Stockholms stad

Stadens informations-säkerhetsarbete

Nr 8, 2018

Projektrapport från Stadsrevisionen

Dnr: 3.1.3-79/2018

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, www.stockholm.se/revision. De kan också beställas från revisionskontoret, revision.rvk@stockholm.se.

Stadens informationssäkerhetsarbete
Nr 8, 2018

Dnr: 3.1.3-79/2018 www.stockholm.se/revision

Till
Kommunstyrelsen
Fastighetsnämnden
Servicenämnden
Farsta stadsdelsnämnd

Stadens informationssäkerhets-arbete

Revisorsgrupp 1 har den 16 oktober 2018 behandlat bifogad revisionsrapport (nr 8/2018)

I flera av stadens styrande dokument beskrivs stadens ambitioner för digitalisering av staden och dess verksamheter samt hur arbetet med informationssäkerhet ska bedrivas. Informationssäkerhet ska inte ses som en isolerad företeelse eller enskild verksamhet utan som en förutsättning för att bedriva en god verksamhet.

Rapporten visar att kommunstyrelsens och nämndernas styrning, ledning och uppföljning av informationssäkerhetsarbete behöver utvecklas. Kommunstyrelsen bör i större uträckning styra, kontrollera efterlevnaden av gällande styrdokument samt följa upp nämndernas arbete med informationssäkerhet. Nämnderna bör säkerställa att stadens styrdokument på området kommuniceras och implementeras i organisationen. Vidare bör det i stadens dokument för incidenthantering tydligare framgå hur incidenter för stads-gemensamma system ska rapporteras. Det finns annars risk för att brister i informationssäkerheten kan ge konsekvenser för staden och för medborgarna genom exempelvis informationsförlust, ekonomisk skada eller bristande förtroende för staden.

Vi hänvisar i övrigt till rapporten och överlämnar den till kommuns-tyrelsen, fastighetsnämnden, servicenämnden och Farsta stadsdels-nämnd för yttrande. Yttrandet ska ha inkommit till revisorsgrupp 1 senast den 25 januari 2018.

På revisorernas vägnar

Bosse Ringholm
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
www.stockholm.se/revision

Sammanfattning

Verksamheterna i Stockholms stads nämnder hanterar en mängd informationstillgångar som är skyddsvärda. Det ställer krav på ett aktivt informationssäkerhetsarbete för att säkerställa att informationen vid varje tillfälle är konfidentiell, riktig, tillgänglig och spårbar. Revisionskontoret har genomfört en granskning för att bedöma om kommunstyrelsen, fastighetsnämnden, servicenämnden och Farsta stadsdelsnämnds styrning, ledning och uppföljning av informationssäkerhetsarbetet är tillräckligt.

Revisionskontoret bedömer att styrningen, ledningen och uppföljningen av nämndernas informationssäkerhetsarbete behöver utvecklas. Staden har på en övergripande nivå relevanta styrdokument. Hur ansvaret för informationssäkerhetsarbetet fördelas inom staden beskrivs i dessa dokument. Granskningen visar dock att de förvaltningar som ingått i granskningen inte tycker att ansvaret i alla delar är tydligt samt att de efterfrågar stöd i hur arbetet ska organiseras och bedrivas. Vidare saknas det inom de nämnder som har granskats en tillräcklig kompetens om hur informationssäkerhetsarbetet ska bedrivas. Enligt ISO-standarden är kompetens en nödvändighet i en organisations arbete med informationssäkerhet.

Nämnderna behöver säkerställa att det bedrivs ett aktivt arbete kring informationssäkerhet och att ledningen har en aktiv roll i detta arbete. Granskningen visar att stadens riktlinjer för informationssäkerhet inte har kommunicerats och implementerats fullt i de granskade nämnderna. Vidare har granskningen visat att det saknas en för staden grundläggande utbildning i informationssäkerhet. Det saknas också kompetenskrav på att särskilt viktiga roller, som till exempel informationssäkerhetssamordnare. Det görs heller inte i tillräcklig omfattning, vare sig på en stadsövergripande nivå eller förvaltningsnivå, kontroller av att ledningssystemet för informationssäkerhet efterlevs.

För att kunna följa upp och utveckla arbetet kring informationssäkerhet bör nämnderna fånga upp vad som framkommer vid informationsklassificering, incidentrapportering och genomförda kontrollaktiviteter. Granskningen visar att nämnderna upplever att det finns oklarheter kring ansvaret för rapportering av händelser vad gäller stadsgemensamma system som till exempel LISA. Det sker heller inte någon stadsövergripande uppföljning och analys gällande

informationssäkerhet av nämndernas riskanalyser eller de händelser som nämnderna rapporterat i IA[1].

I kommunstyrelsens pågående översyn av *Riktlinjerna för informationssäkerhet* bör det enligt revisionskontorets mening, då riktlinjerna är av strategisk betydelse, övervägas om kommunfullmäktige eller kommunstyrelsen ska fatta beslut om dessa.

Den sammanfattande bedömningen är att stadens arbete avseende styrning, ledning och uppföljning av informationssäkerhetsarbetet behöver utvecklas. Kommunstyrelsen bör i större uträckning styra nämndernas arbete med informationssäkerhet. Då kommunfullmäktige har fastslagit inriktning och ambitionsnivå för stadens pågående digitalisering och hur informationssäkerhetsarbetet ska bedrivas bör en tydligare styrning inrymmas i kommunstyrelsen uppdrag.

Utifrån redovisade iakttagelser och bedömningar lämnas följande rekommendationer:

Kommunstyrelsen:

- Utveckla stödet, i form av anvisningar, instruktioner och arbetsverktyg samt utbildningsinsatser, till nämnderna i deras arbete med informationssäkerhet.

- Utveckla uppföljningen och tillsynen av nämndernas arbete med informationssäkerhet.

- Kommunfullmäktige eller kommunstyrelsen bör fatta beslut om riktlinjerna för informationssäkerhet då de utgör ett strategiskt och styrande dokument för stadens nämnder.

- Säkerställa att det finns teknisk kompetens för att säkerställa att leverantörerna hanterar säkerhetsrisker på ett tillfredsställande sätt.

Fastighetsnämnden, servicenämnden och Farsta stadsdelsnämnd:

- Kommunicera och implementera stadens riktlinjer för informationssäkerhet i organisationen.

- Kontrollera efterlevnaden av stadens riktlinjer för informationssäkerhet.

[1] IA, stadens system för händelsehantering.

Innehåll

1. Inledning

1.1 Bakgrund

Verksamheterna i Stockholms stads nämnder och bolag hanterar en mängd informationstillgångar som är skyddsvärda. Det ställer krav på ett aktivt informationssäkerhetsarbete för att säkerställa att informationen vid varje tillfälle är konfidentiell, riktig, tillgänglig och spårbar.

Kommunfullmäktige har i stadens budget för år 2018 tydliggjort att nämnder och bolagsstyrelser ska säkerställa att det i enlighet med stadens styrande dokument inom området finns ett effektivt och ändamålsenligt informationssäkerhetsarbete med åtgärder som består av processer, teknik och medarbetare som tillsammans utgör en kedja av skydd för stadens informationstillgångar.

Inom staden finns flera it-system som är väsentliga för att stadens olika verksamheter ska fungera. Exempelvis it-system för handläggning inom socialtjänsten, verksamhetssystem inom skola och äldreomsorg samt administrativa stödsystem för bland annat ekonomi och lönehantering. Bristande informationssäkerhet kan leda till allvarliga konsekvenser för staden och för medborgarna genom exempelvis informationsförlust, ekonomisk skada eller bristande förtroende för staden.

2. Granskningens genomförande

2.1 Syfte och revisionsfrågor

Syftet med granskningen har varit att bedöma om stadens styrning, ledning och uppföljning av informationssäkerhetsarbetet är tillräckligt.

Granskningen besvaras med följande revisionsfrågor:

- Är ansvar och organisation tydligt beskrivet i stadens riktlinjer, på förvaltningsnivå och för respektive förvaltningsobjekt?
- Hur arbetar verksamheterna för att säkerställa att de styrdokument som finns på området efterlevs?
- Finns en organisationskultur och mognad hos medarbetare som överensstämmer med ansvar och befogenheter?

2.2 Avgränsning

Granskningen omfattar stadens övergripande informationssäkerhetsarbete samt informationssäkerhetsarbetet specifikt för systemet LISA[2] Bas inom förvaltningsobjektet Personaladministrativa system.

2.3 Ansvarig nämnd/styrelse

Granskningen omfattar kommunstyrelsen, servicenämnden, fastighetsnämnden samt Farsta stadsdelsnämnd.

Kommunstyrelsen omfattas av granskningen som ansvarig för stadens informationssäkerhetsarbete på en övergripande nivå. Vidare är personalstrategiska avdelningen inom stadsledningskontoret systemägare av förvaltningsobjektet Personaladministrativa system vilket systemen LISA Bas[3] och LISA Självservice[4] är en del av.

Fastighetsnämnden, Farsta stadsdelsnämnd och Servicenämnden omfattas av granskningen dels som ansvariga för informationssäkerhetsarbetet inom nämndens verksamhetsansvar och dels som informationsägare i systemet LISA. I servicenämndens ansvar ingår ansvar för stadens löne- och pensionsadministration.

2.4 Revisionskriterier

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

- Stockholms stads riktlinje för informationssäkerhet (dnr 307-1396/2014)
- ISO 27001:2014 Ledningssystem för informationssäkerhet.
- Stockholms stads budget 2018 (sid. 34-35, 43-44, 49-50, 59-60)

2.5 Metod

Granskningen har genomförts genom intervjuer och dokumentstudier. Intervjuer har genomförts med medarbetare som på olika nivåer och i olika roller har ett informationssäkerhetsansvar.

[2] Löne- och informationssystem i Stockholms stad.
[3] LISA Bas är lönekärnan i stordatormiljö, där löneadministratörer registrerar enligt underlag från förvaltningarna.
[4] LISA Självservice är ett webbaserat försystem till LISA Bas där medarbetarna registrerar frånvaro, övertid, egna utlägg mm.

Utgångspunkten för hur ett ledningssystem för informationssäkerhet kan utformas och hur arbetet ska bedrivas har varit ISO 27000:2014 Ledningssystem för informationssäkerhet. I stadens Riktlinje för informationssäkerhet anges att de är anpassade till den då gällande ISO-standarden (SS-ISO/IEC 27002:2005).

Lönesystemet LISA har utgjort ett tittat på hur arbetet med informationssäkerhet fungerar i praktiken i den dagliga verksamheten.

Granskningen har genomförts av Susanne Eriksson på revisionskontoret tillsammans med konsulter från Sentor Managed Security Services AB. Rapporten har faktakontrollerats av berörda förvaltningar.

3. Informationssäkerhet i Stockholms stad

Verksamheterna i Stockholms stads nämnder och bolag hanterar en mängd informationstillgångar som är skyddsvärda. Det ställer krav på ett aktivt informationssäkerhetsarbete för att säkerställa att informationen vid varje tillfälle är konfidentiell, riktig, tillgänglig och spårbar. Bristande informationssäkerhet kan leda till allvarliga konsekvenser för staden och för medborgarna genom exempelvis bristande kontinuitet i vård- och omsorg, anseendeförluster eller ekonomiska skada

I takt med att samhället och stadens verksamheter går mot en ökad digitalisering ökar också kravet på att informationssäkerhetsarbetet bedrivs på ett systematiskt sätt. Det bör dock understrykas att informationssäkerhet inte enbart rör it-system och teknik, utan hela kommunens verksamhet och all information oavsett om den finns datorer, på ett papper eller i telefonen. Vidare berör informationssäkerhet samtlig personal i en organisation.

Informationssäkerhet ska inte ses som en isolerad företeelse eller enskild verksamhet utan som en förutsättning för att bedriva en god verksamhet. Det kräver i sin tur att det i likhet med andra områden, exempelvis ekonomi och HR, finns grundläggande processer och rutiner för hur arbetet ska bedrivas.

I flera av stadens styrande dokument beskrivs stadens ambitioner för digitalisering av staden och dess verksamheter samt hur arbetet

med informationssäkerhet ska bedrivas. I stadens *Budget 2018*[5] beskrivs att samtliga nämnder och bolagsstyrelser ska säkerställa att det finns ett effektivt och ändamålsenligt informationssäkerhetsarbete. Det anges även att uppföljning och intern kontroll, för att upptäcka och rätta till brister, är en viktig komponent i säkerhetsarbetet samt att det är angeläget med en hög riskmedvetenhet bland stadens medarbetare. I *Stockholms stads trygghets- och säkerhetsprogram*[6] framhålls att alla nämnder och bolag ska arbeta med informationssäkerhet och ha en utsedd informationssäkerhetssamordnare. Vidare framgår att samtliga nämnder och bolag ska säkerställa att korrekt information finns tillgänglig för behöriga på ett spårbart sätt när den behövs. *Strategi för Stockholm som smart och uppkopplad stad*[7] framhåller behovet av gemensamma arbetssätt och processer samt att en gemensam informationsstruktur utvecklas för att säkerställa enhetlighet i den insamlade informationen. Strategin ska tillsammans med stadens kommande digitaliseringsprogram beskriva hur arbetet ska gå till.

4. Granskningens resultat

4.1 Organisation och ansvar

Kännetecknande för en god informationssäkerhet är en tydlig ansvarsfördelning och befogenheter. Det är också viktigt att ledningen är ledande i arbetet med informationssäkerhet. Det gäller såväl på stadsövergripande nivå som på förvaltningsnivå. Hur ansvaret fördelas och vad det omfattar framgår av riktlinjerna för informationssäkerhet och stadens budget. En förutsättning för att bedriva ett informationssäkerhetsarbete är också att medarbetarna har tillräcklig kompetens i förhållande till ansvar och befogenheter.

Kommunstyrelsen har ansvar för att initiera aktiviteter för att bemöta säkerhetshot och risker. Kommunstyrelsens förvaltning stadsledningskontoret ansvarar för de strategiska och stadsövergripande frågorna inom digitalisering och verksamhetsutveckling med hjälp av it. I detta ingår också ett övergripande ansvar för informationssäkerhet samt att utfärda och förvalta stadens riktlinje för informationssäkerhet. Inom stadsledningskontoret finns avdelningen för digital utveckling som har ett övergripande ansvar för att styra och följa upp informationssäkerhetsarbetet inom staden. På avdelningen är stadens informationssäkerhetsansvarig (CISO[8])

[5] Dnr 180-616/2018, beslutad av KF 2017-11-16
[6] Dnr KS 2017/001309, beslutad av KF 2018-02-19
[7] Dnr 171-908/2016, beslutad av KF 2017-04-03
[8] CISO – Chief information security officer

organisatoriskt placerad. Rollen innebär att hålla samman stadens arbete med informationssäkerhet, förvalta ledningssystemet samt att ha tillsyn av det informationssäkerhetsarbete som bedrivs vid stadens förvaltningar och bolag.

Varje nämnd ska säkerställa att det finns ett effektivt och ändamålsenligt informationssäkerhetsarbete. Varje nämnd har vidare ansvar för informationssäkerheten inom sitt verksamhetsområde och ska årligen planlägga och löpande följa upp informationssäkerhetsarbetet. Som riktlinjerna gör gällande är det förvaltningschefen som är ansvarig för att utöva ett ledande och aktivt informationssäkerhetsarbete. Förvaltningschefen utser också vem som ska vara informationssäkerhetssamordnare för förvaltningen.

Som informationssäkerhetssamordnare är man förvaltningens kontaktperson avseende informationssäkerhet gentemot stadens informationssäkerhetsansvarig, men ska också verka för en god informationssäkerhet i organisationen. Informationssäkerhetssamordnaren ska ha kunskap om stadens regler för informationssäkerhet och om stadens säkerhetsarbete.

4.2 Ledningssystem

Stadens *Riktlinje för informationssäkerhet* utgör ledningssystemet för informationssäkerhet. Den bygger till stor del på ISO-standarden för informationssäkerhet.

Genom att arbeta efter ISO 27000-serien kan man säkerställa en bra struktur på säkerhetsarbetet, intern kontroll och att få en hög grad av förutsägbarhet. Följden blir en minimering av risker och färre misstag som kan leda till kostsamma säkerhetsincidenter.

Nedanstående processer utgör de olika delarna i ett systematiskt informationssäkerhetsarbete.

- Informationsklassning - Klassificering av alla tillgångar utifrån konfidentialitet, riktighet, tillgänglighet och spårbarhet.
- Riskanalys – Genomförande av risk- och sårbarhetsanalys för att identifiera verksamhetens kritiska risker.
- Intern kontroll – Mitigerande kontroller åt de risker som identifierats vid risk- och sårbarhetsanalys.
- Incidentrapportering – Systematisk och kontinuerlig incidentrapportering med tydliga ansvarsroller och spårbarhet.
- Kontinuerlig uppföljning av efterlevnad och förbättring

- Tydlig ansvarsfördelning och befogenheter är en förutsättning för att uppnå tillräcklig nivå av informationssäkerhet.

Granskningen visar att riktlinjerna är anpassade till den ISO-standard[9] som gällde vid beslutstillfället. Vi kan dock konstatera att riktlinjerna inte har granskats och reviderats sedan de upprättades 2014, trots att det i riktlinjen framgår att så ska ske årligen. Riktlinjen är beslutad av stadsdirektören år 2014.

Det pågår enligt uppgift ett arbete med att uppdatera stadens riktlinje för informationssäkerhet och i samband med detta anpassa dem efter den målgrupp de vänder sig till.

Utöver riktlinjen för informationssäkerhet saknas stadsövergripande anvisningar, instruktioner och arbetsverktyg som stöd för förvaltningarnas arbete med att efterleva riktlinjen. I de intervjuer som har genomförts har det framkommit att riktlinjen upplevs som komplicerad och att den inte är anpassad till den målgrupp den vänder sig till. I intervjuerna framkommer också att det efterfrågas mer stöd och tydlighet från stadsledningskontoret i förvaltningarnas informationssäkerhetsarbete. Det stöd som bland annat efterfrågas är hur styrdokument bör utformas på förvaltningen utifrån stadens riktlinje samt forum för dialog. Stadens nätverk för informationssäkerhetssamordnare med syfte att informera och stödja verksamheterna är enligt uppgift vilande.

4.2.1 Analys och bedömning

Staden har på en övergripande nivå relevanta ledningssystem/ styrdokument för hur informationssäkerhetsarbetet ska bedrivas. Vidare finns formellt en tydlig rollfördelning avseende ansvaret för det informationssäkerhetsarbete som ska bedrivas i staden. Vår bedömning är dock att styrningen, ledningen och uppföljningen av nämndernas informationssäkerhetsarbete behöver utvecklas.

Det saknas stöd till nämnderna, i form av exempelvis stadsövergripande anvisningar, instruktioner eller arbetsverktyg, i deras arbete med att implementera och efterleva det styrande ledningssystemet. En konsekvens av detta blir att stadens övergripande arbete och uppföljning försvåras då nämnderna inte arbetar på ett konsekvent och likartat sätt. För att säkerställa att staden har en god informationssäkerhet bör det i likhet med andra stödfunktioner som ekonomi och personal finnas en tydligare styrning från kommunstyrelsen.

[9] SS-ISO/IEC 27002:2005

Då informationssäkerhet omfattar hela stadens verksamhet, all information och samtlig personal är antagandet av ett ledningssystem för informationssäkerhet ett strategiskt beslut för en organisation. Med anledning av detta bör kommunfullmäktige eller kommunstyrelsen fatta beslut om riktlinjerna då de utgör ett strategiskt och styrande dokument för stadens nämnder.

4.3 Implementering

Utbildning och kommunikation ger förutsättningar för att öka kunskapen och acceptansen om informationssäkerhet. Vidare krävs att efterlevnaden av ledningssystemet kontrolleras.

Granskningen visar att det i dagsläget inte finns någon gemensam utbildning som säkerställer att samtliga medarbetare har en grundläggande förståelse för informationssäkerhet. Det finns heller inte något krav på att informationssäkerhetssamordnaren ska ha kompetens inom området.

De intervjuer som har genomförts visar att rollen som informationssäkerhetssamordnare ofta kombineras med andra uppdrag som exempelvis ansvar för ekonomi eller administration. Uppskattningsvis utgör rollen som informationssäkerhetssamordnare 5-10 procent av en årsarbetstid vid de granskade nämnderna.

När det kommer till hur förvaltningarna arbetar med informations–säkerhet visar granskningen att det inte är en fråga som finns på ledningens agenda.

Enligt stadens budget har stadsledningskontoret bland annat ansvar för att styra och följa upp informationssäkerhetsarbete inom staden Intervjuer som genomförts visar att det på stadsövergripande nivå inte sker någon tillsyn av efterlevnaden av ledningssystemet för informationssäkerhet eller av det informationssäkerhetsarbete som bedrivs vid förvaltningar och bolag.

Granskningen visar även att det på förvaltningsnivå endast sker få eller inga kontroller för att säkerställa att ledningssystemet efterlevs i förvaltningens olika verksamheter.

4.3.1 Analys och bedömning

Bristande kompetens och förståelse för informationssäkerhet kan leda till, medvetet eller omedvetet, konsekvenser för staden och för medborgarna genom exempelvis informationsförluster, ekonomisk skada eller bristande förtroende för staden.

Revisionskontorets bedömning är att stadens ledningssystem inte har implementerats fullt ut i de granskade nämnderna. En orsak är att ledningssystemet inte har kommunicerats på ett sätt som bidragit till förståelse för informationssäkerhet i organisationen. Resultatet av detta är att stadens olika förvaltningar och verksamheter inte arbetar på ett konsekvent och likartat sätt. För att säkerställa en god informationssäkerhet bör kommunstyrelsen vara styrande och stödjande i detta arbete på liknade sätt som inom exempelvis ekonomi och HR.

För att öka kunskapen och acceptansen om informationssäkerhet i organisationen krävs att samtliga medarbetare har en grundläggande förståelse för ämnet, varför det bör finnas en för staden gemensam utbildning. Därutöver bör ledningen för respektive förvaltning tillse att medarbetarna har tillräcklig kunskap i förhållande till ansvar och befogenheter. Vidare bör det för informationssäkerhetssamordnare finnas krav på kompetens inom informationssäkerhet då dessa i dagsläget inte i tillräcklig omfattning arbetar i denna roll för att upprätthålla en tillfredsställande kunskapsnivån kring området.

Utan att granska kan ledningen inte säkerställa att det beslutade ledningssystemet efterlevs i organisationen. Revisionskontorets bedömning är att det inte görs tillräckliga kontroller, var sig på en stadsövergripande nivå eller förvaltningsnivå, av att ledningssystemet efterlevs. Detta kan medföra att eventuella brister i efterlevnaden inte upptäcks vilket på olika sätt kan leda till skada för staden och dess medborgare.

4.4 Uppföljning och utveckling

Riskanalysen är viktig för att säkerställa en ändamålsenlig hantering av informationstillgångar i förvaltningarna. En riskanalys bör fånga upp vad som framkommit i bland annat informationsklassificeringen, incidentrapporteringen samt genomförda internkontrollaktiviteter.

I stadens anvisningar för nämndernas arbete med verksamhetsplan år 2018 anges it-säkerhet som ett av tre obligatoriska förvaltningsövergripande riskområden utöver de risker nämnderna själva identifierar. Utöver denna skrivelse i anvisningarna saknas det styrande dokument för riskanalyser avseende informationssäkerhet.

Riskanalyser genomförs årligen som en del i förvaltningarnas arbete med att ta fram en internkontrollplan. I de väsentlighets- och riskanalyser som finns rapporterade i ILS och som revisionskontoret

tagit del av är riskerna på en övergripande nivå och saknar koppling till förvaltningens utvecklingsarbete. Det saknas även en koppling mellan identifierade risker och vad som framkommit i incident-rapportering, informationsklassificering och genomförda internkontrollaktiviteter.

Av ledningssystemet och stadens rutin för rapportering av incidenter framgår att samtliga förvaltningar och bolag ska rapportera och följa upp incidenter som rör informationssäkerhet. Av information[10] på stadens intranät framgår att it-relaterade incidenter ska rapporteras i systemet för händelsehantering, IA. Det kan röra sig om datorintrång, informationsförlust, stillastående system samt missbruk av system, tjänster och funktioner. Enligt stadens SIKT-avtal ska anmälan även göras till driftleverantörens ärendehantering. I granskningen har det framkommit att de granskade nämnderna upplever att det finns en otydlighet kring hur incidentrapportering ska ske, via vilket verktyg och kanaler samt vilken typ av incidenter som ska rapporteras i IA respektive till driftleverantören. Detta gäller dels incidenter som rör stads-gemensamma system men också händelser som rör den egna verksamheten.

På liknade sätt som vid efterlevnaden av ledningssystemet sker det enligt uppgift inte någon stadsövergripande analys och uppföljning av de informationssäkerhetsrisker som nämnderna rapporterat. Det görs inte heller någon uppföljning av de incidenter som rapporterats i IA vad gäller informationssäkerhet.

4.4.1 Analys och bedömning

För att utveckla sitt arbete kring informationssäkerhet är revisions-kontorets bedömning att nämnderna bör säkerställa att riskanalys-erna fångar upp vad som identifierats vid informationsklassi-ficering, incidentrapportering och genomförda internkontroll-aktiviteter.

Nämnderna bör också säkerställa att de har fungerande rutiner för att it-relaterade händelser rapporteras i IA. Det finns inget stöd för att det inträffat händelser som rör informationssäkerhet men det går heller inte att utesluta då endast ett fåtal händelser har rapporterats i IA.

Då incidentrapporteringen är ett viktigt underlag för att identifiera risker bör det säkerställas att staden har en fungerande incident-rapportering. Det är därför av vikt att förtydliga och kommunicera

[10] IA Frågor och svar

ansvaret för incidentrapportering gällande stadsgemensamma system. Det bör tydligt framgå vem som ska rapportera vilka händelser samt hur denna rapportering ska ske. Det finns annars en risk för att incidenter inte rapporteras samt tas om hand på ett korrekt sätt.

Uppföljning och utveckling av stadens arbete med informationssäkerhet kan kopplas till riktlinjen där det framgår att modellen PDCA (Plan-Do-Check-Act) utgör grunden för uppföljning och utveckling av informationssäkerhetsarbetet. Modellen är processorienterad och målet är att nå ständiga förbättringar. Revisionskontoret kan i granskningen inte se att modellen eller motsvarande används för att utvärdera informationssäkerhetsarbetet i de nämnder som ingått i granskningen.

4.5 Systemet LISA

LISA Bas kallas det it-stöd som staden använder för beräkning och utbetalning av löner, arvoden mm.

Personalstrategiska avdelningen vid stadsledningskontoret utövar det fortlöpande systemägarskapet för systemen LISA Bas och LISA Självservice inom Personaladministrativa system. Systemägaren fattar de övergripande besluten om systemets drift och mål. I ansvaret ingår bland annat att fatta beslut om systemens säkerhetsnivå, sekretessbelagda funktioner och behörighetskontroller.

För att nå ut med information till förvaltningarna finns mötesforum för personalchefer och administratörer av Lisa Självservice. Vidare finns det en referensgrupp med löneadministratörer för LISA Bas. Det finns också ett verksamhetsråd där representanter från personalstrategiska avdelningen och serviceförvaltningen deltar. Information finns också att ta del av på stadens intranät.

Styrande i den övergripande förvaltningen av personaladministrativa system är Förvaltningsplan 2018 – Personaladministrativa system. Planen uppdateras årligen och beskriver vilka uppgifter som ska utföras i förvaltningen av systemet samt hur den ska bemannas och styras. Utifrån förvaltningsplanen tas en årlig beställning fram för förvaltning och utveckling av LISA Bas, LISA Självservice samt övriga HR-system. Förvaltningsplanen följs upp löpande tillsammans med driftleverantören. Detta bekräftas av de protokoll som revisionskontoret tagit del av.

Intervjuer har visat att systemägaren har identifierat att det i organisationen saknas teknisk kompetens för att ställa krav på

leverantörer vad gäller tekniskt skydd mot informationssäkerhetsrisker kopplat till systemet LISA.

Som informationsägare är varje förvaltning som använder systemet LISA Självservice bland annat ansvariga för att systemet och informationen används på bästa sätt. I förvaltningarnas ansvar ingår även att tillse att deras del av informationen i systemet LISA Självservice samt de manuella underlag som skickas till serviceförvaltningen för registrering i LISA Bas håller hög kvalitet och är aktuell (registeransvar). Vidare ansvarar förvaltningarna för att säkerhetsrutinerna i LISA Självservice fungerar lokalt (exempelvis hantering av behörigheter) samt att alla som arbetar med LISA Självservice får erforderlig utbildning och instruktioner till LISA Självservice.

Som stöd i förvaltningarnas praktiska arbete i systemet LISA Bas finns en handbok på serviceförvaltningens intranät. Personalstrategiska avdelningen vid stadsledningskontoret har även tagit fram *Riktlinjer för internkontroll av lönehantering*. Riktlinjerna beskriver vilka kontroller som årligen ska genomföras av lönehanteringen. Respektive förvaltning (informationsägare) ansvarar för att integrera arbetssätten i sin verksamhet och tillse att riktlinjerna efterlevs.

I de granskade nämndernas väsentlighets- och riskanalyser som revisionskontoret tagit del av saknas risker som berör informationssäkerhet kopplat till förvaltningarnas ansvar som informationssägare i LISA Självservice.

Löneadministratörerna på serviceförvaltningen är de enda som har behörighet att registrera i systemet LISA Bas. För dessa behörigheter beslutar stadens personaldirektör. Vid de övriga förvaltningarna har vanligen personalchef och HR-konsult begränsad behörighet att titta/läsa information om den egna förvaltningen. När det kommer till behörigheter ansvarar respektive förvaltning för att följa upp behörigheter i LISA Självservice och personalstrategiska avdelningen för behörigheter i LISA Bas. Förvaltningarna har enligt gällande rutin ansvar för att följa upp behörigheterna i LISA Självservice varje månad så att användarna har rätt behörighet och att behörigheter avslutas. Personalstrategiska avdelningen gjorde våren 2018 en genomgång av samtliga behörigheter i LISA Bas vilket resulterade i att vissa användare fick en lägre behörighet samt att behörigheter avslutades. I övrigt gör personalstrategiska avdelningen uppföljning av behörigheter i LISA Bas kvartalsvis.

Genomförda intervjuer med förvaltningarna visar att det finns en oklarhet vad gäller ansvaret för att rapportera incidenter som rör stadsgemensamma system, däribland systemet LISA. Det gäller bland annat om det är systemägaren eller informationsägaren som ska rapportera och om incidenten/händelsen ska rapporteras i IA eller till driftleverantören.

Stadsledningskontorets personalstrategiska avdelning följer löpande upp de incidenter som rapporterats till driftleverantören. Uppföljningen sker i samband med leverans- och förvaltningsmöten. Incidenter som rör LISA Bas och som rapporterats i IA följs månatligen upp av stadens personaldirektör. Vidare genomför personalstrategiska avdelningen informationsklassificering av systemen LISA Bas och LISA Självservice.

I dokumentet *Hantering och förvaring av personalhandlingar i Stockholms stad* beskrivs bland annat ansvarsfördelning för personalhandlingar inom staden, sekretess inom personalområdet, överlämning av personalhandlingar till annan förvaltning, utlämnande av handlingar till allmänheten. Intervjuer visar att det finns en förståelse bland medarbetarna som praktiskt arbetar i systemen LISA Bas och LISA Självservice hur personalhandlingar ska hanteras samt vilka uppgifter och handlingar som får lämnas ut.

4.5.1 Analys och bedömning

Revisionskontorets granskning visar att det finns former för den övergripande förvaltningen av personaladministrativa system. I förvaltningsplanen beskrivs vilka uppgifter som ska utföras i förvaltningen av systemet samt hur den ska bemannas och styras. Vid leverans- och förvaltningsmöten följs förvaltningsplanen upp samt de incidenter som rapporterats till driftleverantören. Det finns vidare etablerade mötesforum där medarbetarna på förvaltningarna ges information. Dock är vår bedömning, enligt vad som framkommit i granskningen, att det finns risk för att informationssäkerhetsarbetet avseende förvaltningarnas ansvar som informationsägare inte är tillräckligt.

Vad gäller den tekniska kompetensen är revisionskontorets bedömning att det är angeläget att denna kompetens finns i organisationen för att kunna ställa krav på samt säkerställa att leverantörer av system upprätthåller en tillfredsställande nivå av säkerhet.

Stadsledningskontorets personalstrategiska avdelning gör en analys för staden utifrån de incidenter som rapporterats till driftleveran-

tören och i IA samt vad som framkommit av informationsklassificeringen av system LISA Bas och LISA Självservice. Analysen sker dock inte samlat.

5. Sammanfattande bedömning och rekommendationer

Staden har på en övergripande nivå relevanta styrdokument i vilka också ansvarsfördelningen för informationssäkerhetsarbetet beskrivs. Granskningen visar dock att de förvaltningar som ingått i granskningen inte tycker att ansvaret i alla delar är tydligt samt att de efterfrågar stöd i hur arbetet ska organiseras och bedrivas. Vidare saknas det inom de nämnder som har granskats tillräcklig kompetens om hur informationssäkerhetsarbetet ska bedrivas. Enligt ISO-standarden är kompetens en nödvändighet i en organisations arbete med informationssäkerhet.

Granskningen visar att nämndernas arbete med att säkerställa efterlevnaden av gällande styrdokument på området behöver utvecklas. Riktlinjerna för informationssäkerhet behöver på ett tydligare och aktivare sätt kommuniceras och implementeras i verksamheterna. Vidare bör det för att skapa acceptans och förståelse för informationssäkerhet bland medarbetarna finnas en för staden grundläggande utbildning i informationssäkerhet. Det görs inte heller i tillräcklig omfattning, vare sig på en stadsövergripande nivå eller förvaltningsnivå, kontroller av att ledningssystemet efterlevs. Granskningen visar också att nämnderna, för att följa upp och utveckla informationssäkerhetsarbetet, bör fånga vad som framkommer vid informationsklassificering, incidentrapportering och genomförda kontrollaktiviteter.

Den sammanfattande bedömningen är att stadens arbete avseende styrning, ledning och uppföljning av informationssäkerhetsarbetet behöver utvecklas. Kommunstyrelsen bör i större uträckning styra nämndernas arbete med informationssäkerhet. Då kommunfullmäktige har fastslagit inriktning och ambitionsnivå för stadens pågående digitalisering och hur informationssäkerhetsarbetet ska bedrivas bör en tydligare styrning inrymmas i kommunstyrelsen uppdrag.

Utifrån redovisade iakttagelser och bedömningar lämnas följande rekommendationer:

Kommunstyrelsen:

- Utveckla stödet, i form av anvisningar, instruktioner och arbetsverktyg samt utbildningsinsatser, till nämnderna i deras arbete med informationssäkerhet.

- Utveckla uppföljningen och tillsynen av nämndernas arbete med informationssäkerhet.

- Kommunfullmäktige eller kommunstyrelsen bör fatta beslut om riktlinjerna för informationssäkerhet då de utgör ett strategiskt och styrande dokument för stadens nämnder.

- Säkerställa att det finns teknisk kompetens för att säkerställa att leverantörerna hanterar säkerhetsrisker på ett tillfredsställande sätt.

Fastighetsnämnden, servicenämnden och Farsta stadsdelsnämnd:

- Kommunicera och implementera stadens riktlinjer för informationssäkerhet i organisationen.

- Kontrollera efterlevnaden av stadens riktlinjer för informationssäkerhet.

Bilaga 1 Intervjupersoner

Farsta stadsdelsförvaltning
- Förvaltningschef
- Informationssäkerhetssamordnare
- Strateg, ekonomiavdelningen

Fastighetskontoret
- Förvaltningschef
- Enhetschef, enheten för digitalt stöd
- Informationssäkerhetssamordnare
- HR-konsult, HR-enheten, HR- och kommunikationsavdelningen
- Enhetschef, HR-enheten, HR- och kommunikationsavdelningen

Serviceförvaltningen
- Tf. förvaltningschef
- Avdelningschef, avdelningen lön och pension
- Informationssäkerhetssamordnare

Stadsledningskontoret
- Personaldirektör, personalstrategiska avdelningen
- Enhetschef, enheten för HR-system, personalstrategiska avdelningen
- Strateg, enheten för HR-system, personalstrategiska avdelningen
- Informationssäkerhetsansvarig, avdelningen för digital utveckling
- Enhetschef, enheten för infrastruktur, plattformar och support, avdelningen för digital utveckling
- Handläggare, enheten för upphandling och avtal, avdelningen för digital utveckling