Stockholms stad

Kontinuitetsplanering - it-avbrott

Nr 6, 2019

Projektrapport från Stadsrevisionen

Dnr: 3.1.3-102/2019

Den kommunala revisionen är fullmäktiges kontrollinstrument för att granska den verksamhet som bedrivits i nämnder och bolag. Stadsrevisionen i Stockholm stad granskar nämnders och styrelsers ansvarstagande för att genomföra verksamheten enligt fullmäktiges uppdrag. Stadsrevisionen omfattar både de förtroendevalda revisorerna och revisionskontoret.

I årsrapporter för nämnder och granskningspromemorior för bolagsstyrelser sammanfattar stadsrevisionen det gångna årets granskningar och bedömningar av verksamheten. Granskningar som genomförs under året kan också publiceras som projektrapporter.

Publikationerna finns på stadsrevisionens hemsida, stad.stockholm/revision. De kan också beställas från revisionskontoret, revision.rvk@stockholm.se.

Kontinuitetsplanering - it-avbrott
Nr 6, 2019

Dnr: 3.1.3-102/2019

Till
Kommunstyrelsen
Trafiknämnden
Norrmalms stadsdelsnämnd
Hägersten-Liljeholmens stadsdelsnämnd

Kontinuitetsplanering - it-avbrott

Revisorsgrupp 1 har den 3 december 2019 behandlat bifogad revisionsrapport (nr 6/2019)

Granskningen visar att stadens arbete med kontinuitetsplanering behöver utvecklas för att minimera skadan för verksamheten vid exempelvis begränsad tillgång till informationsteknik. Utifrån granskningen resultat, vill vi betona vikten av att metodstödet för nämndernas arbete utvecklas. Vidare behöver nämnderna säkerställa att kontinuitetsplanering genomförs i enlighet med stadens styrdokument. Vi vill särskilt betona vikten av att trafiknämnden säkerställer att kontinuitetsplaner tas fram för sina identifierade kritiska åtaganden.

Vi hänvisar i övrigt till rapporten och överlämnar den till kommunstyrelsen, trafiknämnden samt stadsdelsnämnderna Norrmalm och Hägersten-Liljeholmen för yttrande. Yttrandet ska ha inkommit till revisorsgrupp 1 senast den 31 mars 2020. Rapporten överlämnas till övriga nämnder för kännedom.

På revisorernas vägnar

Ulf Bourker Jacobsson
Ordförande

Stefan Rydberg
Sekreterare

Stadsrevisionen
Revisionskontoret

Hantverkargatan 3 D, 1 tr
Postadress: 105 35 Stockholm
Telefon: 08-508 29 000
Fax: 08-508 29 399
stad.stockholm/revision

Sammanfattning

Revisionen 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 stadsdelsnämnderna Norrmalm och Hägersten-Liljeholmen.

Stockholms stads trygghets- och säkerhetsprogram samt riktlinjer för informationssäkerhet anger bland annat att kontinuitetsplaner ska tas fram i syfte att skapa en förmåga i organisationen att hantera störningar och avbrott i verksamheten.

Utifrån granskningen kan vi konstatera att det finns skillnader i hur de granskade nämnderna arbetar med kontinuitetsplanering och om kontinuitetsplaner har upprättats för kritiska åtaganden. Enligt centrala instruktioner behöver kontinuitetsplaner inte upprättas för samtliga kritiska åtaganden som identifierats. Det kan leda till att organisationens förmåga att upprätthålla verksamheten vid exempelvis begränsad informationsteknik försvagas. För att säkerställa att kontinuitetsplanerna är funktionella och uppdaterade bör tester och/eller övningar genomföras. Några sådana tester och/eller övningar har inte genomförts vid de granskade nämnderna. Det sker inte någon stadsövergripande avstämning och kontroll av att nämnderna upprättar kontinuitetsplaner för de kritiska åtaganden som de har identifierat i risk- och sårbarhetsanalysen. Det går därför inte med säkerhet att säga att stadens styrdokument på området efterlevs.

Ett aktuellt metodstöd och utbildning är viktiga delar för att ge nämnderna förutsättningar att arbeta med kontinuitetsplanering. Det ger också förutsättning för ett enhetligt arbetssätt och för att möjliggöra en effektiv kontroll och avstämning av nämndernas arbete med kontinuitetshantering.

Utifrån redovisade iakttagelser och bedömningar lämnas följande 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 utbildnings-möjligheter 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

- Genomfört 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.

Innehåll

1. Inledning

1.1 Bakgrund

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 samhällsviktiga funktioner behöver fungera varje dag även om incidenter inträffar och det för verksamheten är ett så kallat onormalt läge.

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. Att värna stadens funktionalitet innebär också att ha förmåga att minimera konsekvenserna av oönskade händelser när de ändå inträffar samt att skapa tillit hos allmänheten och andra aktörer för att staden har denna förmåga. För att verksamheten ska kunna bedrivas även under onormala förhållanden behövs en adekvat kontinuitetsplanering.

Som en del av den årliga risk- och sårbarhetsanalysen som genomförs i staden ska kontinuitetsplaner tas fram för hur verksamheten ska bedrivas när identifierade och kritiska verksamhetsprocesser allvarligt påverkas av störning under en längre tidsperiod.

Det ökande beroendet till it- och informationssystem leder också till att ett bortfall av dessa kritiska tillgångar får större konsekvenser än tidigare. 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.

1.2 Syfte och revisionsfrågor

Syftet med granskningen 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?

1.3 Avgränsning och omfattning

Granskningen tar sin utgångspunkt i it-störningar som har påverkan på den dagliga verksamheten och som ställer krav på att det finns en beredskap för att kunna upprätthålla verksamheten även under onormala förhållanden. I detta fall avses it-störningar som påverkar nämndernas förmåga att genomföra sitt uppdrag och att it-störningen får betydelse för nämndernas relation med medborgarna.

Följande avgränsningar har gjorts i granskningen:

Kommunstyrelsen.

- För kommunstyrelsens del har granskningen avgränsats till ledning, styrning och uppföljning av processen för risk- och sårbarhetsanalys och kontinuitetsarbetet. Det har inte skett någon granskning av kommunstyrelsens kontinuitetsplaner.

- Stadsledningskontorets olika funktioner har avgränsats till säkerhetsenheten vid avdelningen för kvalitet och stadsutveckling samt avdelningen för digital utveckling. Granskningen har fokuserat på deras grundläggande förmågor att säkerställa uppsiktsplikten genom ledning, styrning och uppföljning av kontinuitetsarbetet.

Nämnder

- Arbetet med risk- och sårbarhetsanalys i sin helhet har inte varit föremål för granskningen, dock omfattar detta arbete viktiga komponenter som utgör underlag för nämndernas arbete i framtagandet av kontinuitetsplaner.

- Granskningen omfattar kontinuitetsplaner som granskade nämnder har upprättat för att säkerställa att verksamheten ska kunna bedrivas även under onormala förhållanden.

- För stadsdelsnämnderna har granskningen avgränsats till verksamhetsområdet äldreomsorg och upprättade kontinuitetsplaner för Sociala system.

- Under granskningen har det framkommit att trafiknämnden saknar dokumenterade kontinuitetplaner för hur verksamheten ska upprätthållas vid störningar eller avbrott som drabbar för verksamheten viktiga it-system. Detta har medfört att det inte varit möjligt att göra någon bedömning av hur nämnden arbetar med kontinuitetsplaner.

1.4 Ansvariga nämnder/styrelse

Kommunstyrelsen, trafiknämnden samt stadsdelsnämnderna Norrmalm och Hägersten-Liljeholmen.

1.5 Revisionskriterier

Revisionskriterier är de bedömningsgrunder som revisionen utgår ifrån vid analys och bedömning. Följande revisionskriterier har tillämpas i granskningen:

- Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och beredskap.
- Stockholms stads trygghets- och säkerhetsprogram 2018-2021, Fokusområde 4 – Bygga motståndskraft och krishanteringsförmåga
- Stockholms stads riktlinje för informationssäkerhet (dnr 307-1396/2014), sid. 91-96.
- Handbok - Stockholms stads risk- och sårbarhetsanalys

1.6 Metod

Granskningen har genomförts genom intervjuer med nyckelpersoner vid berörda nämnder samt dokumentstudier. Därtill har berörda nämnders risk- och sårbarhetsanalyser samt upprättade kontinuitetsplaner granskats.

Granskningen har genomförts av Susanne Eriksson och Erik Skoog på revisionskontoret tillsammans med Willem Stolk och Jessica Malmström från KPMG.

Rapporten har faktakontrollerats av förvaltningarna.

2. Lagstiftning och stadens styrande dokument

Enligt den standard[1] som finns på området handlar kontinuitetshantering/planering om att systematiskt skapa en förmåga att fortsätta bedriva sin verksamhet på en tolerabel nivå, oavsett vilken typ av störning som organisationen utsätts för. Målet är att organisationen ska ha en förmåga att hantera störningar och avbrott i verksamheten så att dessa får en så liten påverkan som möjligt på verksamheten.

[1] SS 22304:2014 Samhällssäkerhet – Ledningssystem för kontinuitet

Lagstiftningen[2] gör gällande att kommuner och landsting är skyldiga att genomföra risk- och sårbarhetsanalyser. Risk- och sårbarhetsanalysarbetet ska ses som en ständigt pågående process och bör samordnas med övrigt förebyggande arbete i kommunen och landstinget. Vidare ska kommuner och landsting enligt lagstiftningen se till att förtroendevalda och anställda regelbundet får den utbildning och övning som behövs för att de ska kunna lösa sina uppgifter vid extraordinära händelser.

Av *Stockholms stads trygghets- och säkerhetsprogram* framgår att nämnder och bolag årligen ska genomföra risk- och sårbarhetsanalyser samt rapportera sina mest framträdande risker till kommunstyrelsen. Detta arbete ska omfatta en bedömning av hur kritiska verksamheternas åtaganden är. Vidare 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. Samtliga åtgärder som vidtas ska följas upp och utvärderas. Utifrån nämndernas underlag ska kommunstyrelsen ta fram en riskbild för staden som helhet. I programmet ställs också krav på att nämnderna ska utse en säkerhetssamordnare med ansvar att samordna nämndens trygghets- och säkerhetsarbete.

Vidare framgår av programmet att kommunstyrelsen bland annat ska följa upp att nämnder och bolag utifrån identifierade risker i risk- och sårbarhetsanalysen vidtagit eller initierat åtgärder för att behandla dessa.

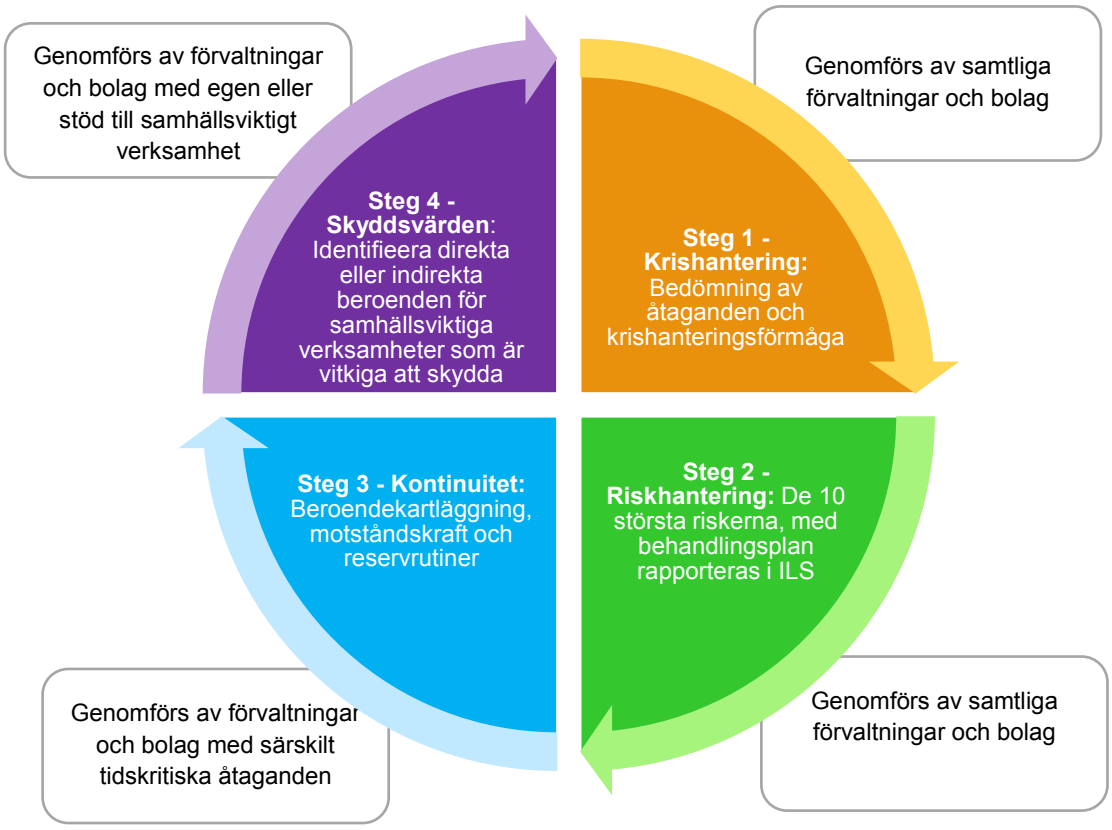
Stadens riktlinje för informationssäkerhet gör gällande att kontinuitetsplanering för verksamheten omfattar åtgärder för att identifiera och minska risker, begränsa konsekvenserna av skadliga incidenter samt säkerställa att den information som krävs för verksamheten är tillgänglig.

För att minska konsekvenserna vid allvarliga störningar eller avbrott i verksamheter med starkt it-beroende krävs en i förväg upprättad och dokumenterad kontinuitetsplan. Kontinuitetsplanerna ska testas regelbundet och uppdateras så att de alltid är aktuella och verkningsfulla. Ansvaret för att det tas fram en dokumenterad kontinuitetsplan åligger verksamhetsansvarig chef.

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

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.

Handboken Stockholms stads risk-och sårbarhetsanalys med tillhörande excelfiler utgör metodstöd i nämndernas och bolagens arbete med risk- och sårbarhetsanalys. Processen för arbetet med risk och sårbarhetsanalys består av fyra olika steg. Kontinuitetshantering utgör ett av dessa steg. Beroende på hur kritiska nämndens åtagande bedöms vara behöver nämnden inte genomföra samtliga fyra steg. Nedan finns en översiktlig bild över den modell som staden använder.



Figur 1 "RSA-hjulet" - modell för Stockholms stads arbete med risk- och sårbarhetsanalys

3. Granskningens iakttagelser

3.1 Organisation och styrning

3.1.1 Organisation och ansvarsfördelning

Kommunstyrelsen

Enligt Kommunallagen (2017:725) ska kommunstyrelsen ha uppsikt över nämndernas verksamhet. I reglementet för kommunstyrelsen[3] framgår bland annat att kommunstyrelsen har hand om uppgifter som rör kommunövergripande frågor om stadens informationsteknologi. Kommunstyrelsen har också ansvarar för uppföljningen av stadens trygghets- och säkerhetsprogram. Stadsledningskontoret biträder kommunstyrelsen i detta uppdrag samt att de enligt gällande instruktion[4] har till uppgift att styra och stötta stadens övriga verksamheter. Stadsledningskontoret har också det övergripande ansvaret för stadens krisledningss-, beredskaps- och säkerhetsarbete.

Stadsledningskontoret har organiserat arbetet genom en säkerhetsenhet som ansvarar för att leda och samordna stadens samlade säkerhetsarbete, i vilket processen för risk- och sårbarhetsanalys omfattas. Avdelning för digital utveckling leder stadens samlade arbete med informationssäkerhet. Framtagandet av kontinuitetsplaner ingår som en process dels i nämndernas risk- och sårbarhetsanalyser, dels i deras arbete med informationssäkerhet.

Av de intervjuer som genomförts framkommer att det i dagsläget inte sker någon stadsövergripande avstämning och kontroll av att berörda nämnder upprättar kontinuitetsplaner för de kritiska åtaganden som identifierats i risk- och sårbarhetsanalysen. Övrig dokumentation som nämnderna upprättar i sitt arbete med risk- och sårbarhetsanalyser ska rapporteras till stadsledningskontorets säkerhetsenhet.

Resultatet av intervjuerna visar också att det finns olika syn inom stadsledningskontorets avdelningar om det centrala ansvaret för att samordna och följa upp om nämnderna upprättar kontinuitetsplaner. Säkerhetsenheten menar att de inte har ansvar för att samordna och följa upp då det är respektive linjeorganisations ansvar att säker-

[3] Kommunal författningssamling för Stockholm, Reglemente för kommunstyrelsen 2017:08.
[4] Vid granskningstillfället gällde Kommunal författningssamling för Stockholm, Instruktion för stadsledningskontoret 2016:02.

ställa att kontinuitetsplaner tas fram för kritiska åtaganden. Avdelningen för digital utveckling ser utifrån sitt ansvar ett behov av att säkerställa att kontinuitetsplaner tas fram men anger att detta inte har gjorts.

Granskningen visar även att det finns ett visst samarbete mellan säkerhetsenheten och avdelningen för digital utveckling när det gäller processen för risk- och sårbarhetsanalys men inte specifikt kopplat till kontinuitetsplanering.

Nämndernas organisation
Nämnder och bolag har ansvar för att årligen upprätta en risk- och sårbarhetsanalys och vid förekommande fall kontinuitetsplaner för de kritiska åtaganden som identifierats i risk- och sårbarhetsanalysen. Vidare ska nämnder och bolag utse en säkerhetssamordnare som ansvarar för att samordna trygghets- och säkerhetsarbetet inom den egna nämnden eller bolaget. I den dokumentation revisionskontoret tagit del av och i de intervjuer som genomförts har det inte specificerats vad rollen som säkerhetssamordnare omfattar.

Granskningen visar att de granskade nämnderna har utsett en säkerhetssamordnare. Den omfattning som säkerhetssamordnaren arbetar med sitt ansvarsområde skiljer sig åt mellan de granskade nämnderna. De intervjuer som genomförts visar att arbetet med nämndens risk- och sårbarhetsanalys ingår i säkerhetssamordnarens roll men att framtagande av kontinuitetsplaner främst görs inom den verksamhet som berörs av ett bortfall av it-system. Bortsett från Norrmalms stadsdelsförvaltning är det ingen av de granskade nämnderna som genomför någon uppföljning av att kontinuitetsplaner upprättats för kritiska åtaganden.

3.1.2 Styrning

Metodstöd
Som stöd i nämndernas arbete med risk- och sårbarhetsanalys har stadsledningskontoret tagit fram ett metodstöd i form av en handbok för risk och sårbarhetsanalys. När arbetssätten för processen med risk- och sårbarhetsanalysen har utvecklats eller förändrats har det tagits fram kortare beskrivningar för utvalda steg. Handboken är daterad år 2013 och har sedan dess inte uppdaterats i sin helhet, vilket gör att den i alla delar inte är aktuell eller stämmer överens med de ovan nämnda beskrivningarna.

Genomförda intervjuer och den dokumentation revisionskontoret tagit del av i granskningen visar att det saknas ett metodstöd för hur kontinuitetsplaner ska upprättas. Den instruktion som finns går att

läsa i stadens riktlinjer för informationssäkerhet men innehåller endast rubriknivåer utan att det under dessa anges mer i detalj vad en kontinuitetsplan bör innehålla/omfatta.

Information och utbildning
På stadsövergripande nivå visar granskningen att det saknas en plan för utbildningsinsatser avseende risk- och sårbarhetsanalys och kontinuitetsplaner som riktar sig till nämnder och bolag. Senast en utbildningsinsats genomfördes var år 2016.

Vi har i granskningen inte kunnat identifiera att det finns någon aktuell utbildning samt informationsmaterial för att säkerställa att verksamheternas olika ansvarsroller förstår sitt ansvar och uppdrag samt är införstådda med varför kontinuitetsplaner ska tas fram, vad dessa syftar till och vad som ska uppnås. Detta gäller såväl på en stadsövergripande nivå som förvaltningsnivå.

3.2 Har granskade nämnder fastställda kontinuitetsplaner?

Kontinuitetshantering handlar om att skapa en systematisk motståndskraft och robusthet för att ordinarie verksamhet ska kunna bedrivas på en acceptabel nivå. Kontinuitetsplanens syfte är att systematisera och sammanfatta de rutiner och resurser som behövs för att upprätthålla verksamhetens nyckelfunktioner vid en störning och för att kunna återställa verksamheten.

Av stadens riktlinjer för informationssäkerhet framgår att en kontinuitetsplan ska 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.

Trafiknämnden
Av de intervjuer som har genomförts och den dokumentation som revisionskontoret tagit del av framkommer att trafiknämnden inte har upprättat kontinuitetsplaner som säkerställer att verksamhet som är beroende av it-system kan upprätthållas vid en störning som medför att tillgång till it-systemen saknas.

Enligt intervjuade arbetar nämnden med åtgärdsplaner för händelser som kan inträffa. De åtgärdsplaner som revisionskontoret tagit del av är mer av karaktären rutinbeskrivning och omfattar inte de uppgifter som riktlinjerna för informationssäkerhet föreskriver.

Stadsdelsnämnderna Norrmalm och Hägersten-Liljeholmen
Kontinuitetsplaner för Sociala system ska upprättas, dels utifrån generella krav i stadens riktlinjer för informationssäkerhet och dels utifrån NIS-direktivet[5]. I NIS-direktivet finns krav på kontinuitetsplaner för hälso- och sjukvårdens verksamheter, så att dessa inte drabbas av störning även om it-systemet eller nätverket drabbas av en störning.

Båda de granskade stadsdelsnämnderna har kontinuitetsplaner för hur verksamheten ska upprätthållas vid en störning som medför att tillgång till Sociala system saknas.

Norrmalms stadsdelsnämnds kontinuitetsplan för Sociala system omfattar i huvudsak de uppgifter som framgår i riktlinjerna för informationssäkerhet. Med utgångspunkt från den övergripande kontinuitetsplanen tas motsvarande planer fram av de enheter som berörs av Sociala system. Det framgår dock inte av dokumenten när eller hur de fastställts.

Hägersten-Liljeholmens stadsdelsnämnds kontinuitetsplan för Sociala system saknar till stor del de uppgifter som en kontinuitetsplan bör innehålla. Exempelvis saknas en tydlig beskrivningar av roller och dess ansvar för att säkerställa att rätt personer tar rätt ansvar vid en aktivering av kontinuitetsplanen. Det framgår heller inte av kontinuitetsplanen när den är upprättad/fastställd, vem som godkänt den samt rutin för uppdatering. Av de intervjuer som genomförts framgår att det saknas kännedom om kontinuitetsplanen i organisationen.

3.3 Kontinuitetsplanens koppling till risk- och sårbarhetsanalysen

Nämndernas arbete med den årliga risk- och sårbarhetsanalysen sker i fyra steg. Steg 1 omfattar krishantering, steg 2 riskhantering, steg 3 kontinuitet och steg 4 skyddsvärden. Samtliga nämnder ska genomföra steg 1 och 2. Steg 3 genomförs av de nämnder som har identifierat kritiska åtaganden där människa, miljö, egendom eller samhällets/stadens funktionalitet kan drabbas av allvarliga störningar inom kort tid efter ett avbrott i åtagandet. Steg 4 genomförs och redovisas av utvalda förvaltningar och bolag och ska innehålla en säkerhetsanalys med fokus på att identifiera/belysa beroenden

[5] NIS-direktivet (The Directive on security of network and information systems) trädde i kraft den 1 augusti 2018 i Sverige genom lagen om informationssäkerhet för leverantörer av samhällsviktiga och digitala tjänster.

mellan staden och samhällsviktig verksamhet samt skapa en konstruktiv uppföljning inom området.

Rapportering av de olika stegen sker inte i en och samma systemlösning, vilket av de intervjuade i vissa fall upplevdes som att det inte finns ett tydligt flöde i arbetet med risk-och sårbarhetsanalysen och kontinuitetsplaner. Detta speglar även 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 (steg 3) genomföras för samtliga identifierade tidskritiska åtaganden. Av instruktionen framgår att minst fem kritiska åtaganden måste hanteras. Detta är enligt stadsledningskontoret för att de med många tidskritiska åtaganden då har möjligheten att hantera ett antal kritiska åtaganden per år istället för vid ett och samma tillfälle.

En genomgång av nämndernas inrapporterade uppgifter visar att nämnderna har identifierat att antal tidskritiska åtaganden som inte återfinns i nämndens kontinuitetshantering (steg 3). Detta innebär att inte alla de åtaganden som anses vara tidskritiska har en plan för att hanteras om det skulle uppstå en störning trots att de bedöms som allvarliga av nämnden. Av den dokumentation revisionskontoret tagit del av framgår det inte hur nämnderna har prioriterat mellan de kritiska åtagandena.

3.4 Uppföljning av kontinuitetsplanerna

Av stadens trygghets- och säkerhetsprogram samt riktlinjer för informationssäkerhet framgår att åtgärder som vidtas ska följas upp och utvärderas. För att säkerställa att en kontinuitetsplan är funktionell krävs att den testas och att personalen är tränad i att agera i enlighet med planen. Detta är också enda sättet att säkerställa att planen fungerar operativt.

Stadsledningskontoret
Av de intervjuer som genomförts framkommer att det i dagsläget inte sker någon stadsövergripande avstämning och kontroll av att berörda nämnder upprättar kontinuitetsplaner för de kritiska åtaganden som identifierats i risk- och sårbarhetsanalysen.

Stadsdelsnämnderna Norrmalm och Hägersten-Liljeholmen
Granskningen visar att det vid de granskade nämnderna inte sker någon uppföljning som leder till att det säkerställs att kontinuitetsplaner fastställs, kommuniceras eller testas. Eftersom det inte sker

någon uppföljning sker det inte heller någon kvalitetssäkring av kontinuitetsplanerna.

Norrmalms stadsdelsnämnd följer årligen upp och uppdaterar vid behov den framtagna kontinuitetsplanen för Sociala system. Det sker dock inte någon kontroll av att berörda enheter följer upp och uppdaterar de enhetsspecifika kontinuitetsplanerna.

Vid Hägersten-Liljeholmens stadsdelsnämnd har det inte gjorts någon uppföljning och uppdatering av kontinuitetsplanen för sociala system sedan den upprättades (2015).

De intervjuer som genomförts visar att det saknas en tydlig organisation och/eller ansvarsfördelning samt rutiner för uppföljning i syfte att säkerställa att kontinuitetsplaner testas och vid behov justeras och utvecklas. Det finns heller inte en strategi eller plan för genomförande och uppföljning av tester och/eller övningar. De granskade stadsdelsnämnderna hade vid granskningstillfället inte genomfört någon test och/eller övning för att säkerställa att kontinuitetsplanerna är funktionella och för att medarbetare ska ha tillräcklig kunskap om och kunna handla i enlighet med planen.

4. Slutsatser

Kontinuitetsplanering är en viktig del av stadens samlade arbete i att upprätthålla verksamheten och minska risken för negativ påverkan vid störningar. Utöver detta, utgör den tid som verksamheten anser sig kunna upprätthålla en acceptabel nivå av service med hjälp av kontinuitetsplaner, en tydlig indikation för hur snart it-stöd måste vara tillgängliga innan en störning övergår i krishantering. Kontinuitetsplanering är alltså inte en enskild och avskild företeelse utan en viktig del av en process för att säkerställa att staden har en beredskap mot oförutsedda händelser.

Otydligt metodstöd
För att ge nämnder och bolag förutsättningar att organisera och genomföra ett kvalitativt arbete med risk- och sårbarhetsanalyser och kontinuitetsplaner krävs ett väl utvecklat metodstöd. I kombination med detta krävs även att adekvata och återkommande utbildningsmöjligheter ges.

Granskningen visar att det metodstöd som i dagsläget finns tillgängligt är daterad år 2013 och är till viss del inaktuellt. Det saknas även 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.

Kontinuitetsplanerna har brister
Av både Stockholms stads trygghets- och säkerhetsprogram och stadens riktlinjer för informationssäkerhet framgår att kontinuitetsplaner ska tas fram i syfte att skapa en förmåga i organisationen att hantera störningar och avbrott i verksamheten så att dessa får en så liten påverkan som möjligt på verksamheten.

Granskningen visar att trafiknämnden inte tagit fram dokumenterade kontinuitetsplaner som säkerställer att verksamheten kan upprätthållas vid störning eller avbrott som medför att tillgång till it- och informationssystem saknas. Revisionskontoret anser att det utgör en risk att kontinuitetsplaner saknas, i första hand med hänvisning till att verksamheten saknar den grundläggande dokumentation som krävs för att upprätthålla verksamheten om tillgången till it- och informationssystemen slås ut men också för att det kan skapa ett personberoende.

De granskade stadsdelsnämnderna har kontinuitetsplaner för hur verksamheten ska upprätthållas vid en störning som medför att tillgång till Sociala system saknas. Det finns dock stora kvalitetsskillnader i de båda nämnderna kontinuitetsplaner. Hägersten-Liljeholmens stadsdelsnämnds kontinuitetsplan saknar till stor de uppgifter som en kontinuitetsplan bör innehålla. Vidare är den inte känd i organisationen. Norrmalms stadsdelsnämnd har kontinuitetsplaner både på övergripande nivå och enhetsnivå, vilket skapar förutsättningar för att dessa är kända i organisationen. Kontinuitetsplanerna omfattar i huvudsak de uppgifter som framgår i riktlinjerna för informationssäkerhet.

Om kontinuitetsplanernas innehåll inte är känt i organisationen och att roller och deras ansvar inte är tydligt beskrivna finns en risk att kontinuitetsplaner aktiveras felaktigt eller inte alls. Detta får naturligtvis konsekvenser för de som är beroende av att verksamheten fungerar. Revisionskontoret anser att samtliga åtaganden som bedömts som allvarliga och tidskritiska ska kontinuitetshanteras.

Koppling till 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[6] 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.

Uppföljning av kontinuitetsplanerna
Av stadens trygghets- och säkerhetsprogram samt riktlinjer för informationssäkerhet framgår att åtgärder som vidtas ska följas upp och utvärderas. För att säkerställa att en kontinuitetsplan är funktionell, krävs att den testas och att personalen är tränad i att agera i enlighet med planen. Detta är också enda sättet att säkerställa att planen fungerar operativt.

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. Detta kan medföra att de kontinuitetsplaner som tagits fram kan vara inaktuella eller inte tjänar sitt syfte då dessa inte testas genom någon form av övning. Avsaknaden av uppdaterade och testade kontinuitetsplaner kan innebära att stadens hantering av oförutsedda händelser försvåras.

[6] Handbok – Stockholms stads risk- och sårbarhetsanalys sid. 35 anger att ett eller ett fåtal kritiska åtaganden ska analyseras per organisation och år. Av mallen för steg 3 – Beroendeanalys, förmåga och åtgärdsplan anges att minst fem kritiska åtaganden ska analyseras per organisation och år.

5. Sammanfattande bedömning och rekommendationer

Den sammanfattande bedömningen är att stadens styrning och uppföljning av den kontinuitetsplanering som ska finnas för att minimera skadan av begränsad tillgång till informationsteknik har brister som behöver åtgärdas.

Utifrån redovisade iakttagelser och bedömningar lämnas följande 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 utbildnings-möjligheter 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

- Genomfört 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.

Bilaga 1 Intervjupersoner

Stadsledningskontoret
Tf. säkerhetsdirektör, säkerhetsenheten
Säkerhetsstrateg, säkerhetsenheten
CTO/Enhetschef, avdelningen för digital utveckling
CISO/Informationssäkerhetsansvarig, avdelningen för digital utveckling

Trafiknämnden
Avdelningschef, infrastrukturavdelningen
Säkerhetssamordnare, infrastrukturavdelningen
Enhetschef it-enheten, administrativa avdelningen
Enhetschef trafiksystem, infrastrukturavdelningen

Norrmalms stadsdelsnämnd
Avdelningschef, äldreomsorgsavdelningen
Enhetschef beställarenheten, äldreavdelningen
Enhetschef hemtjänst, äldreavdelningen
Handläggare/Säkerhetssamordnare, avdelningen för administration och prevention.

Hägersten-Liljeholmens stadsdelsnämnd
Avdelningschef, äldreomsorgsavdelningen
Enhetschef hemtjänst, äldreomsorgsavdelningen
Säkerhetssamordnare, administrativa avdelningen
Paraplysamordnare, administrativa avdelningen