# Bostads AB Poseidon Lägesrapport 2017

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

Vi har under hösten 2017 genomfört förberedande granskning av styrelsens och verkställande direktörens förvaltning och den löpande redovisningen för tiden fram till 2017-09-30. 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 granskning har omfattat bolagets system och processer för:

- Hyresintäkter
- Driftskostnader, inköp och utbetalningar
- Underhålls – och nybyggnadsprojekt
- Löner, skatter och avgifter
- Bokslut och rapportering
- Förvaltning av IT och system (vilket inkluderar behörighetshantering, lösenordssättningar, rutiner för programförändringar samt kontinuitet och drift)

Vår granskning och rapportering syftar också till att identifiera ev redovisnings- och revisionsfrågor som identifierats och som vi rekommenderar att utvärdera och evenutellt åtgärda inför årsbokslutet.

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. För ytterligare förklaringar och kommentarer står vi givetvis till förfogande.

Med vänlig hälsning

Karin Olsson
Huvudansvarig revisor

## Förvaltning och intern kontroll- Poseidon

| Våra iakttagelser | Vår rekommendation | Bolagets kommentar |
|---|---|---|
| **Fast2-konsulter har ständig behörighet i produktionsmiljö**<br><br>Bolaget har generellt 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.<br><br>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.<br><br>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 Poseidon 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.<br><br>Vi rekommenderar vidare att möjligheterna till systembaserad loggning och uttagande av rapporter kring genomförda förändringar utvärderas både för Fast2 och Raindance. | Fast2 konsulter har behörighetskonto som gäller 6 månader och måste därefter aktivt förnyas och godkännas av uppdragsgivaren, om inte så stängs kontot. Detta gäller alla konsulter som har långa uppdrag.<br><br>Fast2 jobbar inte i produktion om det inte finns ett ärende i deras buggtracker.<br><br>När Fast2 loggar in på servern skall man skriva i en logg på servern vad de skall göra och när de är färdiga så skall de skriva i vad som faktiskt har utförts. Loggen finns på servern hos Framtidens IT.<br><br>Fast2 har inte systembaserad loggning i dagsläget.<br><br>Sammanfattning:<br><br>Bolaget anser att vi har tillräckligt väl fungerande rutiner. |

| Våra iakttagelser | Vår rekommendation | Bolagets kommentar |
|---|---|---|
| **Godkännande för produktionssättning av förändring i Raindance kan ej verifieras**<br><br>Bolaget har en rutin för testning och godkännande av förändringar som sker till Raindance. Vid vår granskning noterades dock att versions-uppgraderingen i Raindance saknar formellt godkännande före produktionssättning. Enligt intervju ska godkännande ha skett muntligt (och kan därmed inte verifieras i efterhand). | Vi rekommenderar att den definierade rutinen för testning och godkännande av förändringar efterföljs och att godkännanden dokumenteras och sparas för en spårbarhet av genomförda aktiviteter. | Bolaget har en rutin föra att genomföra testning innan en ny version tas i drift.<br>Dessa tester dokumenteras i testprotokoll och utförs av flera personer i olika roller och driftsättning sker inte innan eventuella avvikelser är utredda och hanterade.<br>När testningen är klar och vi har ett samlat testprotokoll som visar att testningen är godkänd av delansvariga görs avstämning mellan systemansvarig och systemägare och systemansvarig meddelar därefter Framtidens IT samt systemleverantör att driftsättning kan göras av den nya versionen.<br>Vid senaste uppgradering av Raindance meddelade systemansvarig beslutet muntligen via ett telefonsamtal till Framtidens IT. |
| **Utformningen av kontroll för behörighetshantering kan formaliseras för ändring i behörigheter Raindance**<br><br>Poseidon har en kontroll för att godkänna tilldelning av behörigheter innan dessa tilldelas i Fast2 och Raindance. Baserat på granskningen har vi dock noterat att ändringar i befintliga användares behörigheter godkänns muntligen för Raindance, vilket försvårar uppföljningen av att kontrollen har genomförts och att användare har godkänts av behörig person för ändrade behörigheter. | Vi rekommenderar att Poseidon säkerställer att även samtliga ändringar till användares behörigheter godkänns formellt, exempelvis genom mail eller beställningsblankett, innan de tilldelas i kritiska system. I godkännandet bör det tydligt framgå vem som bör godkänna behörigheten, vilken behörighet som ska tilldelas och vilket system detta rör. | I enlighet med Gbg Stads riktlinje för informationssäkerhet finns en formaliserad behörighetshantering i bolaget.<br>Alla förändringar vad gäller uppläggning av nya användare vid nyanställning, avslut i samband med att en anställd slutar sin anställning eller en förändring av roll av en befintlig anställd vid byte av tjänst finns det ett underlag ifrån Personalavdelningen baserat på vad som läggs in i Poseidons behörighetssystem. Beroende på vilken roll en användare har så läggs en specifik behörighetsuppsättning in i Raindance. Dessa kan skilja sig mellan olika personer på olika distrikt eftersom exempelvis arbetsuppgifterna för en distrikts-administratör på ett distrikt kan skilja sig mot vad en distriktsadministratör gör på ett annat distrikt. |

| Våra iakttagelser | Vår rekommendation | Bolagets kommentar |
|---|---|---|
| | | I det fall en användare har kvar samma roll på samma distrikt eller avdelning men att arbetsuppgifterna förändrar sig så att den personen behöver en annan behörighetsuppsättning i Raindance så har det förekommit att det lagts in utan ett skriftligt underlag.<br>Vi tillser att det framgent även finns skriftliga underlag på förändringar av redan existerade användare i Raindance.<br>Det ska dock noteras att vi har en årlig genomgång av samtliga användares behörighetsuppsättning i Raindance som en övergripande kontroll. Likaså går systemägaren igenom loggen för behörighetsförändringar i Raindance fyra gånger per år. Detta bör framgå av iakttagelsen.<br>Sammanfattning:<br>Bolaget tillser att det framgent även finns skriftliga underlag på förändringar av redan existerande användare i Raindance. |

| Våra iakttagelser | Vår rekommendation | Bolagets kommentar |
|---|---|---|
| **Riktlinjer kring lösenords utformning finns ej för Poseidons system**<br><br>Vid granskningen noterade vi att det finns en instruktion för lösenordssättningar framtagen av Framtidens IT. Denna gäller dock framförallt lösenordssättningar för Active Directory (åtkomst till Poseidons filstruktur och systemmiljö) och en riktlinje gällande krav på säkerhetsnivå för system, exempelvis Raindance och Fast2, finns inte framtagen. Därmed finns inte heller någon kontroll på plats som säkerställer att lösenordssättningar följer Poseidons riktlinjer. | Utan formellt definierade och implementerade detaljerade säkerhetskrav, samt uppföljning av efterlevnad, så finns det en ökad risk att den faktiska säkerhetsnivån är lägre än verksamhetens behov kräver. Detta kan öka risken för obehörig åtkomst till kritiska system och data, såväl som driftstörningar. Vi rekommenderar därför Poseidon att säkerställa att det finns en riktlinje framtagen för hur säkerhetssättningar i kritiska system ska utformas. Vidare bör det finnas en kontroll som säkerställer att faktiska lösenordssättningar följer den satta riktlinjen och att det är tydligt kommunicerat vem som ansvarar för att utföra kontrollen (exempelvis Framtidens IT eller Poseidon). | Tekniskt implementerat finns följande inom Framtidenkoncernen via Framtidens IT:<br>• Tvingande AD-lösenordsbyte var 90 dag<br>• Lösenordet måste vara minst 8 tecken<br>• Måste innehålla 1 siffra<br>• Måste innehålla 1 stor bokstav<br>• Systemet lagrar de 10 senaste lösenorden, går inte att återanvända<br>Poseidon, liksom Framtiden, följer Gbg Stads riktlinje för informationssäkerhet för lösenordssättning. Under punkt 8 Styrning av åtkomst, står bla<br>• Autentisering och åtkomstkontroll till IT-baserade informationssystem (gäller ej för öppen information) ska baseras på minst lösenord och bygga på unika användaridentiteter som är personliga och som ej får delas med andra.<br>Under punkt 3 Klassning av information, finns en modell beskriven avseende informationsklassificering. Detta är dokumenterad i respektive förvaltningsobjekt och finns för de mest kritiska systemen bl a: Raindance, Raindanceportalen, Siffervärden, och Fast2.<br>Lösenord i Fast2 följer regelverket för Windows (se ovan). Lösenord i Raindance skiljer något från detta. Regelverken är satta i respektive system.<br>Sammanfattning:<br>Bolaget anser att Göteborgs Stads policy följs vad gäller kravet på lösenordssättning, men ser över om regelverket i Raindance bör vara detsamma som i Fast2 och AD. |

| Våra iakttagelser | Vår rekommendation | Bolagets kommentar |
|---|---|---|
| **Avsaknad av risk- och sårbarhetsanalys och kontinuitetsplanering**<br><br>Vid granskningstillfället hade inte någon formell risk- och sårbarhetsanalys genomförts på bolagsnivå för risker kopplade till IT- och informationssäkerhet. Vidare så noterade vi att kontinuitetsplaner finns för Fast2 och Raindance, dock bör kontinuitetsplan för Raindance även inkludera hur arbetet är tänkt att ske vid eventuellt bortfall av systemstöd. | Vi rekommenderar att Poseidon utför en risk- och sårbarhetsanalys där befintliga IT-system prioriteras baserat på verksamhetens risker och krav och att Poseidon säkerställer att avtal med Framtiden IT uppfyller de identifierade kraven. Baserat på riskerna bör kontinuitetsplanen för Raindance sedan uppdateras för att beskriva arbetsflödet vid tid av systembortfall, exempelvis manuella rutiner och ansvar för uppdatering av systemet vid återgång till normal verksamhet. | Kontinuitetsplan finns framtagen för Raindance och Fast2.<br>Systemansvarig och systemägare har ett övergripande ansvar för att leda systemarbetet i det fall att en sådan situation skulle uppkomma.<br>Sammanfattning:<br>Bolaget ser över kontinuitetsplanen för Raindance så att den vidareutvecklas med de punkter som föreslås. |

## • Redovisnings- och revisionsfrågor – Early Warning

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