

Granskning av informationssäkerhet och fördjupning av beredskap för it-säkerhetshändelser

Rapport

Huddinge kommun

KPMG AB

2024-10-25

Antal sidor 23



Huddinge kommun

Granskning av informationssäkerhet och fördjupning av beredskap för it-säkerhetshändelser

2024-10-25

Innehållsförteckning

1	Sammanfattning	2
2	Bakgrund	4
2.1	Syfte och revisionsfrågor	5
2.2	Avgränsning	5
2.3	Revisionskriterier	6
2.4	Metod	6
3	Resultat av uppföljning av tidigare granskning av IT-säkerhet	8
3.1	Granskning av IT-säkerhet från 2022	8
3.2	Uppföljning 2024	8
4	Resultat av fördjupning	13
4.1	Inledning	13
4.2	Riskbedömning och planering för it-avbrott	14
4.3	Tillgänglighet till informationssystem och redundans	17
4.4	Intern kontroll	20
5	Samlad bedömning och rekommendationer	21

1 Sammanfattning

Granskningen syftar till att följa upp om kommunstyrelsen beaktat och hört sammat tidigare lämnade rekommendationer i granskning av it-säkerhet från 2022.

Vår samlade bedömning avseende uppföljning av den tidigare granskningen av IT-säkerhet är att kommunstyrelsen inte vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer.

Utifrån resultatet av den uppföljande granskningen av IT-säkerhet kvarstår följande rekommendationer till **kommunstyrelsen**:

- Revidera riktlinjer för informationssäkerhet avseende ansvar för den tekniska säkerheten
- Se över vilka ytterligare instruktioner och anvisningar som det finns behov av för att etablera en styrning av informationssäkerhetsarbetet
- Fastställa kommunövergripande incidenthanteringsrutiner som tillämpas av alla verksamheter. Samt tillse att nämnder upprättar kompletterande incidenthanteringsrutiner utifrån verksamhetsspecifika krav och lagar
- Utvärdera befintliga kontinuitetsplaner samt införa tester av de planer som finns för att säkerställa att underlag skulle fungera vid särskilda händelser

Se rapportkapitel 5 "Samlad bedömning och rekommendationer" för samlad bedömning i sin helhet. På följande sida redovisas översiktlig bedömning av den fördjupade granskningen av kontinuitetsplanering.

Vår samlade bedömning är att kommunstyrelsen, både utifrån sitt övergripande ansvar för styrning och ledning av kommunens beredskapsarbete, samt utifrån sitt verksamhetsansvar, inte säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska IT-säkerhetshändelser. Vår bedömning är att vård- och omsorgsnämnden säkerställt detta.

I tabellen presenteras bedömning per revisionsfråga och revisionsobjekt.

Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?	
Kommunstyrelsen	Nej
Vård- och omsorgsnämnden	Ja
Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?	
Kommunstyrelsen	Ja
Vård- och omsorgsnämnden	Ja
Har övningar genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig?	
Kommunstyrelsen	Nej
Vård- och omsorgsnämnden	Ja
Har åtgärder för att säkerställa kontinuiteten identifierats och vidtagits?	
Kommunstyrelsen	Nej
Vård- och omsorgsnämnden	Ja
Finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem?	
Kommunstyrelsen	Nej
Vård- och omsorgsnämnden	Ja
Finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar?	
Kommunstyrelsen	Nej
Vård- och omsorgsnämnden	Delvis

Se rapportkapitel 5 "Samlad bedömning och rekommendationer" för samlad bedömning i sin helhet samt rekommendationer till följd av den fördjupade granskningen.

2 Bakgrund

KPMG har av Huddinge kommuns revisorer fått i uppdrag att följa upp tidigare genomförd granskning samt utifrån tidigare identifierade brister även inkludera granskning av utvalda nämnders arbete för att säkerställa en tillräcklig beredskap för allvarliga it-säkerhetshändelser. Uppdraget ingår i revisionsplanen för år 2024.

Revisorerna genomförde 2022 en fördjupad granskning av IT-säkerhet. I samband med granskningen följdes även en tidigare granskning av informationssäkerhet från 2020 upp. Båda granskningarna visade ett antal brister och den samlade bedömningen att kommunstyrelsen inte hade säkerställt en ändamålsenlig styrning eller intern kontroll av informations- och it-säkerhetsarbetet. Vid tiden saknades ett ledningssystem för informationssäkerhet, vilket utgör ramverk för ansvarsfördelning och hur arbetet ska bedrivas. Likaledes bedömdes kommunen sakna en tillräcklig organisation för att ha förutsättningar att bedriva ett systematiskt informationssäkerhetsarbete.

Utifrån de brister som konstaterats i tidigare granskningar är vår bedömning att kommunen vid en allvarlig it-säkerhetshändelse, exempelvis cyberattacker eller annat sabotage, i nuläget innebär att kommunens verksamheter riskerar att inte kunna upprätthållas på en tillfredsställande nivå utan allvarliga konsekvenser.

Inom ramen för det kommunala åtagandet finns en rad samhällsviktiga funktioner, vilka om de inte fungerar kan leda till skada för såväl enskilda individer som samhället i stort. Dessa funktioner behöver fungera varje dag även om incidenter inträffar och det för verksamheten är ett så kallat onormalt läge. Det ökande beroendet till it- och informationssystem leder till att ett bortfall av dessa kritiska tillgångar får större konsekvenser än tidigare. I det arbetet krävs väl genomarbetade, förankrade och testade kontinuitetsplaner för att upprätthålla verksamheterna vid sådana händelser.

Ett flertal offentliga organisationer har under de senaste åren utsatts för cyberattacker med stora konsekvenser som följd. Exempelvis har skyddsvärd information förlorats eller röjts till obehöriga eller så har kritiska verksamhetsprocesser stoppats. Brister i informationssäkerheten har därigenom orsakat att kommuner och regioner drabbats av ekonomisk skada och/eller förtroendeskada.

Revisorerna bedömer att de negativa konsekvenserna vid en extraordinär händelse eller annan kris som betydande om det inte finns ändamålsenlig kontinuitetsplanering. Revisorerna drar därför slutsatsen att både sannolikheten för, och konsekvenserna av kritiska it-säkerhetshändelser är icke-försumbar och att arbetet med kontinuitetsplanering för it-säkerhetshändelser behöver granskas. Då ett systematiskt informationssäkerhetsarbete är grunden för att kommunen ska ha säkerhetsåtgärder som är anpassade i förhållande till risker och behov samt skyddsvärde hos informationstillgångarna bedömer revisorerna det som väsentligt att följa upp att kommunstyrelsen hörsammat tidigare lämnade rekommendationer i genomförda granskningar.

2.1 Syfte och revisionsfrågor

Granskningen har syftat till att följa upp om kommunstyrelsen beaktat och hörsammat tidigare lämnade rekommendationer (enligt bilaga A) i granskning av it-säkerhet från 2022. Granskningen avser besvara följande revisionsfrågor:

- Har tillräckliga åtgärder vidtagits mot bakgrund av lämnade rekommendationer?

Utifrån tidigare identifierade brister i informationssäkerheten har granskningen även syftat till att bedöma om kommunstyrelsen och vård- och omsorgsnämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Granskningen har besvarat följande revisionsfrågor:

- Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?
- Har åtgärder för att säkerställa kontinuiteten identifierats och vidtagits?
- Finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem?
- Har övningar genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig?
- Finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar?

2.2 Avgränsning

Granskningen har inte tagit del av underlag eller information som är säkerhetsskyddsklassad.

Granskningen av kommunstyrelsen har avsett uppföljning av tidigare lämnade rekommendationer och inkluderar centrala funktioner inom säkerhet, informationssäkerhet och it. Fördjupning av beredskap för it-säkerhetshändelser har avsett ekonomifunktionen.

Granskningen av vård- och omsorgsnämnden har avsett kommunal hälso- och sjukvård och ordinärt boende (hemtjänst).

För samtliga revisionsobjekt avgränsas stickprov av kontinuitetsplanering att omfatta kritiska processer med stort beroende till informationssystem.

2.3 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen (2017:725)
- MSBFS 2015:5
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (där detta är tillämbart)
- MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (där detta är tillämbart)
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- Tillämbbara interna regelverk, policyer och beslut

2.4 Metod

Granskningen har genomförts genom dokumentgranskning, intervjuer och stickprov.

Dokumentgranskning

Följande dokument har ingått i granskningen:

- Reglemente för styrelsen och nämnder
- Styrande dokument inom krisberedskap/kontinuitetsplanering, informationssäkerhet samt trygghet och säkerhet
- Risk- och sårbarhetsanalys (informationsklass under säkerhetsskydd)
- Reservrutiner för berörda verksamheter

Intervjuer

Intervjuer har genomförts med:

- Kommunstyrelsens presidium
- Vård- och omsorgsnämndens presidium
- Biträdande kommundirektör
- Ekonomichef
- Redovisningschef
- Sektionschef digital drift
- Sektionschef digitalt stöd
- IT-säkerhetsansvarig
- Informationssäkerhetssamordnare
- Säkerhetschef



Huddinge kommun

Granskning av informationssäkerhet och fördjupning av beredskap för it-säkerhetshändelser

2024-10-25

- Framtidsdirektör
- Socialdirektör
- Verksamhetschef äldreomsorg
- Sektionschef särskilt boende och hälso- och sjukvård
- Sektionschef ordinärt boende
- Chef stöd- och utvecklingsenheten

Stickprov

Stickprov har gjorts av upprättade kontinuitetsplaner inom berörda revisionsobjekt och mot bakgrund av given avgränsning i de fall dylika underlag erhållits.

Samtliga intervjupersoner har getts möjlighet att faktakontrollera rapporten.

3 Resultat av uppföljning av tidigare granskning av IT-säkerhet

3.1 Granskning av IT-säkerhet från 2022

Syftet med granskningen var att bedöma om kommunstyrelsen säkerställer att kommunen har en tillräcklig styrning och intern kontroll vad gäller IT-säkerhet.

Den sammanfattande bedömningen utifrån granskningens syfte var att kommunstyrelsen inte hade säkerställt att kommunen hade en tillräcklig styrning och intern kontroll gällande IT-säkerheten. Ett flertal rekommendationer som lämnades i en tidigare granskning hade inte åtgärdats. Dessa bedömdes i vissa delar påverka förutsättningarna för en god IT-säkerhet.

3.2 Uppföljning 2024

3.2.1 Uppföljning av rekommendationer

Detta avsnitt utgörs av uppföljning per rekommendation som lämnades i den föregående granskningen. Uppföljningen utgörs av iakttagelse och bedömning huruvida rekommendationen bedöms vara hörsammad eller ej.

3.2.1.1 *Revidera riktlinjer för informationssäkerhet avseende ansvar för den tekniska säkerheten*

Den tidigare granskningen visade att det saknades dokumenterade beskrivningar av fördelning av IT-säkerhetsansvar och IT-avdelningens uppdrag. Styrande dokument fastställde även att IT-säkerhet är ett verksamhetsansvar, vilket bedömdes som en felaktig beskrivning då ansvaret ansågs åvila funktion med ansvar för IT-drift och säkerhet.

Då den uppföljande granskningen genomfördes pågick, enligt intervjuuppgifter, ett större arbete med att se över och revidera styrande dokument inom informationssäkerhet. Arbetet var inte slutfört då granskningen pågick, men revideringen uppges innehålla ett förtydligande i fråga om roller och ansvar.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte hörsammats i tillräcklig omfattning.

Det är positivt att arbete med att se över styrande dokument pågår. För att rekommendationen skall betraktas som hörsammad behöver dokumenten fastställas och inkludera revidering med avseende på tidigare bedömda brister.

3.2.1.2 Rekommendation: Se över vilka ytterligare instruktioner och anvisningar som det finns behov av för att etablera en styrning av informationssäkerhetsarbetet

Vid den tidigare granskningen bedömdes kommunens styrande dokument inom informationssäkerhet som otillräckliga för att ge en sammanhållen styrning av informationssäkerhetsarbetet. Dels var dokumenten föråldrade, dels saknades kravnivåer för IT-säkerhet och styrning av IT-avdelningens arbete, liksom tydliga roller för nyckelfunktioner. Program för informationssäkerhet¹ saknades också, men skulle beslutas senare samma år som granskningen genomfördes.

I den uppföljande granskningen framkommer att kommunen fortfarande saknar ett ledningssystem för informationssäkerhet. Trygghets- och säkerhetssektionen har uppdragits att sådant ska implementeras under 2024, vår bild är emellertid att de intervjuade uppfattar att tidsplanen inte kommer att hålla.

Som vi beskrev under föregående rekommendation pågår arbete med att se över dokument. Därvid har vi inom ramen för den uppföljande granskningen delgetts samma dokument som fanns vid den föregående granskningen. Detta inkluderar även ett Program för trygghet och säkerhet 2018-2021², där informationssäkerhet ingår. Muntligen uppges att programmet ingår i den dokumentöversyn som pågick då granskningen genomfördes. Utmaningen uttrycks vara att skapa dokumentation som är till faktiskt stöd och inte bara en administrativ överbyggnad.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte hörsammats.

Vi anser att kommunstyrelsen behöver säkerställa att framtagandet av styrande dokument prioriteras. Det är anmärkningsvärt att det dokument som är vägledande inom informationssäkerhet inte aktualiserats sedan 2018, liksom att roller och ansvar för arbetet ännu inte förtydligats. Innebörden av det är att kommunstyrelsen inte säkerställt en tillräcklig styrning av kommunens informationssäkerhetsarbete.

Vi anser att kommunstyrelsen behöver beakta ändamålsenligheten i de styrdokument som fastställts. Det är viktigt att dokumenten har tydliga kravnivåer då sådana är en väsentlig del av styrningen.

3.2.1.3 Fastställa en ny och uppdaterad modell för riskanalys och informationsklassning

Vid den föregående granskningen använde kommunen en föråldrad modell för informationsklassning som inte tog hänsyn till aktuella lagar och regelverk.

I den uppföljande granskningen uppges intervjuade att informationsklassningar görs i förhållande till NIS-direktivet och i regel enligt KLASSA-metoden³. Kommunens informationssäkerhetssamordnare har därtill utvecklat en egen klassningsmetod, vilken var på väg att implementeras då granskningen genomfördes.

¹ Benämndes informationssäkerhetspolicy i föregående granskning.

² Kommunfullmäktige, 2018-06-18

³ Metod för informationsklassning som tagits fram av Sveriges kommuner och regioner, SKR.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen hörsammats.

Klassningar genomförs i nuläget enligt en vedertagen modell som beaktar gällande lagstiftning och regelverk.

3.2.1.4 Stärka verksamheternas roll i bedömningen av informations skyddsvärde

Otillräcklig involvering av verksamheterna vid informationsklassningar bedömdes som en brist i den tidigare granskningen. Följden konstaterades vara att det inte var möjligt att avgöra om it-säkerhetsåtgärder som vidtogs efter klassning var tillräckliga eftersom adekvata informationsklassningar bygger på verksamhetskännedom.

Vid den uppföljande granskningen framhåller intervjuade att arbetet med klassningar har stärkts sedan den föregående granskningen på så vis att "rätt" verksamhetsrepresentanter deltar vid klassningar i högre utsträckning. Vidare uppges att den nya klassningsmodell som utvecklats, är enklare, mindre tidskrävande och inte ställer lika höga krav på att deltagarna är it-tekniskt initierade. Den nya klassningsmodellen tros öka förutsättningarna för verksamheterna att ta ytterligare större ansvar.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen i allt väsentligt är hörsammad.

Det är positivt att den nya klassningsmodellen anpassats för att ta hänsyn till verksamheternas förutsättningar. Vi delar uppfattningen att en mer lätthanterlig modell stärker möjligheterna att verksamheterna genomför klassningar. Däremot bedömer vi att den nya modellen behöver börja tillämpas för att rekommendationen ska ses som fullt ut hörsammad.

3.2.1.5 Tillse att beslut om riskreducerande åtgärder i internkontrollen verkställs och att uppföljning sker av att åtgärder lett till minimerad risk

Den tidigare granskningen visade att kommunstyrelsens internkontrollplan för 2022 beaktade två risker inom IT-drift. Nedan redogör vi för de två riskerna samt hur kommunstyrelsen avsåg motverka dessa.

- Risk för exponering för eventuella cyberattacker och intrångsförsök på grund av ökad cyberbrottslighet. Riskreducering skulle ske genom stärkt skydd mot phishingmejl.
- Risk att bryta mot lagstiftning genom användning av icke-europiska molntjänster. Riskreducering skulle ske genom att kommunen avsåg dokumentera sin viljeriktning inom frågan.

Granskningen visade en brist i att riskerna och åtgärderna inte hade följts upp inom ramen för uppföljning av internkontrollplanen.

Enligt intervjuade i den uppföljande granskningen har ett antal åtgärder vidtagits rörande de bägge riskerna. Avseende risker kopplade till cyberhot hade kommunen, då

granskningen genomfördes, nyligen upphandlat en extern leverantör för övervakning av it-miljön samt genomfört utbildningar i syfte att stärka kunskap och medvetenhet om cyberhot. Avseende användning av molntjänster uppges att kommunledningen beslutat att svenska leverantörer ska användas i första hand, därefter europeiska, varvid risken numera ses som obsolet.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen i allt väsentligt hör sammats.

Redovisade åtgärder är ändamålsenliga i förhållande till utpekade riskområden. Vi anser att utfall av genomförda åtgärder bör dokumenteras för att visa att åtgärder vidtagits i förhållande till kontrollmomenten i internkontrollplanen.

3.2.1.6 Att genomföra penetrationstester av IT-miljön

De intervjuade uppger i den uppföljande granskningen att två tekniska genomlysningar genomfördes under 2023. Resultatet har utmynnat i en prioriteringsbaserad åtgärdslista som it-avdelningen arbetar med. Exempel som nämns att multifaktorsautentisering införts till följd av detta.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen hör sammats.

3.2.1.7 Fastställa kommunövergripande incidenthanteringsrutiner som tillämpas av alla verksamheter. Samt tillse att nämnder upprättar kompletterande incidenthanteringsrutiner utifrån verksamhetsspecifika krav och lagar

Av den tidigare granskningen framkom att incidenthantering endast beskrevs ytterst översiktligt i riktlinjen för informationssäkerhet. IT-avdelningen konstaterades ha en intern incidenthanteringsprocess, men mer konkreta anvisningar om hur incidenter kan upptäckas på ett övergripande plan saknades. Därtill saknades en tydlig struktur i hur incidentanmälningar hanterades, vilket fått till följd att vissa incidenter fallit mellan stolarna.

I den uppföljande granskningen beskrivs en kommunövergripande incidenthanteringsprocess som i delar dokumenterats, och som framförs vara beskriven på kommunens intranät. Enligt förfarandet ska incidenter anmälas till IT-avdelningens helpdesk som därifrån eskalerar anmälningar till rätt mottagare. En utmaning som nämns är incidenter som rör molntjänster i extern drift där incidenter eskaleras till leverantören och inte via kommunens helpdesk. De intervjuade menar att det försämrar kommunens överblick samt försvårar för användaren då det innebär ytterligare en ingång för att anmäla incidenter.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen delvis hör sammats.

Vi ser positivt på ambitionen om en väg in för incidentanmälningar då detta likriktar och standardiserar incidenthanteringen i hela kommunen. Vi anser att hela

incidenthanteringsprocessen behöver dokumenteras, vilket är en del i en robust incidenthantering.

3.2.1.8 Utvärdera befintliga kontinuitetsplaner samt införa tester av de planer som finns för att säkerställa att underlag skulle fungera vid särskilda händelser

Den tidigare granskningen visade att det fanns kontinuitetsplaner inom både IT-avdelningen och andra verksamheter, men att dessa i delar saknade väsentligt innehåll. De hade inte heller testats i övningssituationer, vilket bedömdes utgöra en risk då övningar validerar kontinuitetsplaners funktionalitet.

I den uppföljande granskningen framför intervjuade att status i frågan är oförändrad sedan föregående granskning. De planer som finns är de samma som redovisades i den tidigare granskningen. Övningar har inte heller genomförts.

Bedömning

Vi bedömer att rekommendationen från den tidigare granskningen inte hörsammats.

Att kontinuitetsplaner är aktuella och har testats är fundamentalt för kommunens resiliens avseende IT-avbrott. Vi ser det därför som nödvändigt att kontinuitetsplanerna utvärderas för att visa om de är tillräckligt omfattande, samt att de testas för att säkerställa deras ändamålsenlighet.

3.2.2 Samlad bedömning av uppföljning tidigare rekommendationer

Vår samlade bedömning avseende uppföljning av den tidigare granskningen av IT-säkerhet är att kommunstyrelsen inte vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer.

En väsentlig iakttagelse i den föregående granskningen var att kommunstyrelsen inte hade fastställt roller, ansvar och kravställning av informationssäkerhetsarbetet som därvid bedömdes sakna tillräcklig styrning och intern kontroll. Vi kan i den uppföljande granskningen konstatera att kommunstyrelsen ännu inte fastställt dessa delar. Något ledningssystem för informationssäkerhet har inte heller implementerats.

En utveckling har skett gällande vissa enskilda processer som är väsentliga för ett ändamålsenligt informationssäkerhetsarbete.

Oaktat det bedömer vi att kommunstyrelsens styrning och kontroll av informationssäkerhetsarbetet är fortsatt otillräckligt samt att flertalet av tidigare lämnade rekommendationer kvarstår.

4 Resultat av fördjupning

4.1 Inledning

Kommunens ansvar för krisberedskap och civilt försvar regleras i Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap (LEH) med tillhörande förordning och föreskrifter från Myndigheten för samhällsskydd och beredskap, MSB.

Kommunen har ansvar att upprätthålla samhällsviktig verksamhet och ha förmåga att hantera störningar och krishändelser inom dessa. Myndigheten för samhällsskydd och beredskap har definierat samhällsviktiga verksamheter som *"Verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet"*.

Arbetet med krisberedskap och extraordinära händelser tar sin utgångspunkt i en övergripande Risk- och sårbarhetsanalys som kommuner och regioner enligt lagkrav ska genomföra vid varje ny mandatperiod. En del i RSA-processen är att identifiera vilka samhällsviktiga verksamheter som kommunen bedriver samt att kontinuitetsplanera för dessa.

MSB har även gett ut råd för att säkra tillgången till organisationens information. I den framgår att kontinuitetshantering handlar om att planera för att verksamheten ska kunna bedrivas på en acceptabel nivå oavsett vilken störning den utsätts för.

Ofta är organisationens information nödvändig för att verksamheten ska kunna fungera. Information hanteras idag till stor del digitalt. Kontinuitetshandlingen behöver därför säkerställa tillgång till information och därmed it-resurser. Det kan exempelvis handla om verksamhetsspecifika och administrativa system, e-post, filer, molntjänster och hårdvara som PC, servrar, telefoner och nätverk.

Exempel på arbetssätt som kan behöva planeras är chatt- och videoverktyg för möten, e-post för kommunikation och för att förmedla information samt interna nätverk för att spara eller sprida information. Därtill kan det behövas alternativa arbetssätt i form av utskrivna kontaktlistor, lokala kopior av nödvändig information samt beskrivna rutiner för att övergå till alternativa sätt att bedriva den dagliga verksamheten om tillgång till it saknas.

Mot bakgrund av den ökande hotbilden för cyberattacker med risk att informationssystem och it-miljön inte är tillgänglig för de samhällsviktiga verksamheterna avgränsas denna granskning till kontinuitetsplanering och reservrutiner vid it-bortfall.

4.2 Riskbedömning och planering för it-avbrott

Huddinge kommuns överordnade dokument för krisberedskap är Riktlinje för civil beredskap i Huddinge kommun 2024-2027⁴. Riktlinjen fastställer att kontinuitetsplaner avseende kritiska beroenden ska finnas för samhällsviktig verksamhet. Planerna ska utgå från att verksamheterna ska kunna upprätthålla förmågan enligt två angivna nivåer:

- Minst en vecka utan stöd från omgivningen
- Minst tre månader, i samverkan med andra, men med begränsat stöd från omgivningen

Vi har i granskningen tagit del av kommunens Risk- och sårbarhetsanalys 2023⁵ (version utan sekretessbelagt innehåll). Cyberangrepp respektive IT-attack och dataintrång har använts som planeringsscenarier och risker mot vilka kommunens förmåga att kunna bedriva samhällsviktig verksamhet har analyserats.

IT-system och internetförbindelse pekas även ut som två kritiska beroenden för kommunens samhällsviktiga verksamhet. Av dokumentet konstateras att IT-störningar är en aktuell omvärldstrend som kan kräva höjd beredskap under långvarig tid.

I syfte att stärka förmågan att hantera sådana händelser anger planen att befintliga kontinuitetsplaner har reviderats medan verksamheter som saknat kontinuitetsplaner påbörjat framtagandet av sådana.

Även kommunens Program för trygghet och säkerhet 2018-2021⁶ slår fast att kommunen, med avstamp i RSA, ska planera och genomföra åtgärder för att stärka förmågan att bedriva samhällsviktig verksamhet. Kravet på kontinuitetsplanering bekräfts även i Riktlinje för informationssäkerhet⁷ där det framgår att sådana planer ska upprättas inom alla verksamheter.

Arbetet utgår från Uppdragsplan för Kontinuitetsplanering samhällsviktig verksamhet 2020-2023⁸ som är att betrakta som en övergripande uppdragsbeskrivning för arbetet. Planen innehåller en tidssatt aktivitetsplan för framtagande av kontinuitetsplaner inom samhällskritiska verksamheter, som anger att arbetet skulle vara slutfört under 2023.

Dokumentet har emellertid tillfogats en ändringshistorik som visar att tidplanen har förskjutits, slutdatum för upprättande av kontinuitetsplaner framgår dock ej. Av intervjuer framgår ingen tydlig orsak till varför arbetet fördröjts. Intervjuade konstaterar att arbete med kontinuitetsplanering är pågående och har kommit olika långt inom olika verksamheter, där samhällsviktig verksamhet ligger i framkant. Det framförs att flera verksamheter har tagit fram kontinuitetsplaner för ett antal år sedan, men dessa tros vara inaktuella och har inte heller testats.

⁴ Kommunfullmäktige, ej daterad

⁵ Daterad 2023-11-22

⁶ Kommunfullmäktige, 2018-06-18

⁷ Kommunfullmäktige, 2019-12-09

⁸ Reviderad 2022-01-13

Ur ett kommungemensamt perspektiv samordnas arbetet genom trygghets- och beredskapssektionen där fyra medarbetare uppdragits att stötta verksamheterna med beredskapsplanering utifrån kravställningen i de styrande dokumenten.

4.2.1 Kontinuitetsplaner och kritiska beroenden till informationssystem

Vi har delgetts en Vägledning för framtagande av kontinuitetsplan⁹ samt en tillhörande mall¹⁰ som ska utgöra stöd vid kontinuitetsplanering. I intervju uppges emellertid att arbetet utgår från respektive verksamhets förutsättningar då dessa skiljer sig betydligt. Som gemensam nämnare uppges att arbetet utgår från de risker och sårbarheter som beskrivs i RSA.

I granskningen har ingått att göra stickprov av underlag för kontinuitetsplanering för att kontrollera om kritiska beroenden till informationssystem har ingått i analys och planering för granskade verksamheter.

Resultat av stickproven framgår enligt nedan tabell:

Ansvarig nämnd	Verksamhet	Kontinuitetsplan finns	Risk för it-avbrott har inkluderats	Kritiska informations-system är identifierade
Kommunstyrelsen	Ekonomifunktion	Nej	Ja	Ja
Vård- och omsorgsnämnden	Hemtjänst	Ja	Ja	Ja
	Kommunal hälso- och sjukvård	Ja	Ja	Ja

Figuren visar tabell med stickprov avseende underlag för kontinuitetsplanering.

Kommentar till resultat av stickprov

Som vi tidigare nämnt pågår aktivt arbete med kontinuitetsplanering inom de granskade verksamheterna. Arbetet utgår från de dokumenterade kravnivåerna om en veckas respektive tre månaders IT-bortfall. Nedan redogör vi för utfallet av stickprovsgranskningen av kontinuitetsplaner inom granskade verksamheter:

Ekonomifunktionen

Har som resultat av en workshop identifierat två kritiska processer i händelse av it-bortfall, därigenom också kritiska it-system. Processerna rör ekonomiska utbetalningar. Kvarstående arbete fokuserar mot att dels dokumentera en faktisk kontinuitetsplan, dels ha dialog med andra verksamheter då det tros finnas verksamheter som har kritiska beroenden till ekonomisystemen, men som ekonomiavdelningen inte känner till.

⁹ Rutin, daterad 2022-02-25

¹⁰ Rutin, Kontinuitetsplan för verksamhet/enhet

Hemtjänst/kommunal hälso- och sjukvård

Vid granskningen redovisas kontinuitetsplaner för de verksamhetsprocesser som bedömts ha kritiska beroenden till informationssystem: trygghetslarm (hemtjänst) respektive två dokumentationssystem inom hälso- och sjukvården. Planerna avser kontinuitet vid driftstopp för respektive system och omfattar instruktioner och ansvar för olika moment i syfte att upprätthålla alternativa processer.

I intervju framförs att förvaltningen har en lista över verksamhetskritiska system, som reviderades under våren 2024. En anledning till revideringen var att tydliggöra beroenden på kommunövergripande nivå. Vidare uppges att det sedan tidigare finns kontinuitetsplaner för de flesta av förvaltningens processer och att pågående arbete är inriktat mot att tillse aktualiteten i dessa. Styrdokumentet Plan för socialförvaltningens kontinuitetshantering¹¹ utgör vägledning för arbetet med kontinuitetsplanering inom förvaltningen. Dokumentet krävställer vad kontinuitetsplanerna ska omfatta, som beskrivning av roller, ansvar, uppföljning, processer som ska kontinuitetsplaneras samt mall för hur planerna ska utformas. Granskade kontinuitetsplaner är inte fullständiga i förhållande till mallen, men innehåller väsentlig kontinuitetsplanering.

4.2.2 Övning

Enligt intervjuer har krisövningar med IT-scenarier genomförts av olika verksamheter inom kommunen. Övningarna har dock genomförts i begränsad omfattning och intervjuade konstaterar att det fortsatt föreligger behov av att testa befintliga kontinuitetsplaner.

Bland de verksamheter som ingått i denna granskning har vård- och omsorgsförvaltningen genomfört aktuella övningar. I mitten på februari genomfördes en övning på temat "IT-attack slår ut digitala verksamhetssystem". För två år sedan hölls en övning med trygghetslarm, vilken uppges ha gett lärdomar som använts i kontinuitetsplaneringsarbetet. En övning på temat "kommunikation vid driftstopp" uppges vara inplanerad vid ett senare tillfälle.

4.2.3 Bedömning

Vår bedömning är att det inte finns dokumenterade kontinuitetsplaner eller motsvarande underlag inom kommunstyrelsen. Vår bedömning är att vård- och omsorgsnämnden i allt väsentligt har dokumenterade kontinuitetsplaner.

Vi kan konstatera att arbete med kontinuitetsplanering pågår inom hela kommunen och att verksamheterna kommit olika långt i sina processer. Att det finns en övergripande kravställning och en central samordning främjar likriktning av arbetet.

Vi bedömer att kommunstyrelsen beaktat kritiska beroenden till informationssystem, men arbetet behöver utmynna i en dokumenterad kontinuitetsplan som bygger på en gedigen analys av kritiska beroenden.

¹¹ Beslutad av biträdande socialdirektör, reviderad 2023-12-01

Vi bedömer att vård- och omsorgsnämnden har dokumenterade kontinuitetsplaner som utgår från kritiska beroenden till informationssystem för granskade verksamheter.

Vi noterar även att kommunens program för trygghet och säkerhet är daterat. Kommunstyrelsen bör därvid bedöma om det finns behov av ett aktualiserat program.

Vår bedömning är att övningar inte har genomförts i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig.

Vi bedömer att det endast inom vård- och omsorgsförvaltningen genomförts övningar, vilket är viktigt i syfte att säkerställa en tillräcklig kontinuitetsplanering för it-avbrott, varför vi anser att kommunstyrelsen och vård- och omsorgsnämnden behöver tillse att sådan genomförs inom respektive verksamhetsområde.

4.3 Tillgänglighet till informationssystem och redundans

4.3.1 Analys och bedömningar av skyddsbehov och krav på tillgänglighet

I granskningen har ingått att analysera huruvida kontinuitetsplanering innefattar bedömningar över kritiska verksamhetssystem och informationstillgångar samt redundans. Avseende reservrutiner finns det rutiner som är kopplade till den kravställan som verksamheten ställer mot leverantör eller interna it-avdelningen på exempelvis underhåll, beredskap och svarstid på incidenter. Med extern leverantör är detta ett formellt avtal, kallat SLA (service level agreement). Den överenskommelse som finns enligt SLA eller motsvarande interna it-drift är en del av att säkerställa kontinuiteten. Krav på att sådan ska upprättas ställs i Instruktion för förvaltning.

I tabellen redovisas hur granskade verksamheter bedömt informationstillgångar och kritiska verksamhetssystem, samt om SLA finns.

Ansvarig nämnd	Verksamhet och antal verksamhetssystem	Informationsklassning finns och är aktuell	Åtgärder har vidtagits utifrån analys	SLA finns
Kommunstyrelsen	Ekonomiavdelningen 2 system	Nej	Delvis	Nej
Vård- och omsorgsnämnden	Hemtjänst 1 system	Ja	Ja	Delvis
	Kommunal hälso- och sjukvård 2 system	Ja	Ja	Delvis

Kommentar till granskning av systemdokumentation

Då alltför detaljerade uppgifter om system tillsammans med bedömningar av risker och sårbarheter kan utsätta kommunen för risk väljer vi att i rapporten endast redogöra för iakttagelser på en övergripande nivå.

Enligt Riktlinjen för informationssäkerhet ska kontinuitetsplaner tas fram inom alla verksamheter som del i informationssäkerhetsarbetet. Muntligen beskrivs att detta gjorts inom ramen för framtagandet av systemsäkerhetsanalyser som också omfattar informationsklassningar och handlingsplaner med åtgärder.

I samband med att system informationsklassas ska systemen även prioriteras utifrån fyra nivåer som anger behov av tillgänglighet. Detta framförs ha gjorts för flertalet av kommunens system. Prioriteringen utgör delvis ett stöd för IT-avdelningen om ett större avbrott skulle inträffa. Den uppges dock inte vara tillräckligt detaljerad för att ge bild av vilka av de högst prioriterade systemen som behöver återstartas först i händelse av IT-avbrott.

De intervjuade framför att kommunen har en pågående upphandling av IT-driften där det i förberedelserna ingår att kartlägga vilka system som behöver SLA. Kartläggningen konstateras bli ett viktigt underlag för insikt om återstartsordning för prioriterade system. En försvårande omständighet som lyfts är att det för system med extern drift är upp till systemägaren att följa upp att avtalade SLA hålls av leverantören. Risken är att det fallerar då systemägaren saknar tillräcklig IT-teknisk kunskap, enligt de intervjuade.

I det följande redovisar vi huruvida informationsklassning och åtgärdsdokumentation genomförts av de granskade verksamheterna.

Ekonomifunktionen

Ekonomifunktionen har identifierat två kritiska system som båda ligger inom intern drift. SLA eller motsvarande intern kravställning avseende driftöverenskommelser finns inte. En anledning som nämns är att ekonomiska transaktioner utförs under kontorstid varför jourberedskap inte ses som nödvändig.

Vi har tagit del av dokumentation som visar att informationsklassning genomförts. För ett av de utpekade systemen genomfördes klassning 2016 medan tidpunkt för klassning av det andra systemet inte framgår.

Hemtjänst/kommunal hälso- och sjukvård

För hemtjänst samt kommunal hälso- och sjukvård finns kritiska system i både intern och extern drift. SLA uppges finnas för samtliga identifierade system. Vid avbrott beskrivs muntligen att kommunens tjänsteman i beredskap (TIB) kontaktas och krisorganisation upprättas varvid ansvarig för IT-drift kontaktas för IT-teknisk hantering. Som tillägg till redovisad process hänvisar vi till rapportavsnitt 3.2.1.5 där vi redogör för att kommunen stärkt sin incidenthanteringsförmåga genom att ha upphandlat en extern funktion för övervakning av IT-miljön.

4.3.2 Reservrutiner

En del i att säkerställa verksamhetens kontinuitet är en planering för att upprätthålla verksamheten vid ett it-avbrott. Detta kan ske exempelvis genom manuella instruktioner eller rutiner för medarbetare vid bortfall av kritiska system eller funktioner i system eller genom olika sätt tekniska reservåtgärder i verksamheten.

I vår granskning har ekonomifunktionen redogjort muntligen för reservrutiner avseende kritiska processer rörande olika ekonomiska utbetalningar.

Kontinuitetsplanerna för hemtjänst respektive dokumentation inom hälso- och sjukvården omfattar beskrivning av manuella reservrutiner. I intervju beskrivs också manuella åtgärder som vidtas löpande i syfte att främja redundans för digitala processer. Vi delges därtill att vård- och omsorgsförvaltningen följt upp verksamheternas beredskap vid IT-avbrott avbrott med anledning av nationellt beslut om ökad/terrornivå. Detta skedde i början av februari månad 2024 då verksamhetschefer inom äldreomsorg, funktionsstöd samt individ- och familjeomsorg påmindes om att ha upprättade kontinuitetsplaner med reservrutiner som också ska finnas utskrivna i pappersform. Enligt förvaltningens företrädare visade kartläggningen att reservrutiner fanns på plats för att verksamheten ska kunna möta enskildas behov trots IT-avbrott.

4.3.3 Bedömning

Vår bedömning är att åtgärder inte har identifierats och vidtagits för att säkerställa kontinuiteten inom kommunstyrelsens granskade verksamhet. Vår bedömning är att vård- och omsorgsnämnden identifierat och vidtagit motsvarande åtgärder.

Granskad verksamhet inom kommunstyrelsen har genomfört informationsklassningar och lämnat en redogörelse över manuella reservrutiner. Vår uppfattning är dock att reservrutinerna varken baseras på resultat av klassning eller på någon annan formaliserad riskanalys där behov av åtgärder för kritiska system har identifierats på ett tillräckligt strukturerat sätt. Vi ser även att klassning för det ena systemet är inaktuell medan tidpunkt för klassning av det andra systemet inte framgår, varför vi inte kan säkerställa dess aktualitet.

Granskade verksamheter inom vård- och omsorgsnämnden har genomfört informationsklassningar samt dokumenterat identifierade åtgärder.

Vår bedömning är att kommunstyrelsens granskade verksamhet inte har avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem. Vår bedömning är att vård- och omsorgsnämndens granskade verksamheter har detta.

Vi anser att kommunstyrelsen, även om ekonomiska transaktioner utförs dagtid, behöver kartlägga behov av tillgänglighet och återställning för kritiska verksamhetssystem.

Granskade verksamheter inom vård- och omsorgsnämnden har analyserat behov av tillgänglighet och skyddsåtgärder för verksamhetskritiska system, vilket är väsentligt underlag för en adekvat kontinuitetshandling. Vi bedömer att underlaget behöver förtydligas med avseende på information som hjälper IT-avdelningen att avgöra i vilken ordning som prioriterade verksamhetssystem ska återstartas vid ett avbrott. Kommunstyrelsen behöver tillse att motsvarande underlag tas fram för samtliga prioriterade system inom övriga kommunen.

4.4 Intern kontroll

4.4.1 Kommunstyrelsens och vård- och omsorgsnämndens kontroll avseende kontinuitetsplaneringen

Enligt Riktlinje för civil beredskap i Huddinge kommun 2024-2027 ska kommunstyrelsen, inom ramen för det övergripande ansvaret för kommunens arbete med civil beredskap, följa upp arbetet årligen. Likaså ansvarar varje nämnd för beredskapsarbetet inom respektive verksamhetsområde. Nämnderna är också ålagda att årligen rapportera genomfört arbete och aktuell förmågestatus till kommunstyrelsen.

I intervjuer konstateras att det i dag inte finns någon strukturerad uppföljning av kontinuitetsplaneringen inom kommunstyrelsen. Frågan följs situationsbaserat inom ramen för olika beredningsforum samt av kommunstyrelsens arbetsutskott, men formaliserad uppföljning har inte genomförts. Att det inte gått ett helt verksamhetsår sedan riktlinjen antogs beskrivs som en delanledning till att uppföljningen ännu inte följer fastställd struktur. Samtidigt uttrycks ett behov av att kommunstyrelsen ska få en återslaggning av arbetet. Inte minst mot bakgrund av det tidigare beslutade uppdraget som stipulerade att kontinuitetsplaner skulle ha upprättats under 2023, men också då kommunstyrelsen i nuläget uppges sakna överblick över den samlade kontinuitetsplaneringen inom kommunen.

Som utgångspunkt framförs emellertid att löpande uppföljning av kontinuitetsarbetet ska göras som del av ordinarie verksamhetsuppföljning då arbetet har tydlig operativ förankring. Därvid anser de intervjuade att kontinuitetsplaneringen ska följas upp i delårsredovisning och verksamhetsberättelser för respektive verksamhet.

Vård- och omsorgsnämnden har inkluderat kontinuitetsplanering i nämndens internkontrollplan för 2024 i form av risken "Risk för brister i agerande vid allvarlig samhällsstörning". Som åtgärd ska "Alla enheter ska ha uppdaterade kontinuitetsplaner som är kända av medarbetare och chef". Kontrollmomentet beskrivs ha tillkommit till följd av det systematiska kvalitetsarbete som genomförs löpande, där riskanalys visade att kontinuitetsplaner inte finns för samtliga av förvaltningens viktiga områden.

Vi kan av protokollsgranskning per 2024-09-25 inte se att nämnden följt upp internkontrollplanen under året. Muntligen uppges att nämndens arbetsutskott får löpande information om arbetet med kontinuitetsplanering. Nämnden har även beslutat att arbetet ska redovisas för hela nämnden under november månad.

4.4.2 Bedömning

Vår bedömning är att kommunstyrelsen inte har en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

Vår bedömning är att vård- och omsorgsnämnden delvis har detta.

I styrande dokument finns krav avseende samtliga verksamheters kontinuitetsplanering, samt för styrelsens respektive nämndernas ansvar för uppföljning. Vi kan dock konstatera att arbetet på flera håll inte har genomförts i tillräcklig utsträckning, vilket kommunstyrelsen inte har uppmärksammat genom intern

kontroll eller annan uppföljning. Vi ser därför att uppföljningen är i behov av att stärkas. Framför allt för att säkerställa att kommunens kontinuitet i kritiska verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser. Men också utifrån styrelsens verksamhetsansvar för ekonomifunktionen samt utifrån efterlevnad till styrande dokument. Är avsikten att kontinuitetsplanering ska ske inom ramen för ordinarie verksamhetsuppföljning behöver styrande dokument förtydligas med avseende på det.

Vård- och omsorgsnämnden har inkluderat uppföljning av kontinuitetsplanering i internkontrollplanen samt beslutat om specifik uppföljning av arbetet. Vi ser positivt på att nämnden skapat sig förutsättningar till en god internkontroll och ett ansvarstagande i linje med styrande dokument. För att upprätthålla en tillräcklig och löpande intern kontroll anser vi att vård- och omsorgsnämnden behöver säkerställa att uppföljning sker i enlighet med styrande dokument, samt att kontrollmomentet i internkontrollplanen följs upp och åtgärder vidtas om behov så visar.

5 Samlad bedömning och rekommendationer

Granskningen har syftat till att följa upp om kommunstyrelsen beaktat och hörsammat tidigare lämnade rekommendationer i granskning av it-säkerhet från 2022 samt till att bedöma om kommunstyrelsen och vård- och omsorgsnämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning avseende uppföljning av den tidigare granskningen av IT-säkerhet är att kommunstyrelsen inte vidtagit tillräckliga åtgärder mot bakgrund av lämnade rekommendationer.

En väsentlig iakttagelse i den föregående granskningen var att kommunstyrelsen inte hade fastställt roller, ansvar och kravställning av informationssäkerhetsarbetet som därvid bedömdes sakna tillräcklig styrning och intern kontroll. Vi kan i den uppföljande granskningen konstatera att kommunstyrelsen ännu inte fastställt dessa delar. Något ledningssystem för informationssäkerhet har inte heller implementerats.

En utveckling har skett gällande vissa enskilda processer som är fundamentala för ett ändamålsenligt informationssäkerhetsarbete. Oaktat det bedömer vi att kommunstyrelsens styrning och kontroll av informationssäkerhetsarbetet är fortsatt otillräcklig samt att flertalet av tidigare lämnade rekommendationer kvarstår.

Utifrån resultatet av den uppföljande granskningen av IT-säkerhet kvarstår följande rekommendationer till **kommunstyrelsen**:

- Revidera riktlinjer för informationssäkerhet avseende ansvar för den tekniska säkerheten
- Se över vilka ytterligare instruktioner och anvisningar som det finns behov av för att etablera en styrning av informationssäkerhetsarbetet

Huddinge kommun

Granskning av informationssäkerhet och fördjupning av beredskap för it-säkerhetshändelser

2024-10-25

- Fastställa kommunövergripande incidenthanteringsrutiner som tillämpas av alla verksamheter. Samt tillse att nämnder upprättar kompletterande incidenthanteringsrutiner utifrån verksamhetsspecifika krav och lagar
- Utvärdera befintliga kontinuitetsplaner samt införa tester av de planer som finns för att säkerställa att underlag skulle fungera vid särskilda händelser

På nästa sida följer bedömning och rekommendationer avseende fördjupningen av kontinuitetsplanering utifrån IT-avbrott.

Vår samlade bedömning är att kommunstyrelsen, både utifrån sitt övergripande ansvar för styrning och ledning av kommunens beredskapsarbete, samt utifrån sitt verksamhetsansvar, inte säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska IT-säkerhetshändelser. Vår bedömning är att vård- och omsorgsnämnden säkerställt detta.

Vi har i granskningen tagit del av styrdokument, rutiner och processer för hela kommunens arbete med kontinuitetsplanering. Härigenom konstaterar vi att det finns en styrning och kravställning som reglerar upprättande av kontinuitetsplaner samt ansvarsfördelning och uppföljning. Arbetet samordnas centralt av dedikerade funktioner, vilket borgar för en likriktning av kontinuitetsplaneringen inom hela kommunen samt ger förutsättningar för samverkan över verksamhetsgränserna. Vi kan även se att ett aktivt arbete pågår, men detta görs med variation och har kommit olika långt inom de granskade verksamheterna.

Dokumenterad kontinuitetsplan saknas för ekonomifunktionen, den av kommunstyrelsens verksamheter som ingått i vår granskning. Kontinuitetsplaneringen har heller inte följts upp av kommunstyrelsen, varken utifrån verksamhetsansvar eller utifrån styrelsens samlade ansvar för kommunens beredskapsarbete. Vi anser härigenom att styrelsen brustit i sitt ansvar för och kontroll av den övergripande styrningen. Risken för IT-bortfall och åtgärder för att kunna upprätthålla en acceptabel verksamhet vid dylika händelser har därmed inte beaktats i tillräcklig utsträckning av styrelsen.

Inom vård- och omsorgsnämnden har kontinuitetsplaner upprättats för de granskade verksamheterna. Dessa följer nämndens styrdokument inom området. Nämnden har även formaliserat kontroll och uppföljning av arbetet, vilket vi bedömer säkerställt en tillräcklig planering vid kritiska IT-säkerhetshändelser inom granskade verksamheter.

Utifrån resultatet av vår granskning rekommenderar vi **kommunstyrelsen** att:

- Säkerställa att styrande dokument efterlevs
- Fastställa och besluta om förvaltningsövergripande kontinuitetsplan
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräcklig
- Tillse att åtgärdsplanering genomförs och baseras på aktuell informationsklassning och riskbedömning för informationstillgångar som styrelsen ansvarar för
- Överväga att etablera servicenivåöverenskommelser för samhällsviktig verksamhets informationssystem när detta är tillämpligt, detta i syfte att höja beredskapen
- Säkerställa att IT-avdelningen får ett underlag som tydliggör ordning för återstart av prioriterade it-system
- Förtydliga hur kontinuitetsplanering ska följas upp inom ramen för ordinarie verksamhetsuppföljning så att uppföljning likriktas inom hela kommunen



Huddinge kommun

Granskning av informationssäkerhet och fördjupning av beredskap för it-säkerhetshändelser

2024-10-25

- Följa upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt beslutad kommunövergripande systematik

Utifrån resultatet av vår granskning rekommenderar vi **vård- och omsorgsnämnden** att:

- Etablera en struktur för att säkerställa att uppföljning sker i enlighet med styrande dokument

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Sofie Ernerudh
Verksamhetsrevisor

Anders Petersson
*Uppdragsledare och certifierad
kommunal yrkesrevisor*

Detta dokument har upprättats enbart för i dokumentet angiven uppdragsgivare och är baserat på det särskilda uppdrag som är avtalat mellan KPMG AB och uppdragsgivaren. KPMG AB tar inte ansvar för om andra än uppdragsgivaren använder dokumentet och informationen i dokumentet. Informationen i dokumentet kan bara garanteras vara aktuell vid tidpunkten för publicerandet av detta dokument. Huruvida detta dokument ska anses vara allmän handling hos mottagaren regleras i offentlighets- och sekretesslagen samt i tryckfrihetsförordningen.