Sveriges riksbank

Fullmäktiges revisionsfunktion
Slutrapport
Utvärdering av outsourcing av IT-drift

KPMG AB
2014-08-14

Innehåll

Sammanfattning

Revisionsfunktionens bedömning är att Riksbankens arbete med upphandling och utläggning av IT-driften har bedrivits på ett strukturerat och tydligt sätt. Projektet är avslutat och överlämnat till linjen. Vår bedömning är att en översyn av den styr- och samverkansmodell som Riksbanken och leverantören arbetar efter sedan ett drygt år nu är relevant att genomföra.

Våra detaljerade iakttagelser och bedömningar redovisas i rapporten nedan tillsammans med rekommendationer.

1. Inledning

1.1 Bakgrund

Riksbanken beslutade 2011-01-13att initiera en upphandling avseende outsourcing av IT-drift. Ett arbete initierades i april 2011 för att upphandla en leverantör och 2012-09-12 beslutades om att tilldela EVRY uppdraget. Baserat på detta beslut startades ett projekt bestående av ett flertal delprojekt i syfte att lämna över driften till EVRY dels att flytta utrustning till leverantörens lokaler.

Riksbanken har nu genomfört en upphandling avseende outsourcing av IT-drift och överföring av verksamhet till uppdragstagaren har genomförts stegvis och avslutades sommaren 2014. Överlämning till linjen och avslut av projektet kan innebära en förhöjd risk för störningar i verksamheten, försämrad kontroll, etc.

Även om en verksamhet outsourcas till extern part har Riksbanken fortsatt ansvar för verksamheten.

1.2 Mål och ansats

På uppdrag av fullmäktige vid Riksbanken har KPMG under perioden juni 2012 till juni 2014 löpande följt och utvärderat Riksbankens arbete med upphandling och utläggning av IT-drift.

Målet med granskningen har varit att:

- Utvärdera den planerade outsourcingen av IT med avseende på bankens kravställning och tänkta styrning för följsamhet med regler och best practice i den finansiella sektorn.
- Bedöma hur banken implementerar och tillämpar en god intern styrning och kontroll av den utlagda IT-driften samt hur projekt avslutas och lämnas över till verksamheten.

1.3 Omfattning och avgränsning

Vi har gjort en översiktlig utvärdering där avsikten har varit att identifiera de mest väsentliga förbättringsmöjligheterna avseende intern styrning och kontroll som kunnat påverka processerna kring outsourcing.

Vårt arbete baseras främst på information till och med juni 2014 och har skett utifrån Riksbankens perspektiv. Riksbankens utveckling av arbetet med styrning och uppföljning av IT-driften fortgår som en naturlig del av linjeverksamheten och därför kan förändringar ha initierats om innebär att förhållande förändrats när vår rapport lämnas till fullmäktige.

I vår utvärdering har inte ingått:
- Bedömning av motiv och grunder för projektet och outsourcingen
- Granskning av efterlevnad av interna och externa upphandlingsregler
- Granskning av projektet utifrån aspekter som kostnad, tid och kvalitet
- Bedömning av enskilda system/applikationer

1.4 Genomförande och rapportdisposition

Utvärderingen har omfattat faktainsamling och analys av relevant dokumentation, som styrande dokument, protokoll, upphandlingsdokumentation samt projektdokumentation. Intervjuer har vid väsentliga ”milstolpar” under projektet genomförts med representanter för styrgrupp, projektledning och berörda linjeansvariga. Viss verifiering av lämnade beskrivningar har skett genom begränsade stickprov.

Statusrapportering har under utvärderingsperioden löpande skett till projektet, fullmäktige och bankens internrevision.

Utifrån insamlad information har sedan analys och utvärdering gjorts som leder fram till de iakttagelser, bedömningar och rekommendationer som lämnas i denna rapport.

1.5 KPMGs referensram

- Vedertagna ramverk för intern styrning och kontroll, främst COSO[1]-ramverket
- 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.

[1] Committee of Sponsoring Organizations of the Treadway Commission

1.6 Definition intern styrning och kontroll

Enligt 1§ Riksbankslagen ska direktionen säkerställa att det vid Riksbanken finns en intern styrning och kontroll som fungerar på ett betryggande sätt vilket innebär att den bedrivs:

- Effektivt,
- Enligt gällande rätt,
- Med en tillförlitlig och rättvisande redovisning
- Med god hushållning med statens medel

2. Iakttagelser och kommentarer från genomförd granskning

2.1 Projektarbetet

Iakttagelser och bedömning

Vi har under perioden juni 2012 till juni 2014 löpande följt Riksbankens RITVA-projekt avseende outsourcing av IT-driften. Syftet med vår granskning har varit att varit att granska och bedöma hur frågor kring intern styrning och kontroll beaktats och omhändertagits. Vår granskning har inte varit att genomföra en traditionell projektgranskning utifrån metodiktillämpning, tid, kostnad och kvalitet, etc.

RITVA-projektet har under vår granskningsperiod bestått av följande tre huvudfaser:

- Upphandling
- Transition
- Transformation

Initialt genomförde vi dels en översiktlig analys och bedömning av projektdokumentation och väsentliga delar av förfrågningsunderlaget utifrån internkontrollaspekter dels en granskning av Riksbankens utvärdering av hur väl leverantörerna uppfyllde bör-krav med koppling till styrning och uppföljning.

Efter beslut om val av leverantör gick projektet in faserna transition och transformation. Under dessa faser har vi fokuserat på väsentliga milstolpar och hur intern styrning och kontroll har beaktats.

Vi konstaterar att RITVA-projektet bedrivits på ett strukturerat och tydligt sätt. Projektet har också avslutats på ett kontrollerat sätt, dels med tydliga slutrapporter, dels genom att ansvar för vidare hantering av restlista och förbättringsförslag har lämnats över och tagits emot av linjeverksamheten.

Projektet har prioriterat kvalitet i leveransen vilket inneburit att den ursprungliga tidplanen har blivit justerad. Förseningen har inte bedöms ge någon väsentlig påverkan på den slutliga kostnaden då Riksbanken till vissa delar kommer att kompenseras[2] av leverantör för förseningen.

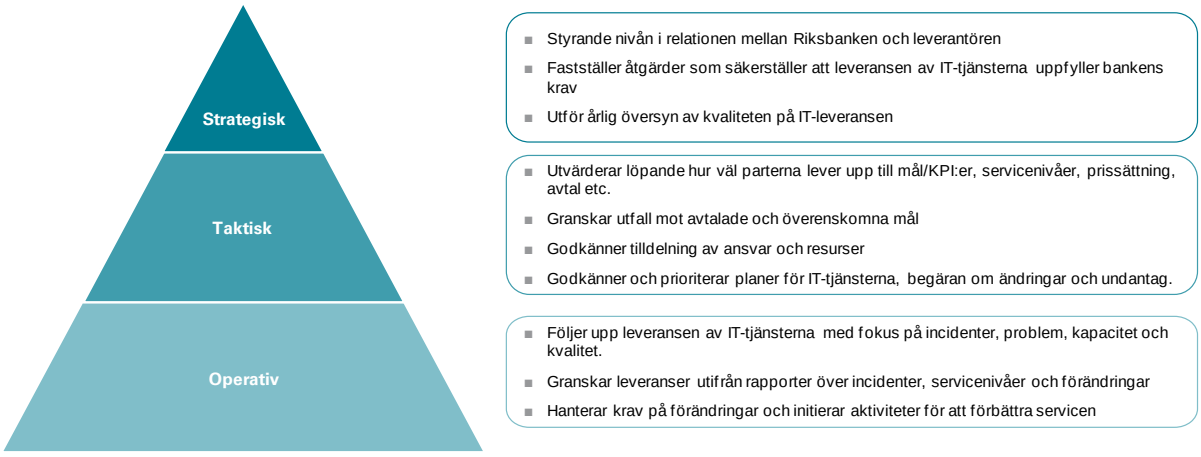
Vår granskning visar att projektet över tiden även har hanterat vissa frågor som normalt ligger inom ansvaret för linjebefattningar främst till följd av att projektet haft tillgång till beslutsfattare både hos Riksbanken och hos leverantören. Även om detta normalt sett inte är optimalt bedömer vi att projektarbetet inte har påverkats negativt av detta.

Den styr- och samverkansmodell[3] som transitionsprojektet hade att etablera utifrån upphandlings- och avtalsdokumentationen har övertagits av linjen från och med 2013-05-31.

En utvärdering av projektets effektmål är planerad att genomföras under 2015, dels för att tillräcklig tid löpt efter projektavslut och dels för att det då kommer att vara aktuellt att ta ställning till förlängning av det avtal om utlagd drift som finns med leverantören. I samband med utvärdering av projektets effektmål rekommenderar vi att det även sker en sammantagen slutrapportering för hela RITVA-projektet.

2.2 Styrning och uppföljning av IT-drift

Nedan bild illustrerar styr- och samverkansmodellen, med tre centrala forum för styrning och uppföljning av den utlagda IT-driften, strategiska, taktiska och operativa. Utöver dessa forum finns även avtals- och ekonomiforum.



2.2.1 Internt mot verksamheten

Iakttagelse och bedömning

Den ordinarie verksamhetsplaneringsprocessen som finns på Riksbanken har även omfattat RITVA-projektet och den verksamhet som lagts ut. I och med att RITVA-projektet nu är avslutat

[2] Diskussioner med leverantören har skett under sommaren 2014.

[3] Se vidare avsnitt 2.2

och verksamheten är helt utlagd och flyttad från Riksbankens lokaler är vår bedömning att förutsättningarna är väsentligt förändrade jämfört med föregående år. Processer för leverans- och leverantörsstyrning har etablerats och förstärkts resurs- och kompetensmässigt. Det har ännu inte genomförts någon strukturerad och dokumenterad utvärdering av hur verksamhetsplaneringsprocessen inklusive riskanalysen bör utvecklas för att hantera den förändrade situationen.

Rekommendation

Vi rekommenderar att Riksbanken i samband med verksamhetsplaneringen 2015 säkerställer att riskanalysen beaktar de nya förutsättningarna, både på kort och på lång sikt.

2.2.2 Externt mot leverantören

Iakttagelse och bedömning

Sedan maj 2013 har EVRY skött IT-driften, först i Riksbankens lokaler och sedan successivt under transformationsprojektet i egna lokaler. Under denna tid har en överenskommen styr- och samverkansmodell tillämpats. Vi noterar att verksamheten själv har identifierat behov av anpassa modellen för en mer ändamålsenlig styrning och uppföljning av leverantören. Detta har skett genom bland annat externa granskningar av väsentliga processer hos leverantören, kravställning avseende underlag för uppföljning, såväl ekonomisk som verksamhetsorienterad.

Det är främst det operativa, men till vissa delar också det taktiska forumet, som hittills varit aktivt där frågor kring intern styrning och kontroll på en övergripande nivå inte omhändertas. Vår granskning visar därför att det nu finns ett behov av en tydlig motpart hos leverantör i frågor kring intern styrning och kontroll med mandat att också styra över resurser för den löpande IT-driften samt utvecklingsfrågor

En ny organisation[4] har under våren införts hos Riksbanken vilken vi bedömer ger goda möjligheter att arbeta vidare med utveckling av styrmodellen. Projektets styrgrupp har som ovan nämnts även kommit att hantera linjefrågor. I och med att projektet är avslutat måste verksamheten säkerställa att resurser, kompetens och beslutskraft finns både internt på Riksbanken och hos leverantören.

Chefen för Avdelningen för verksamhetsstöd (AVS) arbetar aktivt med dessa frågor och planerar bland annat två granskningar hos EVRY under andra halvan av 2014, en med fokus på styrning och ledning (governance) och en inriktad på informationssäkerhet.

Rekommendation

Vi rekommenderar att Riksbanken säkerställer att en översyn av styr- och samverkansmodellen, forumens funktion och samspel med den nya organisationen genomförs.

Vidare rekommenderar vi att Riksbanken säkerställer att kompetens kring kravställning och styrning och uppföljning av leverantören upprätthålls.

[4] Avdelningen för verksamhetsstöd

2.3 Informationssäkerhet, kris- och kontinuitetsarbetet

Iakttagelse och bedömning

Inom ramen för verksamhetsplaneringen har risker på en övergripande nivå identifierats och analyserats, både i RITVA-projektet och i linjeverksamheten.

Vår granskning har visat att det informationssäkerhetsarbete som sker i linjen främst handlar om kontroll- och uppföljning av behörigheter vilket är en viktig aspekt med riskerar att bli för ”snävt” då informationssäkerhet är mer än detta.

Rekommendation

Vi rekommenderar att Riksbankens säkerställer att informationssäkerhetsarbetet omfattar alla delar för att säkerställa fullständighet och täckning i kontroll av risker, samt sker i linje med den riskanalys som sker i verksamhetsplaneringsprocessen.

Iakttagelse och bedömning

När det gäller kris- och kontinuitetsarbetet har vi tidigare rapproterat att det sker genom incidentprocessen, gemensamma kontinuitetsplaner med leverantören och samövningar. Däremot har vi inte kunnat ta del av någon dokumenterad samarbetsprocess där roller och gränssnitt mellan Riksbanken och leverantören tydliggörs. I Riksbankens krismanual berörs inte heller externa leverantörer.

Rekommendation

Vi rekommenderar att Riksbanken tydliggör hur samarbetet och samverkan mellan banken och leverantören, i olika forum och i olika skeenden, i samband med en kris ska se ut.

Anders Thunholm
Partner KPMG

Bilaga A

Granskningen har omfattat genomläsning av relevant dokumentation, viss verifiering samt intervjuer med nyckelpersoner:

Intervjuer

Intervjuerna har genomförts med följande personer inom Riksbanken.

Namn	**Befattning**
Kai Barvèll	Ordförande Ritva styrgrupp
Marianne Olsson	Chef Avdelningen för verksamhetsstöd / styrgruppsmedlem
Mats Wallinder	Projektledare transition och transformation
Anders Hellström	Leverantörsansvarig
Olof Fredriksson	Tf Chef IT avdelningen
Urban Örtberg	Riskenheten, kontinuitetsfrågor
Lars Andersson	Riskenheten, säkerhetsfrågor
Anja Marletta	Compliance
Helena Runnquist	IT avdelningen, kontinuitetsfrågor
Annika Hallin	IT avdelningen, kontinuitetsfrågor

Källförteckning

Dokumentation som inhämtats och ingått i granskningen på olika sätt:

Upphandlingsdokumentation

Avtal inkl. bilagor

Planer och dokumentation Transitions- och transformationsprojektet

Slutrapporter Transitions- och transformationsprojektet

Protokoll styrgrupper och samverkansforum

IT-verksamhetens riskanalys

Styrdokument kring kontinuitetshantering och krisberedskap

ITIL-processer, urval av relevanta för uppdraget