Information om pågående granskning Outsourcing IT

Syfte

Utvärdering av 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.

<u>Avgränsning</u>

- Bedömning av motiv och grunder för projektet och outsourcingen.
- Efterlevnad interna och externa upphandlingsregler.

Information om pågående granskning Outsourcing IT

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.

Information om pågående granskning Outsourcing IT

Genomförda aktiviteter

- Översiktlig analys av projektdokumentation inkl delar av förfrågningsunderlaget.
- Intervju med projektansvariga samt avstämning av iakttagelser.
- Avstämning med internrevisionschefen.

Information om pågående granskning Outsourcing IT

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”.

Information om pågående granskning Outsourcing IT

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.

Information om pågående granskning Outsourcing IT

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.

Information om pågående granskning Outsourcing IT

Fortsatt granskning

Vi avser att under hösten genomföra följande aktiviteter:

- Översiktlig granska Riksbankens utvärdering av hur leverantörerna uppfyller bör-krav med koppling till styrning och uppföljning av outsourcingen.
- Uppföljning av hur Riksbanken omhändertagit gjorda iakttagelser.