Granskning av kontinuitetsplanering vid it-säkerhetshändelser

Rapport

Skövde kommun

KPMG AB

2025-04-14

Antal sidor 18

© 2025 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document classification: KPMG Public

Skövde kommun
Granskning av kontinuitetsplanering vid it-säkerhetshändelser

2025-04-14

Innehållsförteckning

© 2025 KPMG AB. All rights reserved.

Document classification KPMG Public

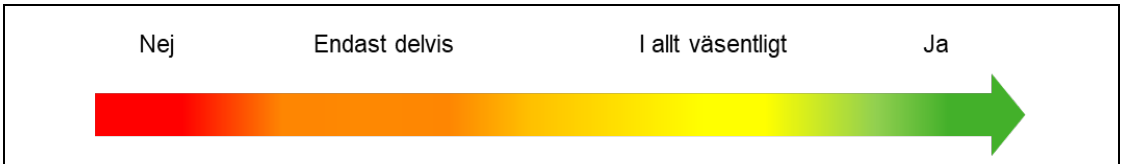
1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Skövde kommun fått i uppdrag att granska kommunens beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa. Uppdraget ingår i revisionsplanen för år 2024. Granskningen har syftat till att bedöma om kommunstyrelsen, vård- och omsorgsnämnden och servicenämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning är att kommunstyrelsen, vård- och omsorgsnämnden samt servicenämnden inte har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska IT-säkerhetshändelser.

Det saknas en tydlig kommunövergripande styrning och process för kontinuitetsplanering inom kommunen. I linje med detta bedömer vi att arbete med kontinuitetsplanering inte genomförts i tillräcklig utsträckning. Brister i styrning och uppföljning stärks av att verksamheter kommit olika långt avseende identifiering av beroenden till kritiska informationssystem och åtgärder för att säkerställa kontinuitet vid it-bortfall.

I det följande redovisas våra samlade bedömningar av respektive revisionsfråga.



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

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

För närmare beskrivning av bakgrunden till våra bedömningar hänvisar vi till respektive avsnitt i revisionsrapporten.

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

- Säkerställa tydliga riktlinjer och kravnivå för kontinuitetsarbete inom kommunen.
- Fastställa och besluta om stabsövergripande kontinuitetsplan.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräckliga.
- Säkerställa att ett mer systematiskt informationssäkerhetsarbete genomförs i hela kommunen.
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som styrelsen ansvarar för.
- Följa upp kontinuitetsplaneringen som en del inom ramen för intern kontroll för att tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

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

- Fastställa och besluta om sektorsövergripande kontinuitetsplan.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Överväga att etablera servicenivåöverenskommelser för samhällsviktig verksamhets informationssystem när detta är tillämpligt, detta i syfte att höja beredskapen.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräckliga.
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som nämnden ansvarar för.
- Följa upp kontinuitetsplaneringen som en del inom ramen för intern kontroll för att tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

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

- Fastställa och besluta om sektorsövergripande kontinuitetsplan.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Överväga att etablera servicenivåöverenskommelser för samhällsviktig verksamhets informationssystem när detta är tillämpligt, detta i syfte att höja beredskapen.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräckliga.
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som nämnden ansvarar för.
- Följa upp kontinuitetsplaneringen som en del inom ramen för intern kontroll för att tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

2 Bakgrund

KPMG har av de förtroendevalda revisorerna i Skövde kommun fått i uppdrag att granska kommunens beredskap och planering för att säkerställa kontinuitet i verksamheter om kritiska it-säkerhetshändelser skulle inträffa. Uppdraget ingår i revisionsplanen för år 2024.

En god krisberedskap är en förutsättning för att kommunens verksamheter ska stå väl rustade inför olika former av samhällsstörningar och för att klara av att hantera olika former av krissituationer. Förmåga att hantera it-säkerhetshändelser baseras även på att det finns ett systematiskt informationssäkerhetsarbete där hot och risker analyserats för att säkerhetsåtgärder ska anpassas efter dessa och skydda kommunens information och verksamhet.

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 den bristande hanteringen lett till att organisationer drabbats av ekonomisk skada eller förtroendeskada. Inledningsvis 2024 utsattes en större leverantör av serverdrift och molntjänster för en ransomware-attack vilken fått en allvarlig påverkan på ett stort antal statliga myndigheters, kommuners och regioners tillgång till sina informationssystem.

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.

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 och reservrutiner behöver granskas.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

2.1 Syfte och revisionsfrågor

Granskningen har syftat till att bedöma om kommunstyrelsen och nämnderna har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Granskningen har avsett besvara följande revisionsfrågor:

- Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?
- 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

För granskningen har vi inte tagit del av underlag eller information som är säkerhetsskyddsklassad.

Granskningen av kommunstyrelsen har avsett dels övergripande styrning och uppföljning, dels verksamhet inom säkerhet, ekonomifunktionen samt i tillämpliga delar även it.

Granskningen av vård- och omsorgsnämnden har avsett verksamheterna inom ordinärt boende samt kommunal hälso- och sjukvård.

Granskningen av servicenämnden har avsett måltidsverksamheten och VA-verksamheten.

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

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

2.3 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen (2017:725)
- Aktiebolagslagen
- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och beredskap.
- Myndigheten för samhällsskydd och beredskaps vägledning för Risk- och sårbarhetsanalyser, MSB245
- MSBFS 2015:5
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (där detta är tillämpbart)
- MSBFS 2018:8 Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster (där detta är tillämpbart)
- MSB:s rekommendationer avseende Ledningssystem för informationssäkerhet
- Tillämpbara interna regelverk, policys och beslut

2.4 Metod

Granskningen har genomförts genom dokumentgranskning, intervjuer och stickprov.

2.4.1 Dokumentgranskning

Följande dokument har ingått i granskningen:

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

2.4.2 Intervjuer

Intervjuer har genomförts med:

- Kommunstyrelsens presidium
- Vård- och omsorgsnämndens presidium
- Servicenämndens presidium
- Kommundirektör
- Säkerhetschef
- Ekonomichef
- Enhetschef systemförvaltning

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

- Sektorchef, sektor vård och omsorg
- Stabschef, sektor vård och omsorg
- Avdelningschef hälso- och sjukvård
- Avdelningschef hemtjänst
- Sektorchef, sektor service
- Stabschef, sektor service
- Teknikchef
- Tf. VA-chef
- Avdelningschef måltidsavdelningen

2.4.3 Stickprov

Stickprov har gjorts av kontinuitetsplanering samt av hur kritiska beroenden till informationssystem bedömts. Granskning har även gjorts av om säkerhetsåtgärder vidtagits för utvalda system samt om det finns avtal om servicenivåer för tillgänglighet och beredskap hos intern it-avdelning eller externa systemleverantörer.

2.5 Bedömningsnivåer

De bedömningar som avlämnas i granskningen har utgått ifrån följande bedömningsnivåer.

2.6 Kvalitetssäkring och faktakontroll

Kvalitetssäkring av granskningen och rubricerad revisionsrapport har skett enligt KPMG:s gängse rutin. Kundansvarig har ansvarat för den interna kvalitetssäkringen av rapporten.

De funktioner som intervjuats har beretts möjlighet att faktakontrollera rapporten i syfte att verifiera dess uppgifter.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

3 Resultat av granskning

3.1 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. Kontinuitetshanteringen 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.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

3.2 Riskbedömning och planering för it-avbrott

Kommunfullmäktige i Skövde kommun har antagit *Övergripande mål och inriktning för arbetet med civil beredskap*[1]. Av detta framgår att två av kommunens prioriterade övergripande uppgifter är att:

- Ha förmåga att hantera en allvarlig eller extraordinär händelse så att människors liv eller hälsa inte riskeras och att skada inte uppstår på fastigheter eller miljö.
- Ha en robust och resilient grundförmåga för att samhällsviktiga verksamheter så långt som möjligt upprätthålls vid en extraordinär händelse eller höjd beredskap.

Vi har i granskningen tagit del av kommunens *Risk- och sårbarhetsanalys 2024–2027*[2] (version utan sekretessbelagt innehåll). I dokumentet listas bland annat central administration, IT och informationsverksamhet, äldreomsorg, kommunens hälso- och sjukvårdsverksamhet, vatten och avlopp samt offentliga måltider som samhällsviktig verksamhet inom kommunens geografiska område. Risk för it-bortfall har inte definierats som ett av områdena som utgör kritiska beroenden för kommunens samhällsviktiga verksamhet. Däremot har elförsörjning och elektroniska kommunikationer identifierats. Beroendet av IT-system nämns även för flera sektorer.

Kommunstyrelsen har enligt sitt reglemente[3] ett ansvar för att leda, utveckla och samordna arbetet med krisberedskap och riskhantering. I *Övergripande mål och inriktning för arbetet med civil beredskap* anges att respektive sektor i enlighet med ansvarsprincipen ska ha en förmåga att så långt som möjligt hantera olika slag av allvarliga händelser inom ordinarie organisation.

Under intervjuer refereras till ansvarsprincipen och sektorernas ansvar, samtidigt som flertalet lyfter behov av en tydligare övergripande styrning, exempelvis avseende kontinuitetsplanering. Säkerhets- och beredskapsenheten inom kommunledningsstaben utgör enligt intervjuade en stödjande funktion för sektorerna. Det framhålls under intervjuer vissa otydligheter gällande enhetens mandat att ge direktiv och styra säkerhets- och beredskapsarbetet.

3.2.1 Kontinuitetsplaner och kritiska beroenden till informationssystem

I *Riktlinje för informationssäkerhet i Skövde kommun*[4] anges att kontinuitetsplanering är av central betydelse för att bedriva verksamheten på en acceptabel nivå under såväl normala förhållanden som vid extraordinära händelser. Det framgår att en kontinuitetsplan ska finnas för driften av IT-verksamheten, baserad på de olika informationssystemens samlade krav och vara integrerade med Skövde kommuns gemensamma kontinuitetsplan.

Av intervjuer framgår att det inte finns någon övergripande process för kontinuitetsplanering i kommunens verksamheter. Som nämnt ovan lyfter flertalet intervjuade behov av en tydligare övergripande styrning avseende

[1] Beslutad av kommunfullmäktige 2024-06-19 § 100
[2] Beslutad av kommunstyrelsen 2023-10-09 § 148
[3] Beslutad av kommunfullmäktige 2022-05-30 § 67
[4] Beslutad av kommunstyrelsen 2010-12-06 § 214

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

kontinuitetsplanering. Exempelvis framhålls önskemål om en acceptabel avbrottstid att utgå från vid kontinuitetsplaneringen av verksamheterna.

Av intervjuer framgår vidare att vissa funktioner utbildats eller ska utbildas i Myndigheten för samhällsskydd och beredskaps (MSB) metod för kontinuitetshantering. Dock tillämpas inte metoden fullt ut i organisationen. Enligt uppgift har kontinuitetsplanering identifierats som ett arbetsområde i kommunledningsstabens verksamhetsplan för 2025.

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[5].

Som nämnt ovan saknas en process i kommunen för kontinuitetsplanering. Stickproven visar att det saknas kontinuitetsplaner för samtliga granskade verksamheter, således finns inte några kontinuitetsplaner där risk för it-avbrott har inkluderats eller kritiska informationssystem har identifierats.

Muntliga uppgifter avseende verksamheternas arbete ger följande lägesbild avseende status på arbetet:

Kommunstyrelsen – ekonomifunktionen

Har identifierat kritiska system och tar vid tidpunkten för granskningen ett omtag gällande informationssäkerhetsklassning. Efter detta planeras en kontinuitetsplan tas fram.

Servicenämnden – måltidsverksamheten samt VA-verksamheten

Det finns kännedom om verksamhetsmässiga sårbarheter för verksamheten, dock har kritiska informationssystem inte identifierats formellt.

Vård- och omsorgsnämnden – hemtjänst samt kommunal hälso- och sjukvård

Har i den egna sektorns risk- och sårbarhetsanalys identifierat kritiska informationssystem.

3.2.2 Övning

I *Övergripande mål och inriktning för arbetet med civil beredskap* anges att regelbundna utbildningar och övningar för att hantera extraordinära händelser ska genomföras inom kommunens organisation.

Kommundirektören ska fastställa övnings- och utbildningsplan. Det anges att samtliga sektorer ska öva en gång per mandatperiod samt att respektive nämnd och styrelse ska fastställa planer inom eget ansvarsområde.

Tidplan och inriktning ska fastställas av kommundirektör i samråd med säkerhetschef och berörd sektorchef.

Gällande rapportering framgår att kommunen är ålagd att redovisa till Länsstyrelsen årligen vilken planering och vilka åtgärder som genomförs inom krisberedskapsområdet. Vidare ska övningar rapporteras till kommunstyrelsen årsvis.

[5] Ekonomifunktionen inom kommunstyrelsen, VA-verksamhet och måltidsverksamhet inom servicenämnden, samt hemtjänst och kommunal hälso- och sjukvård inom vård- och omsorgsnämnden.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

Vi har inte tagit del av något underlag som visar på att det finns en planering av utbildningar eller övningar rörande it-avbrott varken på kommunövergripande nivå eller sektorsspecifika fastställda av respektive nämnd och styrelse.

Av intervjuer framgår att det genomförts och planerats för övningar avseende it-bortfall. Övningar hade vid tid för granskningen genomförts inom kommundirektörens ledningsgrupp samt inom kommunledningsstaben. Övning har planerats för sektor vård och omsorg.

Utifrån de övningar som genomförts har det enligt uppgift konstaterats att det finns behov av ytterligare struktur och systematik. Intervjuade beskriver vidare att vissa kortare it-avbrott skett samt att detta givit möjlighet att testa vissa rutiner under kortare tidsperioder.

3.2.3 Bedömning

Vår bedömning är att det inte finns dokumenterade kontinuitetsplaner eller motsvarande underlag inom kommunstyrelsens, vård- och omsorgsnämndens eller servicenämndens granskade verksamheter.

Vi konstaterar att kommunfullmäktige genom *Övergripande mål och inriktning för arbetet med civil beredskap* kravställer att organisationen ska arbeta med planering för att hantera kriser samt avseende uppföljning/rapportering av arbetet. Vidare konstaterar vi att kommunstyrelsen genom *Riktlinje för informationssäkerhet* ställer krav på kontinuitetsplanering för IT-system. Vi noterar att den sistnämnda antogs av kommunstyrelsen 2010 och inte reviderats därefter.

Vi bedömer att det saknas en tydlig kommunövergripande styrning och process för kontinuitetsplanering inom kommunen.

Vi bedömer även att det saknas kontinuitetsplaner eller motsvarande underlag för samtliga granskade verksamheter. Med motsvarande underlag menar vi dokument som är i linje med MSB:s metod för kontinuitetshantering. Vi noterar att det finns funktioner som utbildats i MSB:s metod för kontinuitetshantering, dock tillämpas inte denna fullt ut i organisationen.

Vi bedömer att sektor vård och omsorg har en mer utvecklad risk- och sårbarhetsanalys och inom ramen för den identifierat kritiska informationssystem som det finns ett beroende till.

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

Det saknas beslutad utbildnings- och övningsplan för kommunen vilket är ett krav enligt lag om kommuner och regioners hantering av extraordinära händelser i fredstid. Detta kravställs även i *Övergripande mål och inriktning för arbetet med civil beredskap*.

I avsaknad av kontinuitetsplaner har övning för att utvärdera dessa inte kunnat genomföras. De övningar som har genomförts har snarare medfört insikt och kunskap om vilka rutiner som behövs.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

Övning är viktigt i syfte att säkerställa en tillräcklig kontinuitetsplanering för it-avbrott, varför vi anser att samtliga revisionsobjekt behöver tillse att sådana genomförs inom respektive verksamhetsområde när kontinuitetsplaner och rutiner har upprättats.

3.3 Tillgänglighet till informationssystem och redundans

3.3.1 Analys och bedömningar av skyddsbehov och krav på tillgänglighet

En del i granskningen har varit att analysera om granskade verksamheter har bedömt vilka skyddsbehov som kritiska it-system har, samt om det finns tydliga krav på tillgänglighetsnivåer och redundans för dessa.

Värdet på informationstillgångar fastställs genom informationsklassningar. Det är även grunden för att bedöma behov av beredskap och reservrutiner vid exempelvis avbrott eller störningar. Mot bakgrund av analys och bedömningar ställs krav från verksamheten till intern it-funktion eller externa leverantörer. Med extern leverantör är detta ett formellt avtal, kallat SLA (service level agreement). Den kravställan som finns i SLA eller motsvarande är en del av att säkerställa kontinuiteten.

KPMG genomförde under 2023 en fördjupad granskning av IT- och informationssäkerhet i Skövde kommun. Granskningen visade på brister i arbetet och resulterade i ett stort antal rekommendationer i syfte att stärka arbetet. Flertalet av rekommendationerna kan ha en påverkan för de frågeställningar som den här granskningen avser att besvara. Särskilt arbetet med riskhantering för informationstillgångar i kritiska verksamhetssystem.

I intervjuer har därför efterfrågats information över hur förbättringsarbetet genomförts med grund i de rekommendationer som den tidigare granskningen av informationssäkerhet lämnade. Den samlade bilden av detta är att det inte genomförts något strukturerat förbättringsarbete med grund i de lämnade rekommendationerna. Dels lyfts stor omsättning av ledande befattningar, dels att omorganisering och andra frågor behövts prioriteras i sektorernas arbete.

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

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

Ansvarig nämnd	Verksamhet	Informations-klassning finns och är aktuell	Åtgärder har vidtagits utifrån analys	SLA finns
Kommunstyrelsen	Ekonomifunktion	Ja	Ja	Ja
Servicenämnden	VA-verksamhet	Nej	Nej	Nej
	Måltidsverksamhet	Nej	Nej	Nej
Vård- och omsorgsnämnden	Ordinärt boende	Ja	Nej	Nej
	Kommunal hälso- och sjukvård	Ja	Nej	Nej

Tabell 1: Sammanställning över kritiska it-system.

Kommentar till granskning av systemdokumentation

Informationsklassningar eller motsvarande kartläggningar för att riskbedöma skyddsbehov och tillgänglighetskrav för informationssystem är ett väsentligt moment i informationssäkerhetsarbetet och syftar till att riskbedöma ett informationssystem och därefter identifiera behov av it-säkerhetsåtgärder.

Muntliga och skriftliga uppgifter avseende verksamheternas arbete ger följande lägesbild avseende status på arbetet:

Övergripande – samtliga verksamheter

Enligt uppgift pågår ett arbete inom IT-avdelningen med att ta fram en förteckning över kritiska system inom sektorerna.

Beträffande incidenthantering och beredskap finns en formell och generell intern beredskap för hantering av it-avbrott och liknande händelser utanför kontorstid. Detta är inte reglerat i avtal.

Kommunstyrelsen – ekonomifunktionen

Vid tidpunkten för granskningen genomförs ett omtag gällande informationssäkerhetsklassning. SLA med extern leverantör finns för ekonomisystem.

Servicenämnden – måltidsverksamheten samt VA-verksamheten

Aktuell informationssäkerhetsklassning saknas.

Vård- och omsorgsnämnden – hemtjänst samt kommunal hälso- och sjukvård

Informationssäkerhetsklassning har genomförts av verksamhetssystem som driftas internt.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

3.3.2 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.

Inom ramen för granskningen har vi tagit del av muntliga uppgifter avseende reservrutiner inom ekonomifunktionen. Vi har tagit del av dokumenterade sådana inom hemtjänst och kommunal hälso- och sjukvård. Inom hemtjänst samt kommunal hälso- och sjukvård finns rutiner i krispärmar på enheterna och det finns enligt uppgift rutiner för regelbunden utskrift av personalplanering och genomförandeplaner.

Vad gäller VA-avdelningen har vi tagit del av vissa muntliga uppgifter samt en tidigare framtagen scenariobeskrivning. Vi har inte tagit del av några reservrutiner för måltidsverksamheten. Det framhålls under intervju att beställningar och personalplanering sköts elektroniskt, dock används inga kostplaneringssystem.

3.3.3 Bedömning

Vår bedömning är att åtgärder endast delvis har identifierats och vidtagits för att säkerställa kontinuiteten inom kommunstyrelsens, vård- och omsorgsnämndens eller servicenämndens granskade verksamheter.

Vi ser att granskade verksamheter har kommit olika långt avseende åtgärder för att säkerställa kontinuitet vid it-bortfall. I de fall det finns identifierade åtgärder bedömer vi att de inte fullt ut vidtagits. Det är positivt att det inom samtliga granskade verksamheter, undantaget måltidsverksamheten, finns reservrutiner. Vi bedömer att det är av vikt att dessa finns, samt att de är dokumenterade och tillgängliga.

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

Vi konstaterar att det inom ekonomifunktionen finns en extern SLA. I övrigt finns en formell och generell intern beredskap inom kommunen.

Vi bedömer att det är en brist att kommunstyrelsen, utifrån sitt övergripande ansvar, inte säkerställt ett systematiskt informationssäkerhetsarbete. Dels mot bakgrund av tidigare lämnade rekommendationer i granskning av informationssäkerhet från 2023. Dels då även denna granskning identifierar behov av åtgärder i syfte att arbetet ska vara systematiskt och tillräckligt i förhållande till aktuella hot och risker.

3.4 Intern kontroll

3.4.1 Kommunstyrelsens, vård- och omsorgsnämndens samt servicenämndens kontroll avseende kontinuitetsplaneringen

I *Övergripande mål och inriktning för arbetet med civil beredskap* fastställs att viss rapportering ska genomföras, dock inte uttryckligen gällande kontinuitetsplanering. Vid

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

tidpunkten för granskningen saknas en formell uppföljning av kontinuitetsplaneringen inom kommunstyrelsen och granskade nämnder.

Intervjuade beskriver att det på kommundirektörens uppdrag tillskapats ett säkerhets- och beredskapsråd i kommunen. Inom rådet har dialoger påbörjats, dock har det enligt uppgift inte lett till konkretiserat arbete och åtgärder vid tidpunkten för granskningen.

I kommunstyrelsens internkontrollplan för år 2024 har nedan två risker med bäring på området identifierats; risk att IT-system utsätts för cyberattacker eller överbelastning samt risk för bristande IT-redundans.

Gällande risken att IT-system utsätts för cyberattacker eller överbelastning var den tillhörande åtgärden att utveckla och stärka IT-säkerhetsarbetet, att undersöka möjligheterna att ingå partnerskap inom IT-säkerhet samt behov av verktyg. Av uppföljning av internkontroll i verksamhetsberättelse framgår att en handlingsplan för IT-säkerhet har tagits fram samt att det parallellt pågår arbete med att stärka rutiner. Vad gäller risk för bristande IT-redundans var den tillhörande åtgärden att göra översyn av behov och möjligheter till ökad redundans Av uppföljning framgår att arbetet med åtgärden är försenat och väntas realiseras under 2025.

Likartade risker eller kontrollområden har inte identifierats inom ramen för internkontrollarbetet för vård- och omsorgsnämnden eller servicenämnden.

3.4.2 Bedömning

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

Granskningen har visat att det finns kravställning i styrande dokument avseende kontinuitetsplanering. Vi kan konstatera att arbetet på flera håll inte har genomförts i tillräcklig utsträckning.

Vi bedömer att det i nuläget saknas både uppföljningsformer över verksamheternas arbete med kontinuitetsplaner och inte heller ingår som kontrollområden inom ramen för intern kontroll-arbetet.

Vi bedömer därför att styrning och uppföljning är i behov av att stärkas avsevärt inom både kommunstyrelsen och granskade nämnder för att säkerställa att kommunens kontinuitet i kritiska verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser. För kommunstyrelsen avser det både den egna verksamheten och det kommunövergripande arbetet. Vi ser att detta med fördel kan inkluderas som uppföljande kontroller inom ramen för internkontrollen.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

4 Samlad bedömning och rekommendationer

Granskningen har syftat till att bedöma om kommunstyrelsen, vård- och omsorgsnämnden och servicenämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Vår samlade bedömning är att kommunstyrelsen, vård- och omsorgsnämnden samt servicenämnden inte har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska IT-säkerhetshändelser.

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

- Säkerställa tydliga riktlinjer och kravnivå för kontinuitetsarbete inom kommunen.
- Fastställa och besluta om stabsövergripande kontinuitetsplan.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräckliga.
- Säkerställa att ett mer systematiskt informationssäkerhetsarbete genomförs i hela kommunen.
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som styrelsen ansvarar för.
- Följa upp kontinuitetsplaneringen som en del inom ramen för intern kontroll för att tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

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

- Fastställa och besluta om sektorsövergripande kontinuitetsplan.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Överväga att etablera servicenivåöverenskommelser för samhällsviktig verksamhets informationssystem när detta är tillämpligt, detta i syfte att höja beredskapen.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräckliga.
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som nämnden ansvarar för.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public

- Följa upp kontinuitetsplaneringen som en del inom ramen för intern kontroll för att tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

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

- Fastställa och besluta om sektorsövergripande kontinuitetsplan.
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering.
- Överväga att etablera servicenivåöverenskommelser för samhällsviktig verksamhets informationssystem när detta är tillämpligt, detta i syfte att höja beredskapen.
- Tillse att övningar genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräckliga.
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som nämnden ansvarar för.
- Följa upp kontinuitetsplaneringen som en del inom ramen för intern kontroll för att tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar.

Datum som ovan

KPMG AB

Jenny Thörn
Verksamhetsrevisor

Lovisa Edvardsson
Verksamhetsrevisor

Mikael Lind
Uppdragsledare och certifierad kommunal revisor

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.

© 2025 KPMG AB. All rights reserved.

Document classification: KPMG Public