Bilaga 1
Styrelsehandling nr 16
2016-05-10

Bostads AB Poseidon

Självdeklaration 2015

Verifiering av den löneadministrativa processen

Utförd av PwC

December 2015



Göteborgs Stad

1 Sammanfattning

Med start hösten 2010 har Deloitte, EY och PwC på uppdrag av Göteborgs Stad, som ett led i Göteborgs Stads arbete att utveckla och stärka riskhantering och intern kontroll, utvecklat en modell (Självdeklaration) för ett antal verksamhetskritiska processer. Tidigare år har områdena ”verksamhetsövergripande”, inköpsprocessen samt rekryteringsprocessen utvärderats och verifierats. För åren 2014 och 2015 tog Göteborgs Stad beslut om att fokusera arbetet med självdeklarationen på löneadministrativa processen.

Självdeklarationen är baserad på COSO, vilket är det internationellt mest erkända ramverket för intern kontroll. COSO-modellen bygger på ett strukturerat sätt att arbeta med intern kontroll omfattande fem olika komponenter. Komponenterna är kontrollmiljö, riskbedömning, kontrollaktiviteter, information och kommunikation samt uppföljning och övervakning.

Bostads AB Poseidon genomförde under hösten 2015 en självutvärdering av intern kontroll inom den löneadministrativa processen. Därefter genomförde PwC under oktober – november 2015 som ett fristående uppdrag en verifiering av bolagets självutvärdering inom området.

Verifiering har utförts genom besök hos Bostads AB Poseidon och har omfattat intervjuer med av bolaget utvalda medarbetare inom respektive verksamhet. Om tillämpligt har även relevant dokumentation insamlats och viss testning utförts.

Återrapporteringen av verifieringen är en avvikelserapportering och är inte av beskrivande karaktär. Verifieringen är på en översiktlig nivå och kan därmed inte jämställas med ett bestyrkandeuppdrag såsom revision eller översiktlig granskning.

Vid verifieringen har ett antal områden där den interna kontrollen kan förbättras framkommit inom den löneadministrativa processen. Den totala bedömningen visar att det finns behov av förbättring avseende intern kontroll i den löneadministrativa processen. Resultatet beror delvis på att bolaget inte kommit hela vägen då det gäller arbetet med riskanalysen avseende den senaste uppdateringen av riskanalysen och kontrollbeskrivningar.

Detaljerade iakttagelser framgår i avsnitt 4 nedan.

2 Avgränsningar

2.1 Avgränsningar

Våra bedömningar bygger på en övergripande verifiering av påståendena i ”Självdeklarationen” 2015 för den löneadministrativa processen. Återrapporteringen är en avvikelserapportering och är därmed inte av beskrivande karaktär. Detta innebär att redan fungerande områden inte lyfts fram i samma utsträckning som eventuella brister och förbättringsområden.

I de fall där testning inte ingått som en del av utvärderingen bygger våra bedömningar på den information vi erhållit via intervjuer med personer valda av bolaget.

Vad gäller styrande dokument har verifieringen inte innefattat en djupare analys av dess ändamålsenlighet.

Verifieringen är på en översiktlig nivå och kan därmed inte jämställas med ett bestyrkandeuppdrag såsom revision eller översiktlig granskning.

Under verifieringen har det framgått att Arkivnämnden för närvarande inte godkänner någon dokumenthanteringsplan efter maj 2015, varför vi valt att låta påståendet, gällande att bolagen/förvaltningarna har en antagen dokumenthanteringsplan avseende bevarande och gallring av dokument (1.4), utgå och därmed behandlas som ej tillämpbar i alla resultat i rapporten.

3 Metod

Vårt arbete har baserats på ett formulär (Självdeklaration) som en styrgrupp sammansatt av specialister från Deloitte, EY och PwC utvecklat på uppdrag av Göteborgs Stad. Det initiala arbetet inleddes hösten 2010 som ett led i Göteborgs Stads arbete att utveckla och stärka riskhantering och intern kontroll inom området ”verksamhetsövergripande” och inköpsprocessen. För år 2013 togs beslutet av Göteborgs Stad att fokusera arbetet med självdeklarationen inom rekryteringsprocessen och sedan beslutads att fokus skulle läggas på den löneadministrativa processen. Frågorna kommunicerades 2014, men verifieras först under hösten 2015 för att ge respektive förvaltning/bolag chans att arbeta med att nå upp till en tillfredställande intern kontroll inom den löneadministrativa processen.

Självdeklarationen har initierats som ett led i att stärka och utveckla kvaliteten i riskhantering och intern kontroll inom Göteborgs Stad. Verktyget är baserat på COSO, vilket är det internationellt mest erkända ramverket för intern kontroll. COSO-modellen bygger på ett strukturerat sätt att arbeta med intern kontroll omfattande fem olika komponenter. Komponenterna är kontrollmiljö, riskbedömning, kontrollaktiviteter, information och kommunikation samt uppföljning och övervakning. I Självdeklaration finns ett antal påståenden, vilka har riskklassificerats i en skala från 1 till 3.

Riskklassificeringen har upprättats av Göteborgs Stad i samråd med styrgruppen.

- **Riskkategori 1** har tilldelats påståenden med liten inverkan på det operativa, finansiella och/eller legala perspektivet.
- **Riskkategori 2** har tilldelats påståenden med medelstor inverkan på det operativa, finansiella och/eller legala perspektivet.
- **Riskkategori 3** har tilldelats påståenden 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 Göteborgs Stads bolag/förvaltningar.[1] PwC:s uppgift har varit att verifiera i vilken utsträckning fastställda påståenden uppnås inom bolaget.

[1] Andelen effektiva påståenden multiplicerat med risknivå har dividerats med totalt antal tillämpliga påståenden per process, multiplicerat med deras risknivå. Kvoten som erhålls från denna beräkning utgör sedan underlaget för utvärdering av respektive process övergripande bedömning. Påståenden som bedömts som ej tillämpliga ingår inte i beräkningen.

Verifieringen har utförts genom besök hos bolaget och har omfattat intervjuer med av dem utvalda medarbetare inom respektive verksamhet. Om tillämpligt har även relevant dokumentation insamlats och viss testning genomförts. Beroende på påståendets karaktär har en av följande tre testmetoder använts för att utvärdera dess effektivitet:

Intervju	Påståenden har utvärderats genom intervju med ledande befattningshavare och övriga nyckelpersoner.
Intervju/ dokumentation	Påståenden har utvärderats genom intervju med ledande befattningshavare och övriga nyckelpersoner. Vidare har även tillämplig dokumentation insamlats och översiktligt utvärderats.
Intervju/ dokumentation/ testning	Påståenden har utvärderats genom intervju med ansvarig befattningshavare och övriga nyckelpersoner. Vidare har testning genomförts enligt 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 påståendet fungerar. Kontrollen måste även ha fungerat under testperioden 2015, vilket validerats genom en av de tre testmetoderna. För de kontroller där det via testning visat sig att minst ett stickprov har en avvikelse har det aktuella påståendet bedömts som ej effektivt även om majoriteten av stickproven visat sig fungera väl. Även i de fall kontroller finns på plats men där dokumentation saknas eller är bristfällig har kontrollerna bedömts som ej effektiva. För de kontroller som implementerats under 2015 har stickprov tagits efter det datum kontrollen implementerades.

Nivån i nedanstående beskriven tregradiga bedömningsskala har beslutats vid Självdeklarationens införande av Göteborgs Stad tillsammans med externa specialister från Deloitte, EY och PwC. Skalan är satt utifrån en hög ambitionsnivå då Göteborgs Stad arbetar med ständiga förbättringar och åtgärdsplaner.

Bedömningsskala	
Stort behov av förbättring	< 70 % effektiva påståenden
Behov av förbättring	70-90 % effektiva påståenden
God måluppfyllelse	90-100 % effektiva påståenden
E/T	Ej tillämpligt

4 Resultat

Vid verifieringen har ett antal områden där den interna kontrollen kan förbättras framkommit inom den löneadministrativa processen. Den totala bedömningen visar att det finns behov av förbättring avseende intern kontroll i den löneadministrativa processen utifrån Stadens bedömningsskala. Resultatet beror delvis på att bolaget inte kommit hela vägen då det gäller arbetet med riskanalysen avseende den senaste uppdateringen av riskanalysen och kontrollbeskrivningar.

Nedan framgår en övergripande sammanställning per område utifrån de fem COSO-komponenterna och i avsnitt 4.1 återfinns detaljerade iakttagelser med tillhörande rekommendationer.

Resultat per COSO-komponent

Löneadministrativa processen	Självutvärdering 2015	PwC:s bedömning 2015
Kontrollmiljö	100%	100%
Riskbedömning	100%	0%
Kontrollaktiviteter	100%	77%
Information & kommunikation	100%	100%
Uppföljning	100%	100%
Total	100%	78%

Resultat per delområde i löneadministrativa processen

Löneadministrativa processen	Självutvärdering 2015	PwC:s bedömning 2015
Övergripande	100%	73%
Roller och ansvar	100%	86%
Grunduppgifter	100%	100%
Kontroll inför lönekörning	100%	67%
Reseräkningar och andra utlägg	100%	100%
Lönekörning och utbetalning	100%	50%
Total	100%	78%

4.1 Löneadministrativa processen

Nedan redovisas de iakttagelser som identifierats som "ej effektiva" under verifieringen av Självdeklaration 2015. Vi har även lämnat förslag på förbättringsåtgärder/rekommendationer för respektive iakttagelse. Göteborgs Stad kommer att kommunicera tidplan för när åtgärdsplan, ansvarig och tidplan för respektive iakttagelse ska vara framtaget.

Löneadministrativa processen				
Nr	**Kontrollfråga självdeklaration**	**Risk-kategori**	**Iakttagelse**	**Rekommendation**
1.5	Förvaltningen/bolaget har identifierat och utvärderat risker i löneprocessen med syfte att etablera ändamålsenliga kontroller.	3	Bolaget har en övergripande riskanalys och har under 2015 arbetat med riskanalys för löneprocessen. Riskerna i analysen är identifierade på bruttonivå och kontrollaktiviteter som är kopplade till riskerna finns beskrivna. Bolaget håller aktivt på att arbeta med riskanalysen för löneprocessen som en del av översynen av riskanalysen inför 2016 och var vid granskningstillfället inte helt klara. Vid granskningstillfället hade bolaget ännu inte gjort en bedömning av om riskerna är tillfredställande hanterade eller om ytterligare kontrollaktiviteter krävs.	Bolaget bör färdigställa sitt arbete med riskanalysen.
1.6	Förvaltningen/bolaget har identifierat och dokumenterat ändamålsenliga kontroller utifrån väsentliga risker i	3	Bolaget har i dokumentet "system och roller för löneadministratörer" beskrivit de flesta kontroller som utförs. Även i flödesschemat för "löneberedning" finns kontroller beskrivna. Det är dock inte	Bolaget bör tydliggöra vilka kontroller det är som utförs samt för respektive kontroll dokumentera: - 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

	riskanalysen i löneprocessen.		tydligt i dokumenten varför kontroller utförs, med andra ord vilken risk som hanteras. I riskanalysen finns det per risk angett vilka kontroller som utförs men här förekommer det kontroller som inte finns beskrivna i dokumentet "system och roller för löneadministratörer".	som skall göras och vad den ska resultera i - 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 som äger respektive utför kontrollen - När? Beskriv frekvens och tidpunkt för kontrollen Dokumenterade kontroller bör kopplas till identifierade risker i riskanalysen och bolaget kan med fördel notera vilka kontroller de anser är nyckelkontroller. Riskanalysen och kontrollbeskrivningarna bör kontinuerligt utvärderas och ansvar för respektive kontroll fastställas.
2.5	Dokumenterad genomgång av behörigheter i systemen sker kontinuerligt och uppdateras vid behov, dock minst årligen.	2	De system som är involverade i bolagets löneprocess är följande: Hogia Lön Hogia Personal Hogia PBM Hogia PBM Integration Tool styr behörigheterna för vilka som kan attestera tidrapporter samt vilka som kan lämna in tidrapporter. Avseende behörigheter i Hogia Lön och Hogia Personal sker en genomgång av behörigheter kvartalsvis men ingen genomgång sker av behörigheterna i Hogia PBM.	Eftersom behörighet att attestera tidrapporter styrs av Hogia PBM bör en genomgång av vilka som attesträtt i detta system också göras. Genomgången bör utföras minst årligen och dokumenteras.
4.2	Förvaltningen/bolaget har en rutin i syfte att kontrollera att lönehändelser/avvikelser (övertid/undertid,	3	Bolaget har rutiner för hur kontroll av att avvikelser är korrekt registrerade i systemet avseende sjukfrånvaro, övertid och semester ska ske men det finns ingen gemensam rutin för hur frånvaro för vård	Bolaget bör upprätta en rutin för hur kontroll av att frånvaro vid vård av barn ska hanteras.

	sjukfrånvaro, semester) blir korrekt registrerade. Inkluderar även att chefen ansvarar för att frånvarande personals avvikelser är korrekt registrerade i systemet. Förvaltningen/bolaget kontrollerar också pågående "långa" ledigheter och avgör om de ska förlängas eller avslutas, samt kontrollerar begränsade anställningar och avgör om de ska förlängas eller avslutas.		av barn ska hanteras. Det är upp till respektive chef att säkerställa att frånvaron vid vård av sjukt barn registreras men vid intervjuer med chefer framkom det att det saknas etablerade rutiner för hur de ska säkerställa det.	
6.2	Förvaltningen/bolaget har etablerat säkra överföringsrutiner gällande överföring av lönedata till bank. Lämpliga åtgärder som t.ex. ”sigill” används före och under överföringen.	3	Lönefilen laddas upp i Internetbanken av två i förening (löneadministratörer och ekonomiavdelningen), varefter banken kvitterar denna via mail med uppgifter om lönesumma och utbetalningsdatum. När filen skickas till banken är den krypterad i bankens miljö men inte innan och det går då att göra ändringar i filen. Enligt Göteborgs Stad måste filen vara skyddad mot ändringar vilket bankfilen inte är innan den är uppladdad i bankens miljö.	Bolaget bör implementera en dokumenterad rutin för att säkerställa säker överföring av lönedata till bank, exempelvis genom användandet av elektroniskt sigill före och under överföringen. Vad gäller den typen av information (löneuppgifter som inte är sekretessbelagda, men måste skyddas från ändringar) räcker det att den är riktighetsskyddad. Den behöver inte vara krypterad och det räcker exempelvis med att filen är signerad enligt informationssäkerhetschefen i Göteborgs stad.