Bilaga 3
Styrelsehandling nr 8c
2017-02-09

Göteborgs Stad, Stadsrevisionen

Granskning av informationssäkerheten i FAST2 – Bostads AB Poseidon

KPMG AB
2017-01-04
Antal sidor: 25

Innehåll

1. Sammanfattning

KPMG har av Stadsrevisionen fått i uppdrag att genomföra en granskning av informationssäkerheten i fastighetssystemet FAST2 inom Bostads AB Poseidon (”Poseidon”). Granskningen har syftat till att ge underlag för att kunna bedöma om det råder tillräcklig intern styrning och kontroll avseende informationssäkerheten i systemet samt om gällande regelverk efterlevs.

Samtlig IT/IS-verksamhet behöver utföras på ett säkert sätt där informationen som bearbetas skyddas mot extern och intern missanvändning. En stor mängd affärskritisk information, varav en del är känsliga uppgifter, hanteras i FAST2. Utvecklingen går mot att än mer information hanteras elektroniskt och därmed minskar den fysiska kontrollen på informationen. IT- och informationssäkerhet är därmed väsentliga områden och det krävs en tydlig hantering för att säkerställa skyddet kring viktig information.

Granskningen har skett genom intervjuer med nyckelpersoner med avseende på informationssäkerhetsarbetet kring FAST2 inom Poseidon. Vi har även analyserat befintliga policydokument och riktlinjer kopplat till informationssäkerhet och intern kontroll, utfärdade av Staden respektive bolaget. För att besvara revisionsfrågorna har, utöver intervjuer och dokumentstudier, ett test av efterlevnad genomförts. I syfte att verifiera att rutiner efterlevs har effektiviteten utvärderats genom stickprovskontroller med bäring på de revisionsfrågor rapporten syftar till att besvara.

KPMG har i granskningen kunnat konstatera att Poseidon i hög utsträckning efterlever de krav på intern kontroll och informationssäkerhet som Göteborgs Stad ställer genom av kommunfullmäktige antagna policys och riktlinjer. Poseidon har på ett tydligt sätt fastslagit vilka roller och vilket ansvar medarbetare har i arbetet med informationssäkerhet genom flertalet dokument, både interna och koncerngemensamma. KPMGs övergripande bedömning är att Poseidon har tydliga strukturer för att samverka, både internt och externt, i syfte att uppnå samordningsfördelar och gemensamma rutiner kring intern kontroll och informationssäkerhet. Organisationen bedöms vara ändamålsenlig med en tydlig roll-, ansvars- och befogenhetsfördelning.

KPMG bedömer att det finns avtal och arbetssätt som på ett tillfredställande sätt reglerar ansvar och befogenheter mellan Poseidon och Framtidens IT respektive Poseidon och systemleverantören för FAST2. Avtalens olika områden har sedan formaliserats i ytterligare dokument, både interna och gemensamma.

KPMG bedömer att Poseidon har formella rutiner implementerade för användar- och behörighetsadministration som ger förutsättningar för en korrekt och enhetlig hantering av användarkonton och användarbehörigheter. Periodiska åtkomstgranskningar utförs i enlighet med den fastställda rutinen som ger möjlighet till identifiering av felaktigheter. Rutinerna för behörighetsadministration innefattar samtliga användare som har åtkomst till systemet inklusive konsulter och externa användare. Antalet användare med kraftfulla behörigheter är restriktivt tilldelat till ett fåtal personer på bolaget. De implementerade lösenordskraven i både nätverk och FAST2 är starka och i linje med KPMG:s rekommendationer. Användarkonton i FAST2 är tydligt knutna till unika individer och för de fåtal konton som inte går att härleda till unika personer bedömer KPMG att bolaget har kontroll kring vilka som använder dem. Poseidon har genom

underliggande dokumentation kunnat styrka att de fastställda rutinerna efterlevs. Avseende åtkomst till databaskontot bedömer KPMG att antalet personer som har åtkomst till lösenordet hos Framtidens IT, och därmed har åtkomst till databaskontot, är lämpligt begränsat.

Systemmiljön har, enligt både Poseidon och Framtidens IT, bra förutsättningar för att logga säkerhetsrelevanta händelser. KPMG bedömer att säkerhetsrelevanta händelser identifieras i rutinen för incidenthantering och att det finns strukturer för att rapportera händelser. KPMG bedömer dock att Poseidon inte identifierat vad som behöver loggas och saknar rutiner för att analysera och följa upp loggar på ett strukturerat sätt.

KPMG bedömer att Poseidon har tillfredställande rutiner implementerade för backup- och ändringshantering i enlighet med *Regler för driftsdokumentation*. Backuphantering skall säkerställa att säkerhetskopierad data går att återläsa, medan ändringshantering skall säkerställa att ändringar och uppgradering som produktionsätts inte är felaktiga eller olämpliga. Det finns formaliserade rutiner för att hantera incidenter och avbrott, vilka KPMG bedömer ger förutsättningar för att säkerställa att incidenter hanteras på ett lämpligt och enhetligt sätt. Årligen återläses säkerhetskopierad data i syfte att ha en uppdaterad testmiljö. Återläsningen genomförs dock inte efter en fastställd rutin för att säkerställa att säkerhetskopierad data är återläsningsbar, utan genomförs för att ha en uppdaterat testmiljö.

Avseende PUL och hantering av känsliga uppgifter bedömer KPMG att ansvarsroller har fördelats inom Poseidon och att det finns strukturer implementerade för att informera hyresgäster om hur deras personuppgifter hanteras i FAST2 genom en samtyckesblankett. Det finns en förteckning som beskriver vilka personuppgifter som behandlas i FAST2. Uppgifterna har dock inte klassificerats fullt ut gentemot kravnivåerna för sekretess, riktighet och konfidentialitet, men KPMG noterar att detta är ett pågående arbete som en del av arbetet med dokumenthanteringsplanen. KPMG bedömer att det finns bra rutiner för att säkerställa gallring av information och att inga olämpliga personuppgifter finns med i fritextfält genom månatlig gallring och ordanalys.

KPMG noterar att FAST2 applikationen (installerad på handläggares klientdatorer) baseras på Java-teknologi som vid installation kommunicerar i klartext. Applikationen kommunicerar också i klartext vid generell användning av funktioner som användaren har behörighet att använda. Även här kan ett internt hot med tillgång till viss infrastruktur (det interna nätverket) skaffa sig tillgång användarens användarnamn och lösenord. KPMG bedömer att bristen är allvarlig men sannolikheten är relativt låg att en aktör ska utnyttja den. KPMG noterar att Bostadsbolagen arbetar med att åtgärda bristerna och att förbättringar har skett sedan penetrationstestet utfördes.

KPMG bedömer att det finns en bra struktur för att ha löpande avstämningar och dialog med Framtidens IT avseende säkerhetsnivån i IT-miljön. Framtidens IT har ett monitoreringssystem för övervakning av IT-miljön samt flertalet interna rutiner för att säkerställa att säkerhetsrelevanta händelser identifieras och följs upp. Utöver det löpande arbetet med Framtidens IT finns ett flertal forum som berör säkerhetsrelevanta händelser såsom IT-rådet och IT-strategiska rådet. KPMG bedömer att säkerhetsrelevanta händelser regelbundet följs upp på ett strukturerat sätt. Uppföljningar av informationssäkerhet kopplat till intern kontroll ska genomföras och rapporteras till styrelsen årligen. KPMG bedömer att detta genomförs på ett sätt som inkluderar informationssäkerhetsperspektivet, då riskanalysen och planen för intern kontroll har ett stort fokus på IT och informationssäkerhet.

KPMG bedömer att det saknas en formell rutin för att följa upp att, för granskningen tillämpliga regelverk och policys, efterlevs i verksamheten. KPMG anser dock att det kan vara svårt för Poseidon att hitta en lämplig rutin för att säkerställa att befintliga regelverk efterlevs, då exempelvis *Riktlinje för informationssäkerhet* saknar instruktioner för hur riktlinjen ska följas upp på lämpligaste sätt.

KPMG noterar i sin granskning följande väsentliga iakttagelser med tillhörande rekommendationer till hur den interna kontrollen kan stärkas:

1. **Analys och uppföljning av säkerhetsrelevanta händelser**

   Det saknas rutiner för att analysera och följa upp loggdata på ett strukturerat sätt.

   KPMG rekommenderar Poseidon att utarbeta rutiner för loggning, analys och arkivering av säkerhetsrelevanta händelser enligt de krav som finns i R*egler för driftsdokumentation* och *Riktlinje för informationssäkerhet*.

2. **Återläsning av säkerhetskopierad data**

   Det saknas en formaliserad rutin för test av återläsning av säkerhetskopierad data. Poseidon genomför återläsningstester när testdatabasen uppdateras, men det görs inte efter en formaliserad rutin.

   KPMG rekommenderar Poseidon att implementera en rutin för regelbunden test av återläsning av säkerhetskopierad data. Tester bör genomföras minst årligen och de bör dokumenteras. Poseidon kan t ex utöka återläsningen av testdatabasen med dokumentation som styrker att det är ett fullständigt återläsningstest.

3. **Klassificering av data**

   Nuvarande förteckning som beskriver vilka personuppgifter som behandlas i FAST2 har inte klassificerats fullt ut gentemot kravnivå, sekretess, riktighet och konfidentialitet.

   KPMG rekommenderar Poseidon att komplettera den nuvarande förteckningen över behandlingar av personuppgifter med en klassificering av data i enlighet med *Riktlinje för informationssäkerhet*. Förteckningen bör innehålla rekommendationerna som återfinns i *Riklinje för informaitonssäkerhet* och kan med fördel mappas mot resultatet av det befintliga arbete som genomförs med dokumenthanteringsplanen.

4. **Uppföljning av att befintliga regelverk efterlevs**

   Det saknas en formell rutin för att följa upp att, för granskningen tillämpliga regelverk och policys, efterlevs i verksamheten.

   KPMG rekommenderar Poseidon att upprätta en formell rutin för att säkerställa att, för granskningen tillämpliga regelverk, efterlevs i verksamheten.

2. Inledning

2.1 Bakgrund

KPMG har, på uppdrag av Stadsrevisionen, genomfört en övergripande granskning av informationssäkerheten i fastighetssystemet FAST2.

Framtidens IT är en enhet inom Förvaltnings AB Göteborgslokaler, som ingår i lokalklustret med Higab AB som moderbolag. Framtidens IT ansvarar för drift och support av infrastruktur, kommunikations- och basapplikationer för bolag inom bostads- och lokalklustren (utom Higab). Enheten sysselsätter 18 personer och sköter driften av närmare 300 servrar, kommunikation till cirka 1 900 punkter i fastigheter och supporten för drygt 1 200 användare.

Bostads AB Poseidon, Familjebostäder i Göteborg AB, Gårdstensbostäder AB och Göteborgs stads bostadsaktiebolag ingår i bostadsklustret med Förvaltnings AB Framtiden som moderbolag. Bostadsbolagens uppdrag är att i ett allmännyttigt syfte medverka till bostadsförsörjningens främjande inom Göteborgs Stad. Tillsammans förvaltar bolagen över 71 000 lägenheter. Framtidenkoncernen har ett IT-råd och ett IT-strategiskt råd med syfte att samordna arbetet kring IT/IS inom koncernen. Ordförande i dessa råd är en representant från moderbolaget Förvaltnings AB Framtiden.

Bostadsbolagen använder sig av fastighetssystemet FAST2 som stödjer följande processer:

- uthyrning av bostäder
- hyresadministration
- förvaltning

Det finns en förvaltningsmodell implementerad för FAST2 som utgör en matris/modell för samtliga gemensamma system inom bostads- och lokalklustren.

Genom särskilda avtal för service och support (Service Level Agreement) mellan respektive bostadsbolag och Framtidens IT hanterar Framtidens IT driften av FAST2. I avtalen regleras bland annat nivån på service och support. Generellt gäller att servicenivån styrs med hänsyn till hur verksamhetskritiskt ett system eller en tjänst är för verksamheten.

I FAST2 finns information om bland annat förflyttningar inom koncernen, avtalsskrivningar, uppsägningar, hyresaviseringar, kravhantering och fel- och underhållshantering. I FAST2 finns också information om bostadssökande och eventuell medsökande.

Mot bakgrund av ovanstående är det viktigt att FAST2 har en hög informationssäkerhet och att känslig information såsom personuppgifter hanteras på ett korrekt sätt. Bolagens styrelser är ytterst ansvariga för att FAST2 och informationen i systemet hanteras och förvaltas enligt gällande lagstiftning och regelverk.

2.2 Syfte och revisionsfrågor

Granskningen har syftat till att ge underlag för att kunna bedöma om det råder tillräcklig intern styrning och kontroll avseende informationssäkerheten i FAST2 och om gällande regelverk efterlevs.

Med informationssäkerhet avses att:

- Informationen i systemet endast är tillgänglig för behöriga
- Informationen är riktig, det vill säga att informationen inte förändras eller påverkas oönskat eller utom kontroll.
- Informationen är tillgänglig när den behövs.

Begreppet ”tillräcklig” ska i sammanhanget ses utifrån aktuella granskningskriterier.

För att uppfylla syftet med granskningen har följande revisionsfrågor besvarats.

1. Finns det en ändamålsenlig organisation med tydlig roll-, ansvars- och befogenhetsfördelning för att hantera informationssäkerhetsarbetet?
2. Finns det avtal och arbetssätt som på ett tillfredsställande sätt reglerar ansvar och befogenheter mellan bostadsbolagen och Framtidens IT respektive mellan Framtidens IT och systemleverantören?
3. Finns det tillfredsställande rutiner för att skapa, underhålla och ta bort behörigheter, inklusive personer med höga behörigheter, konsulter och systemleverantör?
4. Är systemet säkert med avseende på inloggning och lösenord?
5. Sker loggning och uppföljning av säkerhetsrelevanta händelser på ett tillfredsställande sätt?
6. Hanteras säkerhetskopiering, systemuppdateringar och avbrott i systemet på ett tillfredsställande sätt?
7. Hanteras personuppgifter och känsliga personuppgifter i systemet på ett tillfredsställande sätt?
8. Är systemet säkert med avseende på intrång och manipulering?
9. Genomförs det uppföljningar av att säkerhetsnivån i systemet är acceptabel, och rapporteras dessa uppföljningar till styrelsen?
10. Genomförs det uppföljningar av att gällande regelverk följs?

2.3 Revisionskriterier

Granskningen utgår ifrån följande kriterier, som kort sammanfattas nedan. För fullständig beskrivning av kriterierna hänvisas till respektive regelverk.

Riktlinjer för intern kontroll i Göteborgs Stad
Ansvaret för bolagens interna kontroll ligger på styrelsen. I stadens riktlinje framgår bland annat att styrelsen ska säkerställa att bolaget följer gällande regelverk samt eliminera eller upptäcka allvarliga fel och brister.

Säkerhetspolicy för Göteborgs Stad med tillhörande riktlinje för informationssäkerhet samt regler för driftsdokumentation för IT-baserade informationssystem och regler för informationssäkerhetsansvar för chefer i Göteborgs Stad
Stadens säkerhetspolicy med tillhörande riktlinjer och regler fastställer bland annat att bolagens ledning ska säkerställa att externa parter såsom entreprenörer, inhyrd personal, konsulter och leverantörer uppfyller och följer relevanta delar inom säkerhetsområdet. Policyn konkretiseras i ett antal underliggande riktlinjer och regler.

Av riktlinjen för informationssäkerhet framgår att all information ska klassas. Detta ska sedan ligga till grund för hur informationen hanteras och vilka säkerhetsåtgärder som ska vidtas. Riktlinjen beskriver sedan en grundsäkerhetsnivå för information i klass 1. För information som klassas som nivå 2 krävs ytterligare säkerhetsåtgärder. För de specifika krav som Staden ställer, se riktlinjen.

Det framgår också av riktlinjen att verksamhetens ledning kontinuerligt ska följa upp att säkerhetsnivån är acceptabel och att detta ska ske minst årligen. Resultatet ska rapporteras till styrelsen.

Det framgår av riktlinjen för informationssäkerhet att det ska finnas en formellt beslutad driftsdokumentation för verksamhetens IT-system. Regelverket kring detta specificeras närmare i ”Regler för driftsdokumentation för IT-baserade informationssystem”. Detta omfattar bland annat regler och rutiner för rapportering, loggning, ändringshantering och återläsning av säkerhetskopiering.

I regler för informationssäkerhetsansvar för chefer i Göteborgs Stad framgår också att varje chef inom sitt område har ansvar för att följa upp att säkerhetsrutiner och regelverk efterlevs och att informera berörd personal om gällande regelverk, rutiner och ansvar.

Personuppgiftslag 1998:204
Av denna lag framgår bland annat att den som är personuppgiftsansvarig ska vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna. Ju känsligare uppgifterna är, desto mer omfattande säkerhetsåtgärder krävs. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig utifrån:

- tillgänglig teknik
- kostnaderna för åtgärderna
- de risker som kan finnas med personuppgiftsbehandlingen
- hur pass känsliga uppgifterna är

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde (t.ex. en extern skadereglerare) ska den ansvarige säkerställa att denne kan genomföra de säkerhetsåtgärder som måste vidtas. Den personuppgiftsansvarige måste också se till att personuppgiftsbiträdes verkligen genomför eventuella åtgärder. Ytterligare information finns i Datainspektionens allmänna råd om säkerhet för personuppgifter.

Policy och riktlinje för tillämpning av personuppgiftslagen vid Göteborgs Stads förvaltningar och bolag

Riktlinjerna gäller all automatiserad behandling av personuppgifter vid Göteborgs Stads förvaltningar, bolag och stiftelser. Det framgår bland annat att styrelsen har ansvaret för säkerheten kring personuppgiftsbehandling. Riktlinjen förtydligar gällande lagstiftning enligt personuppgiftslagen.

Till detta kommer tillämpliga standards, såsom ISO 27001 och branschöverenskommelser.

Dataskyddsförordningen - Nya regler om personuppgiftsbehandling från 2018

Den 15 december 2015 kom EU-kommissionen, Europaparlamentet och EU:s ministerråd överens om förslaget till ny EU-förordning om dataskydd.

Förordningen medför strängare krav på företags och myndigheters hantering av personuppgifter. Förutom ökade krav på tydlighet vid samtycke, krav på enkelt språkbruk vid integritetspolicydokument och ökad informationssäkerhet, införs en markant skärpning av sanktionerna till fyra procent av årsomsättningen eller 20 MEUR.

Dataskyddsförordningen, GDPR, träder i kraft den 25 maj 2018 och ersätta därmed den svenska personuppgiftslagen.

I den mån granskningarna resulterar i brister kopplade till PUL bör granskade enheter upplysas om vilka konsekvenser bristerna kan få i och med den nya dataskyddsförordningen.

2.4 Metod

Granskningen har utförts genom genomgång av relevant styrande dokumentation, intervjuer, samt granskning av efterlevnad med insamling av bestyrkande dokumentation. Intervjuerna har genomförts med nyckelpersoner inom Poseidon med avseende på granskningens inriktning och omfattning. Granskning av efterlevnad har utförts genom att testa effektiviteten i IT-kontroller som går att härleda till revisionsfrågorna, i syfte att kunna uttala oss om hur väl kontrollerna fungerar.

Inom ramen för granskningen har även ett test i form av intrångsförsök i systemet genomförts. Syftet med testet var att pröva om:

- Om det är möjligt att passera systemets skyddsåtgärder
- Om det är möjligt att läsa respektive kopiera uppgifter i det granskade systemet
- Om det är möjligt att skriva in eller manipulera befintliga uppgifter i systemet

Särskilt stor vikt har lagts vid om personuppgifter respektive känsliga personuppgifter är skyddade från läsning, kopiering och manipulation. Intrångsförsök har genomförts internt inom Framtidenskoncernens nätverk. Burp Pro användes för att avlyssna webbtrafik. Wireshark användes för avskiljning och för analys. Process Monitor användes för att testa applikationens interaktion med de lokala filsystemen och för analys. Java Decompiler användes för att dekompilera .jar-filerna. Teknisk testning utfördes i Familjebostäders lokaler 2016-09-23.

2.4.1 Projektledare vid Stadsrevisionen

Projektledare för deluppdraget är granskningsansvarig revisor för den årliga granskningen av Poseidon AB.

3. Resultat

Nedan besvaras respektive revisionsfråga (se punkt 2.2 ovan) med granskningsresultatet, som är uppdelad på iakttagelser, bedömning och i förekommande fall rekommendationer. Våra bedömningar har kopplats till relevanta revisionskriterier.

3.1 Ändamålsenlig organisation för hantering av informations-säkerhetsarbetet (revisionsfråga 1)

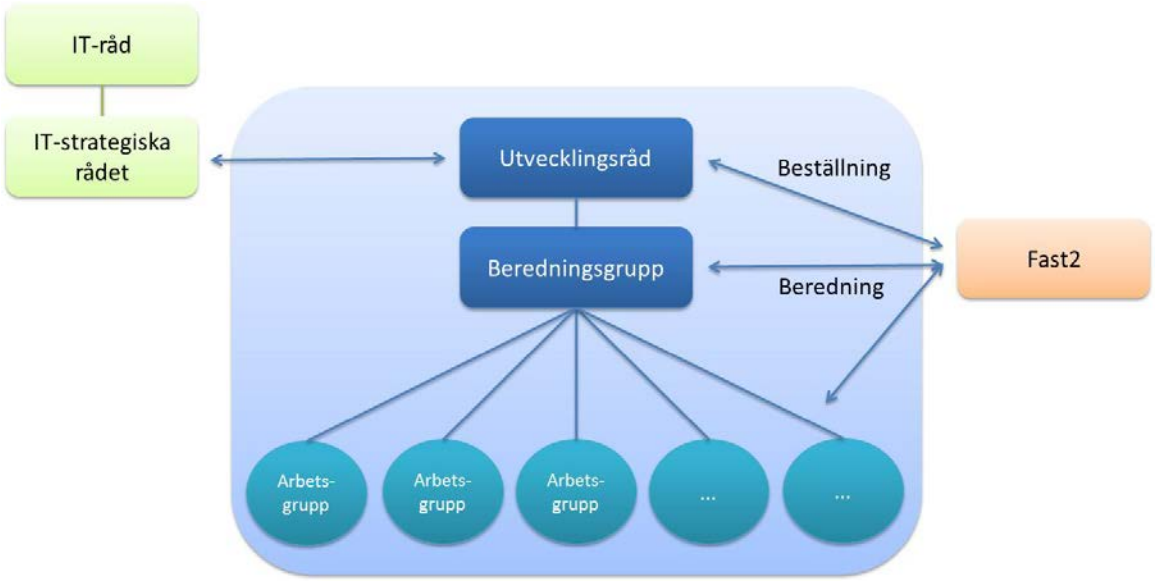
Iakttagelser

Poseidon har en implementerad koncerngemensam förvaltningsmodell, *Gemensam förvaltningsmodell för IT inom Framtidskoncernen.* Modellen har sitt ursprung från en genomlysning som utfördes inom Framtidskoncernens IT-verksamhet under 2013. Rekommendationerna var bland annat att upprätta en gemensam förvaltnings- och utvecklingsmodell och sträva mot ökad samverkan bostadsbolagen emellan.

Den övergripande koncerngemensamma IT-organisationen består av ett IT-råd och ett IT-strategiskt råd. IT-rådet ligger under VD-rådet och är det högsta rådet för beslut och styrning inom IT-området. Det IT-strategiska rådet är ett beredande råd inför beslut i IT-rådet. Under det IT-strategiska rådet finns en gemensam förvaltningsorganisation med sex olika fackgrupper, som hanterar frågor inom sina respektive områden. Modellen delar upp IT i sex olika ämnesområden i syfte att få greppbara områden som kan stämmas av med befintliga verksamhetsråd. Dokumentet beskriver hur den gemensamma förvaltningsmodellen fasas in i den koncerngemensamma IT-organisationen. IT-förvaltningsmodellen består av sex ämnesområden; Fastighetsteknik, FAST2 Förvaltningsorganisation, Ekonomiadministrativa system, Marknadssystem, Gemensamma plattformssystem och Personalsystem.

Dokumentet *Modell för gemensam utveckling av* FAST2 har upprättats för att beskriva hur bostadsbolagen löpande ska arbeta med utveckling av FAST2. Modellen för gemensam utveckling omfattar systemet FAST2 och aktiviteter avseende systemutveckling. Vid granskningstillfället är de olika bolagens installationer av FAST2 olika, även om de är snarlika. Den uttalade målsättningen är dock att under 2017 ha exakt samma version av applikationen installerad.

För området FAST2 finns det ett antal arbetsgrupper. Då en utvecklingspunkt ska beredas utses en tillfällig arbetsgrupp, bestående av en eller flera personer med ledning av en deltagare från beredningsgruppen. Arbetsgruppen tillsätts oftast av ansvarig deltagare i beredningsgruppen. Arbetsgruppen ansvarar för att bereda utvecklingspunkter och ha lämplig kontakt med systemleverantören och bostadsbolagen. Utöver det ska arbetsgruppen stämma av arbetssätt med bostadsbolagen och beskriva de potentiella konsekvenserna för samtliga bolag. Arbetsgrupperna bereder ärenden och ansvarar för att inhämta relevant information för beslutsunderlag till Utvecklingsrådet.



Beredningsgruppen består av systemansvariga för samtliga bostadsbolag samt representanter från IT-supporten. Beredningsgruppens huvudsakliga uppdrag är att utifrån ett koncernperspektiv utreda förslag på nya funktioner i FAST2 utifrån mallen för ändringsbegäran. Det gemensamma arbetet i beredningsgruppen syftar även till att agera som en enad part mot leverantören.

Utvecklingsrådet beslutar om kortsiktiga och långsiktiga planer och vägval gällande utveckling av FAST2. Samtlig IT-verksamhet samordnas genom koncernens IT-strategiska råd, där fastighetssystemet hanteras särskilt via det gemensamma Utvecklingsrådet. Utvecklingsrådet informerar IT-strategiska rådet om det pågående arbetet. Ordförande i Utvecklingsrådet är medlem i IT-rådet. Utvecklingsrådet hanterar frågor kring det långsiktiga arbetet i FAST2 samt tar frågor kring investeringar i systemet vidare för beslut i det IT-strategiska rådet.

Modellen för gemensam utveckling fastslår med tydlighet att följande riktlinjer och policys är styrande för arbetet inom organisationen:

- Koncernens IT-anvisning/policy
- Göteborgs Stads IT-riktlinjer
- Koncernens egna anvisningar

Poseidon har ett eget upprättat dokument, *Förvaltningsobjekt*, som främst systemansvarig för FAST2 ansvarar för, med avseende på uppdateringar vid förändringar. Vissa kapitel i dokumentet har dock Framtidens IT uppdateringsansvaret för. Förvaltningsobjekt beskriver hur den löpande förvaltningen av FAST2 ska framskrida. Dokumentet innehåller information om roller och ansvar och det framgår även vilka personer som har väsentliga roller såsom systemägare, systemansvarig, driftansvarig etc. Då systemet har ett stort antal användare finns det, utöver systemansvarig i FAST2, systemansvariga för de olika processerna. Utöver de interna roller som tilldelats finns information om leverantörers ansvarsroller i FAST2, där samtliga ansvariga finns beskrivna med tillhörande kontaktuppgifter. Förvaltningsobjekt beskriver också vilket processtöd olika roller, såsom uthyrning, hyresadministration och underhåll, har i systemet.

Utöver Förvaltningsobjekt har Poseidon ytterligare ett internt dokument, S*ystemförvaltningsmodell Fast2*. Det tydliggör förvaltningsorganisationen, ansvar och de olika rollerna personer inom organisationen kan ha. I relation till rollen finns även en målbild för vad rollen ska syfta till att uppnå samt dess huvudansvar.

Bedömning

KPMG bedömer att det finns en övergripande organisation med tydlig roll-, ansvars-, och befogenhetsfördelning för att hantera informationssäkerhetsarbetet och främja samverkan. Organisationen finns beskriven både på koncernnivå och på bolagsnivå samt är nedbruten i roller och ansvar. KPMG bedömer att det finns tydliga strukturer för att bedriva ett ändamålsenligt arbete med informationssäkerhet där Göteborgs Stads IT-riktlinjer utgör grunden.

3.2 Avtal mellan Poseidon och Framtidens IT respektive systemleverantören (revisionsfråga 2)

Iakttagelser

Poseidon har ett formellt avtal, ett Service Level Agreement, med Framtidens IT inom Förvaltnings AB GöteborgsLokaler. Avtalet är signerat av respektive VD för Förvaltnings AB GöteborgsLokaler och Bostads AB Poseidon. Avtalet omfattar åtta bilagor:

- Bilaga 1: *Service Level Agreement*, reglerar servicenivån för allt gemensamt IT-stöd samt administrativa tjänster vars drift, förvaltning eller support hanteras av Framtidens IT.

- Bilaga 2: *Framtidens Arbetsplatstjänst*, utgör en tjänstebeskrivning för klientplattformen. Bilagan reglerar avtalet för katalogtjänsten, standardiserad arbetsplats, fillagring, utskrifter samt fjärråtkomst. Målet med tjänsten är att löpande erbjuda leverans av ett lättanvänt verktyg för IT-användandet som uppfyller informationssäkerhetskrav, verksamhetsbehov och krav på kostnadshantering.

- Bilaga 3: *Nätverk och kommunikation (LAN och WAN),* är en tjänstebeskrivning av nätverk och kommunikation. Tjänsten ger tillgång till externa och intern IT-resurser såsom e-post, Internet, hemkatalog samt lokala nät för tele och data etc.

- Bilaga 4: *Verksamhetskritiska system (system och applikationer),* identifierar de system och moduler som är verksamhetskritiska samt definierar SLA-nivån på dessa. Poseidon har tillsammans med Framtidens IT klassificerat hur kritiskt ett system eller en modul är för verksamheten.

- Bilaga 5*: Övriga tillägg och underliggande leveranser*, specificerar de underliggande tjänsterna och tilläggen för drift, support och förvaltning av gemensamma och bolagsspecifika IT-stöd samt administrativa tjänster som utförs av Framtidens IT.

- Bilaga 6: *Pris och kostnadsfördelning*, specificerar kostnaderna och priserna för drift, support och förvaltnings av gemensamma och bolagsspecifika IT-stöd samt administrativa tjänster som utförs av Framtidens IT.

- Bilaga 7: *Process och rutindokumentförteckning*, specificerar de primära processer och rutiner som används i drift, support och förvaltningen av gemensamma och bolagsspecifika IT-stöd samt administrativa tjänster som utförs av Framtidens IT.

- Bilaga 8: *Change- och releaseprocess*, beskriver hur Framtidens IT arbetar med förändringshantering.

Poseidon har ett ramavtal med systemleverantören FAST2 Affärssystem AB som består av flertalet ytterligare bilagor. Ramavtalet är signerat av respektive Vd i november 2008. Ramavtalet består av ett samordningsavtal som sedan mynnar ut i tre bilagor:

- Bilaga 1: *Systemleveransavtalet*, består av flertalet ytterligare bilagor som innehåller tjänstebeskrivningar om leveransen genom avtalad specifikation för FAST2, kundens åtagande etc.

- Bilaga 2: *Underhållsavtalet*, består av flertalet ytterligare bilagor som definierar servicenivåer, ersättning, IT-underhåll etc.

- Bilaga 3: *Konsultavtal*, består av flertalet ytterligare bilagor och reglerar pris och betalningsvillkor, IT-tjänster etc.

Bedömning

KPMG bedömer att det finns avtal och arbetssätt som på ett tillfredställande sätt reglerar ansvar och befogenheter mellan Poseidon och Framtidens IT respektive Poseidon och systemleverantören för FAST2. Avtalens olika områden har sedan formaliserats i ytterligare dokument internt inom bolaget respektive bostadsklustret. Det finns tydliga rutiner som baseras på avtalen, exempelvis incidenthantering och ändringshantering. Dessa rutiner testas i revisionsfråga 5 och 6 (se 3.5, 3.6.2 och 3.6.3 nedan) och bedöms fungera tillfredsställande. I dokumentet Förvaltningsobjekt har roller fastslagits för kontaktpersoner hos FAST2 Affärssystem AB respektive Framtidens IT.

3.3 Användar- och behörighetsadministration samt höga behörigheter (revisionsfråga 3)

Iakttagelser

Poseidon har implementerat formella rutiner för användar- och behörighetsadministration i enlighet med *Riktlinje för informationssäkerhet*. Bolaget använder ett behörighetskontrollssystem, B.A.D. (BAD), för att hantera och administrera användare i Active Directory (AD) och deras verksamhetssystem där FAST2 ingår. Poseidons rutin för att skapa en ny användare är att begäran om åtkomst alltid ska initieras av den anställdes chef.

Rutinen fastslår att chefen ansvarar för att kontakta personalavdelningen och ange fullständig information om personen. Informationen avser fullständigt namn, anställningsform, anställningsdatum, befattning, placering, eventuellt specialsystem och eventuella system som normal inte går i rollen men som personen inte ska ha tillgång till. Personalavdelningen för sedan in informationen i BAD och ett mail skickas då till Framtidens IT med information om att det kommer en nyanställd som ska ha tillgång till en standardiserad uppsättning av system (Lotus Notes, MS Office, AD-konto & Windows/PC). När Framtidens IT har klarmarkerat samtliga system skickas automatiskt mail till systemansvariga som behöver skapa konton i respektive system. När de är klara går systemansvariga in i BAD och klarmarkerar samt skickar mail med inloggningsinformation till användaren.

Det finns även profiler uppsatta som ger åtkomst till specifika funktioner i FAST2. Dessa behörigheter är uppsatta baserat på arbetsuppgifter och organisatorisk tillhörighet och denna rollindelning ska enligt bolaget säkerställa en lämplig segregering av behörigheter i systemet. Därmed tilldelas användare en behörighetsroll som motsvarar arbetsuppgifter. Motsvarande rutin behöver alltid användas vid begäran om en förändring av befintliga behörigheter, exempelvis om utökade behörigheter krävs. Rutinen för avslut följer den generiska rutinen för användaradministration, där ansvarig chef initierar processen genom att kontakta HR som för in informationen i BAD. Systemansvariga är också ansvariga för att den nyanställda personen får rätt utbildning i systemet för att på ett bra sätt kunna utföra sitt arbete.

Poseidon har en behörighetsmatris som beskriver vilken funktionalitet olika behörighetsroller innehar. Samtliga ärenden avseende behörighetsadministration ska dokumenteras och arkiveras. Utöver den beskrivna rutinen finns ett dokument, *Säkerhet samt behörigheter i FAST2*, som beskriver hur behörigheter är uppbygga i applikationen.

Det finns tydliga riktlinjer för hur konsulter, visstidsanställda och externa användare ska hanteras i systemet. Vid tilldelning av behörigheter behöver de följa samma rutin som för övriga användare. Deras behörigheter ska alltid begränsas i så hög utsträckning som möjligt. Avseende vikarier eller externa uppdragstagare ska alltid ett slutdatum sättas på dessa användare i BAD varpå ett systemgenererat mail skickas ut strax innan slutdatumet infaller.

KPMG har testat rutinen för behörighetsadministration genom att ta stickprov på användare som har börjat arbeta på bolaget under året. Poseidon kunde ta fram underliggande dokumentation från samtliga stickprov som verifierade att behörighetsbeställningen skett utefter bolagets rutiner. Vid test av avslut i FAST2, genom jämförelse av en systemgenererad användarlista mot en HR-lista innehållande personer som slutat de senaste 365 dagarna, visades det att användare som har slutat har blivit borttagna i tid. Testen påvisar att rutinen för behörighetstilldelning och avslut av användarkonton fungerar tillfredställande vid granskningstillfället.

Poseidon har en rutin för att periodisk gå igenom användare och användarbehörigheter i FAST2, med syfte att säkerställa att användare som arbetar på bolaget har korrekta behörigheter i systemet. Rutinen ska utföras minst årligen och omfattar en genomgång av att tilldelade behörigheter överensstämmer med verksamhetsrollen och att användare ska ha åtkomst till systemet. Genomgången ska alltid dokumenteras av systemansvarig, granskas och signeras av systemägaren och sedan arkiveras av systemansvarig. KPMG har tagit del av dokumentation från den senast utförda åtkomstgranskningen och kan verifiera att den blivit utförd i enlighet med rutinen.

Den kraftfullaste behörigheten i FAST är rollen ADMINISTRATÖR. Poseidon arbetar utefter rutinen att vara restriktiva med att tilldela användare höga behörigheter. Endaste ett fåtal användare med systemadministrativa uppgifter ska ha administratörsbehörigheter i FAST2. Vid granskningen framkom att 16 användare av 478 har rollen administratör och av dessa är 13 personer anställda av systemleverantören FAST2. Därmed har endast tre användare från Poseidon administratörsbehörighet, vilket bedöms som begränsat. Genom avtal med FAST2 regleras systemleverantörens användande. Det finns en rutinbeskrivning för hur användare från systemleverantören FAST2 ska koppla upp sig mot systemet. Det finns även en loggfunktionalitet, som innebär att den person som varit inloggad behöver beskriva vilken aktivitet användaren har utfört i systemet.

Åtkomst att utföra ändringar direkt i databaserna för FAST2 har Framtidens IT och systemleverantören av FAST2, men inte Poseidon. Ett databaskonto används av både Framtidens IT och systemleverantören, vilket innebär att spårbarheten på genomförda aktiviteter försvinner. Framtidens IT saknar även rutiner för att periodisk byta lösenordet till databaskontot. Lösenordet finns tillgängligt på en filarea inom Framtidens IT:s AD, fem personer hos Framtidens IT har tillgång till filarean och därmed lösenordet.

Bedömning

KPMG bedömer att Poseidon har fastställda och formella rutiner på plats för användar- och behörighetsadministration som bör säkerställa en korrekt och enhetlig hantering av användarkonton och användarbehörigheter. Periodiska åtkomstgranskningar utförs i enlighet med rutinen och bör identifiera möjliga felaktigheter. Rutinerna för behörighetsadministration innefattar samtliga användare som har åtkomst till systemet, dvs även konsulter och externa användare. Antalet användare med kraftfulla behörigheter är restriktivt tilldelat till ett fåtal personer på bolaget.

Poseidon har genom underliggande dokumentation kunnat styrka att de fastställda rutinerna efterlevs. Avseende åtkomst till databaskontot bedömer KPMG att antalet personer som har åtkomst till lösenordet, och därmed har åtkomst till databaskontot, är lämpligt begränsat.

3.4 Autentisering och verifiering (revisionsfråga 4)

Iakttagelser

För åtkomst till FAST2 krävs ett unikt användarID och lösenord. Poseidon arbetar efter policyn att samtliga användare i systemet som är anställda inom bolaget ska vara personliga och knutna till en unik individ**.** Avseende externa leverantörer, använder de gruppkonton vilket är godkänt av Poseidon. Dessa användarkonton har väldigt begränsad åtkomst till funktioner i FAST2.

Poseidon har en lösenordspolicy som klargör att lösenord alltid ska vara personliga och att ansvaret för att skydda lösenordet ligger på användaren. Policyn klargör också hur lösenord måste hanteras om de behöver lämnas ut. Lösenordspolicyn fastlår att lösenord behöver utformas enligt följande krav:

- Bestå av minst 8 tecken
- Innehålla både stora och små bokstäver
- Innehålla av siffror eller specialtecken (båda delarna fungerar)
- Bytas var 90e dag

Ovanstående policy är implementerade i Poseidons Active Directory (AD) och är också systemmässiga krav i FAST2. Lösenordskraven är därmed starka och i linje med KPMGs rekommendationer.

KPMG har genomfört en analys av användarlistan för FAST2 i syfte att identifiera konton som inte tillhör unika användare. Genomgången identifierade inga interna aktiva generiska användarkonton med behörigheter i FAST2.

Bedömning

KPMG bedömer att de implementerade lösenordskraven i AD och FAST2 är starka och i linje med KPMGs ”leading practice”. Användarkonton i FAST2 är tydligt knutna till unika individer.

3.5 Loggning och uppföljning av säkerhetsrelevanta händelser (revisionsfråga 5)

Iakttagelser

I Göteborgs Stads dokument R*egler för driftsdokumentation* framgår det att det ska finnas regler och rutiner för rapportering, loggning, åtgärdande, informationsspridning eskalering, uppföljning och analys av säkerhetsloggar. Samma dokument beskriver även att en rutin eller regel för loggning

av funktionsfel och incidenter ska finnas. Poseidon saknar upprättad dokumentation för dessa rutiner.

Driftsreglerna tydliggör att det ska finnas rutiner för logghantering som omfattar hur länge loggar ska sparas, hur de ska förvaras, hur ofta de ska analyseras, vem som ansvarar för att analysen samt hur rapportering av analysarbetet ska ske. Ytterligare tydliggörs det i *Riktlinje för informationssäkerhet* att loggning och skapande av spårbarhet för viktiga säkerhetskritiska händelser ska ske. Enligt Poseidon har systemet bra funktionalitet avseende spårbarhet på genomförda aktiviteter, både gällande användares aktiviteter och tekniska säkerhetsaspekter. I händelse av att en säkerhetsrelevant händelse inträffar hanteras den i rutinen för incidenthantering. Inträffade incidenter följs alltid upp och är en stående punkt på de kvartalsvisa mötena med Framtidens IT avseende driften.

Enligt Poseidon görs vissa uppföljningar där de rapporterar till koncernen månatligen. Det avser bland annat antal objekt, fastighetsvärderingar, förändringar på objekt och hyresaviseringar.

Bedömning

KPMG bedömer att säkerhetsrelevanta händelser identifieras i rutinen för incidenthantering och att det finns strukturer för att rapportera händelser. KPMG bedömer vidare att Poseidon inte identifierat vad som behöver loggas och saknar rutiner för att analysera och följa upp loggdata på ett strukturerat sätt. Risken med avsaknad av rutiner för att logga och följa upp säkerhetsrelevanta händelser kan innebära att felaktigheter och säkerhetsbrister inte upptäcks.

Rekommendation

KPMG rekommenderar Poseidon att utarbeta rutiner för loggning, analys och arkivering av säkerhetsrelevanta händelser enligt de krav som finns i R*egler för driftsdokumentation* och *Riktlinje för informationssäkerhet*.

3.6 Säkerhetskopiering, ändringshantering, incidenthantering & avbrottsrutiner (revisionsfråga 6)

3.6.1 Säkerhetskopiering

Iakttagelser

Poseidon har etablerade rutiner implementerade för säkerhetskopiering. Backupsystemet som används är Commcault Simpana och backupen utförs av Framtidens IT. Avseende SQL-servrarna kör backupsystemet transaktionsloggs- och fullständiga backuper dagligen. En fullständig backup tas 23.00 varje kväll och transaktionsloggsbackup tas vid 7 tillfällen dagligen. För samtliga virtuella servrar tas backup enligt ett veckoschema som innefattar två fullständiga backuper (tisdag & fredag) och däremellan inkrementella backuper på de förändringar som har skett. Det är endast lördagen som ingen backup tas på samtliga virtuella servrar.

I samtliga produktionsservrar lagras backupdata i backuphanteringssystemets diskpool och ett regelverk är uppsatt för hur länge backuper sparas. Dagliga backuper sparas i 32 dagar,

veckobackuper sparas i 90 dagar, månadsbackuper sparas i 5 år och kvartalsbackuper sparas i 10 år. Gällande testservrar lagras daglig backupdata i 21 dagar. Samtliga backupservrar och diskpooler finns i datahallar hos Göteborgslokaler och Bostadsbolaget och informationen kopieras mellan dessa båda hallar för att uppnå full redundans.

Enligt Poseidon utförs återläsningstest av säkerhetskopierad data årligen i syfte att ha en uppdaterad testmiljö. Detta genomförs inte efter en fastställd rutin för att säkerställa att säkerhetskopierad data är återläsningsbar utan för att ha en uppdaterat testmiljö, vilket inte är i linje med *Regler för driftsdokumentation*.

3.6.2 Förändringshantering

Iakttagelser

Poseidon har en utvecklingsrutin för att hantera konfigurationer, ändringar i FAST2 och versionsuppgraderingar. Den övergripande rutinen härstammar från Framtidenskoncernens modell för gemensam utveckling, som fastställer att samverkan mellan bostadsbolagen ska främjas vid utveckling av FAST2. Grupporganisationen, där FAST2 förvaltningsorganisation ingår, har som syfte att genom samverkan mellan bostadsbolagen vidareutveckla systemet på ett gemensamt sätt. Utveckling av specifika anpassningar ska i största möjliga mån inte utföras, då målbilden är att genomföra gemensam utveckling bostadsbolagen emellan. Rutiner för förändringshantering regleras i flertalet formaliserade dokument och genom SLA mellan Framtidens IT och Poseidon.

Dokumentet *Modell för gemensam utveckling av FAST2* kan ses som ett ramverk över hur utvecklingsfrågor i FAST2 ska hanteras inom Framtidenkoncernen, medan *Framtidens modell för gemensam utveckling* omfattar samtlig IT-verksamhet. Dokumentet kring gemensam utveckling av FAST2 omfattar uppdrag, ansvar, roller och mandat och reglerar hur bolagen ska arbeta gemensamt med utvecklingsfrågorna. Modellen omfattar aktiviteter kopplat till både vidareutveckling och systemutveckling. Inom den gemensamma utvecklingen finns tre huvudsakliga processer:

- Hantering av önskemål och ändringar
- Beredningsprocessen
- Beslutsprocessen

Dessa tre processer, tillsammans med planering och uppföljning, styr utvecklingsrådets och beredningsgruppens arbete. Önskemål om ändringar i FAST2, som uppstår dels i Poseidon och dels i de andra bostadsbolagen, hanteras i den koncerngemensamma processen. Önskemål lyfts och prioriteras i utvecklingsrådet och beredningsgruppen med syftet att ha en gemensam hantering av ärendet. Lokalt hos Poseidon och de andra bostadsbolagen ställer detta krav på att prioritera ärenden i förhållande till kostnad, nytta och långsiktig utveckling av FAST2. Poseidon har rätt att göra viss lokal utveckling, men det ska vara inom ramen för befintlig funktionalitet och inte påverka de övriga bostadsbolagen.

Prioriterade ändringar lyfts sedan i utvecklingsrådet och bereds gemensamt i utvecklingsgruppen, där kommunikation sker med systemleverantören och uppgifter kring bl a kostnad och funktionsspecifikation tas fram. Beslut om beställning av ärendet tas sedan gemensamt i

utvecklingsrådet. Om beställningen klassas som en större investering behöver det förankras i IT-rådet eller i VD-rådet. Beslut om utveckling tas sedan upp i utvecklingsplanen.

Poseidon har ett eget dokument som beskriver processen för att versionsuppgradera deras IT-system i sju steg och omfattar planering inför uppgradering, testning och rutiner vid produktionssättning. Processflödet beskriver väsentliga godkännandesteg som behöver genomföras såsom formellt godkännande av systemägaren inför produktionssättning, vilket sker i dokumentet. Processflödet påvisar vilket ansvar de olika rollerna internt har vid uppgradering av befintliga system.

Framtidens IT har en förändringshanteringsrutin, *Framtidens IT Change Management.* Syftet med denna rutin är att på ett kontrollerat, effektivt, säkerhets- och bestlustsmässigt korrekt sätt införa ändringar i den IT-relaterade produktionsmiljön. Rutinen omfattar samtliga ändringar i IT-miljön, stora som små, och beroende på storlek kan olika ansvarsroller vara involverade. Dokumentet slår fast vilket ansvar olika roller har vid olika typer av ändringar.

KPMG har granskat rutinen för förändringhantering. Poseidon har en testmiljö där uppgraderingar alltid testas enligt etablerade rutiner och utöver testmiljön har Poseidon även en utbildningsmiljö.

3.6.3 Incidenthantering

Iakttagelser

Poseidon har en etablerad rutin för incidenthantering som finns beskriven i Framtidens IT:s dokument, *Incident Management.* Processen beskriver hur incidenter ska hanteras. En felanmälan ska registreras och dokumenteras i Service Desk Plus. Utöver denna rutin finns ett ytterligare dokument som avser problemhantering, *Framtidens IT Problem Management.* Det primära målet med incident- och problemhanteringen är att återställa normal drift så snabbt som möjligt och minimera de negativa konsekvenserna för verksamheten. Detta regleras genom ett SLA med Framtidens IT. Ovanstående dokument beskriver tydligt processen för att registrera ärenden och den efterföljande processen för att åtgärda incidenten eller problemet.

När en incident inträffar som berör ett IT-system ska incidenten rapporteras. Ansvaret för att rapportera en incident har samtliga medarbetare och användare. Incidenten kan antingen rapporteras till systemansvarig eller till IT-supporten. Det finns två sätt att registrera incidenter, dels i Bugtracker samt dels i Service desk. Bugtracker är ärendehanteringssystemet som används tillsammans med systemleverantören FAST2 medan Service desk är ärendehanteringssystemet som används tillsammans med Framtidens IT.

3.6.4 Avbrottsrutiner

Iakttagelser

Poseidon har dokumenterat vissa manuella rutiner i händelse av avbrott kopplat till FAST2. Bolaget har ett dokument som beskriver informationsflödet vid ett längre stopp i FAST2. Där framgår det hur olika målgrupper ska informeras i händelse av ett stopp (mail etc.), vilken information de olika målgrupperna ska få samt vem som är ansvarig för att informera. Motsvarande rutin och informationsflöde finns när beslut om att starta FAST2 tas.

Poseidon har delvis gjort en kartläggning och kontinuitetsplan för verksamheten om det blir allvarliga driftstopp. Informationsflödet, beskrivet ovan, är en del av kontinuitetsplaneringen och utöver den har processer i FAST2 kartlagts samt bedömts med avseende på hur de kan fortskrida vid avbrott. Flertalet processer i systemet är svåra att göra manuellt såsom t ex hyresredovisning, debitering och avisering. För de processer som kan utföras manuellt har vissa beskrivningar tagits fram.

I Förvaltningsobjekt finns information kring katastrofberedskap. Applikationer i FAST2 körs på en virtuell server och databaserna finns inom en SQL-klusternod. I händelse av en kris så återställs den virtuella servern i Framtidens IT:s reservdatorhall och SQL-klusternoden flyttas över till en annan fysisk server i SQL-klustret. Framtidens IT räknar med att FAST2 kan vara uppe inom ett dygn.

3.6.5 Bedömning och rekommendationer

Bedömning

KPMG bedömer att Poseidon till stor del har tillfredställande rutiner implementerade för backup- och ändringshantering i enlighet med *Regler för driftsdokumentation*. Backuphantering bör säkerställa att säkerhetskopierad data går att återläsa, medan ändringshantering bör säkerställa att ändringar och uppgradering som produktionsätts inte är felaktiga eller olämpliga. Dock bedömer KPMG att det finns svagheter i rutinen för återläsning, vilket medför en risk för att integriteten, tillgängligheten och säkerheten i data inte är tillräckligt säkerställd. Vidare bedömer KPMG att det finns formaliserade rutiner för att hantera incidenter och avbrott. Dessa rutiner bedömer KPMG bör säkerställa att incidenter hanteras på ett lämpligt och enhetligt sätt.

Rekommendationer

KPMG rekommenderar Poseidon att implementera en rutin för regelbundet test av återläsning av säkerhetskopierad data. Tester bör genomföras minst årligen och de bör dokumenteras. Komplettera även återläsningen av testdatabasen med dokumentation som styrker att det är ett fullständigt återläsningstest.

3.7 Hantering av personuppgifter och känsliga personuppgifter (revisionsfråga 7)

Iakttagelser

När en hyresgäst tecknar ett hyresavtal med Poseidon behöver hyresgästen samtycka till att hyresvärden behandlar personuppgifter om hyrestagaren, vilket är i linje med Stadens *Policy och riktlinje för tillämpning av PUL*. Hyrestagaren samtycker med följande:

- De personuppgifter som lämnas till hyresvärden i samband med tecknandet av hyresavtalet kommer att behandlas i den utsträckning som behövs för att kunna fullgöra avtalet.

- Informationen kan avse hyresavisering, hyresförhandling, information till hyresgästen och annat som avser den löpande förvaltningen. Personuppgifter som inhämtas under

hyresförhållandet kan komma att behandlas såsom uppgifter om betalningsförsummelser och störningar i boendet.

- Hyresgästens personuppgifter kan också komma att lämnas ut till organisationer eller föreningar som hyresvärden samarbetar med.

I *Policy och riktlinje för tillämpning av PUL* framgår det att det ska finnas en förteckning över vilka behandlingar av personuppgifter som utförs inom verksamhetsområdet. Enligt policyn bör personuppgiftsombudet lämpligen anteckna ändringar och avslut av behandling av personuppgifter. Poseidon har upprättat en förteckning, *Fast2*, som beskriver personuppgiftsbehandling och där framgår följande information:

- Information om personuppgiftsansvarig

- Information om registret och behandling i FAST2. Informationen avser vilket ändamål som finns med behandlingen, som kan vara behandling av personuppgifter i samband med uthyrning av bostäder och/eller löpande förvaltning av hyresrätter. Informationen avser även vilka mottagare som kan få ta del av personuppgifter, om uppgifter kan komma att föras över till tredje land samt åtgärder för att trygga säkerheten i behandlingen.

- Information om den lagliga grunden för behandlingen, vilket är att den registrerade lämnat sitt samtycke och att en arbetsuppgift i samband med myndighetsutövning ska kunna utföras.

- Information om övriga uppgifter om behandlingen, som avser vilka uppgifter som behandlas, att inga känsliga uppgifter registreras och att den registrerade behöver informeras och signera skriftligt vid registrering.

Dokumentet innehåller därmed information om hur Poseidon arbetar med att behandla personuppgifter såsom insamling, lagring, bearbetning och spridning i enlighet med *Policy och riktlinje för tillämpning av PUL*. I Poseidons dokument *Fast2* framgår det vem som är Personuppgiftsombud.

Det finns implementerade rutiner för att hantera persondata i syfte att säkerställa att data är korrekt inlagt i FAST2. Avidentifiering, ordanalys och rensning av personuppgifter görs regelbundet. Har det inte funnits en relation med en kund de senaste 24 månaderna avidentifieras kunden och detta sker manuellt 12 gånger per år. Vid avidentifieringen skapas en logg för kontroll innan den skarpa körningen genomförs och loggen jämförs sedan med testkörningen. Rensning av händelser, dokument och ärenden genomförs även det 12 gånger per år. För att säkerställa att inga olämpliga personuppgifter finns lagrade om hyresgäster i fritextfält genomförs en ordanalys. Analysen initieras av systemansvarig, körs per automatik och går ut på att söka igenom fält för att identifiera ord som kan vara olämpliga kopplat till hyresgäster. Analysen genomförs 12 gånger per år och vid revisionstillfället fanns drygt 200 ord registrerade som möjligt känsliga och olämpliga.

Poseidon har klassificerat data i FAST2 vilket framgår i Förvaltningsobjekt. Klassificeringen har skett utefter en kravnivå bestående av tregradig skala utefter områden sekretess, riktighet och tillgänglighet. Systemet har klassificerats som 2.2.2, alltså den högsta kravnivån utifrån samtliga områden. Klassificeringen saknar en koppling mellan identifierade behandlingar av

personuppgifter och klassificeringen, det är själva systemet som har klassificerats och inte specifika behandlingar.

Det pågår ett stort arbete inom bostadsbolagen med att klassificera samtliga data och fysiska dokument inom bolagen. Den drivande faktorn har varit att Poseidon och de andra bostadsbolagen behöver ha en dokumenthanteringsplan. Dokumentation KPMG har tagit del av verifierar att data har klassificerats utefter bedömningskriterierna i *Riktlinje för informationssäkerhet*.

I och med införandet av Dataskyddsförordningen 2018 har bolagen i Framtidenkoncernen bildat ett PUL-råd. Rådet syftar till att förbereda bolagen i koncernen på de kommande regelförändringarna samt skapa ett gemensamt förhållningssätt och arbetssätt inom bolagen. Första skedet är en genomlysningsfas, med syfte att identifiera vilka områden som behöver anpassas till de kommande reglerna. Det gemensamma arbetet startades i september 2016 och PUL-rådet hade sitt första möte i november 2016.

Bedömning

KPMG bedömer att ansvarsroller med avseende på PUL har fördelats inom bolaget och att det finns strukturer implementerade för att informera hyresgäster om hur deras personuppgifter och känsliga personuppgifter hanteras i FAST2. Kopplat till rollerna finns tydliga beskrivningar av vilket ansvar de olika rollerna har vid arbete med personuppgifter. Det finns även en förteckning som beskriver vilka personuppgifter som behandlas i FAST2, dessa har dock inte klassificerats fullt ut gentemot kravnivå på sekretess, riktighet och konfidentialitet, KPMG noterar att detta är ett pågående arbete. KPMG bedömer att det finns implementerade rutiner för att säkerställa gallring av information och att inga olämpliga personuppgifter finns med i fritextfält genom de månatliga gallringsrutinerna och ordanalyserna.

Rekommendationer

KPMG rekommenderar Poseidon att komplettera den nuvarande förteckningen över behandlingar av personuppgifter med en klassificering av data i enlighet med *Riktlinje för informationssäkerhet*. Förteckningen bör innehålla rekommendationerna som återfinns i *Riktlinje för informationssäkerhet* och kan med fördel mappas mot resultatet av det arbete som genomförs med dokumenthanteringsplanen.

3.8 Säkerhet avseende intrång och manipulering (revisionsfråga 8)

Iakttagelser

Dagens hotbild är väldigt dynamisk och bilden av en ensam aktör är numera förlegad. Aktuella dataintrång genomförs av professionella aktörer och nationer. I FAST2 sammanhang är det främst tillgången till personuppgifter i systemet som motiverar en aktör.

FAST2 applikationen (installerad på handläggares klientdatorer) baseras på Java-teknologi som vid installation kommunicerar i klartext.

Applikationen kommunicerar också i klartext vid generell användning av funktioner som användaren har behörighet att använda. Även här kan ett internt hot med tillgång till viss infrastruktur (nätverket) skaffa sig tillgång användarens användarnamn och lösenord.

För detaljerad information avseende genomförd penetrationstest, se bilaga 1.

Bedömning

KPMG bedömer att bristen är allvarlig men sannolikheten är relativt låg att en aktör ska utnyttja den.

Dock ställs det krav i *Riktlinjer för informationssäkerhet* att ”Säkerhetsaspekter ska beaktas vid utveckling och anskaffning av informationssystem så att tillräckligt skydd uppnås.” Iakttagelser från genomfört intrångsförsök påvisar vissa brister i efterlevnad av riktlinjerna. KPMG noterar att Bostadsbolagen arbetar med att åtgärda bristerna och att förbättringar har skett sedan penetrationstestet utfördes.

Rekommendation

Upprätta en rutin för att säkerställa att gällande regelverk efterlevs i verksamheten.

3.9 Uppföljning och rapportering av säkerhetsnivån (revisionsfråga 9)

Iakttagelser

Uppföljning av säkerhetsnivån i systemet görs kontinuerligt av Poseidon inom ett flertal olika forum och genom olika metoder. Gällande driftrelaterade säkerhetsfrågor har Poseidon en rutin för regelbunden uppföljning tillsammans med Framtidens IT. De har kvartalsvisa driftmöten där säkerhetsrelaterade frågor behandlas såsom incidenter, kapacitetsutnyttjande etc. Mycket av det säkerhetsrelaterade arbetet för att följa upp att säkerhetsnivån är acceptabel faller inom ramen för avtalet mellan parterna. En del av leveransen avseende driften som Framtidens IT ansvarar för är att årligen genomföra en fysisk säkerhetsrevision där datahallar, som FAST2 driftas i, besiktigas okulärt för att säkerställa att skyddskraven är i linje med Stadens riktlinjer. Framtidens IT har även kontinuerlig monitorering av den övergripande driftmiljön genom övervakningsprogrammet WhatsUp. Utöver nämnda monitorering har Framtidens IT en morgonrutin som utförs varje veckodag, där eventuella larm, aktuell status och säkerhetsrelaterade åtgärder gås igenom efter en standardiserad rutin.

Enligt *Riktlinje för informationssäkerhet* ska uppföljning av informationssäkerhetsnivån i form av intern kontroll genomföras årligen och rapporteras till styrelsen. Detta genomförs årligen i december då Poseidon tar fram en intern kontrollplan som presenteras för styrelsen. Den interna kontrollplanen baseras på en riskanalys och fokuserar inte enbart på intern kontroll kopplat till informationssäkerhet. KPMG kan verifiera att kontrollpunkter kopplat till IT och informationssäkerhet finns med i den interna kontrollplanen.

Utöver ovanstående arbete genomförs ett löpande arbete där informationssäkerhetsfrågor diskuteras i både IT-rådet och IT-strategiska rådet.

Bedömning

KPMG bedömer att det finns en struktur för löpande avstämningar och dialog med Framtidens IT avseende säkerhetsnivån i IT-miljön. Framtidens IT har ett monitoreringssystem för övervakning av IT-miljön samt flertalet interna rutiner för att säkerställa att säkerhetsrelevanta händelser identifieras och följs upp. Utöver det löpande arbetet med Framtidens IT finns ett flertal forum som berör säkerhetsrelevanta händelser, såsom IT-rådet och IT-strategiska rådet. KPMG bedömer att säkerhetsrelevanta händelser regelbundet följs upp på ett strukturerat sätt.

Uppföljningar av informationssäkerhet kopplat till intern kontroll ska genomföras och rapporteras till styrelsen årligen. KPMG bedömer att detta genomförs på ett sätt som inkluderar informationssäkerhetsperspektivet, då riskanalysen som ligger till grund för den interna kontrollplanen har ett stort fokus på IT och informationssäkerhet. Baserat på genomförd granskning har KPMG gjort en sammanfattande bedömning av de uppföljningar som genomförs. I riktlinje för informationssäkerhet framgår det *"att verksamhetens ledning kontinuerligt ska följa upp att säkerhetsnivån är acceptabel och att detta ska ske minst årligen. Resultatet ska rapporteras till styrelsen*". I riskanalysen, som ligger till grund för intern kontrollplanen och som rapporteras till styrelsen, genomförs en omfattande analys av säkerhetsfrågor. Det som bolaget har bedömt som kritiskt är också det som lyfts upp till styrelsen. Vår bedömning är att uppföljning av säkerhetsnivå, baserat på de uppföljningar av informationssäkerhet och fysisk säkerhet som utförs, genomförs på ett strukturerat sätt genom alla de forum som finns.

3.10 Uppföljning av gällande regelverk (revisionsfråga 10)

Iakttagelser

Poseidon har i nuläget ingen formell rutin för hur de ska följa upp att, för granskningen tillämpliga, regelverk (se avsnitt 2.3 ovan) efterlevs inom verksamheten. De kontroller som presenteras i den interna kontrollplanen baseras på befintliga policydokument. Enligt Poseidon genomförs ett kontinuerligt arbete för att förbättra den interna kontrollen och säkerställa att regelverk efterlevs exempelvis genom utbildningar etc. KPMGs testning av intern kontroll avseende informationssäkerhet indikerar att tillämpliga väsentliga regelverk efterlevs.

Bedömning

KPMG bedömer att det saknas en formell rutin för att följa upp att, för granskningen tillämpliga regelverk och policys, efterlevs i verksamheten. KPMG anser dock att det kan vara svårt för Poseidon att hitta en lämplig rutin för att säkerställa att befintliga regelverk efterlevs, då exempelvis *Riktlinje för informationssäkerhet* saknar instruktioner för hur riktlinjen ska följas upp på lämpligaste sätt.

Rekommendation

KPMG rekommenderar Poseidon att upprätta en formell rutin för att säkerställa att, för granskningen tillämpliga regelverk, efterlevs i verksamheten.