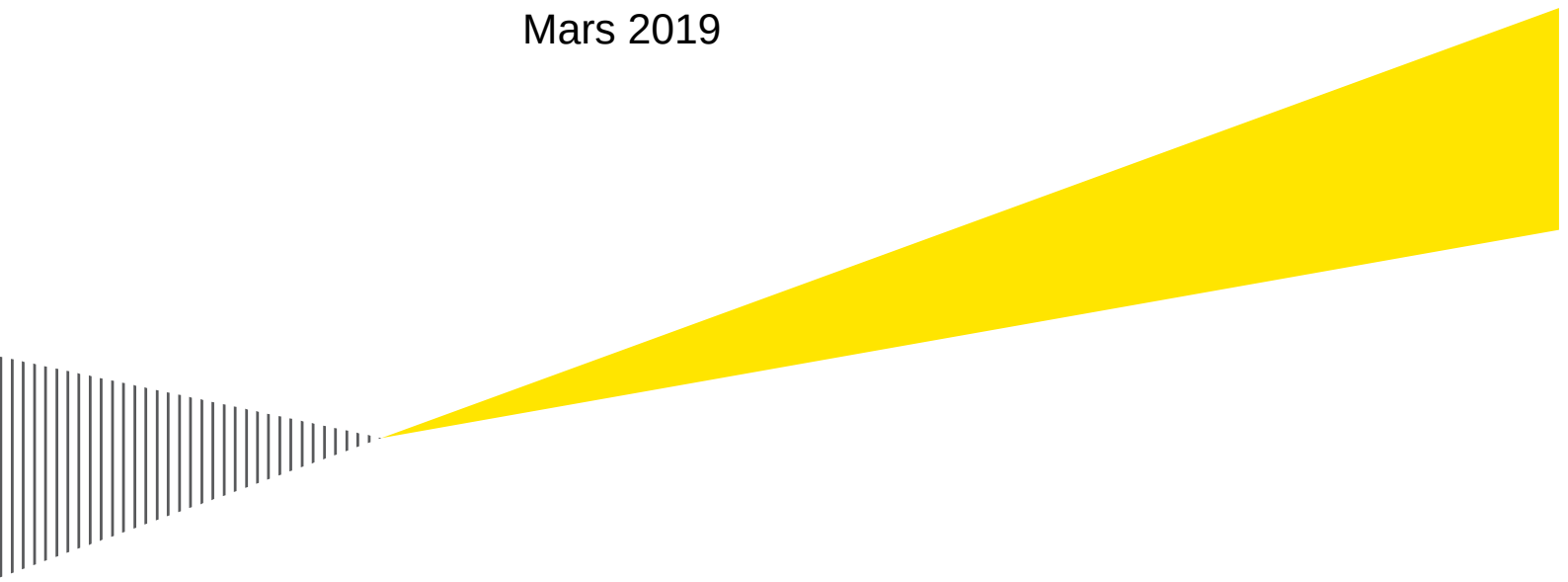
Sundbybergs stad

Granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering

Mars 2019



Building a better working world

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Sammanfattning

EY har på uppdrag av Sundbybergs stads förtroendevalda revisorer genomfört en granskning av stadens arbete med informationssäkerhet. Granskningens syfte har varit att ge en övergripande nulägesbild om huruvida Kommunstyrelsen för Sundbybergs stad har tillsett att arbetet kring informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt.

Granskningen genomfördes under januari till mars 2019 och baserades på intervjuer med identifierade nyckelpersoner i stadens informationssäkerhetsarbete och genomgång av insamlad styrdokumentation. Grunden för intervjufrågorna och granskningen som helhet har byggts på EY:s beprövade informationssäkerhetsramverk *Cybersecurity Program Assessment* (CPA), med fokus på organisation och styrningsrelaterade områden, och *Granskningsprogram Cyber och Informationssäkerhet* (GCI), med fokus på offentlig verksamhet. Både CPA och GCI baseras på erkända ramverk inom informationssäkerhet såsom *ISO27000* och *Myndigheten för Samhällsskydd och Beredskaps* (MSB:s) metodstöd för informationssäkerhet.

Baserat på den utförda granskningen har central uppföljning av arbetet med informationssäkerhet i Sundbybergs stads nämnder, förvaltningar och koncernbolag identifierats som stadens största förbättringsområde. För nämnderna och förvaltningarna inkluderar detta bland annat hur de sköter upphandlingar, hanterar avtal med externa leverantörer, utför informationsklassningar, upprättar driftsdokumentation för verksamhetsspecifika IT-system, kontinuitetsplanerar och hanterar personuppgifter. För stadens koncernbolag har formella rapporteringsvägar till Stadsledningskontoret och den centrala informationssäkerhetsfunktionen inte definierats. Detta innebär att Stadsledningskontoret saknar insyn i hur koncernbolagen arbetar med informationssäkerhet, både som helhet och för viktiga enskilda initiativ såsom informationsklassning, systemförvaltning och arbetet med dataskyddsförordningen.

Vidare rekommenderar EY att formaliseringen av en informationssäkerhetsspecifik organisationsstruktur med tillhörande roller, tydlig ansvarsfördelning, utökade resurser och definierade samverkansformer mellan Stadsledningskontoret och övriga verksamheter bör prioriteras i det fortsatta arbetet med informationssäkerhet. Informationssäkerhetsarbetet var vid tidpunkten för denna granskning begränsat till ett fåtal stadscentrala resurser. Utan stöd från en designerad organisationsstruktur för informationssäkerhet riskerar dessa resurser att få svårt att skapa tillfredsställande förutsättningar för att bedriva ett ändamålsenligt arbete med informationssäkerhet inom staden. Granskningen har även påvisat att brister finns i bland annat stadens genomförande av adekvata utbildningsinsatser inom informationssäkerhet och i hanteringen av åtkomster och programförändringar.

En delvis ändamålsenlig incidenthanteringsprocess anses ha definierats av Sundbybergs stad, då processen utgörs av detaljerade anvisningar för hur stadens Service Desk (hjälpcenter) skall hantera vanliga incidenter. Dock saknas tydlig beskrivning av tillämpbart processflöde med korrelerande roller, ansvar och rapporteringskrav för kritiska incidenter som riskerar att orsaka mer allvarliga förluster av informationstillgångar.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Innehållsförteckning

Bildförteckning

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

1. Inledning

1.1. Bakgrund

Sundbybergs stad, dess nämnder, förvaltningar (nämnder och förvaltningar hänvisas hädanefter till samlingsbegreppet ”stadens verksamheter”) och koncernbolag hanterar stora mängder digital information. Hantering av digital information medför möjligheter i form av effektivare daglig verksamhet, uppföljning och utökad service till medborgarna, samtidigt som risker uppstår när informationen inte hanteras ändamålsenligt. För att uppnå god informationssäkerhet krävs att styrningen och arbetet bedrivs på ett sådant sätt att informationen hålls konfidentiell och är riktig, tillgänglig och spårbar.

Med bakgrund i ovan genomförde EY på uppdrag av Sundbybergs stads förtroendevalda revisorer under januari till mars 2019 en granskning av stadens arbete med informationssäkerhet.

1.2. Syfte och revisionsfrågor

Syftet med granskningen var att ge en övergripande nulägesanalys om huruvida Kommunstyrelsen för Sundbybergs stad har tillsett att arbetet kring informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt. Granskningen syftar att ge svar på tre revisionsfrågor:

- Hur ändamålsenlig är styrningen av arbetet med informationssäkerhet gentemot LIS-ramverket (i enlighet med MSB:s metodstöd och ISO27000) för de behov stadens verksamhet har?
- Hur ändamålsenligt är arbetet med att följa upp att beslut och styrningsdokument relaterat till informationssäkerhet efterlevs?
- Har Sundbybergs stad en ändamålsenlig incidenthanteringsprocess?

1.3. Avgränsningar

De iakttagelser som presenteras i denna rapport baseras enbart på den information som inhämtats under intervjuer och genom inspektion av erhållen dokumentation, såsom styrningsdokument, riktlinjer och planer. Sundbybergs stads nämnder, förvaltningar och koncernbolag har inte granskats mer än utifrån den information som har erhållits från Stadsledningskontorets centrala informationssäkerhetsresurser. Ingen teknisk granskning eller analys har genomförts. Vidare har inga stickprov på efterlevnad tagits.

1.4. Metod och genomförande

Granskningens syfte har adresserats genom intervjuer med identifierade nyckelpersoner i stadens informationssäkerhetsarbete samt genomgång av relevant styrdokumentation (se *Sektion 8*. *Bilaga 2: Källförteckning*). Granskningen är utförd mot god praxis inom informations- och IT-säkerhetsområdet och bygger på EY:s metodstöd *Cybersecurity Program Assessment* (CPA), med fokus på organisation och styrningsrelaterade områden, och *Granskningsprogram Cyber och Informationssäkerhet* (GCI), med fokus på offentlig verksamhet. Både CPA och GCI baseras på erkända ramverk inom informationssäkerhet såsom *ISO27000* och *Myndigheten för Samhällsskydd och Beredskaps* (MSB:s) metodstöd för informationssäkerhet.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

De intervjuade har beretts tillfälle att faktagranska rapporten och lämna synpunkter på dess innehåll. Granskningen har även kvalitetssäkrats av EY:s verksamhetsrevisorer och presenterats för Sundbybergs stads förtroendevalda revisorer.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2. Strategi, styrning och organisation

2.1. Styrdokument

Arbetet med informationssäkerhet i Sundbybergs stad har under de senaste två åren underordnats den informationssäkerhetspolicy som fastslogs och beslutades av Sundbybergs stads kommunfullmäktige den 30 oktober 2017. Dokumentet beskriver på övergripande nivå syftet med och definitioner för stadens informationssäkerhetsarbete. Policyn innehåller även vissa riktlinjer avseende roller och ansvarsfördelning (se mer detaljerad redogörelse i sektion *2.2 Ansvarsfördelning och organisation*). Kommunikation av informationssäkerhetspolicyn till stadens medarbetare har inte aktivt genomförts men dokumentet finns tillgängligt på intranätet för användarna att ta del av. Ett arbete med att uppdatera och utöka informationssäkerhetspolicyn har initierats under början av 2019.

Stadens informationssäkerhetspolicy är i dagsläget ett självständigt dokument och har inte kompletterats av en tillhörande strategi eller plan för Sundbybergs stads informationssäkerhetsarbete. Dock har en projektplan tagits fram av Sundbybergs stads säkerhetsavdelning för ett projekt som löper under våren 2019 med målet att konkretisera innehållet i stadens informationssäkerhetspolicy. Detta skall göras genom att definiera ett antal gemensamma riktlinjer för informationssäkerhetsarbetet i hela Sundbybergs stads kommunkoncern (se sektion *3.1 Användarinstruktioner*).

2.2. Ansvarsfördelning och organisation

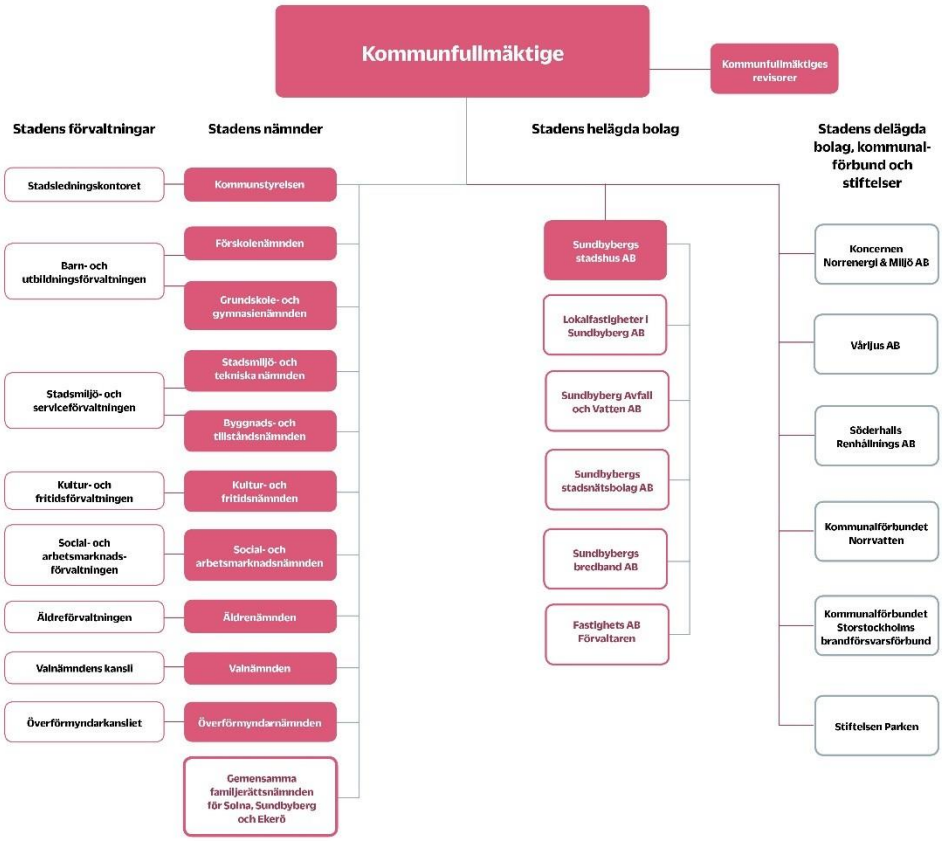


Bild 1: Organisationskarta - Sundbybergs stad [1]

[1] https://www.sundbyberg.se/kommun-politik/kommunens-organisation.html, 2019-02-14

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Säkerhetsavdelningen driver stadens centrala informationssäkerhetsarbete

Sundbybergs stads informationssäkerhetspolicy beskriver att Kommunstyrelsen skall leda, samordna och granska hur stadens informationssäkerhetsarbete fortskrider, men det är de enskilda nämnderna, förvaltningarna och koncernbolagen som bär ansvaret för att informationssäkerheten upprätthålls. Kommunstyrelsen har ingen specifik budget åsidosatt för informationssäkerhetsrelaterade behov.

Länken mellan Kommunstyrelsen och stadens verksamheter och koncernbolag i informationssäkerhetsarbetet utgörs av säkerhetsavdelningen på stadens Stadsledningskontor. Inom säkerhetsavdelningen har en informationssäkerhetsfunktion definierats, innefattandes stadens säkerhetschef och informationssäkerhetssamordnare. Dessa båda innehar det operationella ansvaret för att driva informationssäkerhetsarbetet och utforma de styrande riktlinjer som arbetet skall förhållas till. Rollen som dataskyddsombud räknas även till denna funktion, men innehas vid tillfället för denna granskning (mars 2019) av samma individ som är informationssäkerhetssamordnare.

Förvaltningscheferna bestämmer kring verksamhetsspecifika informationssäkerhetsresurser

Då Sundbybergs stads nämnder och förvaltningar är ansvariga för att upprätthålla säkerheten för sina egna informationstillgångar är det upp till respektive förvaltningschef att bestämma kring förvaltningsspecifika resurser i arbetet med informationssäkerhet. Stadsledningskontorets centrala informationssäkerhetsfunktion framförde under 2018 ett förslag på struktur för att underlätta det stadsövergripande informationssäkerhetsarbetet. Förslaget innefattade bland annat att verksamheterna skulle etablera ett antal informationssäkerhetsombud inom sina respektive organisationer. Dessa skulle rapportera till den centrala informationssäkerhetssamordnaren och på så sätt effektivisera stadsövergripande säkerhetsstandardisering, kunskapsspridning och efterlevnad av rutiner. Förslaget har hittills emellertid inte fått fäste i samtliga verksamheter, bland annat till följd av otillräcklig kommunikation från säkerhetsavdelningen angående fördelarna av den föreslagna strukturen i informationssäkerhetsarbetet. Detta har medfört att verksamheterna genom respektive förvaltningschef har fattat sina egna beslut i frågan. Utfallet har blivit att vissa nämnder och förvaltningar har etablerat informationssäkerhetsombud, dock utan definierade rutiner för säkerställande av central uppföljning och efterlevnad, och att andra nämnder och förvaltningar saknar informationssäkerhetsombud.

Koncernbolagen bedriver sina egna informationssäkerhetsarbeten

Sundbybergs stads koncernbolag har inte omfattats av förslaget att införa informationssäkerhetsombud och bedriver sina egna arbeten med informationssäkerhet. Koncernbolagen har huvudsakligen separata IT-miljöer men delar serverhall och till viss del klientnätverk med staden. Staden har ett och samma fysiska nätverk för alla verksamheter, men med logisk separation mellan olika delar av nätverket och med implementerade nätverksåtkomstkontroller (network access controls, NAC). Detta innebär att för att komma åt stadens interna system krävs en domänansluten kommundator både på det trådlösa och trådbundna nätverket. Koncernbolagen har tillsatt bolagsspecifika dataskyddsombud, men rutiner för att kontrollera att bolagens arbeten efterlever den koncernövergripande informationssäkerhetspolicyn saknas och samverkan mellan den stadscentrala informationssäkerhetsfunktionen och bolagen i arbetet med informationssäkerhet har framförts vara begränsad.

IT-enheten har flertalet roller definierade med inverkan på informationssäkerhetsarbetet

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

För IT-säkerhetsaspekten (se sektion *7. Bilaga 1: Definitioner*) av stadens och verksamheternas informationssäkerhetsarbete ansvarar Sundbybergs stads IT-enhet, som är del av Enheten för Digitalisering och Service under Stadsmiljö- och serviceförvaltningen. Under genomförda intervjuer har det framkommit att ansvarsfördelningen mellan informationssäkerhetsfunktionen och IT-enheten ur ett informationssäkerhetsperspektiv är otydligt definierad. Formella kravställningar mellan funktionerna har inte utförts och det saknas tydligt ägarskap för vilka som äger vad inom ramen för informationssäkerhet. Tidigare fanns forum för samverkan mellan informationssäkerhetsfunktionen och IT-enheten men dessa efterlevs inte idag. Detta har vid tillfällen även haft negativ inverkan på driften av Sundbybergs stads informationssystem, som till följd av avsaknaden av koordinering har medfört att IT-enheten har utfört förändringar i säkerhetslösningar som inte har varit kända för informationssäkerhetsfunktionen förrän efter införande.

IT-enheten definierade år 2010 en systemförvaltningsmodell som vid tidpunkten för denna granskning är under revidering. Dock är 2010 års version tills vidare fortsatt giltig på stadscentral nivå och mot verksamheterna, men mot koncernbolagen ställs inga krav på användning av modellen. Modellen beskriver de roller som ingår i förvaltningen av Sundbybergs stads verksamhetssystem. Av dessa har systemägarna, vilket ofta är respektive verksamhets förvaltningschef, det övergripande ansvaret för systemen och dess utveckling på strategisk nivå. Systemägaren är också ägare av all information som systemet behandlar. Under systemägaren finns systemförvaltare, som ansvarar för systemets dagliga funktionalitet. Systemförvaltarens arbete stöds av systemansvariga och driftsansvariga resurser, som ansvarar för interaktionen med andra system och den tekniska driften. IT-enhetsspecifika forum för samverkan och erfarenhetsutbyte, bland annat de kvartalsvisa systemförvaltarträffarna mellan verksamhetssystemens systemförvaltare och vid behov systemansvariga, har definierats som del av förvaltningsmodellen. Informationssäkerhetsfunktionens resurser är inte listade som obligatoriska deltagare i forumen men har bjudits in vid flertalet tillfällen då agendan har berört informationssäkerhet.

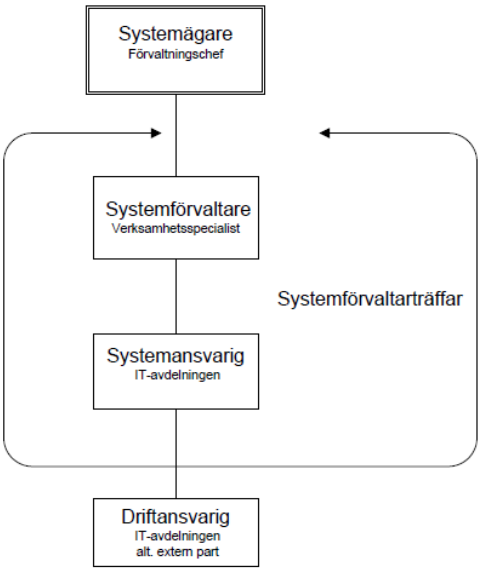


Bild 2: Roller i IT-enhetens systemförvaltningsmodell [2]

[2] Sundbybergs stads systemförvaltarorganisation, 2010

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

2.3. Externa leverantörer och hantering av leverantörsavtal

Alla upphandlingar av stadsövergripande informationssystem i Sundbybergs stad går via en central upphandlingsenhet. . Krav på hur externa leverantörer skall handha stadens information sätts per system och baseras framförallt på utfallet av genomförd klassning av systemets information i SKL:s KLASSA-verktyg (se sektion *3.4 Informationsklassning*). För system vars information erhåller kritiska skyddsvärdsnivåer skall således kraven gentemot externa leverantörer vara hårdare än för system som behandlar mindre skyddsvärd information.

Som stöd till upphandlingsenheten har stadens säkerhetschef tagit fram en upphandlingsinstruktion. Instruktionen skrevs främst för att säkerställa att informationsklassning genomförs för system som skall upphandlas och att avtal med externa leverantörer definieras baserat på dess utfall enligt ovan. Instruktionen stipulerar att informationssäkerhetsfunktionen skall konsulteras av upphandlingsenheten för centralt och standardiserat säkerställande av kvalitet, säkerhetskrav och förvaltning för alla system som kan inverka på stadens säkerhetsarbete. Instruktionen är dock implementerad med begränsad efterlevnad och utan uppföljning från informationssäkerhetsfunktionen.

För befintliga externa leverantörer och redan upphandlade informationssystem har inga särskilda centrala riktlinjer för uppföljning av informationssäkerhet definierats. Regelbundna möten bedrivs med de externa leverantörerna, men dessa är oftast av driftskaraktär och informationssäkerhetsrelaterade ämnen är sällan del av agendan.

För upphandling av verksamhetsspecifika system och hantering av dess leverantörsavtal saknar Stadsledningskontoret och den centrala informationssäkerhetsfunktionen insyn. Varje verksamhet bedriver således sina egna upphandlingar och hanterar sina egna leverantörer, utan stadsövergripande och standardiserade rutiner.

2.4. Personal och utbildning

De stadsövergripande resurser som huvudsakligen arbetar med Sundbybergs stads informationssäkerhet är Stadsledningskontorets säkerhetschef och informationssäkerhetssamordnare. I genomförda intervjuer har det framförts att det finns ett behov av att utöka antalet resurser med kompetens inom informationssäkerhet på central nivå, och som del av detta är ytterligare en informationssäkerhetssamordnare tilltänkt att anställas under våren 2019.

Liknande behov av utökad informationssäkerhetskompetens har i intervjuer efterlysts i verksamheternas organisationer. Inte alla nämnder och förvaltningar har definierat informationssäkerhetsombud i enlighet med informationssäkerhetsfunktionens strukturförslag (se sektion *2.2 Ansvarsfördelning och organisation*), och för de verksamheter som har tillsatt informationssäkerhetsombud har inte säkerhetsavdelningen sett till att samverkansrutiner med Stadsledningskontoret ännu har upprättats. För IT-enhetens roller i systemförvaltningsmodellen uppges systemägare, systemförvaltare, systemansvariga och vid behov även driftsansvariga ha tillsatts för de system som genom utförd informationsklassning har bedömts som kritiska (se sektion *3.4 Informationsklassning*). För övriga verksamhetssystem och korrelerande roller fattas emellertid systematik för att göra en korrekt helhetsbedömning av resurstillgången.

Vidare har behovet av ökad medvetenhet kring informationssäkerhet lyfts under intervjuer med nyckelpersoner. Den generella kompetensen och förståelsen av betydelsen av säker

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

informationshantering inom både Stadsledningskontoret och i verksamheterna har framförts som låg, vilket är ett av säkerhetsavdelningens uttalade områden att förbättra.

Ett fåtal utbildningsinsatser har genomförts i staden inom ramen för informationssäkerhet. Dessa har dock varit begränsade till utbildningar för utförande av informationsklassningar och hantering av personuppgifter, och har endast genomförts för de användare inom staden vars arbete direkt påverkas av informationsklassningsrutinerna respektive innefattar personuppgiftshantering. Ingen övergripande utbildning för stadens anställda inom informationssäkerhet eller förhållningssätt till 2018 års införande av dataskyddsförordningen har genomförts, och en plan med prioriterade utbildningsinitiativ har ej definierats. Ett systemstöd för utbildning har inhandlats men har ännu inte tagits i bruk.

Koncernbolagen är tillsätter sina egna informationssäkerhetsresurser och har inte omfattats av genomförda utbildningsinitiativ.

2.5. Styrning av åtkomsthantering

Sundbybergs stad har inte definierat en övergripande process för åtkomsthantering till stadens IT-system. Tilldelning av åtkomst initieras istället genom ett delvis automatiserat flöde, där en ny användares nätverkskonto skapas baserat på information i stadens löne- och administrationssystem. För åtkomst till IT-systemen krävs beställning till IT-enhetens Service Desk, som arbetar mot alla nämnder och förvaltningar samt ett av Sundbybergs stads koncernbolag (övriga koncernbolag har ett eget Service Desk). Ansvarig chef för användaren som söker åtkomst är ansvarig för att skicka in beställningen. Det har dock framhållits att chefer generellt har låg medvetenhet angående vilka roller som bör ha vilka behörigheter, och detta är ofta någonting som användare får upptäcka själva och göra sina chefer medvetna om. Det händer även att användare beställer och erhåller åtkomst från systemförvaltare eller Service Desk utan inblandning och formellt godkännande av ansvarig chef.

Borttagning av åtkomst initieras också via löne- och administrationssystemet, som inaktiverar nätverkskontot på det datum användaren slutar. Ansvarig chef skall rapportera användare som slutar till respektive systemförvaltare för att manuellt skapade konton även skall inaktiveras.

För priviligierade behörigheter på infrastrukturell nivå finns det riktlinjer på Sundbybergs stads intranät som beskriver att domänadministratörer enbart skall finnas inom IT-enheten. Vanliga anställda, inklusive användare inom IT-enheten, kan få lokala administratörsrättigheter på specifika datorer om särskilda behov finns. Detta kräver emellertid godkännande av IT-chef, driftschef eller infrastrukturansvarig inom IT-enheten. Priviligierade behörigheter granskas på kontinuerlig basis minst årsvis, men protokollförs inte och är personberoende av IT-enhetens infrastrukturansvarig som har varit drivande i genomgångarna. Stadsövergripande krav på genomgångar av vanliga användare i enskilda IT-system har inte definierats. Systemspecifika krav kan genereras ifall system har genomgått informationsklassning (baserat på SKL:s KLASSA verktyg, se sektion *3.4 Informationsklassning*) med utfallsrekommendationen att systemets användare bör granskas med en viss frekvens. Detta följs dock inte upp närmare av Stadsledningskontoret och det är således upp till enskilda systemägare och systemförvaltare att definiera sina egna rutiner för periodiska genomgångar. Inte heller rutiner för säkerställande av ändamålsenlig ansvarsfördelning i användares åtkomstuppsättningar har definierats.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Sundbybergs stad har ingen övergripande lösenordspolicy men har tagit fram vissa riktlinjer för nätverkskonton. Bland annat skall lösenord bytas var 90:e dag och vara minst sex tecken långt. En del applikationer är kopplade till nätverket med enkel inloggning (single sign-on) och för dessa gäller samma riktlinjer. Möjlighet finns dock för stadens användare att använda tvåfaktorsautentisering i form av inloggning via personligt ID-kort utöver inloggning med lösenord, vilket många användare har valt att göra. Inget register har upprättats för tydlig översikt av vilka och hur många system och applikationer som är kopplade via enkel inloggning mot nätverket. För de system som inte omfattas av enkel inloggning bestäms lösenordskomplexitet av respektive systemförvaltare.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

3. Operationella rutiner

3.1. Användarinstruktioner

Sundbybergs stad har definierat en övergripande anvisning för användning av Sundbybergs stads IT-miljö som gäller för alla användare i stadens verksamheter. Anvisningen beskriver allmänna förhållningssätt för användare som nyttjar IT-miljön i staden, inklusive riktlinjer för förvaring och säkerhet. Anvisningen har tagits fram av stadens IT-enhet i samverkan med HR-avdelningen och skall signeras i samband med att nya användare, både anställda och elever, kvitterar ut IT-verktyg från staden. Anvisningen är emellertid inte tillgänglig på stadens intranät och ingen uppföljning av efterlevnad eller signering görs av informationssäkerhetsfunktionen.

Vidare har en instruktion för hantering av sociala medier definierats. Denna finns tillgänglig på intranätet men har inte kommunicerats aktivt till användarna. Ett arbete pågår även med att konkretisera stadens informationssäkerhetspolicy i fyra riktlinjer. Riktlinjerna skall beröra stadens styrning av informationssäkerhetsarbetet, informationssäkerhet för stadens användare, roller och ansvar i verksamheternas informationssäkerhetsarbeten samt informationssäkerhet för IT-enheten, och syftar till att standardisera uppfattningen och förhållningssättet till informationssäkerhet i kommunkoncernen.

3.2. Incidenthantering

Sundbybergs stads IT-enhet har i sitt ärendehanteringssystem för incidenter definierat en incidenthanteringsprocess. Processen är huvudsakligen utformad från ett driftsstörningsperspektiv, men omfattar även informationssäkerhetsrelaterade incidenter. Åtkomst till ärendehanteringssystemet har enbart IT-tekniker, resurser som arbetar med personuppgiftshantering samt enskilda medarbetare inom stadens digitaliserings- och kommunikationsenheter.

För driftsmässiga störningar, eller om stadens anställda misstänker att intrång eller andra säkerhetshot är i skeende, skall detta rapporteras till stadens Service Desk. Service Desk registrerar incidenten i ärendehanteringssystemet och tilldelar den en prioriteringsnivå baserat på hur många som uppskattas vara påverkade av incidenten samt dess angelägenhet. En särskild instruktion för hur incidenter rörande personuppgifter skall registreras i ärendehanteringssystemet har definierats. Incidenten hanteras sedan av tillgängliga och lämpliga driftstekniker baserat på incidentens karaktär och prioritering.

Efter åtgärdad incident rapporteras lösningsbeskrivningen till användaren som rapporterade incidenten. För incidenter av hög prioriteringsgrad skall en detaljerad incidentrapport förberedas. Inga dokumenterade och bindande krav finns på att rapportera incidenter till säkerhetschefen, IT-chefen eller Kommunstyrelsen, även om vissa incidenter rapporteras informellt. Större incidenter rapporteras även till MSB och CERT (MSB:s nationella verksamhet för att hantera och förebygga IT-incidenter, Computer Emergency Response Team).

Då ansvarsfördelningen och samverkan mellan informationssäkerhetsfunktionen och IT-enheten ur ett informationssäkerhetsperspektiv inte tydligt har definierats, saknar för tillfället informationssäkerhetsfunktionen insyn i hur många incidenter av informationssäkerhetskaraktär som staden har registrerat. Dessutom har det i genomförda intervjuer framförts att en avsaknad av samstämmighet råder mellan informationssäkerhetsfunktionen och IT-enheten i vad som utgör en

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

informationssäkerhetsincident, vilket har gjort det svårare att få en överblick av antalet incidenter av informationssäkerhetskaraktär.

För att minska risken för att incidenter skall gå oupptäckta granskas även brandväggs- och nätverksaktivitet genom stickprov av brandväggs- och nätverksloggar, men dessa saknar systematik och formaliserad regelbundenhet.

3.3. Programförändringsrutiner

En dokumenterad process för hantering av programförändringar saknas i Sundbybergs stad och mycket sköts istället under informella former. Bland annat har det sagts att beställningar av programförändringar skall dokumenteras i stadens ärendehanteringssystem, men detta efterlevs generellt sett inte. Detta leder i sin tur till att spårbarheten i programförändringsprocessen som helhet är mycket begränsad.

Ett arbete har initierats med att ta fram blanketter och processflöden för hur programförändringar skall gå till, inklusive upprättande av ett förändringsråd som skall agera beslutsfattare för förändringar som påverkar Sundbybergs stads IT-miljö. Idag finns det heller inga rutiner för att säkerställa ändamålsenlig ansvarsfördelning i arbetet med programförändringar, vilket teoretiskt innebär att samma individ obemärkt skulle kunna utveckla och implementera sina egna programförändringar utan godkännande och vetskap av övriga organisationen. I den utsträckning man använder externa leverantörer av system följs drift- och programutvecklingsfrågor upp i operationella möten med leverantörerna, dock generellt utan vidare inblick i hur leverantörerna garanterar säker informationshantering utifrån de krav som har definierats i leverantörsavtalen.

3.4. Informationsklassning

Sundbybergs stad nyttjar SKL:s KLASSA-verktyg i arbetet att identifiera vilka av stadens informationssystem som innehåller skyddsvärd information. För att standardisera och säkra utförande av klassningsrutinerna definierades under 2016 och 2017 en instruktion för hur Sundbybergs stad skall utföra informationsklassning genom KLASSA-verktyget. Instruktionen beskriver bland annat syftet med klassningsrutinerna, hur åtkomst till KLASSA skall beställas och hur klassningen skall dokumenteras. En mall har även tagits fram som del av instruktionen för att styra att dokumentation av klassningen är av godtagbar kvalitet och skickas till säkerhetsavdelningen efter utförd klassning för lagring.

Enligt stadens systemförvaltningsmodell ligger ansvaret för att utföra informationsklassningarna hos respektive systems systemägare. Dock har det i genomförda intervjuer lyfts att inte alla Sundbybergs stads IT-system har tilldelade systemägare, vilket har medfört att staden genomfört informationsklassningar med det omvända syftet att identifiera vilka system som är mest kritiska och således i behov av systemägare. Utfallet har varit att 55 av stadens ungefär 150 system hittills har registrerats i KLASSA och att 27 av dessa har informationsklassats som känsliga och skyddsvärda. Dessa 27 system har tilldelats systemägare och systemförvaltare i enlighet med IT-enhetens systemförvaltningsmodell (se sektion *2.2 Ansvarsfördelning och organisation*). För de övriga systemen, både för de som är registrerade i KLASSA och för de som ännu inte har omfattats av klassningsrutinerna, saknar informationssäkerhetsfunktionen inblick. Detsamma gäller för koncernbolagens informationsklassningsarbeten.

En övergripande registerförteckning, innefattandes stadens verksamheter, över antalet IT-system är under uppdatering för att få en bättre överblick av omfattningen av stadens IT-

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

miljö. Även för enskilda informationstillgångar, såsom fysiska tillgångar, har ett arbete med registerförteckning påbörjats.

3.5. Driftdokumentation och kontinuitetsplanering

Sundbybergs stads IT-enhet har viss driftsdokumentation tillgänglig på en IT-wiki på stadens intranät. Wikin innehåller information som är kritisk för IT-enheten för att kunna upprätthålla systemleverans och omfattar bland annat information kring operativsystem, integrationer, månadsvisa patchningar och servrar. För nya systemstöd finns instruktioner för hur denna dokumentation skall se ut, vilket medför en viss uppsättning standarddokumentation för nya system. Denna kan dock släpa efter allt eftersom systemen uppdateras. För IT-system som inhandlades innan instruktionen togs i bruk under 2018 har driftsdokumentation samlats in från flertalet olika dokumentationskällor för central uppsamling på wikin. Inga centrala krav har emellertid ställts på att systemförvaltarna för dessa system aktivt skall upprätta och dela med sig av driftsdokumentation till IT-enheten.

Den systemförvaltningsmodell som antogs 2010 inom IT-enheten ställer krav på att varje system skall ha ett antal roller definierade (se sektion *2.2 Ansvarsfördelning och organisation*). Dock har inte alla dessa roller tillsatts för alla stadens IT-system och flertalet system upplevs stå utan övergripligt ansvarig ägare. Systemförvaltningsmodellen stipulerar också att ett systemförvaltningsavtal skall upprättas mellan respektive systems systemägare och IT-enheten. Syftet med avtalet är att säkerställa att den initiala kravställningen på systemet blir rätt och att ansvar tydligt definieras. Dock har det funnits problem med att implementera avtalet med verksamheterna.

År 2012 genomfördes i Sundbybergs stad ett stadsövergripande kontinuitetsplaneringsinitiativ. Arbetet drevs av det som idag är IT-enheten i samråd med systemförvaltare för verksamhetskritiska system. Liknande gemensamma insatser har sedan dess inte gjorts, och fokus har istället ändrats till att från central nivå framförallt förespråka att informationsklassningar och risk- och konsekvensanalyser genomförs för varje system. Tanken har sedan varit att systemspecifik kontinuitetsplanering skall genomföras baserat på utfallet av informationsklassningarna. Som stöd till verksamheterna har en kontinuitetsplaneringsmall definierats av informationssäkerhetsfunktionen. Mallen har anammats i vissa verksamheter beroende på systemägare och systemförvaltare, vilket har resulterat i att vissa system har förhållandevis väldokumenterade kontinuitetsplaner medan andra helt saknar planer. För de 27 system som i genomförd informationsklassning har bedömts som kritiska skall kontinuitetsplaner finnas, dock har detta inte följts upp för säkerställande och relevans från central nivå.

På stadsövergripande nivå saknar Sundbybergs stad definierade kontinuitetsplaner, men har utarbetat en krisberedskapsplan som står för beredning hos Kommunfullmäktige. Beslut om denna väntas tas under våren 2019. Vissa åtgärder från ett kontinuitetsplaneringsperspektiv har vidtagits, exempelvis finns det dubbla datahallar i syfte att erbjuda IT-driftsredundans.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

4. Dataskydd och personuppgiftshantering

4.1. Arbete med dataskyddsförordningen

Sundbybergs stad har efter dataskyddsförordningens (GDPR) införande i maj 2018 bedrivit ett kontinuerligt arbete för att nå efterlevnad av de nya lagkraven. Arbetet har bland annat resulterat i att rollen som dataskyddsombud (DSO) har tillsatts. Dataskyddsombudet arbetar för stadens nämnder och förvaltningar, då koncernbolagen har varit ansvariga för att tillsätta sina egna dataskyddsombud och tillräckliga resurser för att möta kraven på dataskydd

Dataskyddsombudets kontaktuppgifter finns tillgängliga i det avsnitt på stadens externa hemsida som har definierats för att beskriva hur personuppgifter hanteras av staden. Internt har en frågebank tagits fram för att vägleda och ge råd kring hur man som anställd skall hantera personuppgifter på ett sätt som efterlever dataskyddsförordningens direktiv. Det finns däremot ingen kontroll och uppföljning på att denna används eller hur personuppgifter faktiskt hanteras inom staden. Det har inte heller från Stadsledningskontoret kommunicerats några styrande anvisningar för hur nämnder och förvaltningar skall anpassa sina lokala föreskrifter för att uppfylla kraven i dataskyddsförordningen.

Sundbybergs stad har upprättat en registerförteckning över hur personuppgifter behandlas av staden. Förteckningen är emellertid inte fullständig och har inte uppdaterats kontinuerligt sedan dataskyddsförordningens införande. De informationsklassningar som har genomförts för utvalda system kan till viss del ses som en kompenserande åtgärd, men det är inte klarlagt om alla system som innehåller personuppgifter faktiskt har informationsklassats. Dataskyddsförordningen stipulerar även att samtliga personuppgiftsbehandlingar skall ingå i registerförteckningen. Eftersom informationsklassningen endast berör IT-system finns därför inga rutiner för övriga personuppgifter som kan finnas i ostrukturerad form, exempelvis i e-post eller fysiska mappar.

För att hantera begäranden i enlighet med registrerades rättigheter har Sundbybergs stad definierat en fysisk blankett som måste lämnas in av den registrerade för hand till receptionen i Sundbybergs stadshus. Krav ställs på att den registrerade måste identifiera sig i samband med inlämnandet av blanketten. Blanketten levereras sedan till dataskyddsombudet som gör en bedömning av respektive förfrågan. Vid rätt till information eller annan rättighetsutövning begär dataskyddsombudet in relevant information från den berörda nämnden eller förvaltningen för förmedling till den registrerade.

Inom staden har det inte genomförts något specifikt arbete med att granska och anpassa existerande IT-system för att minimera exponering och insamling av personuppgifter till det som enbart är absolut nödvändigt. Detta är till viss del inbyggt i dagsläget med hänsyn till åtkomsthantering, men inga specifika insatser för att bygga in dataskydd i grunden har gjorts.

Ännu har inga rutiner formaliserats för hur staden skall hantera förfrågningar från Datainspektionen gällande arbetet med personuppgifter. I den mån risk- och konsekvensanalyser genomförs för stadens hantering av personuppgifter är det inom ramen för de informationsklassningar som görs i enlighet med SKL:s KLASSA-verktyg. Detta innebär att ostrukturerad data som inte hanteras i IT-system kan undgå att omfattas av risk- och konsekvensanalyserna.

För lagring, gallring och rensning av personuppgifter har krav definierats på att alla avdelningar och enheter skall ha en dokumenthanteringsplan. Dessa skall bland annat

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

reglera lagringstider och gallring av data, men deras efterlevnad har inte aktivt följts upp av Stadsledningskontoret eller Kommunstyrelsen.

4.2. Personuppgifter i molntjänster

Ett antal molnbaserade tjänster hanterar personuppgifter för Sundbybergs stad. Sedan dataskyddsförordningens införande ställer staden krav på att personuppgiftsbiträdesavtal (PUB-avtal) med anvisningar för säker personuppgiftshantering och sekretess skall upprättas för alla upphandlade externa utförare och leverantörer av molntjänster. För existerande avtal med molntjänstleverantörer har ansvaret för att tillse att PUB-avtal skrivs informellt delats mellan stadens systemägare och leverantörernas personuppgiftsbiträden, men staden har inte centralt följt upp på att detta genomförs.

Sundbybergs stads anvisning för användning av stadens IT-miljö beskriver att det i dagsläget inte är tillåtet att koppla stadens enheter till eller spara arbetsmaterial i molntjänster om dessa inte är godkända av staden. I övrigt har inga instruktioner för hur användare av molntjänster skall förhålla sig till och hantera dessa.

4.3. Personuppgiftsincidenter

Personuppgiftsincidenter skall precis som övriga incidenter registreras via Sundbybergs stads Service Desk i ärendehanteringssystemet. Staden har definierat en särskild instruktion för hur incidenter rörande personuppgifter skall registreras och hanteras, och en separat rapporteringsväg via stadens intranät har införts.

Under 2018 registrerades sammanlagt 16 incidenter av personuppgiftskaraktär, främst rörande förlorad IT-utrustning såsom mobiltelefoner och persondatorer. 5 av de 16 personuppgiftsincidenterna rapporterades via dataskyddsombudet vidare till Datainspektionen.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

5. Iakttagelser och rekommendationer

Nedan följer en beskrivning av de iakttagelser och risker som har identifierats under granskningens utförande, tillsammans med rekommendationer och förslag på åtgärder riktat till Sundbybergs stads Kommunstyrelse:

#	Iakttagelse	Risk	Rekommendation
5.1	**Avsaknad av uppföljning på arbetet med informationssäkerhet i stadens nämnder och förvaltningar** Kommunstyrelsen har inte tillsett att det finns formaliserade kontroller och rutiner för Stadsledningskontoret att följa upp på arbetet med informationssäkerhet i Sundbybergs stads nämnder och förvaltningar. Detta inkluderar bland annat hur verksamheterna sköter upphandlingar, hanterar avtal med externa leverantörer, utför informationsklassningar, upprättar driftsdokumentation för verksamhetsspecifika IT-system, kontinuitetsplanerar och hanterar personuppgifter.	Begränsad uppföljning av verksamheternas informationssäkerhetsarbeten medför risk för att nämndernas och förvaltningarnas dagliga informationshantering avviker från sättet som Kommunstyrelsen tror att arbetet bedrivs på. Detta kan leda till bristande kontroll i form av ojämn mognadsnivå mellan verksamheterna och att riktighet, spårbarhet, konfidentialitet och tillgänglighet för informationen som hanteras ej säkerställs.	EY rekommenderar att Kommunstyrelsen tillser att adekvata kontroller och rutiner för uppföljning och efterlevnad mellan Stadsledningskontoret och verksamheterna definieras, samt att designerade informationssäkerhetsroller tas fram och tillsätts i verksamheterna för ökad samverkan med den centrala informationssäkerhetsfunktionen.
5.2	**Bristfällig insyn i koncernbolagens informationssäkerhetsarbeten** Kommunstyrelsen har inte tillsett att godtagbar uppsikt, i enlighet med Kommunallagen 6 kap. 1 §, i koncernbolagens informationssäkerhetsarbeten kan säkerställas då formella rapporteringskrav till Stadsledningskontoret ej har fastställts. Stadsledningskontoret följer inte upp på hur koncernbolagen arbetar med informationssäkerhet, varken som helhet eller för viktiga enskilda initiativ såsom informationsklassning, systemförvaltning och dataskyddsförordningsarbete. Insikt saknas även i hur koncernbolagen hanterar information som delas över det gemensamma nätverk som staden och koncernbolagen använder.	Avsaknad av kontroll och insikt i koncernbolagens informationssäkerhetsarbete medför risk för att eventuella brister som står under Kommunstyrelsens ansvar inte upptäcks och att mognadsnivån i informationssäkerhetsarbetet mellan staden och koncernbolag skiljer sig. Detta kan exempelvis leda till att konfidentiell och känslig information läcks, att information är tillgänglig för individer som inte bör ha åtkomst, att information förvrängs eller att spårbarhet inte är möjlig.	EY rekommenderar att Kommunstyrelsen tillser att koncernbolagens arbete med informationssäkerhet aktivt följs upp och ökar kraven på återrapportering till Stadsledningskontoret, alternativt även inkorporerar bolagen i den övergripande styrmodellen för informationssäkerhet.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

#	Iakttagelse	Risk	Rekommendation
5.3	**Avsaknad av övergripande organisationsstruktur för informationssäkerhet** Kommunstyrelsen har inte tillsett att det finns en övergripande struktur för hur Sundbybergs stad skall organisera sig i arbetet med informationssäkerhet, inklusive beskrivningar av roller, relaterade ansvarsområden och kompetensnivåer som är nödvändiga att finnas på Stadsledningskontoret och i verksamheterna för att driva arbetet med informationssäkerhet.	Avsaknad av övergripande organisationsstruktur för stadens informationssäkerhetsarbete medför risk för att staden besitter otillräckliga resurser och bristfällig kompetens för att driva informationssäkerhetsarbetet på ett sätt som säkerställer riktighet, spårbarhet, konfidentialitet och tillgänglighet för informationen som staden hanterar.	EY rekommenderar att Kommunstyrelsen tillser att en informationssäkerhetsspecifik organisationsstruktur definieras och beslutas.
5.4	**Otydlig ansvarsfördelning mellan säkerhetsavdelningen och IT-enheten i arbetet med informationssäkerhet** Kommunstyrelsen har inte tillsett att ansvarsfördelningen mellan säkerhetsavdelningens informationssäkerhetsfunktion och IT-enheten tydligt har definierats i arbetet med informationssäkerhet. Formella kravställningar mellan funktionerna har inte utförts och det saknas tydligt ägarskap för vem som skall tillse att vad utförs inom ramen för informationssäkerhet. Forumen för samverkan mellan informationssäkerhetsfunktionen och IT-enheten efterlevs inte.	Otydlig ansvarsfördelning i arbetet med informationssäkerhet medför risk för att nödvändiga initiativ för att säkerställa riktighet, spårbarhet, konfidentialitet och tillgänglighet för informationen som staden hanterar ej genomförs.	EY rekommenderar att Kommunstyrelsen tillser att roller och ansvar mellan Stadsledningskontorets informationssäkerhetsfunktion och IT-enhet tydliggörs, samt att regelbundna forum för samverkan kring informationssäkerhetsrelaterade utmaningar och uppföljning av planerade initiativ inrättas.
5.5	**Informationssäkerhetsarbetet är begränsat till ett fåtal resurser** För Sundbybergs stads informationssäkerhetsarbete är de centrala nyckelrollerna som säkerhetschef, informationssäkerhetssamordnare och dataskyddsombud begränsade till två individer. Tillgängliga och definierade stödresurser på Stadsledningskontoret och i verksamheterna är begränsade. Det saknas även uppföljning av hur många och vilka av stadens IT-system som står utan tillsatta systemägare och systemförvaltare i enlighet med systemförvaltningsmodellen.	Att informationssäkerhetsarbetet är begränsat till ett fåtal resurser medför risk för att arbetet som helhet blir beroende av nyckelindivider, som vid händelse av frånvaro eller avslutad anställning leder till oförmåga att driva informationssäkerhetsarbetet på ett sätt som säkerställer riktighet, spårbarhet, konfidentialitet och tillgänglighet för informationen som staden hanterar.	EY rekommenderar att Kommunstyrelsen tillser att nivån av medvetande och involvering i stadens informationssäkerhetsarbete sprids inom både Stadsledningskontoret och i verksamheterna, exempelvis genom formaliserade utbildningsinitiativ, samt att fler designerade informationssäkerhetsroller tas fram och tillsätts centralt och i verksamheterna

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

#	Iakttagelse	Risk	Rekommendation
5.6	**Begränsade utbildningar och kompetenshöjande initiativ rörande informationssäkerhet** Kommunstyrelsen har inte tillsett att stadsövergripande, obligatoriska och regelbundet återkommande utbildningar inom informationssäkerhet genomförs för Sundbybergs stads användare. Ingen uppföljning av tidigare genomförda, enskilda utbildningsinsatser har gjorts och efterlevnad av den användaranvisning för nyttjande av stadens IT-miljö som signeras av nyanställda följs inte upp av informationssäkerhetsfunktionen.	Avsaknad av obligatoriska och regelbundet återkommande utbildningsinsatser rörande informationssäkerhet medför risk för att stadens användare besitter otillräcklig kunskap för att på daglig basis hantera stadens information på ett ändamålsenligt och säkert sätt.	EY rekommenderar att Kommunstyrelsen tillser att en utbildningsplan för informationssäkerhet formaliseras. Denna bör innefatta genomförande av obligatoriska och regelbundna utbildningar inom informationssäkerhet med uppföljning av deltagande. Kommunstyrelsen rekommenderas även tillse att kommunikation och signering av användaranvisningen för nyttjande av stadens IT-miljö säkerställs.
5.7	**Avsaknad av övergripande och formaliserad process för åtkomsthantering** Kommunstyrelsen har inte tillsett att en formaliserad process för att styra tilldelnings- och borttagningsförfarandet av behörigheter till Sundbybergs stads IT-system har definierats, inklusive kontroller för att säkerställa standardisering i beställningar och godkännande av åtkomster.	Avsaknad av en formaliserad åtkomsthanteringsprocess medför risk för att olämpliga användare, både interna och externa, har åtkomst att ta del av och modifiera information i system, servrar och databaser och riktighet, spårbarhet, konfidentialitet och tillgänglighet för informationen som hanteras därmed ej kan säkerställas.	EY rekommenderar att Kommunstyrelsen tillser att en stadsövergripande process för åtkomsthantering formaliseras, inklusive tydliga tilldelnings- och borttagningsförfaranden av behörigheter.
5.8	**Brist på anvisningar för periodiska genomgångar och ändamålsenlig ansvarsfördelning** Kommunstyrelsen har inte tillsett att stadsövergripande anvisningar för periodiska genomgångar av användare med åtkomst till Sundbybergs stads IT-system har definierats, och genomgångar utförs idag informellt och med begränsad utfallsdokumentation. Även funktionalitet och rutiner för att säkerställa ändamålsenlig ansvarsfördelning i användares åtkomstuppsättningar saknas.	Brist på säkerställande av periodiska genomgångar och ändamålsenlig ansvarsfördelning medför risk för att olämpliga användare, både interna och externa, har åtkomst till IT-system, servrar och databaser samt att användares åtkomstuppsättningar innehåller konflikterande behörighetsrättigheter. Detta kan i sin tur leda till att konfidentiell och känslig information läcks eller förvrängs.	EY rekommenderar att Kommunstyrelsen tillser att stadsövergripande kontroller utformas för standardisering av genomförande av periodiska genomgångar. Kommunstyrelsen rekommenderas också tillse att förteckningar eller matriser skapas kring vilka behörigheter som inte är lämpliga att kombinera inom och mellan kritiska IT-system.
5.9	**Begränsade definierade rutiner, roller och ansvar för hantering av kritiska incidenter** Kommunstyrelsen har inte tillsett att incidenthanteringsprocessen innehåller tydliga beskrivningar av tillämpbart processflöde med korrelerande roller och ansvar för kritiska incidenter, samt hur dessa incidenter skall rapporteras under och efter åtgärdande.	Avsaknad av eller begränsade definierade rutiner för hantering av kritiska incidenter medför risk för att Sundbybergs stad misslyckas att ändamålsenligt hantera incidenter som kan orsaka verksamhetskritiska förluster av informationstillgångar.	EY rekommenderar att Kommunstyrelsen tillser att ett tydligt processflöde för hantering av kritiska incidenter, inklusive roller, ansvar och rapporteringskrav, definieras som del av stadens incidenthanteringsprocess.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

#	Iakttagelse	Risk	Rekommendation
5.10	**Avsaknad av formaliserad process för programförändringar** Kommunstyrelsen har inte tillsett att dokumenterade och formaliserade rutiner för styrning och standardiserad hantering av programförändringar har definierats, inklusive kontroller för säkerställande av ändamålsenlig ansvarsfördelning i införandet av programförändringar i stadens IT-miljö.	Avsaknad av en formaliserad programförändringsprocess medför risk för att programförändringar införs i IT-system och säkerhetslösningar på sätt som ej kan säkerställa riktighet, spårbarhet, konfidentialitet och tillgänglighet för informationen som hanteras i systemen.	EY rekommenderar att Kommunstyrelsen tillser att en stadsövergripande process för hantering av programförändringar formaliseras, inklusive kontroller för säkerställande av ändamålsenlig ansvarsfördelning i införandet av programförändringar.
5.11	**Passiv lagring av informationssäkerhetspolicy och relaterade anvisningar** Sundbybergs stads informationssäkerhetspolicy och relaterade användaranvisningar lagras passivt på intranätet och förutsätter att användare avsiktligt letar upp informationen.	Brist på aktiv kommunikation av policys och anvisningar gällande informationssäkerhet medför risk för att stadens användare besitter otillräcklig kunskap för att på daglig basis hantera stadens information på ett ändamålsenligt och säkert sätt.	EY rekommenderar att Kommunstyrelsen tillser att informationssäkerhetsrelaterad dokumentation kommuniceras aktivt till stadens användare med en bestämd frekvens.
5.12	**Brist på uppföljning av kontinuitetsplaner för skyddsvärda verksamhetssystem** Kommunstyrelsen har inte tillsett att central uppföljning från Stadsledningskontoret görs för verksamhetssystem med information som har klassats som skyddsvärd för säkerställande att kvalitativ kontinuitetsplanering har genomförts i enlighet med definierad kontinuitetsplaneringsmall.	Avsaknad av eller bristfälliga kontinuitetsplaner medför risk för att Sundbybergs stad misslyckas att ändamålsenligt hantera katastrofer som kan orsaka verksamhets- eller samhällskritiska förluster av informationstillgångar.	EY rekommenderar att Kommunstyrelsen tillser att kontinuitetsplaner utformas för samtliga verksamhetssystem som i genomförd informationsklassning har bedömts som skyddsvärda, samt att samtliga kontinuitetsplaner samlas ihop på Stadsledningskontorsnivå för central kvalitetssäkring och koordinering av regelbunden testning av kontinuitetsplanerna.
5.13	**Avsaknad av fullständig registerförteckning för personuppgifter** Kommunstyrelsen har inte tillsett att en fullständig och formellt definierad registerförteckning har upprättats över hur personuppgifter behandlas av staden.	Avsaknad av en registerförteckning för personuppgifter medför risk för att behandlingen av personuppgifter genomförs på sätt som ej kan säkerställa riktighet, spårbarhet, konfidentialitet och tillgänglighet för personuppgifterna. Vidare innebär detta att staden inte lever upp till kravet om upprättande av en registerförteckning enligt dataskyddsförordningen, vilket medför risk för böter från datainspektionen.	EY rekommenderar att Kommunstyrelsen tillser att en fullständig registerförteckning upprättas.

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

6. Slutsats

Syftet med granskningen var att ge en övergripande nulägesanalys om huruvida Kommunstyrelsen för Sundbybergs stad har tillsett att arbetet kring informationssäkerhet med fokus på styrning, organisation och incidenthantering är ändamålsenligt.

Efter utförd granskning har central uppföljning av arbetet med informationssäkerhet i Sundbybergs stads nämnder, förvaltningar och koncernbolag identifierats som stadens största förbättringsområde. Även en formaliserad och informationssäkerhetsspecifik organisationsstruktur med tillhörande roller, tydlig ansvarsfördelning, utökade resurser och definierade samverkansformer mellan Stadsledningskontoret och övriga verksamheter anses bör vara ett prioriterad initiativ för Kommunstyrelsen. Utan detta bedömer EY att det kommer bli svårt att skapa tillfredsställande förutsättningar för att bedriva ett ändamålsenligt arbete med informationssäkerhet på både kort och lång sikt inom staden.

Granskningens tre revisionsfrågor besvaras nedan:

Färgkod	Förklaring
	Revisionsfråga uppfylls ej
	Revisionsfråga uppfylls delvis
	Revisionsfråga uppfylls

Revisionsfråga	Svar	
Hur ändamålsenlig är styrningen av arbetet med informationssäkerhet gentemot LIS-ramverket (i enlighet med MSB:s metodstöd och ISO27000) för de behov stadens verksamhet har?	Styrningen av informationssäkerhetsarbetet i Sundbybergs stad gentemot LIS-ramverket bedöms ej vara ändamålsenligt. Svaret grundar sig i att Sundbybergs stad saknar flertalet grundläggande komponenter för att säkerställa ändamålsenlig informationssäkerhetsstyrning, bland annat en stadsövergripande informationssäkerhetsorganisation, tillräckligt bemannade resurser, adekvata utbildningsinsatser och definierade arbetsrutiner för åtkomst- och programförändringshantering.	

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

Hur ändamålsenligt är arbetet med att följa upp att beslut och styrningsdokument relaterat till informationssäkerhet efterlevs?	Arbetet med uppföljning av efterlevnad av beslut och styrningsdokument relaterat till informationssäkerhet bedöms ej vara ändamålsenligt. Svaret grundar sig i att Sundbybergs stads Kommunstyrelse inte tillsett att uppföljning av nämndernas, förvaltningarnas och koncernbolagens arbeten med informationssäkerhet genomförs, innefattandes exempelvis hur upphandlingar genomförs, informationsklassningar utförs, driftsdokumentation upprättas och personuppgifter hanteras.	
Har Sundbybergs stad en ändamålsenlig incidenthanteringsprocess?	Sundbybergs stad bedöms ha en delvis ändamålsenlig incidenthanteringsprocess. Svaret grundar sig i att Sundbybergs stads incidenthanteringsprocess består av detaljerade anvisningar för hur stadens Service Desk skall hantera vanliga incidenter, men saknar tydlig beskrivning av tillämpbart processflöde med korrelerande roller och ansvar för kritiska incidenter.	

Stockholm, 20e mars 2019

Helena Törnqvist
EY

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

7. Bilaga 1: Definitioner

Dataskyddsombud: Särskilt utsedd person med ansvar för personuppgiftshantering och att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser

Driftsansvarig: Specialist på IT-enheten eller extern part som har ansvar för den tekniska driften av ett system

Informationsklassning: Klassning av organisationens informationstillgångar enligt i riktlinjer dokumenterade regler med avseende på informationens sekretess, riktighet, tillgänglighet och konfidentialitet

Informationssäkerhet: Säkerhetsfrågor som berör information, oberoende av system och plattformar

Informationssäkerhetssamordnare: Särskilt utsedd person som innehar det operationella ansvaret att leda utvecklingen av stadens informationssäkerhet och stödja säkerhetschefen

IT-säkerhet: Säkerhet som huvudsakligen relaterar till IT-infrastruktur, systemfrågor och konfigurering

Kontinuitetsplanering: Planering och åtgärder med syfte att motverka avbrott i verksamheten och skydda kritiska verksamhetsprocesser mot konsekvenser av allvarliga fel i system eller katastrofer

Molntjänster: Tjänster och system som inte drivs lokalt av staden och som nås via en internetuppkoppling och inte direkt via det lokala nätverket

Stadsledningskontoret: Sundbybergs stads Kommunstyrelses förvaltning med ansvar för att leda och samordna planering och uppföljning av koncernövergripande verksamhet

Systemansvarig: Specialist på IT-enheten som har tekniskt ansvar för ett system och dess interaktioner

Systemförvaltare: Verksamhetsspecialist som på daglig basis ansvarar för ett systems funktionalitet och interaktioner med andra system

Systemägare: Särskilt utsedd person med övergripande ansvar för ett system och att leda arbetet med utveckling av IT-stödet på strategisk nivå

Säkerhetschef: Särskilt utsedd person som innehar huvudansvaret för stadens informationssäkerhet och har till uppgift att stödja stadsdirektören inför strategiska beslut rörande dataskydd

Ernst & Young AB
Box 7850
103 99 Stockholm
Besöksadress:
Jakobsbergsgatan 24

Tel: +46 (0) 8-5205 90 00
Fax: +00 123 4567 8901
ey.com
Org nr 556053-5873

8. Bilaga 2: Källförteckning

Intervjuade roller:

- Säkerhetschef
- IT-chef
- Informationssäkerhetssamordnare, dataskyddsombud
- IT-driftschef
- Infrastruktursansvarig, IT

Dokumentation:

- Anvisningar för användning av Sundbybergs stads IT-miljö, 2018
- Förslag till struktur för arbetet med informationssäkerhet och dataskydd, 2018
- Information från Sundbybergs stads intranät, 2019:
  - Driftsdokumentationsrutiner för systeminförande
  - Behörighetsinformation (Riktlinjer AD-konton, Säkerhetsriktlinjer AD-grupper)
  - Incidenthanteringsprocess, inklusive bilagor för ärenderegistrering, detaljerad information kring ärendeprioritering samt roller
- Informationsklassificering, 2017
- Informationssäkerhetspolicy, 2017
- Mall för intern incidentrapport, 2012
- Mall för incidentrapportering, MSB
- Mall för kontinuitetsplanering
- Nätverkskonton Sundbybergs stad, 2019
- Projektplan – Riktlinjer för informationssäkerhet, 2018
- Registrering av informationssäkerhetsincidenter
- Riktlinjer vid systeminförande och systemförändringar, 2018
- Systemförvaltningsmodell, 2010