og tjenester i daglig drift

Styringsavtale for digitaliserings- og IKT-tjenester i Bergen kommune

Det er utarbeidet en egen stryringsavtale for digitaliserings- og IKT-tjenester i Bergen kommune. Nåværende IKT-driftstjenesteavtale er under avvikling som del av endret organisering og ansvar innenfor Digitalisering og IKT. Etter opprettelsen av en egen etat, Ansattservice, er driftsansvaret for tjenester en del av styringsavtalen med de ulike tjenesteansvarlige. Med tjenesteansvarlig menes en person eller en rolle som har ansvar for administrering, drift og kvalitetssikring av en eller flere IT-tjenester innenfor en organisasjon. Denne rollen innebærer vanligvis å sørge for at de ulike IT-tjenestene fungerer på en pålitelig måte, oppfyller brukerbehov og er i tråd med organisasjonens mål og strategier. Formålet med avtalen er å definere ansvar og sette rammer for de digitaliserings- og IKT tjenester som utvikles, forvaltes og leveres av Ansattservice på vegne av tjenesteområdeeier[25], eksempelvis Bk360.

Inntil ny tjenestekatalog (se under) i kommunens kundestøttesystem, BkService, er ferdig implementert, vil fortsatt flere av vedleggene dagens driftstjenesteavtale være gjeldende.

6.1.6 Tjenestekatalogen

Ansattservice er ansvarlig for drift av de fleste IT-tjenester og fagsystemer som er i bruk i kommunen i dag. Beskrivelse av tjenestene, ansvarsforhold, eierskap, priser mm er beskrevet i IKT Driftstjenesteavtalen. Per i dag består tjenestekatalogen av totalt 12 ulike tjenestebilag som beskriver teknisk infrastruktur, driftskonsept, IKT-styring mm.

Et tjenestebilag (SLA – Service Level Agreement) er et vedlegg til IKT-driftsavtalen og beskriver i detalj hvilke tjenester som skal leveres rundt systemet som oppetid, vakttjenester med mer. Det skal utarbeides tjenestebilag for systemer og tjenester som benytter kommunens infrastruktur for å sikre formelle strukturer rundt fordeling av oppgaver, vakttjenester avhengig av system/løsning, og forventet nede- oppetid. I Temaplanen stilles det krav til SLA for alle systemer og tjenester som benytter kommunens infrastruktur, herunder også Bk360. I forbindelse med dokumentasjonsgjennomgangen ble Deloitte tilsendt en slik oversikt.

6.1.7 Risiko- og sårbarhetsanalyse - BK360

Under fagområde 3 – sikker og stabil drift og infrastruktur i reglement for digitalisering og IKT – Bergen kommune[26]- stilles det krav til gjennomføring av en risiko- og sårbarhetsanalyse av alle systemer og tjenester som benytter kommunens infrastruktur. Ansvarlig for dette er kommunaldirektør og systemeier for det enkelte system.

På Bergen kommune sitt intranett, Allmenningen, finnes det en egen veileder for hvordan man skal gjennomføre en risiko- og sårbarhetsanalyse for IKT-system[27]. Her beskrives også når det skal gjennomføre en ROS-analyse og hvor den skal dokumenteres. Videre er det utarbeidet en veileder for praktisk gjennomføring av ROS i BkStyring, og til slutt en henvisning til Avdeling for personvern og informasjonssikkerhet (API) ved behov for bistand. Samtlige veiledere er lokalisert under Ansatthjelpen og Personvern og informasjonssikkerhet.

Mål og hensikt med å gjennomføre en ROS er å skaffe en oversikt over risikobildet og samtidig kunne prioritere ressurser effektivt i den hensikt å iverksette nødvendige tiltak som reduserer eventuell uakseptabel risiko.

[25] En person eller en rolle som har ansvar for forvaltningen, koordineringen og styringen av en spesifikk tjeneste eller tjenesteområde innenfor en organisasjon eller bedrifts IKT-struktur.
[26] Se tabell 1 Reglement for digitalisering og IKT – Bergen kommune
[27] https://allmenningen.bergen.kommune.no/ansatthjelpen/informasjonstjenester-og-ikt/personvern-og-informasjonssikkerhet/hvordan-gjennomforer-jeg-en-risikoog-sarbarhetsanalyse-ros-for-ikt-system

For Bk360 er det utarbeidet en overordnet ROS og denne ble revidert i mars 2023. Det ble gjort en avgrensning av hva som skulle gjennomgås da analysen ble revidert som sier at:

> *Analysen omfatter ikke risiko som gjelder kommunens nett eller servere da dette antas er dekket av egne tekniske ROS. Moduler og systemer med integrasjoner mot Bk360 forutsettes har egne ROS-analyser. Datakvalitet er den enkelte saksbehandlers ansvar. Hver byrådsavdeling og Bystyrets organer er selv ansvarlig for egen ROS/DPIA ift bruk av Bk360*

I selve analysen er det identifisert 10 ulike risikofaktorer, der *Taushetsbelagt informasjon sendes feil, eksterne kontakter* er den hendelsen med størst konsekvens – svært alvorlig.

Vedlegg 4: Sentrale dokumenter og litteratur

Lov og forskrift

Justis- og beredskapsdepartementet: Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven). LOV-2010-06-25-45.

Justis- og beredskapsdepartementet: Forskrift om kommunal beredskapsplikt. FOR-2011-08-22-894.

Forarbeider, rundskriv, veiledere mv.

Regjeringen: *Meld. St. 10* (2016-2017) *Risiko i et trygt samfunn.*

Nasjonal sikkerhetsmyndighet: *Grunnprinsipper for IKT-sikkerhet.* Sist endret: 30.03.2023.

NS-ISO 27001: 2022. *Informasjonssikkerhet, cybersikkerhet og personvern – Ledelsessystemer for informasjonssikkerhet*.

NS 5814: *Krav til risikovurderinger*, 2021.

Direktoratet for samfunnssikkerhet og beredskap (DSB): *Veileder til forskrift om kommunal beredskapsplikt,* 2021.

Dokumenter fra kommunen

Bergen kommune: *Reglement for digitalisering og IKT*. Publisert: 27.10.2020.

Bergen kommune: *Temaplan for informasjonssikkerhet og personvern: 2021-2025.* Sist endret: 26.04.2021.

Bergen kommune: *Overordnet beredskapsplan for Bergen kommune – administrativ del*. Sist endret: 28.08.2023.

Bergen Kommune: *Reglement for personvern og informasjonssikkerhet*. 28.10.2020.

Bergen kommune: *Bergen ROS 2020, En trygg by for fremtiden*. Risiko- og sårbarhetsanalyse.

Bergen kommune: *Styringsavtale for digitalisering- og IKT tjenester i Bergen kommune*.

Bergen kommune: *Tjenestekatalog*.

Bergen kommune*: Temaspesifikk beredskapsplan for svikt i informasjonssikkerhet*.

Deloitte.