Göteborgs stads bostadsaktiebolag Lägesrapport 2016

Lägesrapport avseende rekommendationer till förstärkning och effektivisering av intern kontroll samt Early Warning avseende väsentliga redovisnings- och revisionsfrågor.

Vi har under hösten 2016 genomfört förberedande granskning av styrelsens och verkställande direktörens förvaltning och den löpande redovisningen för tiden fram till 2016-09-30. Syftet med vår granskning är att förbereda och planera för vår revision av bolagets årsredovisning och styrelsens förvaltning, inte att genomföra en självständig granskning och uttalande avseende bolagets interna kontroll. Vår interimsgranskning är inte en full revision varför det inte kan uteslutas att det vid senare tillfällen kan framkomma förhållanden som hade kunnat identifieras tidigare om vi hade gjort en fullständig revision.

Vår granskning har omfattat bolagets system och processer för:

- Hyresintäkter
- Hantering av inköp
- Projektredovisning/projektuppföljning
- Löner, skatter och avgifter
- Löpande bokföring inklusive uppföljning av attest- och avstämningsrutiner
- Bokslut och rapportering

I samband med vår förberedande granskning har vi gjort vissa noteringar och iakttagelser där åtgärder skulle kunna förstärka och effektivisera den interna kontrollen i bolaget, samt identifierat redovisnings- och revisionsfrågor som bör åtgärdas inför årsbokslutet, vilka sammanfattas i bifogade brev.

För ytterligare förklaringar och kommentarer står vi givetvis till förfogande.

Med vänlig hälsning

Karin Olsson
Huvudansvarig revisor

Samuel Meytap
Granskningsledare

- **Förvaltning och intern kontroll**

Våra iakttagelser	Vår rekommendation	Bolagets kommentar
Försent inlämnad deklaration och försent inbetalda avgifter till skatteverket Fastighetsbolaget Bredfjäll KB och Fastighetsbolaget Gropens Gård KB har varit sena med att lämna in moms deklaration till skatteverket och även varit sena med inbetalningen vid ett tillfälle. Vi kommer vid bokslutet följa upp att man uppfyller skatteförfarandelagen med att lämna in deklarationer och betala skatter och avgifter i tid till skatteverket.	Vi rekommenderar bolaget att man ser över rutinen kring betalning av skatter och avgifter samt inlämnande av deklarationer till skatteverket, så man uppfyller skatteförfarandelagen.	Under första halvåret då detta skedde hade vi en dålig struktur och organisering av KB bolagen i samband med att man köpte upp Bredfjäll koncernen. Dessutom hade ekonomiavdelningen fullt upp med den Geografiska samordningen. Nu efter sommaren har vi fått ordning på rutinerna och har inte varit sena.
Låg grad av dokumentation av behörighetshanteringsrutiner Gällande tilldelning av behörigheter i Fast2 så finns rutiner inte dokumenterade vilket inte motsäger att korrekt hantering sker av nuvarande administratör, dock ger detta ett personberoende gällande hanteringen. Gällande tilldelning av behörigheter i Raindance är processen för att godkänna och tilldela behörigheter delvis informell då godkännande för tillägg och ändringar i behörigheter inte alltid formellt dokumenteras och tilldelning av behörigheter tilldelas användarna baserat på rimlighetsbedömning av Systemansvarig.	Vi rekommenderar att bolaget dokumenterar de rutiner som finns i behörighetstilldelningsprocessen, exempelvis hur godkännande sker och hur/vilka roller som tilldelas baserat på den behörighetssökandes roll samt att godkännande av behörigheter formellt dokumenteras.	Närmsta chef initierar i vårt system Lotus Notes (BAD) där det skrivs in vilken roll (yrkeskategori) personen har och var denne ska arbeta någonstans. Det skrivs också in när de vill att personen ifråga senast ska få behörighet i de olika systemen samt när någon byter arbetsplats eller slutar. Närmsta chef skriver också vilken resultatenhet som berörd person ska tillhöra. Systemet skickar sedan detta på cirkulation till alla systemansvariga med automatik. Systemansvarige får ett mail om att en person ska läggas till/ändras/sluta. Systemansvarige går in i Lotus Notes (BAD) och hämtar uppgifter om den enskilde personen via en länk i mailet eller direkt in i systemet.

Våra iakttagelser	Vår rekommendation	Bolagets kommentar
		Systemansvarige lägger till/ändrar/avslutar personen i Raindance eller Fast2 och går sedan tillbaka till Lotus Notes (BAD) och klar-markerar att det är utfört. När det gäller Fast2 är det två personer i dagsläget Lena Cederqvist och Helena Karlsson som har behörighet att registrera användare/resurser. I vårt system Raindance är det en person som kan registrera behörigheter och i dagsläget är det Lena Quick. Backukp är CGI. Alla steg loggas i Lotus Notes (BAD) systemet. Det sker även loggning i Fast2 och Raindance **Sammanfattning** **Bostadsbolaget har dokumenterade rutiner avseende ändring av behörigheter. Bostadsbolaget anser att våra rutiner är tillfredställande.**
Lösenordssättningar i applikationer följer inte Göteborgs stads policy Vid granskningen noterade vi att det finns en policy för lösenordssättningar i kritiska system, dock finns det ingen kontroll på plats för att säkerställa att lösenordssättningar förblir enligt policy. Vid granskningen noterades det även att lösenordssättningar i Raindance inte följer den uppsatta policyn samt kan anses som av låg säkerhetsnivå jämför med god praxis. Dock omfattas både Raindance och Fast2	Utan formellt definierade och implementerade detaljerade säkerhetskrav, samt uppföljning av efterlevnad, så finns det en ökad risk att den faktiska säkerhetsnivån är lägre än verksamheten behov kräver. Detta kan öka risken för obehörig åtkomst till kritiska system och data, såväl som driftstörningar. Vi rekommenderar därför Bostadsbolaget att säkerställa att	Går ej att komma åt Raindance utan att vara inloggad på nätverket. Unikt användarnamn + 6-ställigt lösenord (även om systemet endast kräver 4-ställigt), används. **Sammanfattning**

Våra iakttagelser	Vår rekommendation	Bolagets kommentar
av inloggning till Active Directory, vilket hanterar risken i stort.	säkerhetssättningar enligt policy implementeras i Raindance.	**Bostadsbolaget anser att Göteborgs stads policy följs.**
Fast2-konsulter har ständig behörighet i produktionsmiljö Bolaget har goda rutiner på plats för att dokumentera, testa och godkänna beställda förändringar som görs i Raindance och Fast2. Vi noterar emellertid att det i båda systemen saknas systemgenererad loggning av alla förändringar som inte inkluderas i versionsuppgraderingar. Fast2-konsulter har ständig access till produktionsmiljö, och följer ej samma process som övriga konsulter där begäran om åtkomst måste godkännas för att konsulten skall få tillgång till miljön under begränsad tid, dock har konsulterna i Fast2 en begränsad behörighet. Avsaknad av en systembaserad logg innebär att möjlighet saknas för bolaget att säkerställa kontroll av att samtliga ändringar är godkända och dokumenterade enligt ovanstående rutin. Detta är än viktigare för att kompensera för den exponering som det innebär med ständig behörighet för konsulter i Fast2	Vi rekommenderar att Bostadsbolaget utreder möjligheten att begränsa utvecklares åtkomst till produktionsmiljön för Fast2. Ett exempel på begränsning kan vara att utvecklare enbart tilldelas åtkomst vid planerad produktionssättning av ändringar. En sådan rutin bör även möjliggöra uppföljning att åtkomst enbart tilldelats vid godkända behov. Vi rekommenderar vidare att möjligheterna till systembaserad loggning och uttagande av rapporter kring genomförda förändringar utvärderas både för Fast2 och Raindance.	Fast2 har redan begränsade behörigheter då vi tagit bort möjligheten att lägga till och ändra behörigheter för utvecklare hos Fast2. Övriga behörigheter som Fast2 har är nödvändiga för att de ska kunna hjälpa och stödja oss i verksamheten. När Fast2 loggar in måste de uppge vad de ska göra i systemet och när de är klara måste de fylla i vad de har gjort. Fast2 arbetar inte i applikationen utan att vi gett dem i uppdrag att så göra. Det läggs ett ärende i deras ärendesystem Buggtracker innan åtgärd utförs. **<u>Sammanfattning</u>** **Bostadsbolaget anser att vi har tillräckligt väl fungerande rutiner.**
Avsaknad av uppdaterad kontinuitetsplanering för IT-miljö Vid granskningstillfället så noterades det att Bostadsbolaget har avbrottsplaner (hanteras av Framtidens IT) samt kontinuitetsplaner för eventuellt systembortfall, dock kan kontinuitetsplanerna uppdateras kontinuerligt baserat på	Brister i kontinuitetsplanering medför risk för att verksamheten avstannar helt vid systembortfall alternativt att arbetsuppgifter inte kan hanteras på alternativt sätt i den omfattning som är planerad.	Det finns en kontinuitetsplanering för IT-miljö med rutiner dock uppdateras inte dokumenten med en viss periodicitet. **<u>Sammanfattning</u>**

Våra iakttagelser	Vår rekommendation	Bolagets kommentar
en riskanalys som även denna bör utföras med viss periodicitet.	Vi rekommenderar Bostadsbolaget att övergripande analysera behovet av kontinuitetsplanering i syfte att implementera adekvata rutiner och upprätta relevant dokumentation.	**Bostadsbolaget kommer att följa denna rekommendation och göra en uppföljning 1 ggr/år.**

- **Redovisnings- och revisionsfrågor – Early Warning**

Våra iakttagelser	Vår rekommendation	Bolagets kommentar
Vi har inte noterat några väsentliga frågor inom ramen för vår löpande granskning.		