Kommunkoncernens arbete med informationssäkerhet

Sölvesborgs kommun

Koncernen Sölvesborgs Energi

Sölvesborgshem AB

September 2024

Bo Rehnberg, certifierad kommunal revisor

Michael Wissén, projektmedarbetare

Anna Hilmarsson, certifierad kommunal revisor

pwc

Revisionsrapport

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Sölvesborgs kommun och lekmannarevisorer i helägda aktiebolag har PwC genomfört en granskning inom området informationssäkerhet. Granskningens syfte är att bedöma om koncernens arbete inom området bedrivs med tillräcklig intern kontroll.

Nedan ses bedömning för varje revisionsfråga.

Revisionsfrågor	Bedömning	
Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning?	Delvis	
Finns styrande riktlinjer för informationssäkerhet och är dessa implementerade i verksamheten?	Delvis	
Bedriver organisationen ett aktivt arbete med informationssäkerhet? Fokus på aktiviteter och rapportering.	Delvis	

Utifrån genomförd granskning är vår samlade bedömning att kommunkoncernens arbete med informationssäkerhet inte helt bedrivs med tillräcklig intern kontroll.

Granskningen visar att det finns betydande skillnader hur olika kommunala verksamheter arbetar inom området. Vår granskning visar att koncernen Sölvesborgs Energi i allt väsentligt bedriver ett systematiskt arbete med informationssäkerhet.

För fullständiga bedömningar se respektive revisionsfråga i rapporten.

För att utveckla granskningsområdet bör följande rekommendationer prioriteras:

- Att kommunstyrelsen prövar vilka prioriteringar och resurser som krävs för att skapa ett systematiskt arbete med informationssäkerhet.
- Att kommunstyrelsen utvecklar förekommande styrdokument. Utvecklingsområden som noterats rör områdena ansvarsfördelning, systematiskt arbetssätt samt att dokumenten även omfattar kommunal verksamhet som bedrivs i aktiebolag.
- Att kommunstyrelsen säkerställer att den utövar tillfredsställande uppsikt för hur kommunen och dess helägda aktiebolag arbetar med informationssäkerhet.
- Att Sölvesborgshem - i dialog med ägaren - prövar hur bolaget framgent ska arbeta med området informationssäkerhet.

Innehållsförteckning

Inledning

Bakgrund

Kommuner har ett av det svenska samhällets mest komplexa uppdrag. Detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. Med dagens snabba digitalisering blir informationssäkerhet allt viktigare.

Det övergripande syftet med informationssäkerhet är att säkerställa att information för medarbetare, medborgare och andra intressenter hanteras med utgångspunkt i tillgänglighet, riktighet och konfidentialitet.

Information är värdefull och behöver många gånger skyddas. Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering.

Revisionsobjekt i granskningen är kommunstyrelse, nämnder och helägda aktiebolag. I kommunstyrelsens uppdrag ingår att leda, samordna och utöva uppsikt över kommunens samlade verksamhet (inklusive bolagen).

Syfte och revisionsfrågor

Granskningen tar utgångspunkt från kommunallagen kapitel 12 och aktiebolagslagen kapitel 10. Syftet med granskningen är att bedöma om koncernens arbete med informationssäkerhet bedrivs med tillräcklig intern kontroll. Granskningen ska besvara följande revisionsfrågor:

1. Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning?
2. Finns styrande riktlinjer för informationssäkerhet och är dessa implementerade i verksamheten?
3. Bedriver organisationen ett aktivt arbete med informationssäkerhet? Fokus på aktiviteter/åtgärder och rapportering.

Revisionskriterier

Med revisionskriterier avses de bedömningsgrunder som bildar underlag för revisionens analyser och bedömningar.

Följande revisionskriterier används i granskningen:

- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster § 11-14
- Kommunallagen 6:1, 6:6, 6:13
- Aktiebolagslagen 8:4
- Styrdokument inom kommunen och dess bolag som är relevanta för granskningen.
- I övrigt se avsnitt ”syfte och revisionsfrågor”

Avgränsning

I tid avgränsas granskningen i första hand i år 2024. Övrig avgränsning, se avsnitt *Syfte och revisionsfrågor*.

Metod

Granskningen har skett genom analys av för granskningen relevanta styrdokument, däribland riktlinjer/policy för informationssäkerhet. Därutöver har vi även genomfört granskning av kommunstyrelsens protokoll för perioden juli 2023 - juni 2024.

Intervjuer har skett med företrädare för kommunen respektive kommunägda bolag. Följande har intervjuats:

- Kris- och beredskapssamordnare, 3 st nämndsekreterare samt IT-strateg, Sölvesborgs kommun
- VD och Säkerhetschef, koncernen Sölvesborgs Energi
- VD, Sölvesborgshem AB

De intervjuade har beretts möjlighet att sakgranska rapporten.

Revisionell bedömning av respektive revisionsfråga sker utifrån en tregradig skala: ja/uppfyllt (grön); delvis uppfyllt (gul); nej/ej uppfyllt (röd).

Rapporten har kvalitetssäkrats av Anna Hilmarsson, certifierad kommunal revisor, enligt PwC:s rutiner för kvalitetssäkring.

Granskningsresultat

Organisation och ansvarsfördelning

Revisionsfråga 1: Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning?

Iakttagelser

Av kommunallagen framgår att kommunal verksamhet ska kännetecknas av god intern kontroll. En del i den interna kontrollen är att tydliggöra ansvar och roller inom en organisation. Detta gäller inom såväl den politiska organisationen som verksamhetsorganisationen.

Granskningen visar att det inom kommunkoncernen i viss grad har upprättats styrdokument som berör området informationssäkerhet. Granskning av dokumenten visar följande:

Politisk nivå
Inom Sölvesborgs kommun sker styrningen i första hand genom informationssäkerhetspolicy (Kommunfullmäktige, KF 2024). Granskningen visar att styrdokumentet inte ger någon tydlig bild av hur ansvaret fördelas mellan kommunstyrelsen och nämnderna.

Av äldre styrdokument inom området (*IT-reglemente - beslutat av KF 1997*) framgår att det vilar på respektive nämnd att utse systemansvariga inom verksamhetsorganisationen. I övrigt anges inte vilket ansvar som vilar på nämnderna.

I kommunallagen anges att styrelsen ansvarar för att leda och samordna förvaltningen av kommunens *samtliga* angelägenheter. Detta kan tolkas som att styrelsen bär det politiska ansvaret för kommunens arbete med informationssäkerhet. Av granskade dokument framgår att styrelsen ansvarar för att ajourhålla policy för informationssäkerhet.

När det gäller bolagsstyrelsens ansvar för förvaltningen av dess angelägenheter regleras detta i aktiebolagslagen.

I övrigt noteras att det inom koncernen Sölvesborgs Energi finns styrdokument för arbetet med informationssäkerhet. Av dessa dokument framgår vilka uppdrag som vilar på bolagets styrelse. Motsvarande dokument saknas i Sölvesborgshem AB.

Verksamhetsnivå
I kommunens informationssäkerhetspolicy klargörs att den som är ansvarig för en verksamhet tillika är ansvarig för informationssäkerheten inom verksamhetsområdet. Vidare framgår att förvaltningschefen ansvarar för informationssäkerheten inom sin förvaltning.

Policyn ger ingen heltäckande beskrivning hur arbets- och rollfördelningen ser ut inom verksamhetsorganisationen.

Inom kommunen finns en grupp för arbetet med informationssäkerhet. Gruppen utgörs av företrädare för olika förvaltningar. Gruppen har återkommande möten. Vi kan inte finna att gruppens uppdrag och ansvar har dokumenterats.

När det gäller bolagen kan vi inledningsvis konstatera att *aktiebolagslagen* är mer tydlig än *kommunallagen* när det gäller hur ansvaret fördelas inom verksamheten. En verkställande direktör har ett övergripande ansvar för den löpande förvaltningen av bolagets angelägenheter. Motsvarande skrivning saknas i kommunallagen.

Inom koncernen Sölvesborgs Energi finns både policy och riktlinjer för informationssäkerhet. I riktlinjer beskrivs roller och ansvar mellan olika befattningar och verksamhetsområden. Här framgår att respektive sektionschef ansvarar för informationssäkerheten inom sin verksamhet. Ansvar som är specifikt relaterat till ett enskilt IT-system kan delegeras till systemägaren. Granskningen visar att systemägaren i flertalet fall även är sektionschef. Styrdokumenten ger en tydlig bild av hur ansvar och roller fördelas inom bolagskoncernen.

Inom bostadsbolaget har det inte preciserats vem/vilka i verksamheten som ansvarar för området informationssäkerhet.

Vid intervjuer med företrädare för verksamhetsorganisationen framkommer att ansvars- och rollfördelningen inom Sölvesborgs kommun kan förtydligas. Inom Sölvesborgs Energi upplevs organisation och rollfördelning avseende informationssäkerhet i allt väsentligt vara tydlig.

Bedömning

Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning?

Delvis.

Bedömningen baseras på följande:

- Inom koncernen Sölvesborgs Energi finns en tydlig roll- och ansvarsfördelning avseende arbetet med informationssäkerhet.
- Inom Sölvesborgs kommun är roll- och ansvarsfördelningen delvis preciserad. Emellertid finns otydligheter i organisationen på såväl politisk nivå som verksamhetsnivå.
- Inom bostadsbolaget saknas en tydlig organisation för arbetet med informationssäkerhet.

För framtiden föreslås att kommunstyrelsen - i styrdokument - preciserar organisationen och hur ansvar fördelas inom den kommunala organisationen. Otydlighet inom området försvårar möjligheten att utkräva ansvar av organisationen.

Styrdokument

Revisionsfråga 2: Finns styrande riktlinjer för informationssäkerhet och är dessa implementerade i verksamheten?

Iakttagelser

Av kommunallagen framgår att kommunal verksamhet ska styras genom mål, riktlinjer och planer. Mål och riktlinjer ska beslutas av den politiska organisationen.

I Myndigheten för samhällsskydd och beredskaps (MSB) uppdrag ingår att lämna råd och stöd till organisationer hur de ska arbeta med informationssäkerhet. I MSB:s vägledning beskrivs vikten av att ta fram styrdokument. Styrdokumenten kan utgöras av policy, riktlinjer, planer och instruktioner.

Syftet med ett styrdokument är att styra och vägleda hur organisationen ska arbeta inom ett specifikt område. Följande har noterats i denna granskning:

Styrdokument inom Sölvesborgs kommun
Inom kommunen har det under en längre period funnits en medvetenhet om behovet att utveckla styrdokument inom området informationssäkerhet.

Under år 2024 har det tagits fram en informationssäkerhetspolicy. Kommunstyrelsen har i maj 2024 föreslagit kommunfullmäktige att fastställa denna policy, vilket skett 2024-05-27. Policyn innehåller följande delar:

- Syfte/mål
- Definition av information/informationstillgång/informationssäkerhet
- Ansvar
- Uppföljning/revidering

Informationssäkerhetspolicyn omfattar endast verksamhet som bedrivs i Sölvesborgs kommun. Styrdokumentet ger ingen vägledning hur helägda aktiebolag ska arbeta med informationssäkerhet. I sammanhanget kan det framhållas att det vilar på kommunstyrelsen att utöva ägarrollen för verksamhet som bedrivs i helägda aktiebolag.

Granskningen visar att förslag till policy har processats i förvaltningsövergripande grupp för informationssäkerhet (se föregående avsnitt). Som tidigare nämnts ger policyn ingen heltäckande beskrivning av hur kommunens verksamheter ska bedriva ett systematiskt arbete med informationssäkerhet.

I intervjuer framkommer att det för närvarande pågår ett arbete att ta fram kompletterande riktlinjer för arbetet med informationssäkerhet. Detta arbete ska slutföras under hösten 2024. I övrigt noteras att förekommande styrdokument inom kommunen inte har en enhetlig definition när det gäller begreppen systemägare, systemansvarig och systemförvaltare.

Av policyn framgår att respektive förvaltningschef ska se till att policyn är känd och tillämpas inom organisationen. Vidare anges att kommunstyrelsen ska genomföra en årlig uppföljning av policyn.

När samtliga styrdokument är upprättade kommer det enligt uppgift att genomföras utbildningsinsatser inom organisationen.

Styrdokument inom koncernen Sölvesborgs Energi
Följande styrdokument har noterats i granskningen:
1. Informationssäkerhetspolicy (2021)
2. Riktlinjer informationssäkerhet (reviderad 2024)
3. Rollbeskrivning för systemägare och systemförvaltare (reviderad 2024)

Granskningen visar att granskade styrdokument i allt väsentligt ger en heltäckande beskrivning hur organisationen ska arbeta med informationssäkerhet. Styrdokumenten ställer bland annat krav på genomförande av informationsklassning, riskanalyser, upprättande av handlingsplaner samt uppföljning. Styrdokument för informationssäkerhet innehåller även ett årshjul.

I intervjuer lämnas en beskrivning av hur förekommande styrdokument har implementerats inom verksamheten. I övrigt noteras att dokumenten finns samlade på koncernens interna nätverk som samtliga medarbetare har tillgång till.

Styrdokument inom Sölvesborgshem
Bolaget saknar styrdokument som rör området informationssäkerhet.

Bedömning

Finns styrande riktlinjer för informationssäkerhet och är dessa implementerade i verksamheten?

Delvis.

Bedömningen baseras på följande:
- Koncernen Sölvesborgs Energi har styrande riktlinjer för informationssäkerhet. Styrdokumenten ger i allt väsentligt en heltäckande beskrivning av hur organisationen ska arbeta med informationssäkerhet.
- Det pågår ett arbete att ta fram styrande riktlinjer inom Sölvesborgs kommun. I dagsläget saknas heltäckande styrdokument inom området.
- Sölvesborgshem saknar styrande riktlinjer för granskningsområdet.

För framtiden föreslås att kommunstyrelsen prövar om förekommande styrdokument (policy och riktlinjer) även ska omfatta kommunal verksamhet som bedrivs i helägda aktiebolag.

Systematiskt arbetssätt

Revisionsfråga 3: Bedriver organisationen ett aktivt arbete med informationssäkerhet? Fokus på aktiviteter/åtgärder och rapportering.

Iakttagelser

Myndigheten för samhällsskydd och beredskap (MSB) betonar vikten av att svenska myndigheter och organisationer bedriver ett systematiskt arbete med informationssäkerhet. Ett systematiskt arbetssätt kännetecknas vanligtvis av följande moment:

1. Inventering och bedömning av risker
2. Mål och aktivitetsplaner
3. Uppföljning
4. Utvärdering

I lag om informationssäkerhet för samhällsviktiga tjänster (2018:1174) ställs krav på att samhällsviktig verksamhet bedriver ett systematiskt arbete med informationssäkerhet. Med samhällsviktig verksamhet avses bland annat tjänster inom sektorerna energi respektive leverans och distribution av dricksvatten. Lagen ställer krav på att berörda organisationer arbetar kontinuerligt med riskanalys och åtgärdsplaner. Granskningen visar att lag 2018:1174 i första hand är tillämplig för koncernen Sölvesborgs Energi.

Sölvesborgs kommun

Som tidigare nämnts saknar kommunen i dagsläget heltäckande styrdokument som innefattar samtliga moment i ett systematiskt arbetssätt. Vidare saknas ett årshjul för arbetet med informationssäkerhet.

Granskningen visar att det under det senaste året har påbörjats insatser för att systematisera arbetet med informationssäkerhet. Vi noterar att ett flertal workshops har genomförts inom organisationen. Initialt riktas fokus mot att klassa förekommande information i IT-system (moment 1). I intervjuer framkommer att det råder stora skillnader mellan förvaltningarna. Vi noterar att barn- och utbildningsförvaltningen har kommit längst i detta arbete.

Myndigheten MSB erbjuder samtliga kommuner att medverka i undersökningen *Infosäkkollen*. Syftet med undersökningen är dels få en bild över hur långt respektive kommun kommit i sitt arbete med informationssäkerhet. Undersökningen syftar även till att kunna göra jämförelser med andra kommuner. Granskningen visar att Sölvesborgs kommun under senare år har medverkat i denna undersökning. Av resultatet framgår att det skett en viss utveckling i kommunen under år 2024, men att arbetet ännu inte kan betecknas som systematiskt.

I granskningen framkommer att det finns ett behov inom verksamheten att inrätta en befattning som informationssäkerhetssamordnare. Enligt företrädare för verksamheten skulle förutsättningarna i sådana fall förbättras för att bedriva ett systematiskt arbetssätt.

Inom ramen för granskningen har det skett en genomgång av kommunstyrelsens protokoll för perioden juli 2023 - juni 2024. Följande har noterats:

- Styrelsen har i maj 2024 behandlat ett förslag till policy för informationssäkerhet. I policyn anges bland annat att kommunstyrelsen hädanefter ska genomföra årlig uppföljning inom området.
- Styrelsen har i januari 2024 behandlat förslag till styrdokument inom området kris- och beredskapsarbete 2024-2026. Området informationssäkerhet nämns som en insats för att stärka kommunens krisberedskapsarbete.
- Styrelsen har i mars 2024 antagit internkontrollplan 2024. Vi noterar att planen inte inkluderar området informationssäkerhet.

Vi kan inte finna att kommunstyrelsen - inom ramen för sin uppsiktsplikt - under perioden kontrollerat hur kommunens samlade verksamhet (kommun + bolag) arbetar med informationssäkerhet.

Koncernen Sölvesborgs Energi
Verksamheten kan i rimlig grad belägga att den kontinuerligt arbetar med riskanalyser, mål- och aktivitetsplaner samt uppföljning/rapportering.

Granskningen visar att arbetet i allt väsentligt bedrivs enligt upprättat årshjul för informationssäkerhet. I intervjuer framkommer att bolaget även i viss grad gett vägledning och stöd till kommunen i frågor som rör området informationssäkerhet.

I övrigt noteras att statliga tillsynsorgan ännu inte genomfört någon tillsyn av hur koncernen Sölvesborgs Energi arbetar med granskningsområdet.

Sölvesborgshem
Granskningen visar att det ännu inte påbörjats något arbete inom bostadsbolaget som rör informationssäkerhet.

Företrädare från bolaget efterlyser tydligare styrning från ägaren (kommunen) hur bolaget framgent ska arbeta inom området.

Bedömning

Bedriver organisationen ett aktivt arbete med informationssäkerhet? Fokus på aktiviteter/åtgärder och rapportering.

Delvis.

Bedömningen baseras på följande:
- Koncernen Sölvesborgs Energi bedriver ett systematiskt arbete med informationssäkerhet. Granskningen indikerar att arbetet i allt väsentligt sker i enlighet med lagkrav och bolagsinterna riktlinjer.
- Sölvesborgs kommun har påbörjat ett utvecklingsarbete inom området. Arbetet kan i dagsläget inte betecknas som systematiskt.
- Sölvesborgshem bedriver för närvarande inget aktivt arbete med informationssäkerhet.

För framtiden föreslås att kommunstyrelsen prövar vilka prioriteringar och resurser som krävs för att skapa ett systematiskt arbete med informationssäkerhet. Kommunstyrelsen

bör även säkerställa att den utövar tillfredsställande uppsikt för hur kommunen och dess helägda aktiebolag arbetar inom området.

Vi rekommenderar att Sölvesborgshem - i dialog med ägaren - prövar hur bolaget framgent ska arbeta med området informationssäkerhet.

Avslutning

Samlad bedömning

Nedan redovisas revisionell bedömning för respektive delområde på koncernnivå:

Granskningsområde	Bedömning
1. Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning?	**Delvis**
2. Finns styrande riktlinjer för informationssäkerhet och är dessa implementerade i verksamheten?	**Delvis**
3. Bedriver organisationen ett aktivt arbete med informationssäkerhet? Fokus på aktiviteter och rapportering.	**Delvis**

Utifrån genomförd granskning är vår samlade bedömning att kommunkoncernens arbete med informationssäkerhet inte helt bedrivs med tillräcklig intern kontroll.

Nedan redovisas revisionell bedömning för respektive revisionsobjekt:

Revisionsobjekt	Bedömning
Koncernen Sölvesborgs Energi	**Ja**
Kommunstyrelse och nämnder	**Delvis**
Sölvesborgshem AB	**Nej**

- Att koncernen Sölvesborgs Energi bedriver i allt väsentligt ett systematiskt arbete med informationssäkerhet. Den interna kontrollen inom granskade områden bedöms vara tillräcklig.
- Att kommunstyrelse och nämnder påbörjat ett arbete med informationssäkerhet, men att arbetet inte kan betecknas som systematiskt. Den interna kontrollen inom området är i behov av utveckling.
- Att arbetet med informationssäkerhet i Sölvesborgshem inte bedrivs med tillräcklig intern kontroll.

Rekommendationer

För att utveckla området bör följande rekommendationer prioriteras:

- Att kommunstyrelsen prövar vilka prioriteringar och resurser som krävs för att skapa ett systematiskt arbete med informationssäkerhet.
- Att kommunstyrelsen utvecklar förekommande styrdokument. Utvecklingsområden som noterats rör områdena ansvarsfördelning, systematiskt arbetssätt samt att dokumenten även omfattar kommunal verksamhet som bedrivs i aktiebolag.
- Att kommunstyrelsen säkerställer att den utövar tillfredsställande uppsikt för hur kommunen och dess helägda aktiebolag arbetar med informationssäkerhet.
- Att Sölvesborgshem - i dialog med ägaren - prövar hur bolaget framgent ska arbeta med området informationssäkerhet.

2024-09-26

Anna Hilmarsson	***Bo Rehnberg***
Uppdragsledare	*Projektledare*