Deloitte.

JÖNKÖPINGS KOMMUN

Stadsbyggnadsnämnden
Granskning intern kontroll

Jönköpings kommun

September 2014
Torbjörn Bengtsson, Pernilla Lihnell, Jenny Lundin och Louise Abrahamsson

Innehåll

Sammanfattning

Deloitte har av Jönköpings kommuns förtroendevalda revisorer fått i uppdrag att utföra en granskning av den interna kontrollen inom stadsbyggnadsnämnden.

Nämndernas uppdrag är att säkerställa en ändamålsenlig styrning så att verksamheten bedrivs på ett effektivt sätt, att det finns säkra rutiner som förhindrar förluster och att redovisningen är rättvisande.

Mot denna bakgrund har vi granskat stadsbyggnadsnämndens arbete med intern kontroll.

Revisionsfråga

Den övergripande revisionsfrågan är:
Har stadsbyggnadsnämnden en ändamålsenlig intern kontroll?

Svar på revisionsfråga

Vår bedömning är att stadsbyggnadsnämndens interna kontroll inte är fullt ändamålsenlig.

Vår bedömning av resultatet av verifieringen är överlag att anses som förväntat och normalt, i jämförelse med vad andra organisationer uppvisar första gången verifiering sker.

Iakttagelser och rekommendationer

Vi har i vår granskning noterat ett antal iakttagelser. Utifrån våra iakttagelser har vi sedan ett antal rekommendationer. För iakttagelser som identifierats ”ej effektiva” och rekommendationer till dessa vänligen se avsnitt 5.

Vi särskilt lyfta fram behovet av att nämnden arbetar med en fullständig riskanalys som berör samtliga perspektiv och kritiska processer.

Jönköping den 23 september 2014

DELOITTE AB

Torbjörn Bengtsson
Certifierad kommunal revisor

Jenny Lundin
Auktoriserad revisor

1. Inledning

1.1 Bakgrund

Deloitte har av Jönköpings kommuns förtroendevalda revisorer fått i uppdrag att utföra en granskning av den interna kontrollen inom stadsbyggnadsnämnden.

Nämndernas uppdrag är att säkerställa en ändamålsenlig styrning så att verksamheten bedrivs på ett effektivt sätt, att det finns säkra rutiner som förhindrar förluster och att redovisningen är rättvisande.

Inom Jönköpings kommun finns centrala stödfunktioner som IT-avdelning, personalenhet och upphandlingsenhet. De gemensamma enheterna utgör en form av internt konsultativt och administrativt stöd för samtliga nämnder. De gemensamma policydokument och beslut som är fattade av kommunfullmäktige är nämnderna skyldiga att leva upp till. Oaktat de stöd som nämnderna får avseende IT, upphandling och personalfrågor är nämnderna fullt ut ansvariga för sin IT-verksamhet, upphandling samt personalhantering.

Intern kontroll kan övergripande definieras som en process. I processen samverkar såväl den politiska som den professionella ledningen samt medarbetare. Utformningen sker med en rimlig grad av säkerhet kunna uppnå följande mål:

- Ändamålsenlig och kostnadseffektiv verksamhet
- Tillförlitlig finansiell rapportering och information om verksamheten
- Efterlevnad av tillämpliga lagar, föreskrifter, riktlinjer m.m.

Intern kontroll syftar också till att verksamheten ska:

- Trygga tillgångarna
- Säkerställa att lagar efterlevs
- Minimera risker
- Säkra att resurser används enligt tagna beslut
- Säkra en rättvisande redovisning
- Skydda förtroendevalda och anställda från oberättigade misstankar

Lagstiftningen är väldigt tydlig avseende nämndernas ansvar för intern kontroll. I lagstiftningen framgår följande enligt kommunallagen 6 kap 7 §:

”Nämnderna skall var och en inom sitt område se till att verksamheten bedrivs i enlighet med de mål och riktlinjer som fullmäktige har bestämt, samt de föreskrifter som gäller för verksamheten. De skall också se till att den interna kontrollen är tillräcklig samt att verksamheten bedrivs på ett i övrigt tillfredsställande sätt. Detsamma gäller när vården av en kommunal angelägenhet med stöd av 3 kap 16 § har lämnats över till någon annan.”

Lagstiftningen är lika tydlig gällande revisorernas ansvar. Av kommunallagen 9 kap 9 § kan utläsas:

"….revisorerna prövar om verksamheten sköts på ett ändamålsenligt och från ekonomisk synpunkt tillfredsställande sätt, om räkenskaperna är rättvisande och om den interna kontrollen som görs inom nämnderna är tillräcklig…"

1.2 Syfte

Efter genomförd granskning ska Deloitte bedöma om stadsbyggnadsnämnden har en ändamålsenlig intern kontroll.

Deloitte skall även för iakttagelser som identifierats som "ej effektiva" ge förslag på förbättringsåtgärder/rekommendationer.

1.3 Revisionsfråga

Den övergripande revisionsfrågan är:
Har stadsbyggnadsnämnden en ändamålsenlig intern kontroll?

1.4 Metod

Vår granskning har baserats på ett formulär (en s.k. självdeklaration). Självdeklarationen är baserad på COSO-ramverket, vilket är det internationellt mest erkända ramverket för intern kontroll. Granskningen har genomförts i två steg.

I steg ett har nämnden fått svara på ett antal påståenden (självdeklaration) kring den interna kontrollen för ett antal utvalda områden/processer. Nämnden har även fått beskriva vilken dokumentation som finns på plats för att styrka påståendena.

I steg två har Deloitte genomfört en uppföljning, verifiering och utvärdering av nämndernas självutvärdering. Uppföljning och verifiering har genomförts genom intervjuer, stickprovskontroller samt dokumentstudier.

1.5 Avgränsningar

Våra bedömningar bygger på en övergripande verifiering av självdeklarationen. Självdeklarationen innehåller ett stort antal kontrollfrågor. Det har inte varit möjligt att utföra någon djupare analys av respektive kontrollfråga. Våra rekommendationer bygger på den begränsade information vi har tillgång till.

Rapporten baseras på underlag som är framtagna under och giltiga under år 2013. Förändringar som har skett under år 2014, har inte fått genomslag i hela verksamheten.

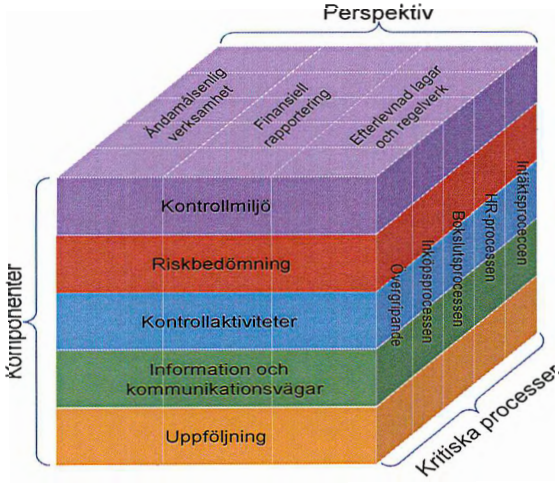
Vår återrapportering är en avvikelserapportering, vilket innebär att redan fungerande områden inte lyfts fram i samma utsträckning som eventuella brister och förbättringsområden.

I de fall där stickprovskontroll inte ingått som en del av utvärderingen bygger våra bedömningar på den information vi erhållit via intervjuer med utvalda personer av nämnden samt via dokumentation.

Vad gäller styrande dokument har verifieringen inte innefattat en djupare analys av dessa, exempelvis har kvaliteten i nämndens mål, strategier och verksamhetsplaner inte analyserats.

2. COSO-ramverket

Vårt arbete har baserats på ett formulär i form av en självdeklaration. Självdeklarationen är baserad på COSO-ramverket, vilket är det internationellt mest erkända ramverket för intern kontroll. COSO-ramverket bygger på ett strukturerat sätt att arbeta med intern kontroll och omfattar ett antal olika perspektiv, komponenter och kritiska processer.



COSO-ramverket är uppbyggt i tre olika perspektiv. Perspektiven verkar för att med rimlig grad av säkerhet uppnå;

- ändamålsenlig och kostnadseffektiv verksamhet
- tillförlitlig finansiell rapportering och information om verksamheten
- efterlevnad av tillämpliga lagar och regelverk

Vidare identifierar COSO-ramverket ett antal för den interna kontrollen väsentliga komponenter. Komponenterna är kontrollmiljö, riskbedömning, kontrollaktiviteter, information och kommunikation samt uppföljning. Alla fem komponenter är väsentliga för att den interna kontrollen ska vara effektiv. Nedan följer en beskrivning av komponenterna samt vilka områden respektive komponent berör.

Kontrollmiljön

- Hur påverkar organisationskulturen intern styrning och kontrollen?
- Vilka signaler får medarbetarna från ledningen om risk och kontroll?
- Hur ser ansvarsfördelningen ut för utvärdering och övervakning av den interna kontrollen?

Riskbedömning

- Hur kan ledningen förlita sig på att risker identifieras och värderas på ett enhetligt och riktigt sätt genom hela organisationen?

Kontrollaktiviteter

- Hur kan ledningen försäkra sig om att lämpliga kontrollaktiviteter utförs i tid, av rätta personer samt att dessa dokumenteras vid behov?

Information och kommunikation

- Hur säkerställa att rätt information når rätta personer i rätt tid?
- Hur kan ledningen informera sig om att verksamheten bedrivs effektivt och ändamålsenligt?

Uppföljning

- Sker utvärderingar och ständiga förbättringar?
- Hur sker löpande och särskild uppföljning?
- Hur hanteras signaler om brister i kontrollsystemet?

COSO-ramverket beskriver även vilka processer inom en organisation som berörs och är kritiska för den interna kontrollen. Exempel på väsentliga processer är; intäktsprocessen, HR-processen, bokslutsprocessen, inköpsprocessen samt övergripande processer. Dessa processer har en direkt koppling till komponenterna och målen inom intern kontroll och styrning.

3. Självdeklaration

I självdeklarationen finns ett antal kontrollfrågor. Varje kontrollfråga har också riskklassificerats i en skala från 1 till 3;

- **Riskkategori 1** har tilldelats kontrollfrågor med liten inverkan på det operativa, finansiella och/eller legala perspektivet.
- **Riskkategori 2** har tilldelats kontrollfrågor med medelstor inverkan på det operativa, finansiella och/eller legala perspektivet.
- **Riskkategori 3** har tilldelats kontrollfrågor med större inverkan på det operativa, finansiella och/eller legala perspektivet.

Syftet med denna klassificering har varit att få en nyanserad och rättvisande bild av den interna kontrollen inom stadsbyggnadsnämnden.

Nämnden har fyllt i självdeklarationen med kommentarer till de olika kontrollfrågorna och om de anser sig ha en effektiv kontroll eller inte. Nämnden har även angett en referens till den dokumentation som styrker bedömningen. För att exemplifiera vilken typ av dokumentation som efterfrågats har exempel på bevis/kriterier lagts till i självdeklarationen.

Deloittes uppgift har därefter varit att verifiera i vilken utsträckning kontrollfrågorna har uppnåtts. Verifieringen har utförts genom intervjuer med utvalda personer av nämnden.

Om tillämpligt har även relevant information samlats in och viss stickprovstestning har genomförts.

Beroende på kontrollfrågans karaktär har en av följande tre testmetoder använts för att utvärdera dess effektivitet:

- Intervju: Kontrollfrågan har utvärderats genom intervju med ledande befattningshavare och övriga nyckelpersoner.
- Intervju/dokumentation: Kontrollfrågan har utvärderats genom intervju med ledande befattningshavare och övriga nyckelpersoner. Vidare har även tillämplig dokumentation insamlats och översiktligt utvärderats.
- Intervju/dokumentation/testning: Kontrollfrågan har utvärderats genom intervju med ansvarig befattningshavare och övriga nyckelpersoner. Vidare har testning genomförts enligt tillämplig metod med gemensamt beslutade urvalskriterier.

Efter utvärderingen enligt ovan har varje kontroll bedömts som ”effektiv” eller ”ej effektiv”. För att ett påstående ska bedömas som effektivt måste det finnas en rutin som säkerställer att kontrollen fungerar. Kontrollen måste även ha fungerat under hela testperioden, vilket kontrollerats genom en av de tre testmetoderna. För de kontroller där det via testning har visat sig att minst ett stickprov har en avvikelse har det aktuella påståendet bedömts som ej effektivt.

4. Resultat

4.1 Bedömningsskala

De kontrollfrågor som bedöms "effektiva" efter vår utvärdering har multiplicerats med riskkategorin för varje enskild fråga. Därefter har en kategorisering skett i enlighet med de fem viktiga komponenterna.

Utvärderingen har sedan skett enligt en tregradig skala samt uppdelat utefter de fem olika komponenterna. De komponenter som har 90-100 % effektiva påståenden anses ha en god måluppfyllelse. Effektiva påståenden som har 70-90 % anses ha ett behov av förbättring. De komponenter vilka har mindre än 70 % effektiva påståenden anses ha ett stort behov av förbättring.

Bedömningsskala	
Stort behov av förbättring	< 70 % effektiva påståenden
Behov av förbättring	70-90 % effektiva påståenden
God måluppfyllelse	90-100 % effektiva påståenden

I vår bedömning beaktar vi om en fullständig riskanalys har genomförts eller inte. Finns ingen fullständig riskanalys i komponenterna kontrollmiljö och riskbedömning som berör samtliga perspektiven och kritiska processer, påverkar det vår bedömning negativt. En bristande eller avsaknad av fullständig riskanalys påverkar också bedömningen av övriga tre komponenter.

4.2 Utvärdering

Nedan framgår en övergripande sammanställning per område utifrån de fem COSO-komponenterna. Nämndens bedömning framgår av mittenkolumnen och Deloittes bedömning av kolumnen till höger.

Verksamhetsövergripande	Nämndens bedömning	Deloittes bedömning
Kontrollmiljö	96 %	75 %
Riskbedömning	100 %	0 %
Kontrollaktiviteter	100 %	44 %
Information & kommunikation	82 %	82 %
Uppföljning	100 %	54 %
Total	97 %	56 %

I tabellen ovan framgår det att stadsbyggnadsnämnden enligt sin egen bedömning anser sig ha god måluppfyllelse i fyra av komponenterna samt behov av förbättringar inom komponenten information och kommunikation.

Vidare kan utläsas att nämndens bedömning avviker från Deloittes i fyra av fem komponenter. Totalt sett bedömer Deloitte att stadsbyggnadsnämnden har 56 % effektiva påståenden, medan stadsbyggnadsnämnden bedömer att de har 97 % effektiva påståenden. Vi kan konstatera att äldrenämnden inte har en fullständig riskanalys.

Vår bedömning av resultatet av verifieringen är överlag att anses som förväntat och normalt, i jämförelse med vad andra organisationer uppvisar första gången verifiering sker.

Under avsnittet "Iakttagelser och rekommendationer" återfinns samtliga kontrollfrågor som har bedöms "ej effektiva" med tillhörande iakttagelser och rekommendationer.

5. Iakttagelser och rekommendationer

Nedan redovisas de iakttagelser som identifierats som "ej effektiva" under verifieringen av självdeklarationen. För respektive kontrollfråga framgår en numrering som är hänförlig till komponenten enligt COSO-ramverket. Nummer 1.x avser utvärdering av kontrollmiljö, nummer 2.x riskbedömning i verksamheten, nummer 3.x kontrollaktiviteter för hantering av risker, nummer 4.x information och kommunikation samt nummer 5.x uppföljning och övervakning. Ur tabellen nedan framgår även den riskkategorisering som kontrollfrågan har graderats till. Vi har även lämnat förslag på förbättringsåtgärder/rekommendationer för respektive iakttagelse.

Verksamhetsövergripande				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
1.6	Ändamålsenligheten i roller och ansvar utvärderas regelbundet och uppdateras vid behov för att stödja en god arbetsfördelning inom förvaltningen.	2	Det saknas dokumenterade arbetsbeskrivningar.	Nämnden bör upprätta roll- och ansvarsbeskrivningar som stödjer en god arbetsfördelning inom förvaltningen och regelbundet uppdateras. Roll- och ansvarsbeskrivningen bör finnas tillgängligt på intranät eller motsvarande informationskälla.
1.7	Dokumenterade arbetsbeskrivningar har upprättats för ledande befattningshavare inom förvaltningens samtliga områden/funktioner och har antagits av nämnden.	2	Det saknas dokumenterade arbetsbeskrivningar.	Se rekommendation 1.6.
1.9	Rutiner finns på plats för att säkerställa en ändamålsenlig ansvarsfördelning, dvs. oförenliga aktiviteter/arbetsuppgifter utförs av skilda personer (exempelvis kontroll och attest).	3	Dokumentation avseende oförenliga aktiviteter/ arbetsuppgifter saknas.	Nämnden bör analysera och dokumentera oförenliga aktiviteter/arbetsuppgifter för samtliga väsentliga processer. Analysen bör dokumenteras i en matris där oförenliga aktiviteter identifieras. I de fall konflikter på grund av oförenliga aktiviteter identifieras bör förslag upprättas till hur dessa hanteras. Dokumentationen bör också inkludera eventuella befintliga kompenserande kontroller inom verksamheten.
1.14	Ledningen upprättar och kommunicerar uppförandekoder/ andra etiska riktlinjer.	2	Nämnden har inga specifika riktlinjer gällande etik, arbetet som rör etik framgår främst i värdegrunden.	Nämnden bör utarbeta en uppförandekod för förvaltningens medarbetare. Utarbetad uppförandekod bör fastställas av nämnden.

Verksamhetsövergripande				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
1.15	Nämnden har etablerat rutiner för att löpande identifiera situationer där risk föreligger för oetiskt eller i övrigt oönskat beteende hos förvaltningens medarbetare och har etablerat kontroller för att reducera risken för att dylika händelser inträffar.	1	Det saknas en dokumenterad rutin/riskanalys för att löpande identifiera situationer där risk föreligger för oetiskt eller i övrigt oönskat beteende.	Nämnden bör inkludera ett avsnitt i riskanalysen där risker för oetiskt eller i övrigt oönskat beteende utvärderas. Om det inte finns risk att anse att oetiskt beteende föreligger bör ändå bakomliggande analys framgå i dokumentationen. Förslag på hur identifierade risker bör kontrolleras ska dokumenteras och följas upp i exempelvis intern kontroll planen.
1.16	Nämnden har fastställt en löne-, ersättnings- och förmånspolicy som är kommunicerad och implementerad i organisationen. Policyn är framtagen i överrensstämmelse med kommunens riktlinjer och etiska normer.	1	Allt som rör löner och personal är kommunövergripande. Vid nyanställning skriver man under anställningsavtal men inga policydokument.	Nämnden skall efterleva Jönköpings kommuns lönepolitik alternativt utarbeta en lokal lönepolicy. Policyn/lönepolitiken bör fastställas av nämnden årligen. Om förvaltningen har ytterligare förmåner respektive ersättningar krävs minst att regler kring dessa kommunicerats av behörig person (ex HR ansvarig) på intranätet, dock bör företrädesvis förvaltningen formellt dokumentera de förmåner och ersättningar som ges till medarbetare. Dokumentet bör fastställas av lämplig ledningsinstans.
1.17	Relationer med externa parter utvärderas regelbundet för att säkerställa att förvaltningen endast samarbetar med externa parter, som uppfyller stadens krav.	1	Det saknas skriftlig rutin för att regelbundet utvärdera relationer med externa parter för att säkerställa att förvaltningen endast samarbetar med externa parter som uppfyller kommunens krav.	Nämnden bör löpande utvärdera externa parter i syfte att säkerställa att de externa parterna uppfyller enhetens behov och kravställning. Väsentliga externa parter (leverantörer/kunder, sponsorer och andra samarbetspartners) bör listas och gås igenom kontinuerligt. Utvärderingen bör dokumenteras.
1.20	Nämnden säkerställer att "back up" personer finns för nyckelpositioner inom samtliga områden/funktioner.	2	Det saknas dokumenterade ställningstaganden avseende back-up-personer för viktiga roller/arbetsuppgifter.	Avseende nyckelpositioner: Nämnden bör identifiera vilka nyckelpersoner som besitter en särskild kompetens, där frånfälle skulle innebära en risk för nämnden. För dessa nyckelpersoner bör ersättare/"back-up"-personer utses. Analysen av dessa positioner bör dokumenteras. Avseende arbetsuppgifter: Ersättare/"back-up"-personer bör utses för att säkerställa att uppgifter, ex attester, kan genomföras vid sjukfrånvaro, semester etc. Alla "back up"-personer bör dokumenteras och kommuniceras till berörda medarbetare.

Verksamhetsövergripande				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
2.1	En process för riskhantering och riskanalys har fastställts av nämnden.	3	En internkontrollplan upprättas årligen. I samband med upprättandet görs en riskanalys där momentens sannolikhet och konsekvens analyseras, denna riskanalys är dock väldigt detaljerad och inte verksamhetsövergripande. Nämnden har beslutat om internkontrollplanen, i verksamhetsberättelsen finns ett avsnitt för intern kontroll där det görs en uppföljning.	Övergripande regler och anvisningar för riskhantering och riskanalys för hela verksamheten bör implementeras, vilken skall ligga till grund för upprättande av internkontrollplanen, bör dokumenteras och fastställas av nämnden. Regler/anvisningar bör inkludera: - Hur riskanalys ska genomföras - Med vilken frekvens riskanalys ska genomföras - Aktiviteter för identifiering av risker - Aktiviteter för bedömningar av risker - Aktiviteter för beslut om riskhantering - - Aktiviteter för löpande rapportering och uppföljning av risker och riskhanteringsaktiviteter.
2.2	Nämnden genomför regelbundet en dokumenterad analys av verksamhetens operationella/affärsmässiga, legal och finansiella risker och risker för oegentligheter.	2	Nämnden genomför inte regelbundet en dokumenterad analys av förvaltningens operationella/affärsmässiga, legal och finansiella risker och risker för oegentligheter.	- En dokumenterad riskanalys bör genomföras minst årligen där samtliga identifierade risker i verksamheten inkluderas, såsom: - Operationella/affärsmässiga risker - Legala risker - Finansiella risker - Risker för oegentligheter
2.3	Riskanalysen är kopplad till verksamhetsplaner och framtagen mot bakgrund av verksamhetens mål, strategier, lagar och förordningar. Följande riskkategorier adresseras: - Operationella risker - Finansiella risker - Efterlevnadsrisker (lagar och förordningar)	3	Verksamheten är väldigt styrd efter plan- och bygglagen. Förändringar i lagstiftningen återspeglas ofta i internkontrollplanen. Vidare görs en riskanalys i samband med upprättandet av internkontrollplanen. Nämnden har ingen strukturerad riskbedömning för hela verksamheten som täcker in alla operationella, finansiella och lagar som finns för organisationen. Det saknas koppling mellan riskanalys och verksamhetsplan.	Riskanalysen bör vara framtagen utifrån verksamhetens mål, strategier, samt relevanta lagar och förordningar. Riskanalysen bör också vara kopplad till verksamhetsplaner.
2.4	Roller och ansvar i riskhanteringsprocessen är tydligt definierade och kommunicerade.	1	Nämnden har ingen strukturerad riskhanteringsprocess. Det saknas information som visar vem som är ansvarig för att genomföra riskanalysen.	Nämnden bör formellt definiera roller och ansvar för samtliga aktiviteter inom processerna för riskhantering och riskanalys, inklusive huvudansvarig för det årliga genomförandet av riskanalysen.

Verksamhetsövergripande				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
2.5	Riskanalysen bygger på en strukturerad modell med tydligt definierade riskbegrepp.	2	Det saknas en implementerad strukturerad modell för riskanalys.	En strukturerad modell för riskanalys bör utarbetas och fastställas av nämnden. Modellen bör inkludera definitioner av relevanta riskbegrepp såsom risk, konsekvens, sannolikhet och väsentlighet (sannolikhet att risken inträffar och vilken konsekvens risken skulle få om den inträffar).
2.6	Inom ramen för riskanalysen har nämnden fastställt relevanta risknivåer som grund för prioritering av risk- och kontrollaktiviteter.	2	Se ovan iakttagelse 2.5.	Nämnden bör definiera risknivåer i syfte att klargöra identifierade riskers inbördes prioritet, dvs. vad som utgör hög, medel respektive låg risk.
2.7	Nämnden är aktivt involverad och delaktig vid genomförandet av riskanalyser och får tydlig input från nämnden.	2	Nämnden har ej på ett strukturerat sätt varit involverad vid genomförande av riskanalysen.	Se rekommendation 2.5 och 2.6.
2.8	Alla verksamhetens huvudprocesser samt väsentliga stödprocesser analyseras för att fånga upp risker som påverkar verksamheten.	2	Analys saknas av väsentlig huvudprocesser samt stödprocesser för att fånga upp risker i verksamheten. Nämnden planerar att kartlägga samtliga processer till kommande kvalitetsrevisioner.	Nämnden bör genomföra en dokumenterad analys av samtliga väsentliga processer. Analysen bör uppdateras minst årligen. Exempel på väsentliga processer är: - Inköpsprocessen - Intäktsprocessen - HR-processen - Bokslutsprocessen - Verksamhetsövergripande processen - Stödprocesser
2.9	Internkontrollplanen är framtagen utifrån en genomförd risk- och väsentlighetsanalys med tydlig koppling till lagar, verksamhetens mål och strategier.	3	Det finns ingen strukturerad riskbedömning.	Internkontrollplanen bör tas fram och dokumenteras i enlighet med rekommendationerna i 2.2 – 2.6.

Verksamhetsövergripande				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
3.1	Kontroller är väldefinierade och dokumenterade med tydlig koppling mellan risk och kontrollåtgärd. Ansvaret för kontrollåtgärder är tydligt. Utvärdering av kontrollstrukturen sker vid förändringar i verksamheten.	2	Det finns ingen strukturerad riskbedömning.	Nämnden bör genomföra en dokumenterad analys av de väsentligaste verksamhetsprocesserna samt i vilken ordning dessa prioriteras. I samband med detta arbete rekommenderar vi även att risker och nyckelkontroller i processerna dokumenteras. Dokumenterade kontroller bör kopplas till identifierade risker, exempelvis i en risk och kontrollmatris. Risk- och kontrollmatrisen bör kontinuerligt utvärderas och ansvar bör utses. Kontrollerna bör dokumenteras vad avser: - Varför? Beskriv kortfattat syftet med kontrollen och vilka risker den skall hantera, dvs. varför kontrollen utförs. - Vad? Beskriv kortfattat vad kontrollen skall utföra dvs. vad det är som skall göras. - Hur? Vilka rapporter/system/moment som används/utförs vid kontrollen samt vilka underlag som skall fungera som bevis för genomförd kontroll - Vem? Vilken avdelning/funktion/roll eller system som utför kontrollen - När? Beskriv frekvens och tidpunkt för kontrollen
3.2	Lagar och förordningar Kontroller har utformats och implementerats för att säkerställa efterlevnad av lagar och förordningar.	2	Det saknas kontroller för att säkerställa efterlevnad av lagar och förordningar.	Implementera kontroller för att säkerställa efterlevnad av lagar och förordningar.

Verksamhetsövergripande				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
3.3	Finansiell rapportering Kontrollerna är väldefinierade och dokumenterade med tydlig koppling mellan risk och kontrollåtgärd. Ansvaret för kontrollåtgärden är tydligt. Utvärdering av kontrollstrukturen sker vid förändringar i verksamheten.	2	Det saknas dokumenterade kontroller för den finansiella rapporteringen.	För att nämnden ska kunna uppvisa en god intern kontroll över den finansiella rapporteringen krävs att befintliga nyckelkontroller dokumenteras. Dokumentationen av den finansiella rapporteringen bör innefatta följande moment: - Identifiering av risker kopplade till balans- och resultaträkning. Syftet är att identifiera väsentliga konton där det kan finnas en förhöjd risk för materiella fel. - Identifiering och dokumentation av risker. - Identifiering och dokumentation av befintliga kontroller för att minimera riskerna. - Identifiering av förbättringsbehov på grund av avsaknad av kontroller. - Utveckling av förbättrade eller nya kontroller. - Implementering av förbättrade eller nya kontroller. Kontrollerna bör utformas enligt vad som anges i rekommendation 3.1.
3.4	Generella IT-kontroller Kontrollerna är väldefinierade och dokumenterade med tydlig koppling mellan risk och kontrollåtgärd. Ansvaret för kontrollåtgärden är tydligt. Utvärdering av kontrollstrukturen sker vid förändringar i verksamheten.	2	Nämnden tillämpar den kommunövergripande IT-policyn. Ansvar för kommunens IT-policy och IT-säkerhetspolicy ligger enligt de intervjuade hos kommunens IS/IT-chef.	Nämnden bör genomföra utvärdera, dokumenterar och formaliserar de kontroller som skall finnas på plats relaterade till generella IT-kontroller. Vidare bör roller och ansvar relaterade till generella IT-kontroller definieras. Generella IT-kontroller omfattar exempelvis följande: - Behörighetsadministration avseende kritiska system - Programförändringar - Backup-rutiner - Kontroller för att säkerställa informationssäkerhet Kontrollerna bör utformas enligt vad som anges i rekommendation 3.1.

Verksamhetsövergripande				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
3.5	Strukturerad process finns på plats för att säkerställa att samtliga nämndens policys och riktlinjer löpande utvärderas och uppdateras.	2	Ingen strukturerad process finns för att säkerställa att policys och riktlinjer uppdateras och utvärderas löpande.	Nämnden bör införa en rutin som innebär att samtliga relevanta policys och riktlinjer utvärderas och uppdateras minst årligen. Detta bör dokumenteras och samtliga policys och riktlinjer bör vara daterade.
4.5	Uppföljning av riskanalys och därtill kopplad intern kontroll är en integrerad del av nämndens ordinarie verksamhetsuppföljning.	2	Det finns en kommunövergripande Whistleblower, informationen ut i organisationen och hur kanalvägen ser ut är bristfällig.	Se rekommendation 1.15.
5.2	Uppföljning av riskanalys och därtill kopplad intern kontroll är en integrerad del av nämndens ordinarie verksamhetsuppföljning.	3	Ingen strukturerad totaluppföljning görs av verksamheten, utan främst görs löpande uppföljningar under året i samband med nämndens sammanträde av de detaljerade punkterna i nuvarande internkontrollplanen.	Förvaltningen bör löpande rapportera resultat från uppföljning av verksamhetens totala riskanalys samt genomförd testning av intern kontroll i högre utsträckning. Rapporteringen bör sammanfalla och ingå i nämndens ordinarie verksamhetsuppföljning.
5.4	Ansvar och roller för operationella och ekonomiska verksamhetsuppföljningar är tydligt definierade.	2	Ekonomiska månadsuppföljningar samt månatliga investeringsuppföljningar görs av ekonom. Finns dock inga dokumenterade ansvarsfördelningar.	Ansvar och roller för operationell och ekonomisk verksamhetsuppföljning bör fastställas och dokumenteras i rollbeskrivningar för nyckelpersoner inom förvaltningen.
5.10	Nämnden har etablerat rutiner som beskriver hur identifierade avvikelser skall hanteras. Rutinerna inkluderar lämpliga korrigerande åtgärder samt beskrivning av hur återrapportering av genomförda åtgärder utförs.	1	Det saknas en skriftlig rutin för återrapportering.	Nämnden bör upprätta rutiner över hur identifierade avvikelser ska rapporteras med förslag till åtgärd, ansvarig person och tidplan för genomförande.
5.11	Uppföljning sker av att avvikelser har åtgärdats på ett tillfredsställande sätt inom rimlig tid.	2	Det saknas rutiner för att följa upp eventuella avvikelser.	Nämnden bör utse en person som ansvarar för uppföljning av åtgärdsplaner, vilket bör ske kontinuerligt för att säkerställa att avvikelser åtgärdas inom fastställd tidsram.
5.12	Nämnden efterlever rekommendationer och förbättringsförslag givna av kommunens förtroendevalda revisorer.	3	Det saknas skriftliga rutiner för att efterleva rekommendationer och förbättringsförslag.	Förvaltningen bör upprätta rutiner för hur rekommendationer och förbättringsförslag från kommunens förtroendevalda revisorer skall efterlevas.

Verksamhetsövergripande				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
5.13	Resultat från övervaknings-aktiviteter används för att utvärdera risk, utforma kontroller och driva verksamhetsförbättringar.	2	Det saknas en dokumenterad total riskanalys av verksamheten.	Resultatet från genomförda övervakningsaktiviteter bör ligga till grund för kontinuerlig utvärdering av verksamhetens risker och utformning av lämpliga kontroller för att hantera dessa risker.