§ 28 Dnr KS/2016:389

Slutredovisningen av internkontroll 2017, KSF

Bakgrund
Mjölby kommun upprättar årligen olika former av internkontroll. Några delar är kommungemensamma och några är förvaltningsspecifika.

Sammanfattning
Kommunstyrelsens förvaltning hade under 2017 två kommungemensamma kontrollpunkter och två förvaltningsspecifika.

1. Krishantering (kommungemensamt)
2. Inköp (kommungemensamt)
3. Process för utgivning av SITHS-kort
4. Säker IT-infrastruktur och system

Kommunstyrelsens förvaltning har sett över sin krisplan så att roller, bemanning och uppgifter har tydliggjort. Kommunens avtalstrohet har kontrollerats och det finns en god följsamhet för att följa upphandlade ramavtal. Båda kommungemensamma kontrollmomenten kommer att följas upp gemensamt för samtliga förvaltningar.

Processen för utgivning av SITHS-kort fungerar som den ska och de kontroller som genomförts visar att allt sker enligt gällande regelverk.

Säker IT-infrastruktur och system, kommunens revision genomförde en granskning och det upptäcktes brister. Flera av bristerna är åtgärdade men arbetet pågår att åtgärda de kvarvarande delarna.

Beslutsunderlag
Missiv 2018-01-30
Uppföljning av interkontrollplan 2017 för kommunstyrelsens förvaltning.
Summering/svar avseende IT-säkerhet

Arbetsutskottets förslag till kommunstyrelsen

1. Kommunstyrelsen godkänner slutredovisningen av interkontrollen 2017, kommunstyrelseförvaltningen.

___

Beslutet skickas till:
Kommunstyrelsen
Akten

Mjölby Kommun
Kommunstyrelsens förvaltning

Missiv

Datum
2018-01-30

Diarienummer
KS/2016:389

Handläggare
Carina Brofeldt
Tfn 0142-851 56

Kommunstyrelsen

Uppföljning av internkontrollplan 2017, kommunstyrelsens förvaltning

Bakgrund
Mjölby kommun upprättar årligen olika former av internkontroll. Några delar är kommungemensamma och några är förvaltningsspecifika.

Sammanfattning
Kommunstyrelsens förvaltning hade under 2017 två kommungemensamma kontrollpunkter och två förvaltningsspecifika.

1. Krishantering (kommungemensamt)
2. Inköp (kommungemensamt)
3. Process för utgivning av SITHS-kort
4. Säker IT-infrastruktur och system

Kommunstyrelsens förvaltning har sett över sin krisplan så att roller, bemanning och uppgifter har tydliggjort. Kommunens avtalstrohet har kontrollerats och det finns en god följsamhet för att följa upphandlade ramavtal. Båda kommungemensamma kontrollmomenten kommer att följas upp gemensamt för samtliga förvaltningar.

Processen för utgivning av SITHS-kort fungerar som den ska och de kontroller som genomförts visar att allt sker enligt gällande regelverk.

Säker IT-infrastruktur och system, kommunens revision genomförde en granskning och det upptäcktes brister. Flera av bristerna är åtgärdade men arbetet pågår att åtgärda de kvarvarande delarna.

Beslutsunderlag
Missiv 2018-01-30
Uppföljning av interkontrollplan 2017 för kommunstyrelsens förvaltning.
Summering/svar avseende IT-säkerhet

Kommunstyrelsens förvaltnings förslag till beslut

Kommunstyrelsen godkänner slutredovisningen av interkontrollen 2017, kommunstyrelseförvaltningen.

Missiv

Datum
2018-01-30

Diarienummer
KS/2016:389

___

Beslutet skickas till:
Kommunstyrelsen
Akten

Kommunstyrelsens förvaltning

Carina Brofeldt
Bitr. kommundirektör

Mjölby Kommun
Kommunstyrelsens förvaltning

Tjänsteskrivelse

Datum
2018-01-17

Diarienummer
KS/2016:389

Handläggare
Carina Brofeldt
Tfn 0142-851 56

Till kommunstyrelsen

Uppföljning av internkontrollplan år 2017 för kommunstyrelsens förvaltning.

Sammanfattning
En uppföljning sker av de punkter som återfinns i kommunstyrelsens förvaltnings egna internkontrollplan för år 2017. En separat uppföljning sker av det samlade resultatet av de kommungemensamma internkontrollmomenten.

Det kan konstateras att resultatet av granskningen visar att så gott som alla processer fungerar tillfredställande. Resultatet av kontrollen av förvaltningens krisplan intygar att planen är uppdaterad samt att samtliga medarbetare har fått information om krisplanens innehåll. Ekonomiavdelningens kontroll av ramavtal för kontorsmaterial och kopieringspapper visar att avtalstroheten mot avtalen är god. De två kontroller som genomförts avseende administrationen av SITHS- kort visar att regelverket följs, inga brister framkom. Slutligen har en extern säkerhetsgranskning av kommunens IT-infrastruktur och system genomförts. Vissa brister framkom. En åtgärdsplan har tagits fram. Några åtgärder är vidtagna, andra pågår fortfarande.

Bakgrund
Följande kontrollpunkter återfinns i Kommunstyrelsens förvaltnings internkontrollplan för år 2017:

1. Krishantering (kommungemensamt)
2. Inköp (kommungemensamt)
3. Process för utgivning av SITHS-kort
4. Säker IT-infrastruktur och system

Resultatet av de kommungemensamma internkontrollmomenten för år 2017 redovisas separat till kommunstyrelsen. Här redovisas endast förvaltningens egna internkontrollarbete.

1. Krishantering
Kontrollmomentet har bestått i att kontrollera att förvaltningens krisplan är uppdaterad. Den första kontrollen visade på att det fanns ett behov av att revidera förvaltningens krisplan. Med stöd av säkerhetssamordnaren arbetade kommunstyrelsens ledningsgrupp igenom dokumentet. Det resulterade bl a i ett förtydligande av krisgruppens roller, uppgifter, bemanning av roller och hur krisgruppen aktiveras. En genomgång av krisplanen gjordes med alla medarbetare under hösten 2017. Nu pågår ett arbete med att resp avdelning ser över behovet av egna kompletterande rutiner inom området. Under år 2018 kommer en övning att genomföras.

Datum Diarienummer

2. Inköp

Kontrollmomentet har bestått i att undersöka om förvaltningen följer avtalstrohet mot ramavtal vid inköp. Ekonomiavdelningen genomförde under året en kontroll avseende ramavtal för kontorsmaterial och kopieringspapper. Motivet till urvalet är att ekonomiavdelningen tidigare genomfört motsvarande kontroll på de utvalda avtalen. Kontrollen visar att avtalstroheten mot avtalen är god och att följsamheten mot avtalet för kontorsmaterial har förbättrats jämfört med tidigare kontroll.

3. Process för utgivning av SITHS-kort

Kontrollmomentet har bestått i att undersöka att de personer som fått SITHS-kort har uppnått kraven för dem. Sammanlagt har två kontroller genomförts avseende administrationen av SITHS- kort. Den första kontrollen ägde rum i slutet av maj och avsåg rutinen ”Utfärdande av SITHS-kort”. Kontrollen visade att utfärdandet genomfördes enligt rutin. Den andra kontrollen genomfördes i november gällande rutinen ” Utgivning av SITHS kort”. Även denna kontroll visade att rutinen följdes av handläggaren. Sammanfattningsvis kan konstateras att gällande regelverk följs, inga brister identifierades. Processen fungerar tillfredsställande.

4. Säker IT-infrastruktur och system

PwC har genomfört en säkerhetsgranskning. Bristerna som upptäcktes är av varierande dignitet och risk. En del av dem innebär en hög risk men kan ändå åtgärdas med enkla medel. Vissa åtgärder är redan vidtagna såsom uppdatering av servrar där 6 av 110 st var eftersatta, lösenordshantering där samma lösenord förekom och oavslutade fjärrsessioner är åtgärdade. Andra kräver större arbetsinsats och tar längre tid att implementera. Åtgärder pågår för att hantera de kvarstående delarna.

Kommunstyrelsens förvaltning

Carina Brofeldt
Bitr kommunchef

Postadress	Besöksadress	Telefon	Internetadress	Bankgironummer
Mjölby kommun	Burensköldsvägen 11-13	0142 - 850 00	www.mjolby.se	791-9848
Kommunstyrelsens förvaltning		Telefax	e-postadress	
595 80 MJÖLBY		0142-851 20	kommunstyrelsen@mjolby.se	

Mjölby Kommun
Kommunstyrelsens Förvaltning
IT-Avdelningen

Sammanfattning PwC säkerhetsgranskning

Datum
2017-09-05

Diarienummer

Handläggare
Markus Andersson/John JM Prpic

Sammanfattning av PwC säkerhetsgranskning 2017 Mjölby kommun

Bakgrungd

PwC har på uppdrag av Mjölby kommun genomfört en teknisk säkerhetsgranskning under juni månad 2017. För att granskningen skulle vara så reell som möjligt var ingen personal informerad om när och hur. Personerna som genomförde granskningen hade som utgångspunkt tillgång till ett vanligt användarkonto samt nätaccess. Granskningen med tillhörande tester utfördes i IT-avdelningens lokaler. Testerna och scenariona var utformade för att efterlikna reella hotbilder. Verktyg som användes är lättillgängliga och är välkända. Målet var att få tillgång till och kunna ändra information, alternativt att störa systemens tillgänglighet.

Nätverk

I nätverket är det framförallt områdena nätverksaccess och nätsegmentering där man bedömer att det finns svagheter och brister. Nätaccess erhålls i dagsläget utan autentisering då en klient ansluts till det trådburna nätverket. Nätsegmentering innebär att accessen mellan t.ex. servernäten och klientnäten bör stärkas upp. Servrar exponeras i för stor utsträckning mot klienter vilket innebär en ökad säkerhetsrisk.

Antivirus, uppdateringar och föråldrad version av operativsystem

Uppdateringar på vissa servrar var inte fullständiga vilket kan innebära säkerhetsrisker(6 av 110 servrar). Även brister i antivirusprogramvaran på både klient och server påvisas då viss skadlig kod inte detekteras. Brister i uppdateringsnivå och antivirus resulterar ofta i samma typ av säkerhetsbrister. PwC påvisade exempel som pekar på att det går exekvera skadlig kod och på så sätt ta över system. Datorer med föråldrat operativsystem som inte längre stöds av tillverkaren vad gäller säkerhetspatchar påträffades. Säkerhets rutiner kring användning av dessa kräver särskilda åtgärder.

Lösenord, användarkonton och fjärrsessioner

Policyn och rutinen för lösenord bör ses över vad gäller både system och användarkonton. PwC påvisade fall där lösenord var enkla att gissa (t.ex. Sommar2017). Även användning av samma lösenord för en del servrar och system förekom. Det påträffades även system där standardlösenordet inte blivit utbytt. PwC stötte på servrar där det fanns öppna fjärrstyrningssessioner vilket kan leda till att någon kan ta över den och få tillgång till servern och dess data. I några av kommunens externt publicerade resurser saknades spärr för låsningsmekanism av kontot vid upprepade felaktiga inloggningsförsök.

Övervakning och loggning

Under revisionen utfördes olika typer av attacker. PwC kunde genomföra vissa typer utan att övervakningssystemen larmade. Exempel på sådan typ av attack kan vara gissning av lösenord vilket så småningom leder till att kontot låses. Vid låsning av konton som används av system och tjänster kan detta leda till avbrott i driften.

Summering

Det bör tillägas att PwC fick anslutning till samma nätverk som IT-avdelningens anställda. Det nätverket har högre accessrättigheter till de övriga näten vilket också bör tas i beaktning. Bristerna som upptäcktes är av varierande dignitet och risk. En del av dem innebär en hög risk men kan ändå åtgärdas med enkla medel. Vissa åtgärder är redan vidtagna såsom uppdatering av servrar där 6 av 110st var eftersatta, lösenordshantering där samma lösenord förekom och oavslutade fjärrsessioner är åtgärdade. Andra kräver större arbetsinsats och tar längre tid att implementera. Åtgärder för att ta till oss av utfallet är nu under skapande med tidsatta aktiviteter