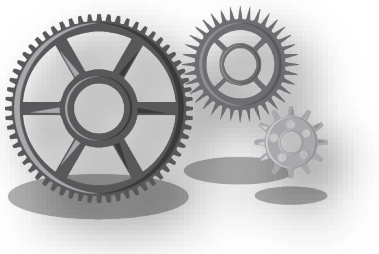
Granskning av informationssäkerhet

Ludvika kommun

KPMG AB

2023-11-06

Syfte och revisionsfrågor



Granskningen syftar till att bedöma om kommunstyrelsen, nämnder och bolagsstyrelser bedriver ett systematiskt informationssäkerhetsarbete så att det sker på ett ändamålsenligt sätt.

- Finns **aktuella styrande dokument** som tydliggör ansvar, krav och hur arbetet ska bedrivas?
- Finns en **ändamålsenlig organisation** för informationssäkerhetsarbetet?
- Finns beslutade **informationssäkerhetsmål** med tillhörande handlingsplaner?
- Har styrelse och nämnder tillsett att det finns en god **säkerhetskultur**?
- Har **riskanalyser och informationsklassning genomförts** för de informationstillgångar som verksamheten ansvarar för?
- Finns **incidenthanteringsrutiner** som inkluderar krav på hur incidenter ska dokumenteras och följas upp tillsammans med tydliggjorda eskaleringsvägar?
- Finns en **etablerad uppföljning** av informationssäkerhetsarbetet och rapporteras denna till styrelse och nämnder med regelbundenhet?

Resultat av granskning

Styrande dokument samt roller och ansvar

- **Antagen policy.**
  - Policyn saknar reglering över bolagens ansvar.
  - Saknas styrande dokument som tydliggör ansvar, krav och hur arbetet ska bedrivas.

- **Saknas en tydliggjord ansvarsfördelning**
  - Linjeansvaret fullföljs inte.

- **Saknas en utvecklad koncernsamverkan i informationssäkerhetsarbetet.**

Riskbedömning och informationsklassning

- **Det saknas kommunövergripande samt bolagsövergripande riskanalyser.**
- **Den klassning som genomförs sker på initiativ från enskilda personer utifrån kompetens och engagemang.**
- **Det riskbedömningsarbete som bedrivs är inte tillräckligt i syfte att kunna identifiera eventuella hot och oönskade händelser.**

Säkerhetskultur

- **Nano-learning som omfattar informations- och it-säkerhet.**
  - Obligatorisk för anställda inom kommunen med tillgång till egen dator.

- **Höja kunskapsnivån i bolagen med utbildning.**

Incidenthantering

- **Rutiner för incidentrapportering redovisar it- och informationssäkerhetsincidenter ska hanteras.**
  - Rutinerna är inte etablerade i kommunen.

- **Saknas ett etablerat analysarbete av inträffade incidenter**.

- **Få anmälda incidenter i förhållande till kommunens storlek.**

Uppföljning och återrapportering

- **Enligt policy ska styrelse och nämnder följa upp informationssäkerheten inom den egna verksamheten.**
  - Uppföljning saknas i nuläget.

- **Saknas även ett etablerat uppföljningsarbete inom bolagen.**

Rekommendationer

Rekommendationer

Kommunstyrelsen (utifrån sitt övergripande ansvar):

- **Revidera policyn** med reglering avseende de helägda bolagen.
- Upprätta **styrande dokument** som tydliggör ansvar, krav och hur informationssäkerhetsarbetet ska bedrivas samt säkerställa att de implementeras i kommunkoncernens organisation.
- Fastställa en kommun/koncerngemensam **modell för riskbedömning och informationsklassning** samt säkerställa att informationsklassning och riskbedömning av kommunens informationstillgångar genomförs.
- Etablera ett **uppföljningsarbete** för informationssäkerhet samt säkerställa att en informationssäkerhetsberättelse upprättas.

Rekommendationer

Ludvika kommun Stadshus AB (utifrån sitt övergripande ansvar):

- Säkerställ att **koncernövergripande dokument implementeras** i de helägda bolagen.
- Årligen **värdera informationssäkerhetsrisker och konsekvenser** för koncernen.
- Säkerställa att styrelsen **erhåller regelbunden information** om informationssäkerhetsarbetet hos kommunen och dotterbolagen för att vid behov kunna besluta om åtgärder för att stärka säkerheten i koncernen.

Rekommendationer

Övriga revisionsobjekt samt kommunstyrelsen utifrån sitt verksamhetsansvar):

- Säkerställa att kommunövergripande **styrdokument implementeras** i organisationen.
- Säkerställa att **informationsklassning och riskbedömning** av nämndens/bolagens informationstillgångar **genomförs**.
- Säkerställa att obligatoriska **utbildningsinsatser genomförs** samt att medarbetarnas samt förtroendevaldas medverkan följs upp.
- Säkerställa att **incidenthanteringsrutinen implementeras** i organisationen samt att inträffade **incidenter analyseras** i syfte att utgöra underlag för förbättringar.
- **Följa upp** det nämnd/bolagsspecifika informationssäkerhetsarbetet som bedrivs i syfte att erhålla en nulägesbild för **beslut om eventuella insatser** i syfte att stärka informationssäkerheten.