



Granskning av kontinuitetsplanering för it-säkerhetshändelser

Rapport

Borgholms kommun

KPMG AB

2024-10-30

Antal sidor 17

© 2024 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



Borgholms kommun
Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

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	Inledning	8
4	Resultat av granskningen	9
4.1	Riskbedömning och planering för it-avbrott	9
4.2	Tillgänglighet till informationssystem och redundans	12
4.3	Intern kontroll	14
5	Samlad bedömning och rekommendationer	16



1 Sammanfattning

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

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen och socialnämnden inte har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser.

Vi har i granskningen har tagit del av styrdokument, rutiner och processer som reglerar arbetet med kontinuitetsplanering. Vi kan även se att det pågår ett aktivt arbete med kontinuitetsplanering inom granskade verksamheter, men detta görs med variation och har kommit olika långt inom verksamheterna. Enligt vår bedömning saknas kontinuitetsplaner inom samtliga granskade verksamheter. Risken för it-bortfall och åtgärder för att kunna upprätthålla en acceptabel verksamhet vid dylika händelser har därmed inte beaktats i tillräcklig utsträckning.

Vi bedömer även att granskade verksamheter brister i efterlevnaden till styrande dokument då informationsklassning och riskbedömning av it-system inte genomförts eller saknar aktualitet. Dessa moment är nödvändiga som underlag för en ändamålsenlig kontinuitetsplanering.

Vår samlade bild är att det i nuläget saknas en tillräcklig kontroll och uppföljning så att arbetet bedrivs enligt den struktur som fastställts i styrdokument och den kravnivå för planering inför it-avbrott som risk- och sårbarhetsanalysen anger. Vi ser därför att uppföljningen är i behov av att stärkas avseende efterlevnad av styrande dokument samt för att säkerställa att kommunens kontinuitet i kritiska verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser. Vi ser i detta behov av att tydliggöra ansvarsfördelning mellan kommunstyrelsen och nämnderna samt i vilken form det är lämpligt att de förtroendevalda är involverade i uppföljning och rapportering av kontinuitetsplaneringen.

I tabellen redovisar vi vår bedömning per revisionsfråga och revisionsobjekt.

Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?	
Kommunstyrelsen	Nej
Socialnämnden	Nej
Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?	
Kommunstyrelsen	Delvis
Socialnämnden	Delvis

**Borgholms kommun**

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

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



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

2 Bakgrund

KPMG har av de förtroendevalda revisorerna och lekmannarevisorerna i Borgholms 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.



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

2.1 Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om kommunstyrelsen och socialnämnden har säkerställt en tillräcklig planering för att upprätthålla kontinuitet i verksamheten vid kritiska it-säkerhetshändelser.

Granskningen har besvarat 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

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

Granskningen har avsett kommunstyrelsen och socialnämnden.

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

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

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



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

2.3 Revisionskriterier

I granskningen har revisionskriterierna utgjorts av:

- Kommunallagen (2017:725)
- 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 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, policys 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 och informationssäkerhet
- Risk- och sårbarhetsanalys (informationsklass under säkerhetsskydd)
- Reservrutiner för berörda verksamheter

Intervjuer

Intervjuer har genomförts med:

- Kommunstyrelsens presidium
- 1 vice ordförande i socialnämnden
- Kommunchef
- Ekonomichef
- It-chef
- Säkerhetssamordnare
- Förvaltningschef socialnämnden



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

- Verksamhetsutvecklare socialnämnden
- Verksamhetschefer inom måltidsverksamheten, ordinärt boende, hälso- och sjukvården och VA.

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.



Borholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

3 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.



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

4 Resultat av granskningen

4.1 Riskbedömning och planering för it-avbrott

Kommunfullmäktige har antagit Föreskrifter för Borgholms kommuns arbete med krisberedskap och höjd beredskap¹ som reglerar och krävställer hantering av samhällsstörningar. Dokumentet gäller hela kommunkoncernen och stipulerar att kommunen ska ha en organisation som möjliggör samhällsviktig verksamhet att kunna bedrivas under minst en veckas tid vid samhällsstörning. Vidare anges att kommunen under varje mandatperiod ska genomföra en risk- och sårbarhetsanalys samt ta fram en utbildnings- och övningsplan som ska syfta till att kunna upprätthålla kommunens ledningsförmåga vid samhällsstörningar.

Vi har i granskningen tagit del av kommunens Risk- och sårbarhetsanalys 2023² (version där sekretessbelagda delar maskats). Dokumentet pekar ut långvarigt IT-avbrott som en typhändelse med risk för allvarliga konsekvenser, där vård och omsorg och teknisk service nämns som kritiskt utsatta. Enligt RSA-dokumentet är krisplaner och kontinuitetshantering av vikt för dessa verksamheter, vilket konstaterats till följd av ett tidigare långvarigt elbortfall.

Inom kommunen finns också informationssäkerhetspolicy³ och Informationssäkerhetsinstruktioner förvaltning⁴ som reglerar kontinuitetsplanering för enskilda it-system.

Härigenom finns styrande dokument som krävställer kontinuitetsplanering ur såväl ett krisberedskapsperspektiv som utifrån informationssäkerhetsarbete. Inriktningen på kontinuitetsplanering förtydligas i intervjuer där det framförs att arbetet i första hand kopplar till verksamhetsrisker och planering som krävs för att kunna upprätthålla verksamhet i ett läge med höjd beredskap och krigsberedskap. Kontinuitetsplanering ska vara en del av beredskapsplaneringen, enligt intervjuade.

Arbetet med kontinuitetsplanering samordnas via ett nätverk med funktioner från socialförvaltningen, utbildningsförvaltningen, tekniska avdelningen, Borgholm Energi samt kommundirektör. Grupperingen leds av säkerhetssamordnare och beskrivs ha satts samman delvis i syfte att kunna hantera gemensamma beroenden verksamheter emellan.

Den bild som ges är att de övergripande ramarna för kontinuitetsarbetet har etablerats, och att nästa steg är respektive verksamhets arbete med att ta fram dokumenterade kontinuitetsplaner. De intervjuade anger vidare att arbetet prioriterats till den samhällsviktiga verksamheten. Kontinuitetsarbetet beskrivs ha katalyserats av incidenten med elbortfall vilket nämnts ovan. Därtill uppges det ha skett en perspektivförskjutning där kontinuitetsplanering tidigare genomförts utifrån en krisberedskapskontext, men där arbetet numera genomförs utifrån ett krigsberedskapsperspektiv.

¹ Beslutad 2023-12-11

² Kommunfullmäktige 2023-09-18

³ 2019-01-02

⁴ 2018-12-28



4.1.1

Kontinuitetsplaner och kritiska beroenden till informationssystem

I RSA 2023 beskrivs processen för RSA-arbetet översiktligt. Här framgår att förvaltningarna och bolagen följt upp tidigare RSA från 2019 och åtgärdat brister samt genomfört verksamhetsbaserade risk- och sårbarhetsanalyser. Närmare konkretiseras inte former för det faktiska arbetet. Intervjuade verksamhetsföreträdare beskriver muntligen att arbetet följer vedertagen metodik från Myndigheten för samhällsskydd och beredskap. Genomförande uppges följa en metodik där säkerhetssamordnare faciliterar ett scenariobaserat kontinuitetsplaneringsarbete inom respektive verksamhet. Då granskningen genomfördes fanns inget uttalat krav när kontinuitetsplanerna ska vara färdigställda.

Utöver respektive verksamhets arbete uppges att kommunledningen 2021 gjorde en prioritering av kommunens tio viktigaste it-system. Enligt de intervjuade ska listan tjäna som vägledning för it-avdelningen i händelse av it-bortfall och situationer som kräver en återgångsprioritering. I avsnitt 4.2 fördjupas iakttagelser om åtgärder och planering för de kritiska beroenden till informationssystem som har gjorts i kontinuitetsplaneringen.

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.

Resultat av stickproven framgår enligt nedan tabell:

Ansvarig nämnd	Verksamhet	Kontinuitetsplan finns	Risk för it-avbrott har inkluderats	Kritiska informationssystem är identifierade
Kommunstyrelsen	Ekonomifunktion	Nej	Delvis	Delvis
Kommunstyrelsen	Måltids-verksamheten	Nej	Nej	Nej
Socialnämnden	Hemtjänst/kommunal hälso- och sjukvård	Nej	Delvis	Delvis

Figuren visar tabell med stickprov avseende underlag för kontinuitetsplanering.

Kommentar till resultat av stickprov

Som vi tidigare nämnt pågår aktivt arbete med kontinuitetsplanering inom flera verksamheter, vilket vidareutvecklas i intervjuer där översiktliga beskrivningar av kontinuitetsprocesser ges muntligen. Processerna konstateras av de intervjuade vara ofullständiga och därmed inte färdiga att dokumentera. Därtill får vi bild av att arbetet kommit olika långt inom de granskade verksamheterna, men att dokumenterade kontinuitetsplaner saknas hos samtliga. Nedan redogör vi för utfallet av stickprovsgranskningen av kontinuitetsplaner.

Commented [E51]: •Finns dokumenterade kontinuitetsplaner eller motsvarande underlag?
•Har kritiska beroenden till informationssystem beaktats i verksamhetens kontinuitetsplanering?



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

Ekonomifunktionen

Intervjuade uppger att framtagande av kontinuitetsplan tar avstamp i it-bortfall för it-system för utbetalning av ekonomiskt bistånd och löner. Dessa processer och system har identifierats som verksamhetskritiska.

Måltidsverksamheten

Har inte identifierat kritiska beroenden till it-system. I intervju uppges att verksamheten använder ett fåtal system varför frågeställningen inte setts som nödvändig att beakta. Intervjuade konstaterar dock att måltidsverksamheten har kritiska verksamhetsberoenden till andra verksamheter.

Socialförvaltningen

Arbetet beskrivs utgå från ett läge med höjd beredskap, varvid förvaltningen gjort en behovsanalys för att prioritera vilka processer som behöver kontinuitetsplaneras. Analys av kritiska system uppges också ha genomförts. Hittills beskrivs arbetet ha gjorts på övergripande nivå medan det framgent ska förankras och konkretiseras inom berörda verksamheter. Enligt de intervjuade ska dokumenterade kontinuitetsplaner påbörjas under hösten 2024 för att vara färdiga under 2025.

4.1.2 Övning

Det har enligt intervjuer inte skett någon planerad övning med specifikt fokus på it-avbrott i kommunen.

4.1.3 Bedömning

Vår bedömning är att det inte finns dokumenterade kontinuitetsplaner eller motsvarande underlag inom kommunstyrelsen eller socialnämnden.

Vi har i granskningen tagit del av styrdokument, rutiner och processer som reglerar arbetet med kontinuitetsplanering. Vi kan även se att det pågår ett aktivt arbete med kontinuitetsplanering inom granskade verksamheter, men det görs med variation och har kommit olika långt. I nuläget saknas dokumenterade kontinuitetsplaner inom samtliga granskade verksamheter.

Att det i stora delar finns en gemensam systematik och samordning av arbetet främjar likriktning av arbetet. Dock bedömer vi att kommunstyrelsen behöver kravställa nivåer och genomförande av kontinuitetsplanering på ett tydligare sätt. Berörda nämnder bör även tillse att de samhällsviktiga verksamheterna prioriterar arbetet med kontinuitetsplanering, i enlighet med interna styrdokument. Att samtliga kommunens verksamheter bedriver arbetet utifrån en gemensam planering är en avgörande faktor för att en fungerande samverkan ska finnas, exempelvis avseende kritiska beroenden över förvaltnings- och verksamhetsgränserna.

Vår bedömning är att kritiska beroenden till informationssystem delvis beaktats i kontinuitetsplanering för socialnämnden samt delvis beaktats inom kommunstyrelsen.

Även om inga dokumenterade kontinuitetsplaner fanns vid tid för granskningen är vår bedömning att samtliga granskade verksamheter förutom måltidsverksamheten i viss



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

utsträckning beaktat kritiska beroenden till informationssystem i de processer som genomförts i arbetet med att upprätta en dokumenterad planering. Oberoende av hur många system som används anser vi att analys av kritiska beroenden behöver göras för att ge en fullständig bild över vilka åtgärder som krävs för att upprätthålla kontinuitet vid it-bortfall.

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

Övning är viktigt i syfte att säkerställa en tillräcklig kontinuitetsplanering för it-avbrott, varför vi anser att kommunstyrelsen behöver tillse att sådan genomförs med avseende på samtliga verksamheter.

4.2 Tillgänglighet till informationssystem och redundans

4.2.1 Analys och bedömningar av skyddsbehov och krav på tillgänglighet

Kommunens informationssäkerhetspolicy anger inriktning av informationssäkerhetsarbetet på övergripande nivå. Ur ett systemperspektiv konkretiseras detta i Instruktion för förvaltning där krav på informationsklassning, riskanalys och kontinuitetsplanering pekas ut som delar i kommunens systematiska informationssäkerhetsarbete.

I granskningen har ingått att analysera huruvida underlag för 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 på nästa sida redovisas hur granskade verksamheter bedömt informationstillgångar och kritiska verksamhetssystem, samt om SLA finns. Som tidigare konstaterats saknas dokumenterade kontinuitetsplaner varför nedanstående uppgifter endast baseras på muntlig information.



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

Ansvarig nämnd	Verksamhet och antal verksamhetskritiska system	Informationsklassning finns och är aktuell	Åtgärder har vidtagits utifrån analys	SLA finns
Kommunstyrelsen	Ekonomiavdelningen 2 system	Nej	Nej	Delvis
Kommunstyrelsen	Måltidsverksamheten Har ej identifierat verksamhetskritiska system	Nej	Nej	Nej
Socialnämnden	Hemtjänst/kommunal hälso- och sjukvård Har identifierat verksamhetskritiska system	Nej	Nej	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.

Med undantag för måltidsverksamheten som inte genomfört informationsklassningar i någon utsträckning får vi bild av att informationsklassningar genomfördes av granskade verksamheter runt år 2020. Genomförandet av klassning beskrivs som en engångshändelse snarare än som ett delmoment i ett systematiskt informationssäkerhetsarbete och arbetet inkluderade inte riskanalyser vilket är en väsentlig del i processen för att fastställa vilka skyddsåtgärder som är nödvändiga.

Vi delges att SLA finns för system som driftas av extern leverantör, vilket är fallet inom ekonomiavdelningen och socialförvaltningen. Internt har inte överenskommelser om driftnivåer fastställts mellan berörd verksamhet och it-avdelningen. It-avdelningen uppges även sakna jour- och beredskapsbemanning.

4.2.2 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.

Vår dokumentationsgenomgång visar att socialförvaltningen har ett fåtal dokumenterade rutiner som i viss utsträckning inkluderar manuell hantering vid it-bortfall. I övrigt beskrivs ickedokumenterade manuella rutiner muntligen av socialförvaltningen, ekonomiavdelningen och måltidsverksamheten.



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

4.2.3 Bedömning

Vår bedömning är att åtgärder inte har identifierats eller vidtagits för att säkerställa kontinuiteten inom kommunstyrelsens eller socialnämndens granskade verksamheter.

Aktuella informationsklassningar och riskanalyser utgör grund för att bedöma risker, konsekvenser och skyddsnivåer för bland annat aspekten tillgänglighet. Då detta endera inte genomförts alls, eller saknar aktualitet, saknas tillräckliga underlag för att påbörja åtgärder och planering.

En betydelsefull kontinuitetsbefrämjande åtgärd är jourberedskap för it-händelser och förmåga att bedöma misstänkta eller pågående incidenter i tidigt skede. Vi anser att avsaknad av intern it-beredskap innebär en risk för möjligheten att upprätthålla kommunens samhällsviktiga verksamhet och ser därigenom behov att nuvarande beredskap utvärderas i förhållande till behov som de samhällsviktiga verksamheter identifierar i arbetet med riskhantering och kontinuitetsplanering.

Vår bedömning är att det inte finns avtalade servicenivåer och beredskap baserade på skyddsvärde och behov av tillgänglighet för verksamhetskritiska informationssystem.

Vi konstaterar att åtgärder har vidtagits med kravställning i förhållande till externa leverantörer men att det internt i nuläget inte finns förutsättningar för högre beredskap eller jour. Då aktuell informationsklassning inte genomförts bedömer vi även att det saknas tillräckliga underlag för upprättade SLA, då behov av säkerhetsåtgärder inte utgår från aktuell riskbedömning.

4.3 Intern kontroll

4.3.1 Kommunstyrelsens och socialnämndens kontroll avseende kontinuitetsplaneringen

I granskningen har det framkommit att det idag inte finns någon strukturerad uppföljning av kontinuitetsplaneringen i kommunen, varken inom kommunstyrelsen eller socialnämnden. Den uppföljning som görs beskrivs ske inom ramen för krigsberedskapsplanering och avrapporteras i första hand som muntlig information från kommundirektör till kommunstyrelsens arbetsutskott. Kommunstyrelsens internkontrollplan⁵ har vidare ett riskmoment med bäring på området ("Risk att kommunen utsätts för cyberattack/skadlig kod"), som framförs ha genererat uppföljning utifrån ett informationssäkerhetsperspektiv.

Inga av de förtroendevalda som vi intervjuat ser behov av ökad delaktighet i kontinuitetsplanering, till exempel i form av beslut eller uppföljning. Motivering är att frågan till största del ses som en verksamhetsfråga.

⁵ Verksamhetsplan med budget 2024 och plan 2025-2027, KS 2023-12-19



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

4.3.2 Bedömning

Vår bedömning är att det inte finns en tillräcklig intern kontroll över att kontinuitetsplaneringen kan tillgodose att verksamheter fungerar tillfredsställande om kritiska it-säkerhetshändelser inträffar. Bedömningen avser både kommunstyrelsen och socialnämnden.

Vi konstaterar att det finns krav i styrande dokument avseende samtliga verksamheters kontinuitetsplanering till exempel kopplat till strukturen för informationssäkerhetsanalys och tillhörande åtgärder samt att kontinuitetsplanering ska göras med hänsyn till it-bortfall. Vi kan samtidigt konstatera att arbetet på flera håll inte har genomförts i tillräcklig utsträckning vilket vare sig kommunstyrelsen eller socialnämnden har uppmärksammat genom intern kontroll eller annan uppföljning. Vi anser inte heller att kontrollmomentet i kommunstyrelsens internkontrollplan är tillräckligt för att kommunstyrelsen ska kunna säkerställa att kommunens kontinuitet i kritiska verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser.

Som vi bedömt i tidigare avsnitt så har inte heller nuvarande beredskap testats eller övats genom planerade krisövningar för att utvärdera att den är tillräcklig. Sammantaget ser vi därför att uppföljningen är i behov av att stärkas avseende efterlevnad av styrande dokument samt för att säkerställa att kommunens kontinuitet i kritiska verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser. Vi konstaterar att det finns behov av att tydliggöra ansvarsfördelning mellan kommunstyrelsen och nämnderna samt i vilken form det är lämpligt att de förtroendevalda är involverade i uppföljning och rapportering av kontinuitetsplaneringen.



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

5 Samlad bedömning och rekommendationer

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

Vår samlade bedömning utifrån granskningens syfte är att kommunstyrelsen och socialnämnden inte har säkerställt en tillräcklig planering för att upprätthålla kontinuiteten i verksamheten vid kritiska it-säkerhetshändelser.

Vi har i granskningen har tagit del av styrdokument, rutiner och processer som reglerar arbetet med kontinuitetsplanering. Vi kan även se att det pågår ett aktivt arbete med kontinuitetsplanering inom granskade verksamheter, men detta görs med variation och har kommit olika långt inom verksamheterna. Enligt vår bedömning saknas kontinuitetsplaner inom samtliga granskade verksamheter. Risken för it-bortfall och åtgärder för att kunna upprätthålla en acceptabel verksamhet vid dylika händelser har därmed inte beaktats i tillräcklig utsträckning.

Vi bedömer även att granskade verksamheter brister i efterlevnaden till styrande dokument då informationsklassning och riskbedömning av it-system inte genomförts eller saknar aktualitet. Dessa moment är nödvändiga som underlag för en ändamålsenlig kontinuitetsplanering.

Vår samlade bild är att det i nuläget saknas en tillräcklig kontroll och uppföljning så att arbetet bedrivs enligt den struktur som fastställts i styrdokument och den kravnivå för planering inför it-avbrott som risk- och sårbarhetsanalysen anger. Vi ser därför att uppföljningen är i behov av att stärkas avseende efterlevnad av styrande dokument samt för att säkerställa att kommunens kontinuitet i kritiska verksamheter kan upprätthållas på en tillfredsställande nivå utan alltför stora konsekvenser. Vi ser i detta behov av att tydliggöra ansvarsfördelning mellan kommunstyrelsen och nämnderna samt i vilken form det är lämpligt att de förtroendevalda är involverade i uppföljning och rapportering av kontinuitetsplaneringen.

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

- Säkerställa tydliga riktlinjer och kravnivå för kontinuitetsarbete inom kommunkoncernen
- Fastställa och besluta om förvaltningsövergripande 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 tillräcklig
- Tillse att åtgärdsplanering genomförs och baseras på aktuell informationsklassning och riskbedömning för informationstillgångar som styrelsen ansvarar för



Borgholms kommun

Granskning av kontinuitetsplanering för it-säkerhetshändelser

2024-10-30

- Överväga att etablera servicenivåöverenskommelser för samhällsviktig verksamhets informationssystem när detta är tillämpligt, detta i syfte att höja beredskapen
- Utvärdera behov av intern jourverksamhet för it-verksamheten i förhållande till de samhällsviktiga verksamheternas behov
- Fastställa former för hur kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar
- Följ upp kontinuitetsplaneringen för kritiska it-säkerhetshändelser i de egna verksamheterna enligt en beslutad kommunövergripande systematik

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

- Fastställa och besluta om förvaltningsövergripande kontinuitetsplan
- Säkerställa att kritiska beroenden till informationssystem beaktas i den egna verksamhetens kontinuitetsplanering
- Tillse att åtgärdsplanering genomförs och baseras på informationsklassning och riskbedömning för informationstillgångar som nämnden ansvarar för
- Säkerställa att SLA baseras på aktuella informationsklassningar och riskbedömningar
- Tillse att övningar som genomförs i syfte att säkerställa att kontinuitetsplaneringen för it-avbrott är tillräckliga
- Fastställa former för hur kontinuitetsplaneringen ska följas upp för att tillgodose att verksamheter fungerar tillfredställande om kritiska it-säkerhetshändelser inträffar

Datum som ovan

KPMG AB

Jenny Thörn

Verksamhetsrevisor

Sofie Ernerudh

Verksamhetsrevisor

Fredrik Ottosson

*Kundansvarig 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.