Mölndals stad

Granskning av kontinuitetshantering inom IT
december 2024

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Mölndals stad har EY genomfört en granskning av stadens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att bedöma om kommunstyrelsen säkerställt ett ändamålsenligt arbete med kontinuitetshantering inom IT, samt ge rekommendationer för att minska risken för att störningar inom IT får betydande konsekvenser.

Följande revisionsfrågor har legat till grund för granskningen:

- Har kommunstyrelsen säkerställt ett ändamålsenligt arbete med att identifiera vad som bör omfattas av kontinuitetsplanering?
- Har kommunstyrelsen säkerställt att riskanalyser genomförts på lämplig nivå för att hantera störningar och avbrott?
- Har kommunstyrelsen säkerställt planer och rutiner för de väsentliga riskerna och scenariona?
- Har kommunstyrelsen säkerställt att övning och utbildning inom kontinuitetshantering genomförs i lämplig omfattning?
- Har kommunstyrelsen säkerställt att ändamålsenliga återläsningstester görs av kritiska system?

Uppdraget genomfördes under maj till november 2024 och baserades på intervjuer med identifierade nyckelpersoner inom stadsledningsförvaltningen i Mölndals stad och två utvalda förvaltningar, samt genomgång av insamlad dokumentation.

Granskningen visar att kommunstyrelsen till viss del säkerställt ett ändamålsenligt arbete med kontinuitetshantering inom IT. Stadsledningsförvaltningen har vidtagit flera åtgärder och utvecklat styrdokument för att stödja övriga förvaltningar i deras kontinuitetsarbete, men det finns brister i samordning och implementering av dessa strategier. Riskanalyser genomförs inte systematiskt på alla nivåer, vilket är ett resultat av att stadens decentraliserade ansvarsmodell skapar otydligheter avseende ansvar inom kontinuitetsarbetet. Övning och utbildning inom kontinuitetshantering genomförs i viss omfattning, men förvaltningarna efterfrågar mer praktiska och realistiska krisövningar. Vidare utförs återläsningstester av kritiska system inte systematiskt eller enligt en etablerad rutin, utan endast på begäran av enskilda förvaltningar.

Baserat på granskningen lämnar EY tre övergripande rekommendationer till kommunstyrelsen:

- Tydliggöra uppdrag och ansvar mellan stadsledningsförvaltningen och förvaltningarna.
- Säkerställa kontinuerlig uppföljning avseende förvaltningarnas kontinuitetshanteringsarbete.
- Säkerställa hårdvarukapacitet och rutiner för återläsningstester.

Innehållsförteckning

1. Bakgrund

Mölndals stad och dess nämnder hanterar stora mängder digital information. Möjligheten att effektivt hantera sådan information i IT-system är idag en förutsättning för i stort sett all verksamhet som bedrivs inom offentlig sektor. Bristfällig säkerhet i informationshanteringen kan därför innebära risker för både anställda och invånare.

Antalet IT- och cyberangrepp ökar och flera organisationer har under senare tid utsatts för storskaliga IT-attacker. I många fall har angriparen ekonomiska incitament och avser att utpressa de drabbade på pengar. I andra fall kan syftet vara att underminera offentliga institutioner legitimitet. För de organisationer som utsatts har konsekvenserna blivit stora, då åtkomsten till verksamhetskritiska system förlorats helt.

År 2021 lät de förtroendevalda revisorerna genomföra en granskning av informationssäkerhet. Denna granskning syftar till att komplettera den tidigare granskningen genom att specifikt omfatta området kontinuitetshantering inom IT. För en kommun är det mycket viktigt att kunna fortsätta leverera samhällsviktiga tjänster även vid störningar. Exempel på störningar kan vara naturrelaterade fenomen som översvämningar och skogsbränder, tekniska störningar och problem eller rena angrepp på IT-miljön från kriminella, terrorister eller statsaktörer.

Med en ändamålsenlig kontinuitetshantering har kommunen möjlighet att minska problemen från ovan störningar och antingen gå tillbaka till normal drift, eller använda alternativa metoder. En god kontinuitetshantering bygger på analys av väsentliga processer, identifiering av risker och ett gediget arbete med att bygga upp planer och rutiner för att hantera störningar och avbrott.

Genom en granskning av kontinuitetshantering inom IT kan revisorerna dra slutsatser om huruvida kommunens förutsättningar för att hantera digital information vid en eventuell störning är ändamålsenlig. Det kan ge såväl revisorer som verksamheten en förståelse för eventuella förbättringsområden som kan stärka kommunens motståndskraft mot framtida angrepp eller andra störningar.

Revisorerna har utifrån ovan bedömt att det är väsentligt att under 2024 göra en fördjupad granskning avseende kontinuitetshantering inom IT.

1.1 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelsen säkerställt ett ändamålsenligt arbete med kontinuitetshantering inom IT, samt ge rekommendationer för att minska risken för att störningar inom IT får betydande konsekvenser.

1.2 Avgränsningar

Granskningen avgränsas i enlighet med ställda revisionsfrågor samt till kontinuitetshantering inom IT-området. IT- och informationssäkerhet i stort eller kontinuitetshantering utanför IT-området kommer inte att granskas.

1.3 Metod och genomförande

Granskningen inleddes med ett uppstartsmöte tillsammans med relevanta personer i Mölndals stads olika verksamheter för att skapa en förståelse kring kontinuitetsarbetets omfattning. Därefter utredde EY hur staden bedriver arbetet med att säkra kontinuerlig drift av IT under störningar och andra svåra förhållanden. Detta genomfördes genom en granskning av styrande dokumentation och annat material som fanns tillgängligt för att besvara revisionsfrågorna.

Som en del av granskningen utförde EY intervjuer med nyckelpersoner från stadsledningsförvaltningen för att få en övergripande förståelse av hur informationssäkerhetsarbetet bedrivs och koordineras från ett centralt perspektiv. Därutöver valde EY att intervjua representanter från vård- och omsorgsförvaltningen och stadsserviceförvaltningen, vars verksamheter är av intresse utifrån ett kontinuitetshanteringsperspektiv. Detta för att få insyn i hur kommunstyrelsens arbete förankras och implementeras ute i verksamheterna.

Granskningen resulterade i föreliggande rapport som beskriver iakttagelser och bedömningar avseende stadens kontinuitetshantering inom IT, samt ger rekommendationer på vad staden framöver kan göra för att stärka sin motståndskraft mot framtida störningar. Innan den slutliga rapporten presenterades för revisionen gav EY representanter från staden möjlighet att genomföra en sakkontroll.

1.4 Tidsplan

Granskningen genomfördes från maj till november 2024, se tabell 1 nedan för granskningens tidsplan.

Tabell 1. Tidsplan

Förberedelser och planering	Maj - Juni 2024
Intervjuer och dokumentinsamling	Augusti - September 2024
Observationer	September 2024
Avstämning	Oktober 2024
Sammanställning och kvalitetssäkring	Oktober 2024
Färdigställande av rapport	Oktober - November 2024
Avrapportering och slutpresentation	November 2024

1.5 Definitioner

Se bilaga 3.

2. Granskning

Till följd av ett försämrat säkerhetspolitiskt läge i Europa såväl som i Sverige har IT-angrepp mot statliga organisationer blivit alltmer förekommande. Kommuner och andra offentliga organisationer som bedriver samhällsviktig verksamhet har således ett ökat krav på att skydda sin verksamhet gentemot angripare, vars syfte är att komma åt känslig information. Det är därför av stor vikt att kommuner i större utsträckning än tidigare arbetar förebyggande, bland annat genom att identifiera cyberangrepp och cyberattacker som risker samt att säkerställa styrdokument som möjliggör för samhällsviktiga verksamheter att bedriva sin verksamhet under och efter cyberattacker.

I följande kapitel analyseras det underlag som ligger till grund för EYs granskning av Mölndals stads kontinuitetshantering inom IT. Granskningen presenteras i fem delar med utgångspunkt i rapportens fem frågeställningar. Dessa avser att besvara huruvida kommunstyrelsen säkerställt ett ändamålsenligt arbete med kontinuitetshantering inom IT.

2.1 Revisionsfråga 1: Har kommunstyrelsen säkerställt ett ändamålsenligt arbete med att identifiera vad som bör omfattas av kontinuitetsplanering?

För svenska kommuner är det idag inte uttryckligen kravställt att bedriva kontinuitetshantering. Däremot framgår det av lag *(2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjdberedskap* och *MSBFS 2015:5 föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser* att det finns ett antal krav på kommuner, som i praktiken innebär att man behöver ha ett fungerade arbete med kontinuitetshantering. MSB listar existensen av kontinuitetsplaner som en faktor för att avgöra om man möter kraven i dess riktlinjer. Denna kontinuitetshantering kan exempelvis innebära att kommuner identifierar viktiga system och ta fram planer för hur dessa ska kunna upprätthållas vid extraordinära händelser.

2.1.1 Iakttagelser

Av styrdokumentet *Strategi för krisberedskap civilt försvar Mölndal 2023-2027* framgår att ansvars-, likhets- och närhetsprincipen ligger till grund för stadens krishanteringsarbete avseende styrning och ansvarsfördelning. Principerna innebär bland annat att *den som har ansvar för en verksamhet under normala förhållanden har samma ansvar under en kris eller ett krig*. Enligt kommunstyrelsens reglemente paragraf tre har kommunfullmäktige i Mölndals stad beslutat att kommunstyrelsen har det övergripande ansvaret för stadens krisberedskap och krishantering. Således är vård- och omsorgsnämnden och den tekniska nämnden ytterst ansvariga för kontinuitetshantering. Detta då nämndernas reglemente paragraf ett beskriver att vård- och omsorgsnämnden och den tekniska nämnden ansvarar för kommunens uppgifter inom sina egna verksamhetsområden.

Kommunstyrelsen har givit stadsledningsförvaltningen till uppgift att leda och samordna krisberedskapsarbetet med stöd av säkerhets- och beredskapschefer. Arbetet med krisberedskap verkställs och genomförs i sin tur av stadens olika förvaltningar. Stadsledningsförvaltningen har i sitt förberedande risk- och krishanteringsarbete tagit fram flera styrdokument som ska ge stöd och vägleda stadens olika förvaltningar i

kontinuitetsplaneringsarbetet. Det framgår att kommunstyrelsen anser att kontinuitetsplanering är av stor vikt för att säkerställa en motståndskraftig beredskap mot avbrott och störningar i kritiska system. Genom dokumentet *Instruktion för systematisk kontinuitetshantering* tillhandahåller stadsledningsförvaltningen instruktioner för hur förvaltningarna kan arbeta för att kartlägga och identifiera kritiska aktiviteter inom sina respektive verksamheter.

Intervjuade nyckelpersoner uppger att stadsledningsförvaltningen har till uppgift att inrikta det strategiska arbetet inom kontinuitetsplanering, men att flera förvaltningar har en viktig roll för att säkerställa att det färdigställs. Vidare uppger intervjudeltagarna att förebyggande insatser vidtagits, såsom arrangerandet av årliga temadagar, diskussionsforum och nätverksmöjligheter. Dessa insatser ska sammantaget uppmuntra till ett aktivt kontinuitetplaneringsarbete bland stadens förvaltningar. Det ska dessutom underlätta utformningen av relevanta beredskapsplaner för respektive verksamhet. Intervjudeltagarna betonar att det formella ansvaret för att säkerställa kontinuitetsplaner och beredskap vid en samhällsstörning är fördelat på stadens nämnder.

Intervjudeltagarna berättar även att kontinuitetsplaneringsarbetet följer stadens strategiska inriktning som sträcker sig fram till 2026, vilket säkerställs genom regelbunden uppföljning. Stadsledningsförvaltningens uppgift är att fungera som en rådgivande funktion och vägleda förvaltningarna i att skapa redundans inför potentiella risker. Kommunstyrelsen presenterar även en strategi för systematisk uppföljning i sin *Strategi för arbetet med krisberedskap och civilt försvar i Mölndals stad* och har därtill arrangerat workshops i syfte att förbättra verksamheternas förutsättningar att bedriva ett motståndskraftigt kontinuitetsplaneringsarbete.

2.1.2 Bedömning

Vi bedömer att stadsledningsförvaltningen till stor del vidtagit förebyggande åtgärder för att säkerställa ett ändamålsenligt arbete med kontinuitetshantering. Vi kan genom granskning av styrdokument och övrig dokumentation styrka att kommunstyrelsen har säkerställt att stadsledningsförvaltningen som ledande och samordnande organ, har tagit fram ett metodstöd för systematisk kontinuitetshantering, vilket tyder på att det finns en tydlig struktur för arbetet med kontinuitetsplanering.

2.2 Revisionsfråga 2: Har kommunstyrelsen säkerställt att riskanalyser genomförts på lämplig nivå för att hantera störningar och avbrott?

För att säkerställa att samhällsviktiga kärnfunktioner kan fortlöpa under en kris är det viktigt att kommunen genomför riskanalyser. Genom att förstå vilka risker som finns kan kommunen vidta proaktiva åtgärder som syftar till att minska eller hantera konsekvenser. Ett förebyggande riskhanteringsarbete kan även påverka hur snabbt en kommun återhämtar sig efter en kris.

2.2.1 Iakttagelser

På central nivå har stadsledningsförvaltningen på uppdrag av kommunstyrelsen sammanställt en risk- och sårbarhetsanalys som identifierar och bedömer risker inom olika

områden. I dokumentet framkommer det att cyberattacker, IT-avbrott och förlust av data utgör en del av stadens hotbild. Flera åtgärder som vidtagits i syfte att säkerställa robusta IT-system och öka sin motståndskraft beskrivs också. Dessa åtgärder innefattar bland annat IT- och informationssäkerhetsgranskningar samt workshops som syftar till att djupare analysera cyberrelaterade risker. Därtill tillhandahåller stadsledningsförvaltningen flera styrdokument, såsom *Anvisningar för informationsklassning och riskanalys för informationssäkerhet* samt *Instruktioner för systematisk kontinuitetshantering*. Dessa dokument beskriver bland annat hur förvaltningarna kan arbeta med riskanalys för väsentliga risker och scenarier.

Intervjuade nyckelpersoner inom stadsledningsförvaltningen uppger att varje nämnd ansvarar för att genomföra riskanalyser för sina IT-system och verksamhetsprocesser. Stadsledningsförvaltningens huvudsakliga uppgift är att finnas som en stödfunktion och genom utbildning, samverkan och nätverksbyggande skapa förutsättningar för att varje förvaltning ska kunna genomföra och bedriva sitt riskhanteringsarbete.

Enligt intervjuade nyckelpersoner på de utvalda förvaltningarna finns det brister avseende kommunstyrelsens nuvarande hantering av risk- och beredskapsplaner för störningar och avbrott. Dessa brister, menar förvaltningarna, har orsakats av ett bristfälligt stöd centralt och avsaknad av en tydlig uppgiftsfördelning mellan stadsledningsförvaltningen och förvaltningarna. För att de intervjuade förvaltningarna ska kunna bedriva ett bättre risk- och sårbarhetsarbete inom IT- och informationssäkerhet behöver en kontinuerlig dialog upprättas, vilket skulle möjliggöras genom etablerandet av samordningsroll inom IT- och informationssäkerhet hos förvaltningarna. Det skulle, enligt förvaltningarna, skapa förutsättningar att bedriva ett mer strukturerat arbete.

2.2.2 Bedömning

Vi gör bedömningen att kommunstyrelsen inte har säkerställt att riskanalyser genomförts på lämplig nivå för att hantera störningar och avbrott. Stadsledningsförvaltningen tillhandahåller visserligen anvisningar som presenterar hur arbetet med riskanalyser ska bedrivas, vilket indikerar att det finns en medvetenhet kring vikten av riskanalyser och en vilja att säkerställa kontinuitet kring detta. Strategin är dock inte förankrad och implementerad hos de granskade förvaltningarna. En orsak som ligger till grund för denna problematik är stadens decentraliserade ansvarsmodell, som skapar en bristande förståelse bland förvaltningarna gällande samverkan och förväntningar. Därmed påverkas också graden av engagemang.

Intervjuer med nyckelpersoner inom stadsledningsförvaltningen visar, liksom granskad dokumentation, att det finns en fastställd struktur för hur uppföljning av riskanalysarbetet ska genomföras. Däremot följer stadsledningsförvaltningen inte upp de utvalda förvaltningarnas arbete med kontinuitetshantering på regelbunden basis, vilket överensstämmer med de utvalda förvaltningarnas upplevelser. Vi bedömer att bristen på uppföljning har resulterat i otydliga riktlinjer och avsaknad av enhetliga metoder, vilket i sin tur försvårat nämndernas och förvaltningarnas möjligheter att effektivt kunna bemöta kommunstyrelsens förväntningar.

2.3 Revisionsfråga 3. Har kommunstyrelsen säkerställt planer och rutiner för de väsentliga riskerna och scenariona?

Dokumentet *instruktioner för systematisk kontinuitetshantering* och tillhörande riktlinjer som upprättats av Mölndals stads Säkerhets- och beredskapsenhet, ställer krav på att förvaltningarna ska analysera och bedriva ett arbete inom kontinuitetshantering. I policyn betonas även att förvaltningarna ska kunna upprätthålla och utföra sina uppgifter på en tolerabel nivå oavsett vilken typ av störning som organisationen utsätts för.

2.3.1 Iakttagelser

Kommunstyrelsen har vidtagit förebyggande åtgärder som syftar till att stärka stadens motståndskraft och täcka risker som kan uppstå i samband med störningar och avbrott. Genom styrdokument tillhandahåller styrelsen metoder för hur riskanalyser kan genomföras för att identifieras potentiella hot och oönskade incidenter som kan orsaka skada inom förvaltningarnas verksamheter. Därtill har stadsledningsförvaltningen tagit fram instruktioner för att stödja förvaltningarna i arbetet med att utveckla kontinuitetplaner. Det finns även exempel som illustrerar hur en kontinuitetsplan kan utformas för att hantera specifika situationer

Av genomförda intervjuer med representanter från stadsledningsförvaltningen framgår att de upplever att det finns en tydlig struktur för vem som ansvarar för olika aspekter av kontinuitetshantering. Intervjuade nyckelpersoner uppger att man uppmuntrar till dialog och samarbete, vilket möjliggörs genom årliga temadagar och workshops som används för att öka medvetenheten och kunskapen inom kontinuitetshantering. Därtill finns ett stående erbjudande till alla förvaltningar att de kan be om stöd med sitt arbete inom kontinuitetshantering. Det övergripande arbetet inom kontinuitetshantering fastställs i stadens *Strategi för arbetet med krisberedskap och civilt försvar i Mölndals stad* som sträcker sig till 2026. Det bedrivs även löpande arbete med återläsningstester av kritiska verksamhetssystem i samarbete med förvaltningarna.

I kontrast till det ovan nämnda efterfrågar de utvalda förvaltningarna en mer tydlig och samordnad ansvarsfördelning gällande frågor som berör kontinuitetshantering. Bland annat efterfrågar intervjudeltagarna och pekar på behovet av en säkerhetssamordnare som kan skapa och upprätthålla rutiner, utbilda personal och säkerställa att kontinuitetshanteringsarbetet efterlevs. En av de intervjuade förvaltningarna menar dock att organisatoriska brister, såsom avsaknaden av ett formellt uppdrag och mandat, resulterat i att en sådan roll uteblivit. Därtill efterfrågar de utvalda förvaltningarna regelbunden uppföljning för att förvaltningarna mer effektivt ska kunna säkerställa att planer och rutiner hanterar relevanta sårbarheter och risker.

I styrande dokumentation som tillhandahålls av staden beskrivs ansvar och roller avseende kontinuitetplaneringsarbetet. Bland annat beskriver *Instruktioner för systematisk kontinuitetshantering* och *Risk- och sårbarhetsanalys Mölndals stad 2023* att förvaltningarna har till uppgift att säkerställa motståndskraft vid störning, genom att planera och kartlägga kritiska behov inom sin respektive verksamhet. Enligt dokumenten tillfaller uppgiften att genomföra kontinuitetsplanering inte enbart stadens förvaltningar, utan det betonas även att centrala funktioner såsom stadens stadsledningsförvaltning har till uppgift för att styra, samordna och följa upp stadens arbete med krisberedskap.

Reservrutiner för att hantera IT-avbrott varierar i utförlighet och nivå inom stadens intervjuade förvaltningar.

- Centralt saknas redundanta IT-system. Intervjuade nyckelpersoner inom stadsledningsförvaltningen uppger att enskilda förvaltningar har till uppgift att hantera och skapa egna reservrutiner.
- På vård- och omsorgsförvaltningen har redundans skapats genom bland annat utskrivna läkemedelslistor och fysiska scheman. Dessa reservrutiner testades framgångsrikt i samband med att en underleverantör av trygghetslarm utsattes för en cyberattack 2023.
- På stadsserviceförvaltningen finns informella rutiner, men dessa är starkt beroende av enskilda individer, vilket kan leda till sårbarheter vid tekniska problem.

2.3.2 Bedömning

Vi bedömer att kommunstyrelsens till viss del säkerställt rutiner för att hantera väsentliga risker och scenarier. Ett aktivt arbete har bedrivits som syftar till att förbättra stadens motståndskraft genom att implementera förebyggande insatser, såsom styrdokument som tillhandahåller modeller hur stadens förvaltningar kan arbeta för att utveckla kontinuitetsplaner för risker inom den egna verksamheten.

Trots positiva inslag i kommunstyrelsens arbete bedömer vi att det finns behov av att vidta åtgärder för att förbättra samordningen mellan stadsledningsförvaltningen och enskilda förvaltningar. Även om styrande dokumentation visar på en förhållandevis väldokumenterad ansvarsfördelning avseende stadens krisberedskap, bedömer vi att det i större utsträckning finns ett ökat behov av centralt stöd som förtydligar de förväntningar inom krisberedskap som ställs på stadens förvaltningar. Kommunstyrelsen som samordnande organ behöver på ett bättre sätt fånga upp förvaltningarnas behov, som är avgörande för att förvaltningarna effektivare kunna säkerställa sin del av kontinuitetshanteringsarbetet. Detta baseras bland annat på att intervjuade nyckelpersoner inom en av de intervjuade förvaltningarna uppger att det råder en bristande förståelse kring förväntningar, vilket bidrar till att det förberedande krisberedskapsarbetet inte fullt ut blir en del av verksamheternas dagliga arbete. Bland annat har en av de intervjuade förvaltningarna uttryckt att de behöver en säkerhetssamordnare för att bättre kunna leva upp till de riktlinjer som ställs av stadsledningsförvaltningen avseende kontinuitetshantering och krisberedskap.

2.4 Revisionsfråga 4: Har kommunstyrelsen säkerställt att övning och utbildning inom kontinuitetshantering genomförs i lämplig omfattning?

För att säkerställa att en organisation är väl förberedd för att hantera oförutsedda händelser och kriser är det avgörande att kontinuitetshantering integreras i den dagliga verksamheten. Detta inkluderar regelbundna övningar och utbildningar för att säkerställa att all personal är medveten om sina roller och ansvar i en krissituation.

2.4.1 Iakttagelser

Intervjuade nyckelpersoner inom stadsledningsförvaltningen uppger att det inte finns någon central plan för övning och utbildning inom kontinuitetshantering; ansvaret för att

genomföra övningar och utbildningar ligger i stället på respektive nämnd. Kommunstyrelsen har dock tagit flera initiativ för att främja övning och utbildning inom kontinuitetshantering. Bland annat har säkerhets- och beredskapsenheten, som är en del av stadsledningsförvaltningen, tagit fram en detaljerad utbildnings- och övningsplan som sträcker sig fram till 2026 och som omfattar regelbundna utbildningar och samverkningsövningar. Av detta dokument framgår att Säkerhets- och beredskapsenheten utgör en central roll och ansvarar för att årligen följa upp att stadens utbildningar och övningar genomförs i enlighet med de fastställda målen. Enligt samma dokument ska stadens förvaltningar delta i dessa övningar och utbildningar och säkerställa att medarbetarna får tillräckligt med utbildning för att kunna utföra sina uppgifter. Förvaltningarna ska även enligt dokumentet *Strategi för arbetet med krisberedskap och civilt försvar i Mölndals stad* planera för utbildnings- och övningsverksamhet. Stadsledningsförvaltningen genomför även workshops och temadagar som fungerar som ett forum där förvaltningarna kan samlas för att diskutera relevanta ämnen och öva på olika scenarion. Den decentraliserade ansvarsfördelningen gör det möjligt för förvaltningarna att anpassa sina övningar och utbildningar efter specifika behov och förutsättningar, menar stadsledningsförvaltningen. Dessutom ska den centrala rollen för säkerhetssamordning fungera som en rådgivande och stöttande funktion i förvaltningarnas kontinuitetsarbete.

Intervjuade förvaltningar betonar vikten av lättillgängliga rutiner och tydliga processer som kan säkerställa att stadens personal vet hur, och på vad, de ska utbildas. Förvaltningarna upplever att ansvaret för kontinuitetshantering har varit utspritt på olika personer och roller, vilket har lett till bristande kontinuitet och tydlighet. En centraliserad och utpekad roll skulle säkerställa att rutiner och processer inte bara skapas utan också underhålls och följs upp regelbundet, samt möjliggöra en transparant dialog mellan stadsledningsförvaltningen och förvaltningarna. Därtill lyfter de utvalda förvaltningarna behovet av regelbundna tester av kontinuitetsplaner, inklusive årliga avstämningar och kontinuerliga uppföljningar, eftersom detta är avgörande för att rutiner inte ska bli ineffektiva och avta i relevans.

Det är i sammanhanget värt att påpeka att Mölndals stad enligt styrdokumentet *Strategi för arbetet med krisberedskap och civilt försvar i Mölndals stad* vilar på ansvarsprincipen för sin styrning inom krishantering. Det innebär att *den som ansvarar för en verksamhet under normala förhållanden har samma ansvar under en kris eller ett krig.* Utifrån denna grundprincip är Säkerhets- och beredskapsenheten, enligt dokumentation, ytterst ansvariga för att säkerställa att utbildnings- och övningsplanen följs.

2.4.2 Bedömning

Vi bedömer att kommunstyrelsen delvis har säkerställt att övning och utbildning har genomförts i lämplig omfattning. Denna bedömning baseras på att säkerhets- och beredskapsenheten inom stadsledningsförvaltningen, som bär det övergripande ansvaret för stadens utbildning och övningsplanen för krisberedskap, har tagit flera initiativ som syftar till att säkerställa övning och utbildning inom kontinuitetshantering. Bland annat har workshops och temadagar ordnats som möjliggjort kunskap och erfarenhetsutbyte mellan stadens förvaltningar, vilket visar på att initiativtagande avseende utbildning. Dessutom tillhandahålls flera styrdokument som förklarar hur förvaltningarna kan arbeta för att själva skapa tillämpliga kontinuitetsplaner.

De granskade förvaltningarna anser däremot att stadens övnings- och utbildningstillfällen i stor utsträckning är otillräckliga, irrelevanta och inte faller inom ramen för vad som efterfrågas. De påpekar att det finns ett stort behov av mer praktiska och realistiska krisövningar, särskilt för IT-bortfall och andra kritiska situationer. Vi bedömer att tydligheten gällande genomförande och utformning av övningsplaner inte har förankrats och tydliggjorts med de granskade förvaltningarna. Detta leder till att övning av enskilda förvaltningars kontinuitetsplaner inte blir ändamålsenliga. För att skapa ett aktivt deltagande bland stadens förvaltningar bedömer vi att de utvalda förvaltningarna är i behov av ett ökat stöd.

2.5 Revisionsfråga 5: Har kommunstyrelsen säkerställt att ändamålsenliga återläsningstester görs av kritiska system?

Återläsningstester är en viktig del av kontinuitetshantering och IT-säkerhet. En regelbunden uppföljning av återläsningstester i kritiska system och verksamhetsviktiga funktioner kan vara avgörande för att minska skadeomfattningen efter en IT-störning eller cyberattack.

2.5.1 Iakttagelser

Representanter från stadsledningsförvaltningen uppger vid intervju att återläsningstester endast utförs på begäran av förvaltningarna och att endast ett system i Mölndals stad utför regelbundna återläsningstester. Det saknas fastställda rutiner och återläsningstester utförs enbart när behov uppstår. Den centrala IT-funktionen har inte direkt tillgång till förvaltningarnas system, vilket innebär att återläsningstester måste utföras i samarbete med förvaltningarna. Trots dessa begräsningar finns det ett system som regelbundet testas varje månad, vilket utgör ett undantag från den generella praxisen. I dagsläget saknar de utvalda förvaltningarna etablerade rutiner för hur återläsningstester ska genomföras. För att stärka krisberedskapen har stadsledningsförvaltningen fått i uppdrag ta fram en planering för återupprättande av IT-system efter eventuell inträffad IT-störning, som ska vara klart senast 2025. Vid tid för granskningen uppger intervjuade nyckelpersoner att staden saknar hårdvarukapacitet som krävs för att utföra återläsningstester för flera system på en och samma gång. Vi noterar att sedan granskningen inleddes har staden införskaffat hårdvarukapacitet som är under implementation.

2.5.2 Bedömning

Vi bedömer att kommunstyrelsen inte fullt ut har säkerställt att ändamålsenliga återläsningstester genomförs av kritiska system. Återläsningstester initieras endast på förvaltningarnas begäran och har hittills endast utförts i en begränsad omfattning, vilket indikerar att det inte finns någon etablerad rutin för detta. En etablerad rutin är viktig för att stadens medarbetare ska vara medvetna om hur de ska, och ifall de kan, återläsa säkerhetskopieringar, då detta kräver båda övning och förberedelser. Regelbundna återläsningstester är viktigt för att kunna säkerställa att säkerhetskopieringar kan återläsas vid eventuell förlust av data. Kommunstyrelsen behöver enligt vår bedömning således vidta ytterligare steg för att säkerställa att kritiska system kan återställas på ett tillförlitligt sätt i händelse av en störning eller kris.

3. Övergripande rekommendationer

Baserat på genomförd granskning har Vi identifierat tre övergripande rekommendationer kopplat till kommunstyrelsens informationssäkerhetsarbete. Rekommendationerna som presenteras nedan syftar till att öka stadens motståndskraft inom informationssäkerhetsområdet.

3.1 Tydliggöra uppdrag och ansvar mellan stadsledningsförvaltningen och förvaltningarna

Genomförd granskning visar att den decentraliserade ansvarsmodell som staden tillämpar har skapat otydligheter avseende ansvar i kontinuitetshantering, vilket har lett till bristande samsyn mellan stadsledningsförvaltningen och enskilda förvaltningar. För att möjliggöra en samordnad syn på kontinuitetshantering inom staden, rekommenderar vi att kommunstyrelsen tydliggör roller och ansvar mellan kommunstyrelsen och nämnderna samt mellan stadsledningsförvaltningen och övriga förvaltningar. Detta kan exempelvis uppnås genom att inrätta en säkerhetssamordnarfunktion på respektive förvaltning, med ansvar för att utveckla, implementera och övervaka kontinuitetsplaneringsarbetets efterlevnad. Regelbundna utbildningar och övningar bör även genomföras för att alla medarbetare ska förstå sina roller och veta hur de ska agera i samband med en IT-incident, vilket bör ske i samförstånd med förvaltningarnas behov.

3.2 Säkerställa kontinuerlig uppföljning avseende förvaltningarnas kontinuitetshanteringsarbete

Vi rekommenderar att kommunstyrelsen implementerar en systematisk uppföljningsstrategi som kan skapa en transparant och strukturerad process för regelbunden granskning och utvärdering av förvaltningarnas kontinuitetsarbete. Detta eftersom flera intervjuade nyckelpersoner inom stadens utvalda förvaltningar som deltagit i EY granskning, pekar på att en otydlig samverkan resulterat i en bristande förståelse för ansvarsfördelning och rutiner inom kontinuitetshantering. Genom att införa regelbundna uppföljningar kan förvaltningarna få en tydligare bild av sina roller och ansvar, vilket i sin tur främjar bättre samordning och kommunikation.

Kontinuerlig uppföljning kan också hjälpa till att säkerställa att kontinuitetsplaner är fortsatt relevanta och uppdaterade, bland annat genom att identifiera eventuella brister och sårbarheter i nuvarande system och processer. Detta kan sammantaget leda till en mer samordnad och mer effektiv kvalitetssäkring av förvaltningarnas kontinuitetsarbete, där alla parter är medvetna om sina uppgifter och kan agera snabbt och korrekt vid en samhällsstörning.

3.3 Säkerställa hårdvarukapacitet och rutiner för återläsningstester

För att stärka stadens förmåga att hantera eventuellt IT-bortfall, behöver kommunstyrelsen säkerställa att återläsningstester av kritiska IT-system regelbundet genomförs. Intervjuade nyckelpersoner inom stadsledningsförvaltningen uppger att det finns en begränsning i stadens hårdvara för att utföra återläsningstester i en större skala. Vi rekommenderar därmed att kommunstyrelsen investerar i IT-infrastruktur för att

säkerställa att ändamålsenliga återläsningstester kan utföras för stadens kritiska system. Mölndals stad har inte heller någon rutin som specificerar frekvens och omfattning av återläsningstester. Vi rekommenderar således att kommunstyrelsen fastställer rutiner för att utföra återläsningstester på åtminstone årlig basis för kritiska system.

4. Sammanfattande svar på revisionsfrågor

Färgkod	Förklaring
	Ej tillfredsställande
	Delvis tillfredsställande
	Tillfredsställande

Revisionsfråga	Svar	
► Har kommunstyrelsen säkerställt ett ändamålsenligt arbete med att identifiera vad som bör omfattas av kontinuitetsplanering?	Ja. Vår bedömning baseras på att förebyggande åtgärder vidtagits som gör det möjligt för stadens förvaltningar att bedriva systematisk kontinuitetshantering.	
► Har kommunstyrelsen säkerställt att riskanalyser genomförts på lämplig nivå för att hantera störningar och avbrott?	Nej. Vår bedömning baseras på att stadens riskanalysarbete inte förankrats och implementerats effektivt bland stadens förvaltningar.	
► Har kommunstyrelsen säkerställt planer och rutiner för de väsentliga riskerna och scenariona?	Delvis. Vår bedömning baseras på att det finns styrdokument som tillhandahåller tillvägagångsätt för hur stadens förvaltningar kan arbeta för att utveckla kontinuitetsplaner för sina verksamheter. Däremot ser vi ett behov av regelbunden uppföljning för att säkerställa förväntningar och att arbetet genomförs på verksamhetsnivå.	
► Har kommunstyrelsen säkerställt att övning och utbildning inom kontinuitetshantering genomförs i lämplig omfattning?	Delvis. Vår bedömning baseras på att stadsledningsförvaltningen har arrangerat utbildningstillfällen vilket möjliggjort kunskaps- och erfarenhetsutbyte mellan stadens förvaltningar. Trots dessa insatser bedömer vi att tydligheten gällande förvaltningarnas uppgifter, i tillräcklig mån, inte har förankrats i de utvalda förvaltningarna.	

► Har kommunstyrelsen säkerställt att ändamålsenliga återläsningstester görs av kritiska system?	Nej. Vår bedömning baseras på att återläsningstester endast utförs i en begränsad omfattning och ad hoc. Kommunstyrelsen behöver således vidta ytterligare steg för att säkerställa att data från kritiska system kan återläsas på ett tillförlitligt sätt i händelse av en störning eller kris.	

5. Slutsatser

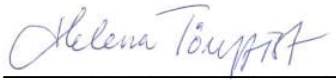
På uppdrag av de förtroendevalda revisorerna i Mölndals stad har EY genomfört en granskning av stadens arbete med IT- och informationssäkerhet. Syftet med granskningen har varit att bedöma om kommunstyrelsen säkerställt ett ändamålsenligt arbete med kontinuitetshantering inom IT, samt ge rekommendationer för att minska risken för att störningar inom IT får betydande konsekvenser.

Granskningen visar att kommunstyrelsen till viss del säkerställt ett ändamålsenligt arbete med kontinuitetshantering inom IT. Stadsledningsförvaltningen har vidtagit flera åtgärder och utvecklat styrdokument för att stödja förvaltningarna i deras kontinuitetsarbete, men det finns brister i samordning och implementering av dessa strategier. Riskanalyser genomförs inte systematiskt på alla nivåer, vilket är ett resultat av att stadens decentraliserade ansvarsmodell skapar otydligheter avseende ansvar inom kontinuitetsarbetet. Övning och utbildning inom kontinuitetshantering genomförs i viss omfattning, men förvaltningarna efterfrågar mer praktiska och realistiska krisövningar. Vidare utförs återläsningstester av kritiska system inte systematiskt eller enligt en etablerad rutin, utan endast på begäran av enskilda förvaltningar.

Kommunstyrelsen rekommenderas därför att vidta åtgärder för att stärka sitt arbete med kontinuitetshantering inom IT. Ett förbättrat arbete med kontinuitetsplanering kan bidra till att verksamheten kan upprätthålla samhällsviktiga tjänster under störning och påskynda återhämtningsprocessen efter en kris. Baserat på granskningen lämnar vi tre övergripande rekommendationer till kommunstyrelsen:

- Tydliggöra uppdrag och ansvar mellan stadsledningsförvaltningen och förvaltningarna.
- Säkerställa kontinuerlig uppföljning avseende förvaltningarnas kontinuitetshanteringsarbete.
- Säkerställa hårdvarukapacitet och rutiner för återläsningstester.

Stockholm, 2024-11-15



Helena Törnqvist

Kvalitetssäkrare IT

Bilaga 1: Lista över intervjuade

- IT- och digitaliseringschef, stadsledningsförvaltningen.
- Säkerhet- och beredskapschef, stadsledningsförvaltningen.
- Säkerhetssamordnare, stadsledningsförvaltningen.
- Informationssäkerhetssamordnare, stadsledningsförvaltningen.
- IT-infrastrukturansvarig, stadsledningsförvaltningen.
- Systemansvariga, vård- och omsorgsförvaltningen.
- Produktionschef, stadsserviceförvaltningen.

Bilaga 2: Dokumentförteckning

- Anvisning informationsklassning och riskanalys
- Instruktion för systematisk kontinuitetshantering
- It-sakerhetsinstruktioner_for_anvandare_i_molndals_stad
- Major Incident
- Presentation WS Cyberattack – urval
- Riktlinje för informationssäkerhet, antagen av Kf 20221214
- Risk- och sårbarhetsanalys för Mölndals stad 2023
- Strategi för krisberedskap civilt försvar Mölndal 2023-2027
- Utbildnings- och övningsplan 2023-2026
- Utvärdering av WS
- Kontinuitetsplaner för VA-Mölndal
- Kommunstyrelsens reglemente, reviderat 2024-06-19.pdf
- Reglemente_tekniskanamnden.pdf
- Reglemente_vardochomsorgsnamnden.pdf

Bilaga 3: Definitioner

Cyberattack/angrepp: En cyberattack/angrepp är ett samlingsnamn för olika typer av brott som utförs på IT-system. Attackerna kan utföras för att få tillgång till hemlig information, begränsa tillgången till IT-systemen, samt förstöra data eller IT-system.

IT-miljö: En IT-miljö avser all hårdvara, mjukvara, nätverk och data som utgör verksamhetens resurser för informationsteknik.

IT-infrastruktur: De grundläggande komponenter inom IT-miljön som behövs för att mer användarnära delar, som persondatorer, mobiltelefoner och applikationer, ska fungera. Infrastrukturen omfattar vanligtvis nätverk, servrar och säkerhetsutrustning. Enligt vissa definitioner ingår även databaser, vissa operativsystem och liknande. IT-infrastrukturen är en förutsättning för att en verksamhets IT-miljö ska fungera.

Kontinuitetsplan: Kontinuitetsplan är ett viktigt dokument i en organisations riskhanteringsstrategi. Kontinuitetsplaner upprättas i syfte att säkerställa att kritiska funktioner inom en organisation fortsatt bedrivs och upprätthålls på en tolerabel nivå, under och efter en störning.

Riskanalys: En systematisk process för att identifiera och utvärdera potentiella hot och sårbarheter som kan påverka kritiska funktioner och tjänster.

Säkerhetskopia: En säkerhetskopia eller backup är en kopia av lagrad information som skapas för att förhindra att originaldata går förlorad. Säkerhetskopian kan användas för att återställa originalinformationen vid dataförlust i samband med exempelvis en cyberattack.

Återläsningstest: Återläsningstest är en metod som används för att säkerställa att en organisation kan återställa sin data och sina system från en säkerhetskopia i händelse av en incident.