Södertälje kommun

KS20150327

2015-01-15
Tjänsteskrivelse

Kontor
Kommunstyrelsens kontor

Handläggare
Johan Wahlström
08-523 016 92
johan.wahlstrom@sodertalje.se

Kommunstyrelsen

Revisionsrapport nr 7/2014 – Uppföljande granskning av IT-säkerhet

Dnr KS14/346

Sammanfattning av ärendet

Ernst & Young har på uppdrag av Södertälje kommuns revisorer bl.a. granskat utförda åtgärder till följd av rekommendationer som lämnats i 2011 och 2012 år granskningar. Detta svar avser området IT- och informationssäkerhet och granskningen ger följande rekommendation:

> **Uppföljning av granskning av IT- och informationssäkerhet**
> Syftet med granskningen var att skapa en utgångspunkt för arbetet med IT- och informationssäkerhet inom kommunen. Mot bakgrund av vad som framkommit i uppföljningen lämnas följande rekommendation till Kommunstyrelsen:
>
> - Säkerställ att tidigare lämnad rekommendation avseende generella riktlinjer för hantering av programändringar genomförs på sådant sätt och i sådan utsträckning att rekommendationens syfte kan anses vara uppfyllt.

Här beskrivs vilka åtgärder som genomförs och planeras utgående från denna rekommendation. Tjänsteskrivelsen föreslås överlämnas som kommunstyrelsens svar till revisionen. De åtgärder som beskrivs genomförs av IT-enheten respektive systemförvaltare och systemägare.

Beslutsunderlag

Kommunstyrelsens kontors tjänsteskrivelse den 15 januari 2015
Revisionsrapport 7/2014 – Uppföljande granskning

Ärendet

Merparten av de rekommendationer som revisorerna tidigare lämnat har genomförts, eller i annat fall motiverat vilka delar i rekommendationerna som inte är relevanta. De delar som kvarstår rör riktlinjer för hantering av programändringar. Dessa riktlinjer förtydligas här med utgångspunkt i revisorernas rekommendation.

Definitioner

För att det ska bli tydligt vad som gäller för "generella riktlinjer för programförändringar" som revisorerna ger behöver en distinktion göras mellan dels det som är program, dels vad som är system. När det gäller system finns också en skiljelinje mellan system som vi har kontroll över driften av hos vår driftsleverantör (för närvarande Tieto) och system som köps som tjänst/molntjänst.

Program – mjukvara eller komponenter som avses att installeras på användarnas datorer (eller på sikt även t.ex. appar som installeras på andra fristående verktyg som t.ex. surfplattor).

System – mjukvara, komponenter eller tjänster som finns installerade på en server och som användaren har tillgång till. Vissa system består både av en programvaru- och systemkomponent.

Program

Program kan i sin tur delas upp i tre kategorier, program i basklienten (PC) som installeras för alla användare, program som it-enheten är systemägare för (beställningsbara) och program som verksamheten är systemägare för (verksamhetsspecifika program).

Program i basklienten

I basklienten finns de program ska finnas som standard på alla datorer som tillhandahålls av IT-enheten. Exempel på dessa är Microsoft Office, antivirusprogram och Citrixklienten. För dessa program finns en etablerad rutin för hur regelbundna uppdateringar och programförändringar ska genomföras enligt ett överenskommet schema. Uppdateringarna testas först av teknikern (hos vår it-driftsleverantör) innan de installeras på en kontrollgrupp (t.ex. systemförvaltare av olika verksamhetssystem) som verifierar att det inte uppstår några problem med deras system. Även normala patchar av till exempel Windows hanteras på detta sätt. IT-enheten beställer och ansvarar för dessa uppdateringar enligt rutin och särskild beställningsblankett som finns på Kanalen.

Program som IT-enheten är systemägare för

I den här kategorin finns program som används av flera användare på flera kontor. I vissa fall har man valt att låta IT-enheten hantera dessa för att få såväl en centraliserad och kontrollerad licensförsörjning som uppdatering. Exempel i den här kategorin är Adobe Photoshop, en FTP-klient och Microsoft Visio.
Dessa program uppdateras när behov uppstår, antingen av säkerhetsskäl, kompatibilitetsskäl eller för att få ny funktionalitet. Initiativtagare till en uppgradering kan antingen vara IT-avdelningen eller verksamheten, som då begär att IT-avdelningen beställer programvarorna.

Programmen testats av tekniker samt ett urval av de som kommer använda programmen (expertanvändare) på samma sätt som för program i basklienten.

Program som verksamheten är systemägare för

I den här kategorin finns program som normalt används inom ett kontor och som är, eller tillhör, ett verksamhetssystem. Verksamheten ansvarar för licenser och inköp av dessa program. Installationer görs dock av driftleverantören, användarna har inte rätt att installera program själva. Exempel på sådana program är program för att hantera nyckelskåp, beräkna gatubuller eller för att kommunicera med temperaturgivare o.d.

Dessa program uppdateras normalt när verksamheten har behov. I vissa fall kan IT-avdelningen ta initiativ till en uppdatering, oftast på grund av säkerhets- eller kompatibilitetsskäl.

Programmen testats av tekniker samt ett urval av de som kommer använda programmen (expertanvändare) enligt samma rutin som ovan.

Verksamheten (systemägaren) beställer uppdateringarna, IT-enheten godkänner beställningen. Verksamheten testar och godkänner resultatet.

System

System kan dels vara centrala system som AD (katalog över användare och datorer), Exchange (e-post), TEIS (integrationsmotor) eller Portwise (Accesskontroll), dels verksamhetssystem som Aditro (ekonomi), Heroma (Lönesystem), Skolplatsen (Skolans system) eller Procapita (Vård och omsorg). Verksamheten ansvarar själva för att utvärdera verksamhetsnyttan av systemändringar. Ofta genomförs pilotprojekt för att uppskatta verksamhetsnyttan innan beställning eller större förändringar.

Många av framför allt våra verksamhetssystem köps som tjänst/molntjänst, vilket innebär att kommunen ***inte*** har ansvar för drift- och utveckling, utan det hanteras av leverantören.

Beställningar

Beställningar av förändringar för system som finns hos den vår centrala driftleverantör görs normalt av systemförvaltare eller systemägare, och godkänns av IT-avdelningen enligt en mall. Dessa beställningar sparas och utgör dokumentation.

När det gäller molntjänster har vi inte samma kontroll som för system som driftas på servrar hos vår driftsleverantör. I många fall görs förändringar som påverkar alla leverantörens kunder och i dessa fall får vi rätta oss efter leverantörens planer och utgår från att det i avtal och det åliggande som leverantören tar på sig finns de rutiner som behövs. I de fall vi beställer ändringar/anpassningar i sådana system utförs, testas och dokumenteras enligt den ordning verksamheten och leverantören kommit överens om.

Testmiljöer och tester

För molnstjänsterna kan det finnas en test- och utvecklingsmiljö. Om det finns en testmiljö regleras detta och hanteringen av denna i av avtalet verksamheten har träffat med leverantören.

För centrala system finns testmiljöer hos vår driftsleverantör till exempel för Portwise. Då vi har en vitaliserad serverinfrastruktur går de relativt snabbt att sätta upp en testmiljö om det behövs för ett större projekt, och testmiljöer sätts därför ofta inte upp förrän behovet uppstår.

De minsta systemen kan vara så enkla som en Accessdatabas som finns på en gemensam filarea. De saknar normalt testmiljö, men å andra sidan sker heller inga större förändringar av dessa system heller.

Efter en systemuppdatering görs en test av systemet av systemförvaltarna och/eller en utvald grupp av användare. Generellt är befogenheten att godkänna en förändring delegerad till systemförvaltarna av systemägarna. Testplan kan ingå i beställningar till den centrala driftleverantören, fält för detta finns i beställningsblanketten.

Changehantering

Ändringar i den centrala IT-miljön hos vår driftsleverantör görs enligt en definierad changeprocess med veckovisa möten "Change Advisory Board" (CAB). Från kommunen deltar utvecklingsansvarige och driftansvarige som godkänner eller avslår de förändringar

som läggs fram.

System- och programdokumentation
Information om systemen och programmen i form av systemägare och -förvaltare, ansvarigt kontor, version, systemtyp och om systemet är verksamhetskritiskt dokumenteras i systemet Itsy-SAR.

Information om vilka datorer programmen är installerade på finns dels dokumenterat i System center/AD, dels i Snow som är ett inventeringsverktyg för program/licenser.

Slutsats
Utgående från revisorernas rekommendationer och den sammanställning och uppdatering av rutiner för programförändringar som beskrivs ovan menar kommunstyrelsens kontor att kommunen nu har generella riktlinjer för programförändringar som är adekvata utifrån verksamhetens behov och revisionens rekommendationer.

Ekonomiska konsekvenser och finansiering
Ärendet i sig har inga direkta ekonomiska konsekvenser, men det löpande arbetet med att implementera och följa upp de ändrade riktlinjerna medför kostnader för verksamheten och IT-enheten, dels i tid för genomförande och dokumentation, dels för vissa tekniska åtgärder (som t.ex. att kravställa/införa tesmiljö för olika system). Framförallt när det gäller hantering av appar kommer det i framtiden att behövas resurser, rutiner och verktyg för att hantera dessa på ett kontrollerat sätt.

Kommunstyrelsens kontor förslag till kommunstyrelsen:

Kommunstyrelsens kontors tjänsteskrivelse lämnas som svar till kommunrevisorerna och de beskrivna åtgärderna genomförs av IT-enheten samt systemförvaltare och systemägare.

Martin Andreae
Stadsdirektör

Johan Wahlström
IT-strateg

Beslutet expedieras till:
Kommunrevisionen
Systemägare
Systemförvaltare

Södertälje kommun
Revisorerna

Revisionsskrivelse
2014-12-10

Till Kommunstyrelsen
Stadsbyggnadsnämnden
För kännedom: Kommunfullmäktige

Revisionsrapport nr 7/2014 – Uppföljande granskning

EY har på uppdrag av oss revisorer i Södertälje kommun granskat vilka åtgärder berörda nämnder har vidtagit till följd av de rekommendationer som lämnades i ett urval av 2011 och 2012 års granskningar. I sammanställningen nedan framgår vilka granskningar som omfattades av uppföljningen och vilka slutsatser som dragits av respektive uppföljning.

Uppföljning av granskning av bygglov

Syftet med granskningen var att bedöma om Stadsbyggnadsnämndens styrning och uppföljning av bygglovsprocessen är ändamålsenlig och effektiv. Mot bakgrund av vad som framkommit i uppföljningen upprepas tre av de fyra rekommendationer som lämnades till Stadsbyggnadsnämnden i granskningen.

- Nämnden bör i ökad utsträckning utvärdera effektiviteten i handläggningsprocessen av bygglovärenden. Detta för att identifiera ytterligare områden där effektivisering kan göras.
- Dokumenterade rutiner bör tas fram för hur hanteringen av ärenden i det nya ärendehanteringssystemet Public 360 ska göras.
- En kvalitetssäkrande funktion bör införas i handläggningsprocessen.

Uppföljning av granskning av IT- och informationssäkerhet

Syftet med granskningen var att skapa en utgångspunkt för arbetet med IT- och informationssäkerhet inom kommunen. Mot bakgrund av vad som framkommit i uppföljningen lämnas följande rekommendation till Kommunstyrelsen:

- Säkerställ att tidigare lämnad rekommendation avseende generella riktlinjer för hantering av programändringar genomförs på sådant sätt och i sådan utsträckning att rekommendationens syfte kan anses vara uppfyllt.

Uppföljning av granskningar av bisysslor resp. hantering av bisysslor

Syftet med granskningarna var att bedöma ändamålsenlighet och intern kontroll i hanteringen av de anställdas bisysslor respektive kontroll och uppföljning av bisysslor. Mot bakgrund av vad som framkommit i uppföljningen lämnas följande rekommendation till Kommunstyrelsen:

- Fastställa vilken status processbeskrivningen för hantering av bisysslor har samt besluta om vilken funktion som ansvarar för att informera eller informera sig om eventuella revideringar av processbeskrivningen.

Vi önskar svar från kommunstyrelsen och stadsbyggnadsnämnden på de slutsatser och rekommendationer som framgår av rapporten. Svar önskas senast till den 31 mars 2015.

För revisorerna i Södertälje kommun

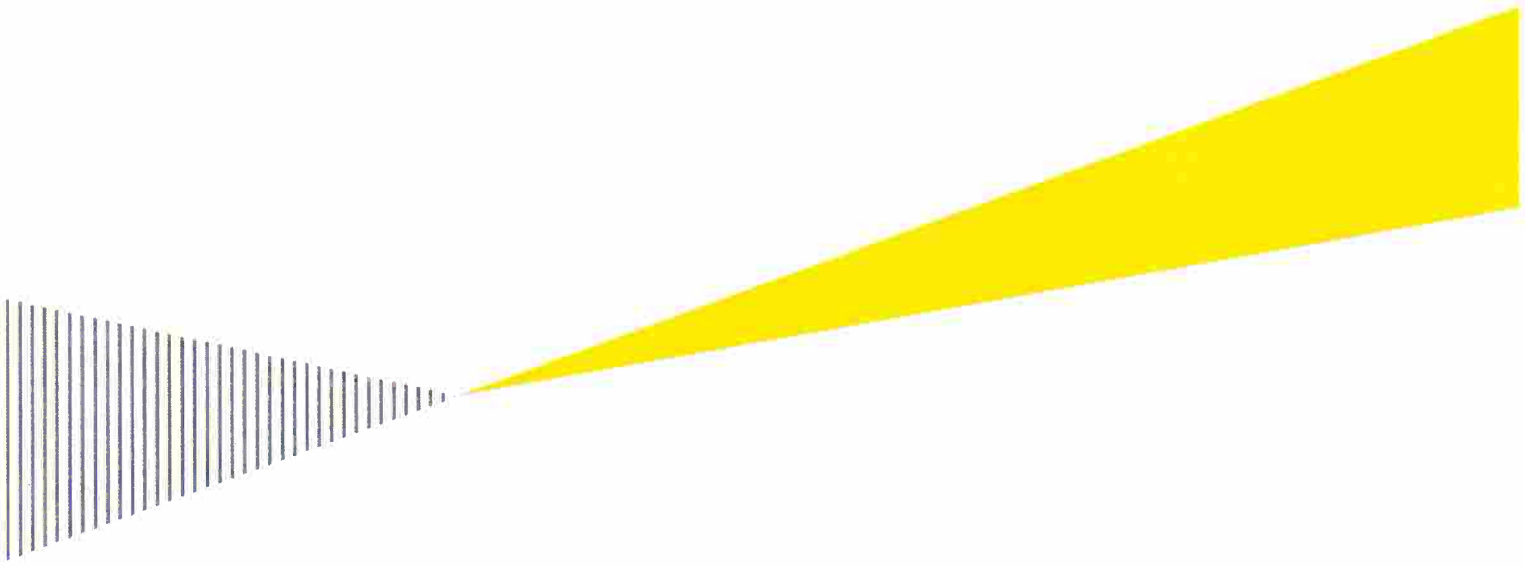
Elisabet Kornhéden

Erik Ternert

Bilaga: Revisionsrapport nr 7/2014 – Uppföljande granskning av tidigare granskningar

Uppföljning av tidigare granskningar

Södertälje kommun



Building a better working world

Innehåll

1 Inledning

1.1 Syfte och revisionsfrågor

Syftet med denna granskning har varit att följa upp vilka åtgärder berörda nämnder har vidtagit till följd av de rekommendationer som lämnades i ett urval av 2011 och 2012 års granskningar.

1.2 Revisionskriterier

Revisionskriterierna, dvs. de målsättningar mot vilka verksamheterna mäts och bedöms, utgörs av de rekommendationer som lämnades i de utvalda revisionsrapporterna.

1.3 Metod

Granskningen har gjorts genom studier av nämndprotokoll och dokument samt genom kompletterande telefonintervjuer.

1.4 Avgränsning

Granskningen omfattar följande revisionsrapporter:

- Revisionsrapport 7/2011 – Granskning av bygglov
- Revisionsrapport 2/2012 – Granskning av IT- och informationssäkerhet
- Revisionsrapport 8/2011 – Granskning av bisysslor
- Revisionsrapport 5/2012 – Granskning av hantering av bisysslor

2 Granskning av bygglov

2.1 Sammanfattning och rekommendationer

Syftet med granskningen var att bedöma om Stadsbyggnadsnämndens styrning och uppföljning av bygglovsprocessen är ändamålsenlig och effektiv. I granskningen konstaterades att åtgärder hade vidtagits för att skapa en mer effektiv handläggningsprocess men att tillräckliga system och rutiner för uppföljning eller kvalitetssäkring inte fanns. Det saknades också rutiner för hantering av ärenden i det då nyligen införda ärendehanteringssystemet Public 360. Intervjuade medarbetare uppfattade att ärenden inte handlades i enlighet med lagstadgade krav.

Revisorernas förslag till Stadsbyggnadsnämnden
Nämnden bör i ökad utsträckning utvärdera effektiviteten i handläggningsprocessen av bygglovärenden. Detta för att identifiera ytterligare områden där effektivisering kan göras.
Dokumenterade rutiner bör tas fram för hur hanteringen av ärenden i det nya ärendehanteringssystemet Public 360 ska göras.
En rutin bör upprättas för att mäta den genomsnittliga handläggningstiden.
En kvalitetssäkrande funktion bör införas i handläggningsprocessen.

Revisorerna önskade svar från Stadsbyggnadsnämnden senast den 15 mars 2012.

2.2 Stadsbyggnadsnämndens svar

Den 28 februari 2012 beslutade Stadsbyggnadsnämnden att anta en kommentar till revisionsrapporten. I denna kommentar ansåg nämnden att de fyra förslagen var bra och bedömdes som möjliga att genomföra. Ingen närmare åtgärdsplan presenterades.

2.3 Genomförda åtgärder

Följande åtgärder har enligt uppgift från förvaltningen utförts:

Revisorernas förslag	Stadsbyggnadsnämndens planerade åtgärder	Genomförda åtgärder
Nämnden bör i ökad utsträckning utvärdera effektiviteten i handläggningsprocessen av bygglovärenden. Detta för att identifiera ytterligare områden där effektivisering kan göras.	De fyra förslagen är bra och bedöms som möjliga att genomföra. (Stadsbyggnadsnämndens kommentar till revisionsrapporten)	Kontoret har enligt uppgift genomfört ett kontinuerligt förbättringsarbete. Ingen formell utvärdering av effektiviteten har dock gjorts.
Dokumenterade rutiner bör tas fram för hur hanteringen av ärenden i det nya ärendehanteringssystemet Public 360 ska göras.		Dokumenterade rutiner har inte tagits fram. Detta på grund av att en ny version av systemet, speciellt anpassad för bygglov, ska börja användas under 2015. I denna version finns en hjälpfunktion inbyggd. En rutin anses därför inte behövas.
En rutin bör upprättas för att mäta den genomsnittliga handläggningstiden.		Kontoret använder ett kalkylblad där handläggare fyller i vid vilka datum olika steg i bygglovsprocessen tas. Bygglovschefen följer med hjälp av detta upp den genomsnittliga handläggningstiden kvartalsvis.
En kvalitetssäkrande funktion bör införas i handläggningsprocessen.		Kvalitetssäkring av handläggningstider sker genom att en person manuellt följer upp ovan nämnda kalkylblad och påminner handläggare om ärenden inte

	håller sig inom givna tidsramar. En person förbereder beslut och en person expedierar beslut. Förberedelse av beslut ska innefatta vissa moment. Denna process finns dock inte nedskriven.

2.4 Slutsatser

Stadsbyggnadsnämnden har tagit fram en rutin för att mäta den genomsnittliga handläggningstiden men har inte gjort någon formell utvärdering av effektiviteten i handläggningsprocessen eller infört någon kvalitetssäkrande funktion av handläggningsprocessen i sin helhet. Någon rutin för hanteringen av ärenden i ärendehanteringssystemet kommer enligt uppgift inte att behövas eftersom ärendehanteringssystemet i sig kommer att vara anpassat för bygglovsärenden. EY gör dock bedömningen att en rutinbeskrivning generellt sett kan ses som ett förtydligande av hur exempelvis ett ärendehanteringssystem ska användas och att systemet som sådant därmed inte kan ersätta en rutinbeskrivning.

Mot bakgrund av detta upprepas tre av de fyra tidigare rekommendationerna till Stadsbyggnadsnämnden:

- Nämnden bör i ökad utsträckning utvärdera effektiviteten i handläggningsprocessen av bygglovärenden. Detta för att identifiera ytterligare områden där effektivisering kan göras.
- Dokumenterade rutiner bör tas fram för hur hanteringen av ärenden i det nya ärendehanteringssystemet Public 360 ska göras.
- En kvalitetssäkrande funktion bör införas i handläggningsprocessen.

3 Granskning av IT- och informationssäkerhet

3.1 Sammanfattning och rekommendationer

Granskningen syftade till att skapa en utgångspunkt för arbetet med IT- och informationssäkerhet inom kommunen. I granskningen framkom att kommunen uppfyllde flertalet rekommendationer i BITS[1] med högre måluppfyllnad än genomsnittet av granskade kommuner.

Utifrån bedömd risk och väsentlighet lämnades elva rekommendationer. Tre av dem bedömdes ha hög angelägenhetsgrad.

Revisorernas rekommendationer till Kommunstyrelsen

Hantering av behörigheter

Vi rekommenderar Södertälje kommun att dokumentera och implementera generella riktlinjer för att skapa nya/förändra/ta bort behörigheter i systemen, samt för att granska rättigheter i systemen.

Följande kontroller och aktiviteter bör finnas med:

- Det skall framgå vem som får beställa nya behörigheter, ändring av behörigheter och borttag av behörigheter (vanligtvis enhetschef eller personalavdelning)
- Mottagare av beställning bör kontrollera att beställaren har befogenheter att göra beställning
- Information om att konto har skapats bör skickas med kopia till beställaren
- Kontouppgifter bör ej skickas okrypterade över publika nätverk
- Användaren bör byta lösenord vid första inloggning
- Det skall framgå vem som ansvarar för att en person som slutar ej längre har rättigheter till systemen (vanligtvis enhetschef eller personalavdelning)
- Det skall framgå vem (vanligtvis systemägaren) som är ansvarig för att periodvis gå igenom behörigheterna i respektive verksamhetssystem, för att säkerställa att dessa är korrekta, och hur ofta denna kontroll skall genomföras

Generella riktlinjer för hantering av programändringar

Vi rekommenderar Södertälje kommun att dokumentera och implementera generella riktlinjer för beslut om programförändringar. Följande kontroller och aktiviteter bör finnas med:

- Det skall framgå vem som får beställa förändringar
- Alla beställningar av förändringar skall vara dokumenterade
- Beställning skall godkännas av systemägare (eller motsvarande)
- Acceptanstest av förändring skall göras i miljö separerad från produktionsmiljö. Testfall i testprotokoll bör vara länkade till krav i beställning
- Testresultat skall godkännas av systemägare (eller motsvarande)
- Vid större förändringar bör uppföljning av förändringens verksamhetsnytta göras.

Kontinuerlig uppföljning av arbetet med informationssäkerhet

Vi rekommenderar Södertälje kommun att kontinuerligt följa upp arbetet med informationssäkerhet. Södertälje kommun bör bland annat genomföra regelbundna penetrationstester, liksom granskningar kring efterlevnaden av gällande policys och riktlinjer.

Revisorerna önskade svar från Kommunstyrelsen senast den 20 december 2012.

3.2 Kommunstyrelsens svar

Kommunstyrelsen instämde i de flesta fall i de slutsatser som dragits i granskningen och beslutade den 14 december 2012 att fastställa kommunstyrelsekontorets förslag till åtgärder.

[1] *Basnivå för informationssäkerhet*, en vägledning i författandet av IT-säkerhetsregelverk som tidigare rekommenderades av dåvarande Krisberedskapsmyndigheten.

Revisorernas rekommendationer till Kommunstyrelsen	Kommunstyrelsens planerade åtgärder
Hantering av behörigheter Vi rekommenderar Södertälje kommun att dokumentera och implementera generella riktlinjer för att skapa nya/förändra/ta bort behörigheter i systemen, samt för att granska rättigheter i systemen. Följande kontroller och aktiviteter bör finnas med: - Det skall framgå vem som får beställa nya behörigheter, ändring av behörigheter och borttag av behörigheter (vanligtvis enhetschef eller personalavdelning) - Mottagare av beställning bör kontrollera att beställaren har befogenheter att göra beställning - Information om att konto har skapats bör skickas med kopia till beställaren - Kontouppgifter bör ej skickas okrypterade över publika nätverk - Användaren bör byta lösenord vid första inloggning - Det skall framgå vem som ansvarar för att en person som slutar ej längre har rättigheter till systemen (vanligtvis enhetschef eller personalavdelning) - Det skall framgå vem (vanligtvis systemägaren) som är ansvarig för att periodvis gå igenom behörigheterna i respektive verksamhetssystem, för att säkerställa att dessa är korrekta, och hur ofta denna kontroll skall genomföras	Kommunstyrelsens kontor har inlett framtagandet av generella riktlinjer för behörigheter. Dessa riktlinjer kommer även utformas för att möta den tekniska utvecklingen, t.ex. inom identitetsfederationer.
Generella riktlinjer för hantering av programändringar Vi rekommenderar Södertälje kommun att dokumentera och implementera generella riktlinjer för beslut om programförändringar. Följande kontroller och aktiviteter bör finnas med: - Det skall framgå vem som får beställa förändringar - Alla beställningar av förändringar skall vara dokumenterade - Beställning skall godkännas av systemägare (eller motsvarande) - Acceptanstest av förändring skall göras i miljö separerad från produktionsmiljö. Testfall i testprotokoll bör vara länkade till krav i beställning - Testresultat skall godkännas av systemägare (eller motsvarande) - Vid större förändringar bör uppföljning av förändringens verksamhetsnytta göras.	Kontorets bedömning är att det är av vikt att krav avseende programförändringar finns i de avtal som systemägare tecknar med externa leverantörer.
Kontinuerlig uppföljning av arbetet med informationssäkerhet Vi rekommenderar Södertälje kommun att kontinuerligt följa upp arbetet med informationssäkerhet. Södertälje kommun bör bland annat genomföra regelbundna penetrationstester, liksom granskningar kring efterlevnaden av gällande policys och riktlinjer.	Kontoret har inlett arbetet med att ta fram ett ramverk för regelbunden uppföljning av informationssäkerhet. Detta kommer att inkludera dels den tekniska uppföljningen i form av penetrationstester, dels granskningar av efterlevnaden av gällande policys och riktlinjer. Kommunstyrelsen avser att uppdatera informationssäkerhetspolicyn under 2013. Denna uppdatering kommer att utgå från de vägledningar som Myndigheten för samhällsskydd och beredskap har arbetat fram, men också basera sig på de erfarenheter och rekommendationer som KSL (Kommunförbundet Stockholms län) och Stockholms stad har publicerat.

3.3 Genomförda åtgärder

Följande åtgärder har enligt uppgift från förvaltningen utförts.

Revisorernas rekommendationer till Kommunstyrelsen	Kommunstyrelsens planerade åtgärder	Genomförda åtgärder
Hantering av behörigheter Vi rekommenderar Södertälje kommun att dokumentera och implementera generella riktlinjer för att skapa nya/förändra/ta bort behörigheter i systemen, samt för att granska rättigheter i systemen. Följande kontroller och aktiviteter bör finnas med: - Det skall framgå vem som får beställa nya behörigheter, ändring av behörigheter och borttag av behörigheter (vanligtvis enhetschef eller personalavdelning) - Mottagare av beställning bör kontrollera att beställaren har befogenheter att göra beställning - Information om att konto har skapats bör skickas med kopia till beställaren - Kontouppgifter bör ej skickas okrypterade över publika nätverk - Användaren bör byta lösenord vid första inloggning - Det skall framgå vem som ansvarar för att en person som slutar ej längre har rättigheter till systemen (vanligtvis enhetschef eller personalavdelning) - Det skall framgå vem (vanligtvis systemägaren) som är ansvarig för att periodvis gå igenom behörigheterna i respektive verksamhetssystem, för att säkerställa att dessa är korrekta, och hur ofta denna kontroll skall genomföras	Kommunstyrelsens kontor har inlett framtagandet av generella riktlinjer för behörigheter. Dessa riktlinjer kommer även utformas för att möta den tekniska utvecklingen, t.ex. inom identitetsfederationer.	Riktlinjer för hantering av behörigheter har tagits fram. I dessa beskrivs roller och system för - Skapande och tilldelning av behörighet - Avslut och återkallande av behörighet - Förändring av behörighet - Utformning av behörighet Riktlinjerna nämner inte att kontouppgifter ej bör skickas okrypterade över publika nätverk. Detta enligt uppgift för att inga uppgifter skickas över okrypterade nätverk.
Generella riktlinjer för hantering av programändringar Vi rekommenderar Södertälje kommun att dokumentera och implementera generella riktlinjer för beslut om programförändringar. Följande kontroller och aktiviteter bör finnas med: - Det skall framgå vem som får beställa förändringar - Alla beställningar av förändringar skall vara dokumenterade - Beställning skall godkännas av systemägare (eller motsvarande) - Acceptanstest av förändring skall göras i miljö separerad från produktionsmiljö. Testfall i testprotokoll bör vara länkade till krav i beställning - Testresultat skall godkännas av systemägare (eller motsvarande) - Vid större förändringar bör uppföljning av förändringens verksamhetsnytta göras.	Kontorets bedömning är att det är av vikt att krav avseende programförändringar finns i de avtal som systemägare tecknar med externa leverantörer.	Rutin finns för den s.k. changeprocessen, dvs. för förändringar som görs i den gemensamma infrastrukturen, samt för beställningsprocessen avseende bl.a. programvaror. I de förra anges att programvaror som inte finns i kommunens standardsortiment beställs genom kontakt med IT-enheten, som ska godkänna nya programvaror innan de köps in. För varje nytt system ska en kommunövergripande systemägare utses. I övrigt behöver riktlinjer enligt uppgift förtydligas i respektive upphandling och avtal. Kommunen har därför tagit fram riktlinjer för upphandling av IT-system. I dessa nämns dock inte de kontroller och aktiviteter som efterfrågats av revisorerna.

Kontinuerlig uppföljning av arbetet med informationssäkerhet Vi rekommenderar Södertälje kommun att kontinuerligt följa upp arbetet med informationssäkerhet. Södertälje kommun bör bland annat genomföra regelbundna penetrationstester, liksom granskningar kring efterlevnaden av gällande policys och riktlinjer.	Kontoret har inlett arbetet med att ta fram ett ramverk för regelbunden uppföljning av informationssäkerhet. Detta kommer att inkludera dels den tekniska uppföljningen i form av penetrationstester, dels granskningar av efterlevnaden av gällande policys och riktlinjer.	Riktlinje för uppföljning av informationssäkerhet har tagits fram. I dessa beskrivs vilket ansvar för uppföljning av efterlevnad av riktlinjer för informationssäkerhet som åvilar systemförvaltare och systemägare av verksamhetskritiska system samt verksamhetsansvariga. Penetrationstester berörs ej. Detta enligt uppgift för att kommunens bild är att traditionella penetrationstester inte längre är lika aktuella som tidigare, då hotbilden förändrats.

3.4 Slutsatser

Vi bedömer att de åtgärder som vidtagits med anledning av revisionens rekommendationer avseende hantering av behörigheter samt kontinuerlig uppföljning av arbetet med informationssäkerhet är tillräckliga. Kommunen har inte följt rekommendationerna i sin helhet men motiverat varför den inte uppfattar de icke åtgärdade delarna som relevanta.

Rekommendationen avseende generella riktlinjer för hantering av programändringar har dock inte åtgärdats i en utsträckning som kan anses tillräcklig. Av kommunens beskrivning av beställningsprocessen framgår att IT-enheten ska genomföra beställningar och godkänna programvaror innan de köps in samt att en övergripande systemansvarig ska utses. Övriga delrekommendationer är inte åtgärdade.

Mot bakgrund av detta lämnas följande rekommendation till Kommunstyrelsen:

- Säkerställ att tidigare lämnad rekommendation avseende generella riktlinjer för hantering av programändringar genomförs på sådant sätt och i sådan utsträckning att rekommendationens syfte kan anses vara uppfyllt.

4 Granskning av bisysslor

4.1 Sammanfattning och rekommendationer

Revisorerna granskade bisysslor både år 2011 och år 2012.

Granskningen år 2011 gällde ändamålsenlighet och intern kontroll i hanteringen av de anställdas bisysslor. Granskningen omfattade Kommunstyrelsen, Stadsbyggnadsnämnden, Tekniska nämnden och Socialnämnden. Granskningen konstaterade att gällande regler och riktlinjer var förhållandevis gamla och hänvisade till funktioner som inte längre fanns kvar i den kommunala organisationen. Vidare framgick av granskningen att någon dokumentation av inrapporterade bisysslor inte gjordes. Inte heller genomfördes några uppföljningar av huruvida anställda med inrapporterade bisysslor avslutat desamma då de uppmanats till detta.

Revisorernas rekommendationer till Kommunstyrelsen, Stadsbyggnadsnämnden, Tekniska nämnden och Socialnämnden 2011

De skriftliga regler som finns rörande bisysslor och hur de ska hanteras och bedömas bör uppdateras för att passa den nuvarande kommunala organisationen.
Lokala anvisningar rörande hur frågan om bisysslor ska hanteras vid respektive kontor bör utformas anpassade till den egna verksamhetens förutsättningar.
En skrivning bör införas i den kommunövergripande rekryteringshandboken som rör bisysslor.
En rutin bör tas fram om att vid arbetsplatsträffar lyfta frågan om bisysslor.
En rutin bör införas där samtliga bisysslor, såväl tillåtna som otillåtna, dokumenteras.
En rutin bör tas fram om att vid det årliga utvecklingssamtalet med samtliga medarbetare lyfta frågan om bisysslor.
En rutin bör införas att efter en tid genomföra en uppföljning av huruvida bisysslor som inte är acceptabla har avslutats.

Revisionen önskade nämndernas och Kommunstyrelsens kommentarer till granskningens slutsatser och förbättringsområden senast den 30 april 2012.

År 2012 gjordes en fördjupad granskning av kommunens hantering av bisysslor för samtliga personer som har en chefsposition inom kommunen. Syftet var att bedöma kommunens kontroll och uppföljning av bisysslor. I granskningen konstaterades att kommunen fortsatt saknade enhetliga och ändamålsenliga rutiner för hantering av bisysslor samt en central kontroll över vilka bisysslor som rapporterats och godkänts.

Revisorernas rekommendationer till Kommunstyrelsen 2012

Vi rekommenderar kommunen, liksom tidigare, att utveckla den interna kontrollen kring hantering av bisysslor. Främst gäller detta att införa tydliga systematiska och dokumenterade rutiner för hur kommunen som arbetsgivare ska följa upp och hantera bisysslor. Utgångspunkten för en god intern kontroll inom området är enligt vår bedömning att identifiering av bisyssla, godkännande av bisyssla, beslut om att inte godkänna bisyssla samt uppföljning av bisysslor ska dokumenteras.

Revisorerna önskade svar från Kommunstyrelsen senast den 31 mars 2013.

4.2 Kommunstyrelsens och nämndernas svar

Som svar på 2011 års granskning beslutade Kommunstyrelsen, Stadsbyggnadsnämnden, Tekniska nämnden och Socialnämnden att yttra sig till revisionen genom att hänvisa till ett PM författat gemensamt av kommunstyrelsens kontor, social- och omsorgskontoret samt stadsbyggnadskontoret. Där konstaterades att det är Kommunstyrelsen, inte facknämnderna, som ansvarar för personalfrågor även om alla nämnder har ett delat intresse av att motverka olämpliga bisysslor.

I PM:et står att alla de sju förslagen är goda och kommer därför att genomföras, i den mån de inte redan är genomförda. Därtill ska Kommunstyrelsens kontor även definiera de personalgrupper som man i fortsättningen systematiskt kommer att begära in uppgift om bisyssla från. Kontoret kommer att överväga om det finns skäl att fråga all personal vid kontoret. Det kan finnas skäl också för andra kontor att granska bisysslor mer systematiskt än hittills.

Som svar på 2012 års granskning yttrade sig Kommunstyrelsen den 26 april 2013 genom att hänvisa till ett PM från förvaltningen och dessutom notera vad personalutskottet beslutat i frågan. Personalutskottet hade beslutat om riktlinjer för bisysslor. I anslutning till riktlinjerna finns även en preliminär processbeskrivning.

4.3 Genomförda åtgärder

Av ovan nämnda riktlinjer och processbeskrivning framgår följande åtgärder. Åtgärderna svarar mot rekommendationer från både 2011 och 2012 års granskning.

Revisorernas rekommendationer till Kommunstyrelsen, Stadsbyggnadsnämnden, Tekniska nämnden och Socialnämnden 2011	**Kommunstyrelsens genomförda åtgärder**
De skriftliga regler som finns rörande bisysslor och hur de ska hanteras och bedömas bör uppdateras för att passa den nuvarande kommunala organisationen.	Kommunens riktlinjer för bisysslor uppdaterades i anslutning till att revisorerna lämnade sin andra granskning till Kommunstyrelsen.
Lokala anvisningar rörande hur frågan om bisysslor ska hanteras vid respektive kontor bör utformas anpassade till den egna verksamhetens förutsättningar.	I kommunens riktlinjer för bisysslor anges att kontorschef beslutar om anvisningar som är anpassade till kontorets verksamhet. Där står vilka personalgrupper som ska anses särskilt känsliga ur bisysslesynpunkt (SKB-märkta) och hur dessa samt övriga grupper ska redovisa bisysslor. Respektive kontor äger enligt uppgift sin egen anvisning. HR-specialist har bistått vissa men inte alla kontor i att ta fram kontorsspecifika anvisningar och har vid senare tillfälle träffat samtliga kontorschefer för genomgång av både generella och specifika anvisningar. Enligt uppgift finns specifika anvisningar vid samtliga kontor.
En skrivning bör införas i den kommunövergripande rekryteringshandboken som rör bisysslor.	Enligt processbeskrivningen ska anställande chef vid nyanställning till SKB-märkta uppdrag fråga om bisyssla redan innan man kommer överens om anställning. När anställningsavtalet undertecknas ska den nyanställde också lämna skriftlig uppgift. För övriga personalgrupper ska anställande chef fråga om bisyssla under introduktion av nyanställd. Rekryteringshandboken har ersatts av annat stödmaterial som fyller motsvarande funktion. I detta ingår bland annat skriftliga intervjumallar som innehåller frågor om bisyssla.
En rutin bör tas fram om att vid arbetsplatsträffar lyfta frågan om bisysslor.	Enligt processbeskrivningen görs genomgång av riktlinjerna årligen vid arbetsplatsträff, APT.
En rutin bör införas där samtliga bisysslor, såväl tillåtna som otillåtna, dokumenteras.	I processbeskrivningen anges att skriftlig uppgift om bisyssla ska lämnas på kommunens blankett, undertecknat på papper. Skriftlig uppgift ska lämnas vid nyanställning till SKB-märkta uppdrag samt om den anställde muntligen nämner en bisyssla som chefen anser bör prövas närmare eller om det finns annan anledning att undersöka om den anställde har en sådan bisyssla.

En rutin bör tas fram om att vid det årliga utvecklingssamtalet med samtliga medarbetare lyfta frågan om bisysslor.	I riktlinjerna anges att HR-avdelningen fastställer en processbeskrivning som bygger på att frågor ställs vid nyanställning, årligen vid planerings- och utvecklingssamtal och dessutom i vissa fall när en medarbetare får nya uppgifter. Vid det årliga planerings- och utvecklingssamtalet begär chefen enligt processbeskrivningen in ny skriftlig uppgift.
En rutin bör införas att efter en tid genomföra en uppföljning av huruvida bisysslor som inte är acceptabla har avslutats.	I processbeskrivningen anges att resultatenhetschefen följer upp att förbjudna bisysslor har avvecklats. Ny skriftlig uppgift om detta ska lämnas in.
Revisorernas rekommendation till Kommunstyrelsen 2012	**Kommunstyrelsens genomförda åtgärder**
Vi rekommenderar kommunen, liksom tidigare, att utveckla den interna kontrollen kring hantering av bisysslor. Främst gäller detta att införa tydliga systematiska och dokumenterade rutiner för hur kommunen som arbetsgivare ska följa upp och hantera bisysslor. Utgångspunkten för en god intern kontroll inom området är enligt vår bedömning att identifiering av bisyssla, godkännande av bisyssla, beslut om att inte godkänna bisyssla samt uppföljning av bisysslor ska dokumenteras.	Personalutskottet fattade 2013 ett beslut om att anta riktlinjer för bisysslor. Dessa beskriver vilka bisysslor kommunen inte accepterar samt, på ett övergripande plan, hur kommunen granskar och följer upp bisysslor. Till dessa hörde en processbeskrivning för granskning, dokumentation och uppföljning av bisysslor. Kommunstyrelsen hänvisade till personalutskottets beslut samt till ett PM i sitt svar till revisorerna. I PM:et bedömdes att de nya kommungemensamma riktlinjerna lever upp till revisorernas rekommendationer.

Processbeskrivningen är enligt uppgift en tjänstemannaprodukt och antogs därför inte formellt av personalutskottet. Den har vid tillfället för den uppföljande granskningen uppdaterats och uppdateras i samband med granskningen ånyo. Den sprids enligt uppgift till berörda parter genom att HR-specialist tar kontakt med alla kontorschefer och informerar om riktlinjerna och processbeskrivningen.

4.4 Slutsatser

Vi bedömer att de åtgärder som centralt vidtagits med anledning av revisorernas rekommendationer är tillräckliga och bör fungera som övergripande formell ram för kontroll av bisysslor. Vi uppfattar det dock som otydligt vilken status kommunens processbeskrivning för hantering av bisysslor har. Därmed är det också otydligt vem som ansvarar för att informera respektive informera sig om eventuella revideringar av processbeskrivningen.

Mot bakgrund av detta lämnas följande rekommendation till Kommunstyrelsen:

- Fastställ vilken status processbeskrivningen för hantering av bisysslor har samt besluta om vilken funktion som ansvarar för att informera eller informera sig om eventuella revideringar av processbeskrivningen.

Källförteckning

Granskning av hantering av bygglov
Revisionsrapport nr 7/2011 – Granskning av bygglov
§38 Revisionsrapport nr 7/2011 – Granskning av bygglov, Stadsbyggnadsnämndens sammanträdesprotokoll 2012-02-08 samt tjänsteutlåtande i ärendet.
Mätpunkter_mall (excelfil för mätning av handläggningstid av bygglovsärenden)

Granskning av IT- och informationssäkerhet
Revisionsrapport nr 2/2012 – Granskning av IT- och informationssäkerhet.
§ 276 Revisionsrapport nr 2/2012 – Granskning av IT- och informationssäkerhet, Kommunstyrelsens sammanträdesprotokoll 2012-12-14 samt tjänsteutlåtande i ärendet.

Changeprocessen. IT-enheten, Kommunstyrelsens kontor. 2014-09-25
Beställningsprocessen. IT-enheten, Kommunstyrelsens kontor. 2014-07-21
Riktlinjer för behörighetshantering. Stadsdirektörens kansli. 2013-04-15
Uppföljning av riktlinjer för informationssäkerhet. Stadsdirektörens kansli. 2013-04-15
Inköp av IT-system. Riktlinjer upphandling och avtalsförlängning av IT-system

Granskning av hantering av bisysslor
Revisionsrapport nr 8/2011 – Granskning av bisysslor
§79 Yttrande över Revisionsrapport nr 8/2011 – Granskning av bisysslor, Socialnämndens sammanträdesprotokoll 2012-04-17 samt handlingar i ärendet.
§86 Yttrande över Revisionsrapport nr 8/2011 – "Granskning av bisysslor", Stadsbyggnadsnämndens sammanträdesprotokoll 2012-04-24 samt handlingar i ärendet.
§97 Revisionsrapport nr 8/2011 – Granskning av bisysslor, Kommunstyrelsens sammanträdesprotokoll 2012-04-20 samt handlingar i ärendet.

Revisionsrapport nr 5/2012 – Hantering av bisysslor
§27 Riktlinjer för hantering av bisysslor, Personalutskottets protokoll 2013-04-25 samt handlingar i ärendet.
§96 Yttrande över Revisionsrapport nr 5/2012 – Hantering av bisysslor, Kommunstyrelsens sammanträdesprotokoll 2013-04-26 samt tjänsteskrivelse i ärendet.

Intervjumall – chef
Intervjumall – medarbetare
Processbeskrivning/Anvisningar för granskning, dokumentation och uppföljning av bisysslor