Handläggare
Anna-Carin Wallin
Telefon: 0850809014

Till
Norrmalms stadsdelsnämnd
2020-03-19

Kontinuitetsplanering - it-avbrott

Yttrande över revisionsrapport nr 6/2019 från stadsrevisionen

Förslag till beslut

Förvaltningens tjänsteutlåtande överlämnas som yttrande till revisionskontoret.

Sammanfattning

Revisionskontoret har genomfört en granskning av stadens styrning och uppföljning av den kontinuitetsplanering som ska finnas för att minimera skadan av begränsad tillgång till informationsteknik. Granskningen har omfattat kommunstyrelsen, trafiknämnden samt Norrmalms och Hägersten-Liljeholmens stadsdelsnämnder.

Granskningen har utgått från följande frågor:

- Är staden och nämndernas organisation och ansvarsfördelning tydlig vad gäller kontinuitetsplanering?
- Har granskade nämnder fastställt kontinuitetsplaner?
- Har nämndernas kontinuitetsplaner en tydlig koppling till genomförd risk- och sårbarhetsanalys?
- Sker löpande uppföljning av kontinuitetsplanerna?

Revisionskontoret lämnar rekommendationer till de granskade nämnderna samt till kommunstyrelsen. Revisionskontoret rekommenderar Norrmalms stadsdelsnämnd att genomföra tester/övning på upprättad kontinuitetsplan för it-avbrott.

Förvaltningen delar revisionens uppfattning om vikten av genomarbetade, förankrade och testade kontinuitetsplaner för it-bortfall, att metodstöd bör integreras med informationssäkerhet samt att metodstödet i vissa delar kan förtydligas.

Förvaltningen tar till sig lämnade rekommendationer och avser att genomföra tester/övning på upprättad kontinuitetsplan för it-avbrott.

Bakgrund

Revisionskontoret har genomfört en granskning av stadens styrning och uppföljning av den kontinuitetsplanering som ska finnas för att

Norrmalms stadsdelsförvaltning
Avdelningen för administration och prevention

Sankt Eriksgatan 117
Box 45075
10430 Stockholm
Växel 08-508 090 00
Fax 08-508 09 099
norrmalm@stockholm.se
stockholm.se

minimera skadan av begränsad tillgång till informationsteknik. Granskningen har omfattat kommunstyrelsen, trafiknämnden samt Norrmalms och Hägersten-Liljeholmens stadsdelsnämnder.

Syftet med granskningen var att bedöma stadens styrning och uppföljning av den kontinuitetsplanering som ska finnas för att minimera skadan av begränsad tillgång till informationsteknik.

I stadens trygghets- och säkerhetsprogram *”För ett tryggare och säkrare Stockholm”* anges att staden kontinuerligt ska utveckla förmågan att förebygga störningar och upprätthålla dessa verksamheter.
Som en del av den årliga risk- och sårbarhetsanalysen ska kontinuitetsplaner tas fram för hur verksamheten ska bedrivas vid allvarliga störningar.

För att undvika allvarlig påverkan på samhället krävs därför väl genomarbetade, förankrade och testade kontinuitetsplaner. Arbetet med kontinuitetsplaner behöver därför vara en del av ett strukturerat informationssäkerhetsarbete.

Ärendets beredning

Ärendet har beretts av avdelningen för administration och prevention i samverkan med äldreavdelningen och socialtjänstavdelningen.

Ärendet

Syftet med Revisionskontorets granskning är att bedöma stadens styrning och uppföljning av den kontinuitetsplanering som ska finnas för att minimera skadan av begränsad tillgång till informationsteknik.

Granskningen besvaras med följande revisionsfrågor:

- Är staden och nämndernas organisation och ansvarsfördelning tydlig vad gäller kontinuitetsplanering?
- Har granskade nämnder fastställt kontinuitetsplaner?
- Har nämndernas kontinuitetsplaner en tydlig koppling till genomförd risk- och sårbarhetsanalys?
- Sker löpande uppföljning av kontinuitetsplanerna?

Granskningen har begränsats till att avse it-störningar som påverkar nämndernas förmåga att genomföra sitt uppdrag och att it-störningarna får betydelse för nämndernas relation med medborgarna.

Norrmalms stadsdelsförvaltning
Avdelningen för administration och prevention

Sankt Eriksgatan 117
Box 45075
10430 Stockholm
Växel 08-508 090 00
Fax 08-508 09 099
norrmalm@stockholm.se
stockholm.se

Lagstiftning och stadens styrande dokument
Granskningen har utgått ifrån gällande lagstiftning och stadens säkerhetsprogram, stadens handbok för risk- och sårbarhetsanalys samt stadens riktlinjer för informationssäkerhet.

Enligt lagstiftning[1] är kommuner och landsting skyldiga att genomföra risk och sårbarhetsanalyser samt att regelbundet öva och utbildas för att kunna utföra sina åtaganden även vid extraordinära händelser.

Av *Stockholms stads trygghets- och säkerhetsprogram* framgår det att nämnder och bolag årligen ska genomföra risk- och sårbarhetsanalyser. I det årliga arbetet görs en bedömning av de kritiska verksamheternas åtaganden gentemot exempelvis liv och hälsa och stadens funktionalitet. Därefter ska nämnder och bolag identifiera risker mot sina respektive verksamheter och löpande vidta åtgärder. Som ett sista steg genomförs en beroendeanalys och kontinuitetsplaner upprättas för kritiska beroenden, som exempelvis elektricitet och telekommunikation. Samtliga åtgärder som vidtas ska följas upp och utvärderas.

I programmet ställs också krav på att nämnderna ska utse en säkerhetssamordnare med ansvar att samordna nämndens trygghets- och säkerhetsarbete.

Stadens riktlinje för informationssäkerhet gör gällande att kontinuitetsplanering för verksamheten omfattar åtgärder för att identifiera och minska risker, begränsa konsekvenserna av skadliga incidenter samt säkerställa att den information som krävs för verksamheten är tillgänglig. Enligt riktlinjerna ska en kontinuitetsplan omfatta uppgifter om ansvar och befogenheter för viktiga rollinnehavare, informationskanaler och vilka som ska informeras, reservplaner för olika händelser, plan för återgång till normalläge, plan för återtagning av förlorad information och annat av vikt, samt rutin för uppdatering av kontinuitetsplanen.

Kontinuitetsplanerna ska testas regelbundet och uppdateras så att de alltid är aktuella och verkningsfulla. Ansvaret för att det tas fram en kontinuitetsplan åligger verksamhetsansvarig chef.

Handboken Stockholms stads risk-och sårbarhetsanalys utgör metodstöd i nämndernas och bolagens arbete med risk- och sårbarhetsanalys. Processen för arbetet med risk och sårbarhetsanalys består av fyra olika steg varav steg 1-2 är obligatoriska för samtliga nämnder och bolag. Steg tre genomförs utifrån kritiska åtaganden och ska även innehålla en

Norrmalms stadsdelsförvaltning
Avdelningen för administration och prevention

Sankt Eriksgatan 117
Box 45075
10430 Stockholm
Växel 08-508 090 00
Fax 08-508 09 099
norrmalm@stockholm.se
stockholm.se

[1] Lag (2006:544) om kommuner och landstings åtgärder inför och vid extraordinära händelser i fredstid och i beredskap.

kontinuitetshantering. Steg fyra genomförs av utvalda nämnder och bolag med fokus på att identifiera/belysa beroenden mellan staden och samhällsviktig verksamhet och skapa en konstruktiv uppföljning inom området.

Resultat från granskningen

- ***Är staden och nämndernas organisation och ansvarsfördelning tydlig vad gäller kontinuitetsplanering***?

Stadsledningskontorets säkerhetsenhet ansvarar för att leda och samordna stadens samlade säkerhetsarbete, i vilken processen för risk- och sårbarhetsanalys omfattas. Avdelning för digital utveckling leder stadens samlade arbete med informationssäkerhet.

I granskningen framkommer det att det inte råder samsyn över vilken av stadsledningskontorets avdelningar som ska utföra uppföljning och kontroll av kontinuitetsplan för it-avbrott, och inte heller om det är stadsledningskontorets ansvar att genomföra det.

Granskning av nämndernas organisation visar att utsedda säkerhetssmordnare finns, även om omfattning och ansvarsområde skiljer sig åt mellan de granskade nämnderna. Vilken roll som tar fram kontinuitetsplan för bortfall av IT-system utförs av vissa nämnder av den verksamhet som berörs av IT-bortfall och i vissa fall av säkerhetssamordnare. Norrmalms stadsdelsnämnd har utsedd säkerhetssamordnare som samordnar nämndens risk- och sårbarhetsanalyser (RSA). Förvaltningens Paraply-samordnare ansvarar för framtagande av kontinuitetsplan för sociala system (avbrottsplan).

Metodstöd

Revisionskontoret anmärker på att metodstödet för risk- och sårbarhetsanalys är daterad år 2013 och är till viss del inaktuellt. Granskningen tar även upp att det saknas ett metodstöd för att skapa ett enhetligt arbetssätt och för att möjliggöra en effektiv uppföljning av kontinuitetshantering. Vidare har det inom staden inte genomförts någon utbildning vare sig i metodstöd eller inom området sedan 2016. Revisionskontorets uppfattning är att förutsättningarna för nämndernas arbete behöver förbättras genom ökad central styrning och stöd.

- ***Har granskade nämnder fastställt kontinuitetsplaner?***

Granskningen visar att trafiknämnden inte tagit fram dokumenterade kontinuitetsplaner.

De granskade stadsdelsnämnderna har kontinuitetsplaner för hur verksamheten ska upprätthållas vid en störning som medför att

Norrmalms stadsdelsförvaltning
Avdelningen för administration och prevention

Sankt Eriksgatan 117
Box 45075
10430 Stockholm
Växel 08-508 090 00
Fax 08-508 09 099
norrmalm@stockholm.se
stockholm.se

tillgång till Sociala system saknas. Det finns dock stora kvalitetsskillnader i de båda nämnderna kontinuitetsplaner. Norrmalms stadsdelsnämnd har upprättad kontinuitetsplan för sociala system som bedöms uppfylla kraven.

- ***Har nämndernas kontinuitetsplaner en tydlig koppling till genomförd risk- och sårbarhetsanalys?***

Granskningen visar att framtagande och rapportering av risk- och sårbarhetsanalysens sker i olika system, vilket medför att det inte finns ett sammanhållet flöde i arbetet med att ta fram en risk-och sårbarhetsanalys och kontinuitetsplaner. Detta återspeglas i att det är svårt att i risk- och sårbarhetsanalysen härleda vilka områden/åtaganden som förväntas omfattas av en kontinuitetplan. Enligt instruktionerna från stadsledningskontoret behöver inte kontinuitetshantering genomföras för samtliga identifierade tidskritiska åtaganden. Av instruktionen framgår att minst fem kritiska åtaganden måste hanteras. Detta innebär att inte alla de åtaganden som anses vara tidskritiska har en plan för att hanteras om det skulle uppstå en störning. Revisionskontoret anser att samtliga åtaganden som bedömts som allvarliga och tidskritiska ska kontinuitetshanteras.

Norrmalms stadsdelsnämnd har identifierat tidskritiska åtaganden som är beroende av att IT-stöd fungerar och därmed skapat en avbrottsplan.

- ***Sker löpande uppföljning av kontinuitetsplanerna?***

Det sker inte någon stadsövergripande avstämning och kontroll av att berörda nämnder upprättar kontinuitetsplaner för de kritiska åtaganden som identifierats i risk- och sårbarhetsanalysen. Det går därför inte med säkerhet att säga att kontinuitetsplaner har tagits fram för identifierade kritiska åtaganden. Då ingen kontroll görs går det heller inte att med säkerhet att avgöra om stadens styrdokument på området efterlevs.

De granskade stadsdelsnämnderna har inte genomfört några tester och/eller övningar för att säkerställa att kontinuitetsplanerna är funktionella samt att medarbetarna har kännedom om och handlar i enlighet med denna.

Av de granskande nämnderna är det bara Norrmalms stadsdelsnämnd som genomför uppföljning av kontinuitetsplan för bortfall av IT-system.

Norrmalms stadsdelsförvaltning
Avdelningen för administration och prevention

Sankt Eriksgatan 117
Box 45075
10430 Stockholm
Växel 08-508 090 00
Fax 08-508 09 099
norrmalm@stockholm.se
stockholm.se

Sammanfattande bedömning och rekommendationer

Kommunstyrelsen

- Utarbeta ett relevant och aktuellt metodstöd till nämnderna.
- Integrera metodstöd och kommande anvisningar för informationssäkerhet.
- Tydliggöra stadsledningskontorets ansvar för uppföljning av de olika processerna i nämndernas arbete med risk- och sårbarhetsanalyser och kontinuitetshantering/planer.
- Tillhandahålla adekvata och återkommande utbildningsmöjligheter för nämnderna.

Trafiknämnden

- Utarbeta och implementera kontinuitetsplaner för nämndens tidskritiska åtaganden enligt stadens styrdokument.
- Genomföra tester och/eller övningar för att säkerställa att kontinuitetsplanerna är funktionella och uppdaterade.

Norrmalms stadsdelsnämnd

- Genomföra tester och/eller övningar för att säkerställa att kontinuitetsplanerna är funktionella och uppdaterade.

Hägersten-Liljeholmen stadsdelsnämnd

- Utveckla och implementera kontinuitetsplaner för verksamhets- och tidskritiska åtaganden enligt stadens styrdokument.
- Genomföra tester och/eller övningar för att säkerställa att kontinuitetsplanerna är funktionella och uppdaterade.

Synpunkter och förslag

Förvaltningen delar uppfattningen om vikten av genomarbetade, förankrade och testade kontinuitetsplaner för it-bortfall. Ett ökat beroende till it- och informationssystem leder till att ett bortfall får stora konsekvenser.

Förvaltningen anser även att stadsledningskontorets organisation och ansvar mellan avdelningarna kan utvecklas, och att metodstöd och anvisningar bör bli integrerade med informationssäkerhet. Med återkommande utbildningsmöjligheter kan förvaltningarnas förmåga stärkas. Att nämnder med it-beroende verksamheter har kontinuitetsplan för it-bortfall är av största vikt, samt att det finns tydlig ansvarsfördelning för framtagande och uppföljning.

När det gäller kopplingen mellan risk- och sårbarhetsanalyser, kontinuitetshantering och kontinuitetsplaner så ser förvaltningen att det finns en tydlig koppling. Det kan dock uppstå oklarheter mellan de olika begreppen; kontinuitetshantering, kontinuitetsplaner och

Norrmalms stadsdelsförvaltning
Avdelningen för administration och prevention

Sankt Eriksgatan 117
Box 45075
10430 Stockholm
Växel 08-508 090 00
Fax 08-508 09 099
norrmalm@stockholm.se
stockholm.se

avbrottsplaner (som kontinuitetsplan för IT-system benämns i stadens riktlinjer för informationssäkerhet). Detta kan förtydligas i metodstöd.

Revisionskontorets granskning är begränsat till att avse it-störning. Förvaltningen har i den årliga RSA-cykeln uppmärksammat att flera åtaganden är beroende av ett fungerande IT-system, främst sociala system, och därmed skapat en avbrottsplan för detta.

Förvaltningen tar till sig revisionskontorets bedömning och rekommendation att genomföra test/övning på upprättad kontinuitetsplan för it-störning.

Jesper Ackinger
stadsdelsdirektör

Maria Härenstam
avdelningschef

Bilagor

1. Missiv Stadsrevisionens kontinuitetsplanering it-avbrott
2. Projektrapport 6, Kontinuitetsplanering it-avbrott Dnr 3.1.3–102/2019

Norrmalms stadsdelsförvaltning
Avdelningen för administration och prevention

Sankt Eriksgatan 117
Box 45075
10430 Stockholm
Växel 08-508 090 00
Fax 08-508 09 099
norrmalm@stockholm.se
stockholm.se

Attesterat av

Detta dokument har godkänts digitalt av följande personer:

Namn	Datum
Jesper Ackinger, stadsdelsdirektör	2020-03-04
Maria Härenstam, avdelningschef	2020-03-04