

Kommunstyrelsen

Kommunfullmäktige – för kännedom

Förstudie IT- och informationssäkerhet

Revisorerna i Bollebygds kommun har gett PwC i uppdrag att genomföra en förstudie gällande IT- och informationssäkerhet i kommunen.

Revisionsfrågan som skall besvaras är:

- *Har kommunstyrelsen ändamålsenliga policys, rutiner och beskrivningar gällande IT-säkerhet, med fokus på design av rutiner för skydd mot obehörig åtkomst av data och information?*

Granskningen visar att:

Vår samlade bedömning är att IT-säkerheten, ur ett övergripande perspektiv, är tillräcklig för att stödja verksamheten och ge tillräcklig intern kontroll. Dock så finns det ett antal områden där Bollebygds kommun inte har en tillräcklig nivå och IT- och informationssäkerhetsarbetet kan förstärkas för att säkerställa en god intern kontroll.

Våra bedömningar baseras på de kontrollmål som det redogörs för i bifogad revisionsrapport där även ett antal förslag för att vidareutveckla arbetet lämnas.

Vår rekommendationer:

- Kommunstyrelsen bör upprätta instruktioner och rutinbeskrivningar för IT-organisationen för att säkerställa att nuvarande kompetens i IT-organisationen kan tillvaratas av andra personer än enbart nuvarande nyckelpersoner.
- Vi rekommenderar kommunstyrelsen att upprätta en avbrottsplan avseende IT och systemstöd. Kommunstyrelsen bör dokumentera åtgärder som behöver vidtas, i vilken ordning och av vem, för att effektivt återställa system och applikationer vid en eventuell incident. Baserat på verksamhetens riskanalyser bör kritiska system definieras och få en tydlig prioritering i avbrottsplanen. Vidare bör ansvarsområden beskrivas och kommuniceras till alla berörda, exempelvis genom träning samt testning av planen.

- Kommunstyrelsen bör införa en formaliserad rutin för behörighetshantering. Rutinen bör säkerställa att nya, ändrade eller borttagande av behörigheter baseras på en formell ansökan som är attesterad av närmaste chef och/eller systemägare. Slutligen bör rutin även inkludera periodiska genomgångar av befintliga behörigheter för att säkerställa att behörigheter är uppdaterade över tid. Rutinbeskrivningen bör delas med både IT-personal och systemansvariga för verksamhetssystem för att säkerställa att rutinerna implementeras för samtliga system.
- För att stärka ändamålsenligheten i den interna kontrollen kopplat till IT- och informationssäkerhet rekommenderar vi även kommunstyrelsen att åtgärda de iakttagelser och beakta de rekommendationer som finns beskrivna i appendix till bifogad revisionsrapport.

Vi önskar kommunstyrelsens kommentarer i anledning av vår förstudie senast 2018-06-30.

Bollebygd den 17 april 2018

För revisorerna

Margaretha Almqvist-Malmsjö
Ordförande

Per Wignäs

Bilaga: Revisionsrapport PwC; ”Förstudie IT- och informationssäkerhet”