

Revisionskontoret
Leif Gabrielsson
Revisionsdirektör
Tfn 063-147528

2023-06-28

Dnr: REV/6/2023

Projektplan för uppföljande granskning av IT-säkerhet

1 BAKGRUND

Regionens revisorer genomförde 2020 en granskning av regionens IT-säkerhet. I granskningen framkom bland annat att det fanns en bristande efterlevnad av de styrande dokumenten då delar av det ansvar som utpekats i dokumenterad ansvarsfördelning inte uppfylls av avdelnings- och områdeschefer. Vidare framkom att det fanns risk att organisationen är sårbar då det vilar ett stort ansvar för både det strategiska och operativa arbetet på de nyckelpersoner som leder arbetet med informationssäkerhet och IT-säkerhet. Granskningen visade att medarbetare inte fått tillräcklig utbildning och därigenom den kunskap och medvetenhet som krävs för att efterleva de lagkrav och interna regler som finns för hantering av känslig information och informationstillgångar.

Det noterades att det saknades ett systematiskt arbete med informationsklassning och riskbedömning för verksamhetens informationstillgångar samt att det saknades ändamålsenliga rutiner för behörigheter och lösenord. Det saknades också en dokumenterad och etablerad rutin för incidenthantering avseende informationssäkerhetsincidenter och befintlig kontinuitetsplan avseende IT-drift var inte uppdaterad. I granskningen noterades att det inte fanns kontrollområden avseende information- eller IT-säkerhet i internkontrollplaner.

Regionens revisorer har mot bakgrund av sin risk- och väsentlighetsanalys bedömt det angeläget att genomföra en uppföljande granskning av regionens IT-säkerhet.

2 SYFTE

Granskningens syfte är att svara på om regionstyrelsen har vidtagit åtgärder utifrån de brister som framkom i granskningen 2020 för att säkerställa att regionens organisation och interna kontroll är ändamålsenlig gällande IT-säkerhet.

Revisionsfrågor

Granskningen ska besvara följande revisionsfrågor:

- Finns det en övergripande styrning av informations- och IT-säkerhet inklusive uppdaterade styrande dokument?
- Finns det en fungerande intern kontroll av att den IT-säkerhet som föreskrivs i lagar, förordningar och interna regelverk efterlevs?

- Finns erforderliga resurser och är arbetet med IT-säkerhet prioriterat i förhållande till de risker som finns?
- Sker säkerhetsklassning av funktioner och tjänster?
- Finns ändamålsenliga rutiner för behörigheter och lösenord? Inkluderar även leverantörer av enskilda system.
- Har regionen en ändamålsenlig incidenthanteringsprocess?
 - Upptäcks och hanteras icke önskvärda incidenter både intern och externt?
 - Finns det rutiner för att säkerställa att nya risker och hot identifieras och hanteras?
- Är medborgarnas integritet säkerställd (patientlagen) och har patientinformation i journalsystem ett tillräckligt skydd mot obehörig åtkomst?
- Är känsliga patientdata lagrade på ett säkert sätt, till exempel genom kryptering?
- Är det säkerställt att personal som hanterar lagring och hantering av känsliga uppgifter om enskilda patienter har den utbildning i informationssäkerhet som behövs utifrån tilldelade arbetsuppgifter?
- Genomförs riskanalyser på ett tillfredsställande sätt inom IT-säkerhetsområdet?

3 AVGRÄNSNING

Granskningen är avgränsad till regionstyrelsen.

4 REVISIONSKRITERIER

Uppfylls kraven i:

- [Kommunallagen](#) (2017:725)
- Internationella standarder enligt ISO (International Organization for Standardization) avseende Informationsteknik, Säkerhetstekniker och Ledningssystem för informationssäkerhet (ISO 27001:2013)
- Internationella standarder enligt COBIT (Control Objective for Information and Related Technology Standards) avseende informationssäkerhet.
- Relevanta interna styrdokument.

5 ANSVARIG NÄMND/STYRELSE

Ansvarig nämnd är regionstyrelsen.

6 METODER

Granskningen utförs genom inhämtning och granskning av relevanta dokument och intervjuer med berörda tjänstemän.

Substansgranskning utförs för att i erforderlig omfattning verifiera gjorda utsagor samt att system och rutiner fungerar på avsett sätt.

7 PROJEKTORGANISATION

Projektet genomförs av konsult under ledning av regionens revisionskontor. Ansvarig projektledare vid regionens revisionskontor är Leif Gabrielsson, revisionsdirektör.

8 PRÖVNING AV YRKESREVISORNS OBEROENDE

En prövning kommer att genomföras för att säkerställa att det inte föreligger några omständigheter som bedöms rubba förtroendet för den sakkunniges oberoende och integritet (*Bilaga 1*).

9 RESURSER

Konsult upphandlas. Omfattningen i tid och resursinsatsen av konsulten bestäms i avtal mellan denne och regionens förtroendevalda revisorer före projektstart.

10 INTRODUKTION OCH AVRAPPORTERING

Granskningen påbörjas under hösten och beräknas kunna slutföras under 2023.

Granskningen introduceras genom att beslutad projektplan skickas för kännedom till nämnden och berörd förvaltningschef.

Avrapportering sker dels i skriftlig form, dels i muntlig form till de förtroendevalda revisorerna, nämnden/styrelsen och verksamhetsansvariga. Den skriftliga rapporteringen skall upprättas med följsamhet till SKYREVs rekommendation om dokumentation av revisionsprojekt (R1 och R4).

Rapporten utgör underlag för ansvarsprövningen för år 2023 samt för revisorernas riskbedömning för kommande revisionsår.

11 KVALITETSSÄKRING

Uppgiftslämnare och berörd chef kommer att ges möjlighet att faktagranska och lämna synpunkter på rapportutkast innan rapporten fastställs.

Konsulten svarar för kvalitetssäkring gentemot uppgiftslämnare och av de insamlade uppgifter som används i analysen. Konsulten har det primära ansvaret för att den analys och de bedömningar och förslag som förs fram är tillräckligt underbyggda.

Revisionsdirektören har ett övergripande ansvar för att kontrollera om granskningen har en tillräcklig yrkesmässig och metodisk kvalitet samt att det finns en överensstämmelse mellan revisionsfrågorna/kontrollmålen, metoder, fakta, slutsatser/beslutsfattningar och framförda förslag.

12 GODKÄNNANDE

Projektplanen har godkänts av de förtroendevalda revisorerna vid möte den 2023-09-13

För Regionens revisorer


Jan Rönngren
Ordförande

13 BILAGA 1

PRÖVNING AV DEN SAKKUNNIGES OBEROENDE OCH INTEGRITET

Hot mot oberoende	Hot föreligger	Hot föreligger ej	Kommentar
Egenintressehot ¹	☐	☒	
Självgranskningshot ²	☐	☒	
Partställningshot ³	☐	☒	
Vänskapshot ⁴	☐	☒	
Skrämselhot ⁵	☐	☒	
Övriga hot ⁶	☐	☒	

Härmed intygas att prövning av oberoende och integritet genomförts i enlighet med Skyrevs rekommendation 2.

Ort och datum

Östersund 2023-09-12



Leif Gabrielsson

Revisionsdirektör

¹ – Har yrkesrevisorn eller anhörig till denne ekonomiska, juridiska eller andra intressen inom verksamheter som är relaterade till uppdraget?

² – Har yrkesrevisorn varit engagerad som konsult/rådgivare inom aktuellt granskningsområde?
– Har yrkesrevisorn varit engagerad som konsult/rådgivare inom ett näraliggande område till aktuellt granskningsområde?
– Har yrkesrevisorn i tidigare tjänst haft ansvar inom aktuellt granskningsområde eller inom område som berör granskningsområdet?
– Har yrkesrevisorn lämnat råd eller gjort ställningstaganden som han/hon måste pröva som ett led i ett granskningsuppdrag?

³ – Har yrkesrevisorn i något sammanhang, nu eller tidigare, uppträtt till stöd för eller emot granskningsobjektets ståndpunkt eller intresse i något rättslig eller ekonomisk angelägenhet?

⁴ – Har yrkesrevisorn någon form av personlig relation till någon inom det område som är aktuellt för granskning?
– Har yrkesrevisorn blivit erbjuden/mottagit gåvor eller andra tjänster som kan äventyra en oberoende ställning?
– Har yrkesrevisorn arbetat inom samma område i många år och skapat nära relationer mellan sig och de granskade som kan utgöra vänkapshot?

⁵ – Är yrkesrevisorn utsatt för påverkan eller påtryckningar från ansvariga tjänstemän eller politiker inom det område som är föremål för granskning?
– Är yrkesrevisorn utsatt för sådan påtryckning från de förtroendevalda revisorerna som kan påverka yrkesrevisorns oberoende i revisionsarbetet?
– Uppfattar yrkesrevisorn att han/hon utsätts för hot eller andra påtryckningar från uppdragsgivaren, de som är föremål för granskning eller annan, utformade på ett sådant sätt att de är ägnade att ge yrkesrevisorn obehag.

⁶ – Bedömer yrkesrevisorn att det finns andra förhållanden som kan rubba förtroendet för dennes opartiskhet och självständighet?