PROTOKOLLSBILAGA G
Fullmäktiges protokoll 2013-12-20, § 10

SVERIGES RIKSBANK

Outsourcing IT

Fullmäktiges revisionsfunktion
Anders Thunholm, KPMG
2013-12-20

Outsourcing IT – drift

Syfte

2012-2013

Utvärdera den planerade outsourcingen av IT med avseende på bankens kravställning kring organisation och tänkta styrning av uppdraget för att:

- Uppnå god intern kontroll
- Följsamhet med regler och ”best practice” i den finansiella sektorn.

2013-2014

Fortsatt följa genomförandet av outsourcingen av IT-drift med avseende på bankens kravställning och tänkta styrning för följsamhet med avtal, interna och externa regler samt ”best practice” i den finansiella sektorn.

Avgränsning

- Bedömning av motiv och grunder för projektet och outsourcingen ingår ej.
- Granskning efterlevnad interna och externa upphandlingsregler ingår ej
- Utvärdering av projektstyrning ingår ej

Outsourcing IT- drift

Revisionsfunktionens referensram

- Finansinspektionens (FI) allmänna råd om styrning och kontroll av finansiella företag, FFFS 2005:1, kapitel 7 Uppdragsavtal.
- EBAs nya regelverk för corporate governance i banker (GL44) som är under införande som ny föreskrift från FI.
- Erfarenhet av hur andra organisationen arbetar med outsourcing generellt och outsourcad IT-verksamhet specifikt.
- Vedertagna ramverk för intern styrning och kontroll.

Outsourcing IT - drift

Genomförda aktiviteter 2012/2013 samt 2013/2014

- Översiktlig analys av projektdokumentation och väsentliga delar av förfrågningsunderlaget.
- Översiktlig granskning av Riksbankens utvärdering av hur leverantörerna uppfyller bör-krav med koppling till styrning och uppföljning.
- Uppföljning av hur iakttagelser omhändertagits, dels i transitionsprojektet och dels i verksamheten efter driftövertag 1 maj 2013.
- Följa transformationsprojektet i syfte att utvärdera hur intern styrning och kontroll beaktas i de olika delleveranserna.

Intervjuer och avstämningar med Riksbanken

- Beställare
- Styrgruppsmedlemmar
- Leverans- och leverantörsansvariga
- Projektledare
- Processansvariga
- Chef ITA
- Enhetschefer ITA
- Kontinuitetssamordnare

Outsourcing IT - drift

Vår bedömning är att Riksbankens del i IT-driften och i transformationsprojektet fortsatt bedrivs på ett strukturerat och tydligt sätt. Iakttagelser från augusti 2012 avseende ytterligare tydliggörande av krav och organisation för styrning och uppföljning har i stora delar omhändertagits.

Öppna iakttagelser per december 2013

- Styrdokument för outsourcing

  Utkast till policy för val av verksamhetsform har under hösten tagits fram. Denna omfattar främst fasen som föregår beslut om utläggning av verksamhet. Ytterligare riktlinjer, där Riksbankens modell för styrning och uppföljning av utlagd verksamhet mer konkret beskrivs och kopplas ihop med externa/interna krav, saknas.

Outsourcing IT - drift

- Kris- och katastrofhantering – forum och samarbetsformer

  Arbete sker genom exempelvis incidentprocessen, gemensamma planer och övningar. Vi har däremot inte kunnat ta del av någon dokumenterad samarbetsprocess där roller och gränssnitt mellan Riksbanken och leverantören tydliggörs. I den krismanual som finns för banken som helhet berörs inte heller externa leverantörer.

Åtgärdade iakttagelser per december 2013

- Förändringar i roller och ansvar – delvis otydliga
- Operativa risker – snäv definition och otydlig motpart hos leverantör
- Intern styrning och kontroll – krav om intyg från leverantören saknas
- Riktighet i data – ansvarsfördelning otydlig

Bilaga 1
Iakttagelser augusti 2012

Vår bedömning är att projektet bedrivs på ett strukturerat och ambitiöst sätt. Iakttagelser har främst noterats avseende att ytterligare tydliggöra krav och organisation för styrning och uppföljning:

Styrdokument för outsourcing

Riksbanken saknar policy eller annat styrdokument för outsourcing, vilket skapar risk för otydlighet och icke enhetlig hantering. Det är också ett krav för andra finansiella verksamheter.

Förändringar i roller och ansvar

Gränssnitten mellan de roller som förändras/skapas i o m outsourcingen kan tydliggöras. Otydlighet ökar risken för dubbelarbete och att uppgifter hamnar ”mellan stolarna”.

Bilaga 1, forts.
Iakttagelser augusti 2012

Operativa risker – definition och samarbete

Riksbanken saknar tydlig motpart hos leverantören i frågor om risk, vilket kan medföra att dessa frågor och aktiviteter inte hanteras på ett fullständigt och systematiskt sätt.

Operativ risk används i flera fall synonymt med ”säkerhetsrisk”. Risk finns då att fokus blir för smalt.

Kris- och katastrofhantering – forum och samarbetsformer

Beskrivning av forum och arbetsformer avseende kris- och katastrofhantering saknas. Vi bedömer det viktigt att Riksbankens beredskapsplaner synkroniseras med leverantörens samt löpande testas.

Bilaga 1, forts.
Iakttagelser augusti 2012

Intern styrning och kontroll – krav på leverantören

Krav på intyg avseende intern styrning och kontroll (ISK) hos leverantören saknas. Vår uppfattning är att ett sådant intyg, eller motsvarande information, är en viktig del för att kunna bedöma leverantörens ISK-arbete.

Vi rekommenderar också att krav ställs på att leverantören utser ansvarig för intern styrning och kontroll gentemot Riksbanken.

Riktighet i data – ansvarsfördelning mellan Riksbanken och leverantören

Krav samt beskrivning av roller och ansvar kopplat till åtkomst och tillgänglighet till system och data finns. Däremot är det inte uttryckt vilken part som ansvarar för riktigheten i data. Risk finns för otydlighet i roller och ansvar vilket kan påverka styrningen och uppföljningen och i slutänden datakvalitén.