Granskning av kommunens IT-säkerhet 2017

KOMMUNREVISIONEN

NORRKÖPING

NORRKÖPING

Kommunrevisorerna

REVISIONSSKRIVELSE 1(1)

2017-12-13

KR-2017/0039

Kommunstyrelsen

Granskning av kommunens IT-säkerhet

Kommunrevisionen har genomfört en fördjupningsgranskning av kommunens IT-säkerhet. Det övergripande syftet med granskningen är att översiktligt följa upp 2013 års revision samt att bedöma om kommunen har en sammanhållen styrning och kontroll över webbaserade verktyg.

Den sammantagna bedömningen är att kommunstyrelsen behöver ta ett samlat och strategiskt ansvar omkring informationssäkerhet. Även en strategi för e-tjänster (en digitaliseringsstrategi) behöver utvecklas. Den interna styrningen och kontrollen inom IT-säkerhetsområdet behöver förbättras. Kommunstyrelsen bör ta ansvar för att ett ledningssystem för informationssäkerhet utarbetas samt ta fram en plan för hur kommunens digitaliseringsarbete ska bedrivas.

Med anledning av rapporten vill vi ha ett skriftligt svar på följande:

- Hur avser kommunstyrelsen att säkerställa den interna styrningen och kontrollen avseende IT-säkerhet?
- Hur tänker kommunstyrelsen arbeta för ett samlat och strategiskt ansvar omkring informationssäkerhet i kommunen?
- Hur tänker kommunstyrelsen arbeta för ett samlat och strategiskt ansvar omkring digitaliseringsarbetet?

Vi vill ha kommunstyrelsens skriftliga svar senast den 23 mars 2018.

KOMMUNREVISIONEN
2017-12-13

Eva Andersson
Vice ordförande för revisorerna

Postadress
Norrköpings kommun
Kommunrevisionen
601 81 Norrköping

Besöksadress
Dalsgatan 14

Telefon
011-15 17 99

Telefax
011-15 17 90

E-post
revisionskontoret@norrkoping.se
Internet
www.norrkoping.se/revision

NORRKÖPING

Revisionskontoret

2017-12-13
KR 2017/0039

Granskning av kommunens IT-säkerhet

Innehållsförteckning

Postadress
Norrköpings kommun
Kommunrevisionen
Dalsgatan 14
601 81 Norrköping

Besöksadress
Dalsgatan 14

Telefon
011-15 00 00

Telefax
011-15 17 90

E-post
revisionskontoret@norrkoping.se
Internet
www.norrkoping.se/revision

1. Sammanfattning

Revisorerna i Norrköpings kommun har gett ett uppdrag att granska kommunens IT säkerhet. Det övergripande syftet med granskningen är att översiktligt följa upp 2013 års revision samt att bedöma om kommunen har en sammanhållen styrning och kontroll över webbaserade verktyg.

Granskningen är genomförd med hjälp av dokumentstudier och intervjuer. Två webbaserade verktyg har ingått i studien och medarbetare som använder dessa vid utbildningskontoret, bygg- och miljökontoret samt stadsplaneringskontoret har intervjuats. De två verktygen är Reachmee och Easyresearch, vilka även är molntjänster. Totalt har 20 personer intervjuats.

Den sammantagna bedömningen är att kommunstyrelsen behöver ta ett samlat och strategiskt ansvar kring informationssäkerhet. Det inkluderar samtliga områden som denna revisionsrapport berör: styrning och ledning av informationssäkerhet, kontinuitetsplaner, förändringshantering, behörighetsadministration samt styrning av leverantörer. Även en strategi för e-tjänster (en digitaliseringsstrategi) behöver utvecklas.

Den interna styrningen och kontrollen inom IT-säkerhetsområdet behöver förbättras. Flera av riktlinjerna och rutinerna som gäller för IT-säkerhet saknar diarienummer, vilket bör åtgärdas omgående.

Kommunstyrelsen bör ta ansvar för att ett ledningssystem för informationssäkerhet utarbetas samt ta fram en plan för hur kommunens digitaliseringsarbete ska bedrivas

2. Inledning

2.1. Bakgrund

Revisorerna i Norrköpings kommun har genom sin granskning och i olika sammanhang identifierat att den interna styrningen och kontrollen inom kommunstyrelsen brister. I revisionsplanen för 2017 har revisorerna identifierat ett behov av att följa upp en tidigare IT säkerhetsgranskning från 2013. Vid tillfället framgick att det fanns brister i krav på de system som förvaltas och driftas i kommunen, att utbildningar av informationssäkerhet behöver ske regelbundet samt att avslut i systemen när medarbetare slutar brast. Det kan även finnas en risk för att IT-säkerheten kan brista om lösenord och inloggningar ger access till kommunala verktyg till personer utanför organisationen.

I kommunstyrelsens svar till revisorerna framgick att flera områden skulle ses över och att en IT- och informationssäkerhetsansvarig skulle anställas. Fler av de brister som identifierats skulle därmed undanröjas. Revisorerna har därför beslutat om att genomföra en uppföljning av hur detta arbete fortlöpt samt en översyn av hur styrningen och förvaltningen av gemensamma verktyg fungerar. Detta är särskilt angeläget när kommunen erbjuder allt fler e-tjänster.

2.2. Syfte och revisionsfrågor

Det övergripande syftet med granskningen är att översiktligt följa upp 2013 års revision samt att bedöma om kommunen har en sammanhållen styrning och kontroll över webbaserade verktyg.

Granskningen ska besvara följande revisionsfrågor:

- På vilket sätt har kommunstyrelsen reglerat ansvar i avtal vad gäller IT-säkerhet mot tredje part?
- Vilka rutiner finns för hur programförändringar och uppdateringar ska genomföras?
- Finns en kontinuitetsplan för hela organisationen?
- Vilka internkontroller görs av informationssäkerheten? (åtkomsträttigheter, avslut/förflyttning, regler för distansarbete och brandväggspolicy)
- Hur sker styrning och kontroll av IT-baserade verktyg?
- Har kommunstyrelsen en tydlig och kommunicerad strategi för e-tjänster?

2.3. Revisionskriterier

De bedömningsgrunder som bildar underlag för granskningens analyser, slutsatser och bedömningar bygger på:

- Kommunallagen (Kap 6:7 som reglerar nämndernas ansvar)
- Lag om offentlig upphandling (2007:1091)
- Förbundsöverenskommelse (KS-833/2012)
- Riktlinje för intern styrning och kontroll (KS 2015/0144)
- Riktlinje för upphandlingar och inköp (KS 2013/0644)

2.4. Metod och avgränsning

Ansvarig sakkunnig har tillsammans med konsult från PwC genomfört granskningen genom dokumentstudier och intervjuer. Intervjuer har skett genom huvudsakligen fysiska möten, men även med hjälp av telefonintervju. Totalt har 20 intervjuer genomförts varav 16 är fysiska möten och 4 är telefonintervjuer. Granskningen omfattar kommunstyrelsen, men i syfte att bedöma hur styrning och strategier fungerar i praktiken har intervjuer skett med medarbetare vid stadsbyggnadskontoret, utbildningskontoret samt bygg- och miljökontoret. Två IT baserade verktyg har varit föremål för granskningen utifrån användning och säkerhet, det är rekryteringsverktyget Reachmee och enkätverktyget Easyresearch.

Ett utkast av granskningsrapporten har faktagranskats av de intervjuade.

2.5. Prövning av oberoende och integritet

Sakkunniga har i enlighet med Skyrevs[1] rekommendation nummer två prövat sitt oberoende.

2.6. Kvalitetssäkring

Denna rapport är sakgranskad, vilket innebär att de fakta som rapporten hänvisar till är kvalitetssäkrade av de som granskats. Rapporten är även kvalitetssäkrad enligt Skyrevs regler vid revisionskontoret.

[1] Skyrev är yrkesförening för sakkunniga revisorer i kommunal sektor.

3. Viktiga begrepp

Ledningssystem för informationssäkerhet

Systematiskt arbete med informationssäkerhet i enlighet med ISO27001:2014 – Ledningssystem för informationssäkerhet. Kommunen kan med fördel hämta inspiration från Myndigheten för Samhällsberedskaps skrivelse ”Kommunens informationssäkerhet – en vägledning[2]”

Kontinuitetsplan

Kontinuitetsplaner syftar till att säkerställa att en organisation har effektiva processer som stöd för att motverka avbrott i verksamheten. Planen bör inkludera alternativa rutiner för hur verksamheten kan bedrivas om t.ex. IT-system eller lokaler inte är tillgängliga, roller och ansvar, kontaktuppgifter till relevant personal inom och utom verksamheten som planen gäller för, kommunikationsplan samt plan för att återställa verksamheten efter att avbrottet är avhjälpt.

GDPR – General Data Protection Regulation

EUs nya dataskyddsförordning som träder i kraft 25 maj 2018 innebär bland annat hårdare krav på hantering av personuppgifter. Det kommer att ställas krav på nya rutiner och processer för säker hantering av register samt krav på ansvarig på ledningsnivå. Nya dataskyddsförordningen kommer att gälla för alla organisationer och branscher som sparar eller på något sätt hanterar personlig och känslig information om sina anställda eller medborgare. Datainspektionen[3] är tillsynsmyndighet för förordningen.

[2] https://www.msb.se/RibData/Filer/pdf/26420.pdf
[3] http://www.datainspektionen.se/dataskyddsreformen/

4. Iakttagelser

I det följande presenteras våra iakttagelser utifrån de revisionsfrågor vi undersökt.

4.1. På vilket sätt har kommunstyrelsen reglerat ansvar i avtal vad gäller IT-säkerhet mot tredje part?

I riktlinjen för upphandling och inköp framgår att verksamheterna kan anlita Upphandlingscenter för olika typer av upphandlingar och inköp. Målet är att uppnå en effektiv upphandlingsprocess. I riktlinjen framgår det att avtalen ska följas upp med avseende på leverantörens prestationer exempelvis avseende kvalitet, volym och pris.

Upphandling sker i enlighet med den riktlinje för upphandlingar som fullmäktige fastställt och Upphandlingscenter involveras, enligt de intervjuade. Det är den enskilda verksamheten som är ägare till det upphandlade systemet. Som exempel kan nämnas att kommunstyrelsen genom personalavdelningen är systemägare till rekryteringsverktyget ”Reachmee” och de är även ägare till enkätverktyget ”Easyresearch” genom ekonomi och styrningsavdelningen. IT enheten involveras av den upphandlande enheten i kravställning på programmet genom informationsklassing och säkerhetsklassning av systemet som ska upphandlas.

Fler av de intervjuade nämner att vid upphandling av nya system finns en uppfattning att kommunen inte tillåter upphandling av molntjänster. Det framgår trots det att flera molntjänster finns bland de upphandlade systemet t ex Reachmee (rekryteringsverktyg) och Raindance (ekonomisystem).

I de tecknade avtalen framgår det inte om kommunen har rätt att granska den upphandlade leverantören. Däremot uppger fler av de intervjuade att de följer upp avtalen.

I en intern rutin vid IT enheten regleras avtal om tystnadsplikt samt personalkontroller för vissa mer känsliga roller och funktionen vid enheten. Rutinen fastställdes 2016-08-31 av chefen för enheten, säkerhetsansvarig vid kommunen samt IT-säkerhetsansvarig. I rutinen framgår att även extern personal som arbetar på uppdrag av kommunen och som kan komma i kontakt med känsliga uppgifter i samband med support och service av system omfattas av rutinen. Ett antal bakgrundskontroller ska göras av lämplighet för rollen, av finansiell lämplighet samt legalt lämplig. Detta innebär att kontroller görs i kronofogdens register, polisens belastningsregister liksom lämplighet i övrigt.

Revisionsbedömning

Kommunen använder sig av molntjänster trots att det upplevs finnas ett principbeslut att all IT ska hanteras internt av IT-enheten. Revisionen bedömer att det finns brister i hur kommunen har formaliserat arbetet med att upphandla och styra leverantörer. Vår bedömning är att kommunen saknar dokumenterade rutiner för hur leverantörer ska riskklassas och följas upp i enlighet med klassningens fastställda principer. Klassningen bör t ex beakta typ av information som leverantören har tillgång till, typ av tjänst som levereras samt komplexitet av den tjänst som tillhandahålls. Rutinerna bör beakta traditionella tjänster och molnbaserade tjänster.

4.2. Vilka rutiner finns för hur programförändringar och uppdateringar ska genomföras?

Vid IT-enheten finns en processbeskrivning för ändringshantering, fastställd 2017-09-04. Dokumentet fungerar som en processhandbok och syftet är att effektivisera verksamheten, minska personberoendet och risken för missförstånd, höja kvaliteten, skapa tydlighet mot kunderna, öka kontrollen över förändringsbehoven, öka produktiviteten samt få bättre riskanalyser. I processbeskrivningen framgår rollfördelningen med befogenheter och ansvar inom ändringsprocessen. Som ärendehanteringssystem används programmet ”Easit”.

I intervjuer framgår att programförändringar och uppdateringar ska gå igenom den sk ”Change processen”.

Revisionsbedömning

IT-enheten följer den etablerade processbeskrivningen för förändringshantering som också är en del av förvaltningsmodellen PM3. PM3 är en etablerad modell för att säkerställa en affärsmässig styrning av IT och används av en mängd privata och offentliga organisationer.

Vi bedömer att IT-enheten har etablerat ett arbetssätt avseende programförändringar som följer god praxis för en majoritet av kommunens IT-miljö. IT-enheten bör fortsätta arbetet med införande av förvaltningsmodellen PM3 och inkludera flera applikationer i detta arbetssätt.

Sammanfattningsvis så bedömer revisionen att kommunen har etablerade rutiner för programförändringar och uppdateringar på plats för en större del av IT-miljön.

4.3. Finns en kontinuitetsplan för hela organisationen?

Någon kommunövergripande kontinuitetsplan finns inte, enligt intervjuer. Enligt uppgift pågår ett arbete i samarbete med länsstyrelsen inom ramen för krisberedskap och vård-och omsorgskontoret är först ut, därefter kommer utbildningskontoret. Det är även upp till varje verksamhet att avgöra hur väl de klarar ett avbrott i IT leveranserna, enligt intervjuer.

Enligt de intervjuade så har kommunen redundanta datahallar för drift av kommunens IT-miljö. De redundanta datahallarna etablerades efter att en brand bröt ut i UPS-rummet för några år sedan. De intervjuade beskriver också att rutinerna för att växla mellan de två datahallarna inte fullt ut är dokumenterade och testade.

Revisionsbedömning

Arbetet med att etablera kontinuitetsplaner för delar av kommunens verksamhet är påbörjat, vilket revisionen bedömer som positivt. IT-enheten bör även fokusera på att etablera rutiner för hantering av avbrott i IT-miljön. Arbetet bör fokuseras på hur driften av IT-miljön kan växlas över mellan de två datahallarna genom att ta fram en så kallad ”disaster recovery plan”. Planen bör synkroniseras med de tillgänglighetskrav som verksamheterna ställer på sitt IT-stöd.

Vi bedömer att kommunen bör fortsätta arbetet med att etablera kontinuitetsplaner för verksamheten. För IT-enheten bör en formaliserad rutin för kontinuitetsplanering avseende IT-miljön etableras.

Sammanfattningsvis kan revisionen konstatera att en kontinuitetsplan för kommunens hela verksamhet inte finns på plats, men att arbetet med att etablera planer för delar av verksamheten är påbörjat. Kommunen rekommenderas att ta fram en övergripande plan för hur arbetet med att utarbeta kontinuitetsplaner ska prioriteras.

4.4.Vilka internkontroller görs av informationssäkerheten?

Från intervjuerna framgår att det saknas en IT strategi för kommunen, behovet av en samordning kopplat till kommunstyrelsen har lyfts av flertalet intervjuade. IT-enheten fungerar som en driftsavdelning i hög grad och i mindre grad finns de strategiska frågorna på enheten, enligt intervjuer.

Det är systemförvaltningarna som delar ut och avgör behörigheter till systemen efter beslut av chef i flertalet system. För systemen Reachmee och Easyresearch är det systemägaren som delar ut och avgör behörigheter till systemen. Ofta är systemägaren kontorschef eller verksamhetschef på det kontor som är i behov av det aktuella programmet/verktyget. I de aktuella system vi granskat är det möjligt att en individ kan ha samma lösenord under flera år. Det är upp till systemägaren att bestämma när och om byte av lösenord ska ske.

Vid IT-enheten finns en rutin för inventering och klassning av informationstillgångar i kommunen. Den är fastställd 2014-04-22 av säkerhetsansvarig chef vid IT-enheten. Det finns även en övergripande riktlinje för sårbarhetsskanning fastställd 2016-07-29 av säkerhetsansvarig chef vid IT-enheten.

Det är stadsjuristen som arbetar med kommunens införande och anpassning till den nya dataskyddsförordningen, GDPR. En checklista har skickats ut till systemägare inför införandet.

Revisionsbedömning

Vår bedömning är att kommunen saknar ett formaliserat arbete med informationssäkerhet. Arbetet bör struktureras i ett ledningssystem för informationssäkerhet. Ledningssystemet bör etableras på kommunledningsnivå och en struktur med styrande dokument, roller och ansvar och riskbedömningar bör etableras inom hela kommunen. Ledningssystemet bör utgå från gällande standard på området, ISO27001:2014 – Ledningssystem för informationssäkerhet.

Kommunen bör använda den nya dataskyddsförordningen som en drivkraft vid införandet av ett ledningssystem för informationssäkerhet.

Sammanfattningsvis kan revisionen konstatera att kommunen saknar en god intern kontroll avseende informationssäkerhet. Kommunen bör snarast initiera ett arbete med att etablera ett ledningssystem för informationssäkerhet. Den rekrytering som nu sker av en informationssäkerhetsstrateg möjliggör ett mer aktivt arbete med ledningssystem för informationssäkerhet i kommunen.

4.5.Hur sker styrning och kontroll av IT-baserade verktyg?

För åtkomsten till systemen är det den enhet som upphandlat verktyget som har åtkomsten. Det är systemägaren (objektägaren) som tilldelar behörigheter till systemen. I allmänhet följer behörigheten till system det sk dei/nrk nummer som varje medarbetare och förtroendevald i kommunen får vid anställning och/eller uppdrag. Dessa är unika och identifierar varje person. Vid tjänstens och/eller uppdragets avslut ska även behörigheter och åtkomst avslutas till alla applikationer. Det förekommer dock att behörigheter och åtkomsträttigheter funnits kvar lång tid efter att anställningen och/eller uppdraget avslutats, enligt de intervjuade.

Revisionsbedömning

Vår bedömning är att det saknas dokumenterade rutiner för hur behörighet ska hanteras inom kommunen. Principer för styrning av behörighet kan med fördel inkluderas i införandet av ett ledningssystem för informationssäkerhet.

4.6. Har kommunstyrelsen en tydlig och kommunicerad strategi för e-tjänster?

Vi har inte fått del av någon nedskriven strategi för e-tjänster. Fler av de intervjuade uppger att de saknar en tydlig strategi för området och att det blir rörigt i organisationen när en sådan saknas. De intervjuade beskriver att e-tjänster organisatoriskt hanteras av kommunikationsenheten inom kommunen.

Det finns ett avtal avseende utveckling av e-tjänster mellan kommunen och sex andra kommuner i Östergötland. Parterna i avtalet samverkar om e-tjänsteutveckling i samverkansform Cesam Öst. Något formellt beslut inom Norrköpings kommun som stödjer denna samverkan vad gäller e-tjänster har vi inte funnit.

Revisionsbedömning

Vår bedömning är att e-tjänster bör hanteras på högsta kommunledningsnivå då e-tjänster påverkar kommunens alla verksamheters möjligheter att leverera elektroniska tjänster till medborgarna. E-tjänster handlar inte bara om att presentera erbjudanden på en webbplats utan om att omforma kommunens traditionella verksamheter till en mer modern digital mötesplats för kommunens invånare där så är möjligt. En sådan omstöpning av verksamheter kräver långtgående involvering från kommunens ledning, IT-enheten samt kontor över en länge tid och på ett strukturerat sätt. Den pågående rekryteringen till den nyinrättade tjänsten som digitaliseringsdirektör vid kommunstyrelsens kontor, är därför positiv.

En granskning av Cesam Östs roll kopplat till kommunens strategi för e-tjänster på kort och lång sikt föreslås.

5. Slutsatser och samlad bedömning

Den sammantagna bedömningen är att kommunstyrelsen behöver ta ett samlat och strategiskt ansvar kring informationssäkerhet. Det inkluderar samtliga områden som denna revisionsrapport berör: styrning och ledning av informationssäkerhet, kontinuitetsplaner, förändringshantering, behörighetsadministration samt styrning av leverantörer. Även en strategi för e-tjänster (en digitaliseringsstrategi) behöver utvecklas.

Den interna styrningen och kontrollen inom IT-säkerhetsområdet behöver förbättras. Flera av riktlinjerna och rutinerna som gäller för IT-säkerhet saknar diarienummer, vilket bör åtgärdas omgående.

Kommunstyrelsen bör ta ansvar för att ett ledningssystem för informationssäkerhet utarbetas samt ta fram en plan för hur kommunens digitaliseringsarbete ska bedrivas.

REVISIONSKONTORET

Caroline Nyman
Stadsrevisor

Magnus Sjölander
PwC