Region Gävleborg

REVISORERNA

2019-12-16

Till
Regionfullmäktige

För kännedom
Styrelse/nämnder

Granskning – generella IT-säkerheten i regionens redovisningssystem

I samband med revisionsplaneringen för Region Gävleborg har en risk- och väsentlighetsanalys genomförts där system samt applikationer kopplat till den finansiella rapporteringen bedömts som kritiska.

Regionen har i sin verksamhet ett stort beroende av sina IT-system, vilket i sig kan medföra risker. Redovisningssystemet (Agresso) är komplext med många systembaserade försystem. Det sker en mängd olika filöverföringar från försystem till redovisningssystemet som sker automatiskt utifrån tidsschema. Flera av försystemen har en väsentlig inverkan på redovisningen. Om en filöverföring inte fungerar som tänkt kan det skapa stora fel i redovisningen. Eller om användare med felaktiga behörigheter vidtar felaktiga åtgärder kan det också skapa stora fel i redovisningen. Vidare kan det få förödande konsekvenser om systemet kraschar och rutinerna för säkerhetskopiering är bristfälliga.

Syftet med granskningen har varit att bedöma förvaltning och intern kontroll för ekonomisystemet, vilken innehåller data som är kritiska för den finansiella informationen. Granskningen har även syftat till att säkerställa att data hanteras fullständigt och riktigt.

Granskningen har besvarat följande revisionsfråga:
Har regionstyrelsen säkerställt att förvaltningen av kritiska applikationer stödjer kraven enligt ISA 315[1]?

Granskningsresultatet har bedömts utifrån skalan "ej uppfyllt", "i begränsad utsträckning", "till övervägande del" eller "helt uppfyllt" och den sammanfattade bedömningen är:

Vår sammanfattade revisionella bedömningen är att regionstyrelsen **till övervägande del** har grundläggande processer och rutiner på plats gällande förvaltning av redovisningssystemet Agresso för att stötta kraven i ISA315.

[1] ISA - behandlar revisorns ansvar för att identifiera och bedöma riskerna för väsentliga felaktigheter genom att förstå företaget och dess miljö. Här ingår företagets interna kontroll.

Med utgångspunkt från de iakttagelser och bedömningar som har framkommit i granskningen lämnar vi följande rekommendationer till regionstyrelsen:

- Fortsätta arbetet med förvaltningsdokumentationen för redovisningssystemet. Förvaltningsdokumentationen behöver bland annat omfatta riskanalys, roller och ansvar samt instruktioner och riktlinjer kring IT-styrning och förvaltning såsom förändringshantering samt kontinuitets- och katastrofhantering.
- Implementera en rutin där användare i redovisningssystemet Agresso granskas regelbundet.
- Implementera processer och rutiner för uppföljning av priviligierade användares aktivitet i syfte att validera fullständighet och riktighet i transaktioner och förändringar.
- Upprätta en process för genomförande och dokumentation av återläsning av data för redovisningssystemet Agresso.
- Analysera och utvärdera möjligheterna till att automatiskt övervaka kritiska batchjobb[2] i redovisningssystemet Agresso.

Gävle 2019-12-16

För Region Gävleborgs revisorer

Olof Bengtsson
Ordförande

Sture Sandberg
Vice ordförande

[2] Ett batchjobb är ett schemalagt program som körs utan användarintervention och används ofta för att automatisera uppgifter som måste utföras regelbundet