VÄSTRA GÖTALANDSREGIONEN

Uppföljning av IT-granskningar

Dnr Rev 22-2013

Genomförd av: Revisionsenheten
Sofi Ericsson

Behandlad av Revisorskollegiet den 19 juni 2013

1 Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Västra Götalandsregionen har revisionsenheten genomfört en uppföljning av de revisionsrapporter som har bäring på informationssäkerhet under åren 2009-2010. Syftet med granskningen är att följa upp om och hur nämnder och styrelser har hanterat de synpunkter som framkommit i revisionens tidigare granskningar av området informationssäkerhet. Frågorna har besvarats skriftligen av VGR IT.

Följande granskningar har följts upp:

- Granskning av IT-visionen och verkligheten
- Styrning av VGRnet
- Styrning, prioritering och samordning av regiongemensam verksamhetsutveckling med stöd av IT
- Kan IT-säkerheten påverka patientsäkerheten?

Vi kan konstatera att det har hänt en hel del inom området IT sedan revisionsrapporterna skrevs. Sedan rapporterna skrevs har ansvaret för VGR IT övergått från regionservice till regionstyrelsen. Styrelsen har utsett fyra ledamöter att ansvara för bevakning av IS/IT-frågor, de ska också hålla övriga ledamöter informerade i ämnet. Svaren från VGR IT visar att många av de problem som lyftes fram i revisionsrapporterna förväntas bli avhjälpta i och med att den nya organisationen trätt i kraft. Med den ska rutiner och processer bli tydligare för både användare, beställare och de ansvariga för systemen. Dock är det svårt för revisionen att bedöma om den nya styrmodellen fungerar som tänkt och därmed har hanterat de risker som revisorerna tidigare lyft fram. En uppföljning av den nya styrmodellen för att säkerställa att arbetet fortskrider enligt plan är planerad att ske under 2013. Då modellen ännu inte är fullt ut implementerad bedömer revisorerna att det finns en risk för att givna rekommendationerna ännu inte är åtgärdade.

2 Inledning

2.1 Bakgrund

Revisionsenheten har som en del i den årliga granskningen och på uppdrag av de förtroendevalda revisorerna i Västra Götalandsregionen följt upp de revisionsrapporter som har bäring på informationssäkerhet under åren 2009-2010.

Revisorerna har fått indikationer om att en rad beslut gällande informationssäkerhet inte har implementerats i den omfattning som förutsatts i besluten. Då en del av besluten är föranledda av tidigare granskningar, är det viktigt att de synpunkter som framkommit blivit åtgärdade.

Denna rapport följer upp hur revisorernas rekommendationer hanterats.

2.2 Syfte

Syftet med granskningen är att följa upp om och hur nämnder och styrelser har hanterat de synpunkter som framkommit i revisionens tidigare granskningar av området informationssäkerhet.

2.3 Metod

Granskningen är en dokumentstudie med en genomgång av revisionsrapporterna och nämnders och styrelsers svar, från 2009 och 2010. Specifika frågor har därefter riktats till granskad nämnd/styrelse i syfte att få belyst hur revisorernas iakttagelser och rekommendationer har beaktats i det fortsatta arbetet. Frågorna har besvarats skriftligen.

3 Uppföljning av tidigare års granskningar rörande IT

Nedan presenteras korta sammanfattningar av granskningsrapporterna i kronologisk ordning tillsammans med revisorernas rekommendationer. Därefter följer beskrivningar av det uppföljningsarbete som nämnderna/styrelserna vidtagit efter granskningarna. Beskrivningarna bygger på VGR IT:s skriftliga svar avseende uppföljningsarbetet.

3.1 Granskning av IT-visionen och verkligheten

Syftet med granskningen var att göra en gap-analys mellan målen i Västra Götalandsregionens IT-vision och det verkliga utfall som projekten i handlingsplanen då hade lett till. Ambitionen var att i analysen få en samlad bild av regionens förmåga att styra mot målen i IT-visionen och till effekthemtagning.

I denna uppföljning ligger fokus på de generella iakttagelser samt de analyser och rekommendationer som lämnas i revisionsrapporten IT-visionen och verkligheten.

I rapporten lyfts ett antal rekommendationer:

- tydligare berednings- och beslutsprocess samt bättre kommunicering av dess principer
- bättre samordning mellan olika projekt
- ökat inflytande från politiken

3.1.1 Uppföljning av vidtagna åtgärder

För bättre kontroll på förvaltningars behov av IS/IT-stöd finns nu en styrmodell med en tydlig beredningsprocess inarbetad. Till denna finns berednings- och prioriteringsprinciper beskrivna tillsammans med instruktioner för hur beredning och kommunikation med kunder/förvaltningar skall ske.

Ett IS/IT projektkontor med uppgift att samordna och följa upp alla IS/IT projekt i regionen har inrättats.

IS/IT-direktören har möte en gång i månaden med fyra ledamöter från regionstyrelsen, vilka utgör den politiska styrgruppen för IT.

3.2 Styrning av VGRnet

Syftet med granskningen var att utvärdera om styrningen av VGRnet var ändamålsenlig. VGRnet är regionens gemensamma kommunikationsnät för utbyte av information, både data- och telekommunikation.

I granskningen av styrningen av VGRnet lämnades ett antal rekommendationer fram, från hög prioritet till låg prioritet. I denna rapport följs endast rekommendationerna med hög prioritet upp.

- Översyn av investeringsprocessen för infrastruktur, i syfte att göra den mer ändamålsenlig för både nyttjare, beställare och utförare.

- Genomföra ytterligare aktiviteter för att kommunicera ut information om den nya organisationen, dess funktioner och förekommande ansvarsområden. Bland annat bör klargöras vem som är systemägare av VGRnet.

3.2.1 Uppföljning av vidtagna åtgärder

Investeringsprocess finns framtagen och beskriven, tillsammans med investeringshandbok. Beslut om ny version kommer innan sommaren.

Systemägarskapet för VGRnet ingår tillsammans med ny styrmodell i objekt Teknisk plattform.

3.3 Styrning, prioritering och samordning av regiongemensam verksamhetsutveckling med stöd av IT

Syftet med granskningen var att bedöma om organisationen för regionens styrning av IT-verksamheten och dess projekt var ändamålsenlig och effektiv.

I granskningen identifierades ett antal risker med tillhörande rekommendationer. Nedan följer de som bedömdes kunna utvecklas från ”risk” till ”hög risk” och som kompletterades med rekommenderade förbättringar eller förändringar. Inga väsentliga brister kunde identifieras.

- Risk för att beslut om regiongemensam verksamhetsutveckling med stöd av IT fattas, utan någon fullständig bild av nytta och effekthemtagning. Revisorerna rekommenderade att projekten och dess effektmål skulle förtydligas, samt hur de knyter an till de prioriterade målområdena. Den strategiska informationen behöver utnyttjas mer effektivt för att leveransförmågan avseende föreslagna projekt ska kunna bedömas.
- I syfte att förtydliga kopplingen mellan de prioriterade målen och nyttan med hemtagningseffekter på projektnivå bör en analys på portföljnivå göras
- Analysera nyttan och hemtagningseffekterna från alla prioriterade projekt.
- Undersök möjligheten att använda Cognos eller annat verktyg för att följa upp och samordna tänkbara förbättringar
- Gör en riskanalys, som del av prioriterings- och urvalsprocessen, innan beslut om årlig handlingsplan tas.
- Analysera effekter mot accepterad risknivå löpande, tex innan projekt godkänns för införande och/eller beslut om breddinförande fattas.
- Fastställ principer för hanteringen av kostnader för förvaltningarnas deltagande i projekt.
- Stärk IT-direktörens roll i strategiska IS/IT-frågor.
- Förtydliga de lokala beställarnas roll avseende utveckling av IT-stöd. Om de prioriterade projekten i handlingsplanen ska genomföras måste troligtvis beställarrollen begränsas
- En verksamhetsstyrd IT-utveckling förutsätter att formerna för verksamhetens prioriteringar förtydligas och att fler personer från kärnprocesserna kommer in tidigt i processen
- Förtydliga IT-rådets mandat samt de beslutsvägar som gäller

3.3.1 Uppföljning av vidtagna åtgärder

Här hänvisas till den styrmodell som håller på att implementeras, inklusive pågående effekthemtagningsprojekt. Styrmodellsägare är Ingela Tuvegran.

3.4 Kan IT-säkerheten påverka patientsäkerheten?

Granskningen syftade till att ge en bild av hur arbetet med IT-säkerhet kan påverka patientsäkerhetsarbetet, utifrån hur fem olika avvikelser hanterats i Västra Götalandsregionen.

Följande rekommendationer lämnades i samband med revisionsrapporten:

- Förtydliga kopplingen mellan avvikelsehantering och arbetet med informationssäkerhet. Det krävs ett träget arbete för att all personal ska bli medveten om vikten av och sambandet mellan patientsäkerhet och informationssäkerhet.
- Säkerställ att rutinerna kring ett regionalt MedControl omfattar IT-relaterade avvikelser och se till att alla berörda aktörer blir delaktiga. En framgångsfaktor är att arbetet följs upp och att resultaten redovisas. För detta har politikerna ett särskilt ansvar.
- Regionservice och VGR IT i synnerhet, bör utveckla rutiner och utse ansvariga för hantering av avvikelserna i ett ärendes olika steg. Detta fordrar förmodligen en särskild utbildning eller informationsinsats för personalen vid regionservice.
- I beställar-/utförarmodellen kan det vara lämpligt att regionservice åtagande vid avvikelsehantering betraktas som en tjänst, med en definierad servicenivå. Det ger en tydlighet där förväntningar omsätts i krav.
- Granskningen har visat på behovet av fler fora för dialog och samverkan samt en bättre återkoppling. Det ska ge en sömlös avvikelsehantering över förvaltningsgränser och verksamhetsområden. Detta gäller särskilt mellan verksamhetschefer i vården och VGR IT respektive VGR IT och medicinteknik.

3.4.1 Uppföljning av vidtagna åtgärder

Kommentar till ovanstående rekommendationer ur ett VGR IT-perspektiv:
Det finns ett regionalt MedControl som hanterar omfattande IT-relaterade avvikelser. Gemensamma rutiner och utbildningsinsatser är införda sedan tidigare, då VGR IT var en del av regionservice. Arbetssätt och rutiner för avvikelsehantering anpassas just nu efter regionens nya styrmodell, där dialogen kring avvikelser borde ha ännu bättre förutsättningar i och med införandet av så kallad objektifiering i regionens samtliga IT-system.

3.5 Vår bedömning

Vi kan konstatera att det har hänt en hel del inom området IT sedan revisionsrapporterna skrevs. I hälso- och sjukvården utvecklas hela tiden nya system som ska leda till bättre och säkrare vård för patienterna. Denna snabba utveckling leder också till ett ökat behov av regional samordning av IS/IT.

Sedan rapporterna skrevs har ansvaret för VGR IT övergått från regionservice till regionstyrelsen. Styrelsen har utsett fyra ledamöter att ansvara för bevakning av IS/IT-frågor, de ska också hålla övriga ledamöter informerade i ämnet.

Under 2012 beslutades om en ny styrmodell för IS/IT. Syftet var att få en samordning, styrning, prioritering och finansiering där samtliga regionens verksamheter är delaktiga. Verksamheterna delas in i branscherna: hälso- och sjukvård, regional utveckling, kultur och

miljö, trafik (ej startad) och regiongemensam bas och service. Varje bransch leds av en branschledning. Det är ett forum vars uppgift och ansvar är att leda IS/IT-utvecklingen i sin bransch för att ge de gemensamma verksamhetsbehoven ett effektivt stöd. Ytterst ansvarig för strategiska IS/IT-beslut, prioritering och fördelning av resurser till de olika branscherna är IS/IT-ledning Koncern.

Svaren från VGR IT visar att många av de problem som lyftes fram i revisionsrapporterna förväntas bli avhjälpta i och med att den nya organisationen trätt i kraft. Med den ska rutiner och processer bli tydligare för både användare, beställare och de ansvariga för systemen. Dock är det svårt för revisionen att bedöma om den nya styrmodellen fungerar som tänkt och därmed har hanterat de risker som revisorerna tidigare lyft fram. En uppföljning av den nya styrmodellen för att säkerställa att arbetet fortskrider enligt plan är planerad att ske under 2013. Då modellen ännu inte är fullt ut implementerad bedömer revisorerna att det finns en risk för att givna rekommendationerna ännu inte är åtgärdade.