Granskning av informationssäkerhet

Storumans kommun

Storumans kommunföretag AB

Fastighets AB Umluspen

Hemavan Tärnaby Airport AB

Industri- och logistikcentrum i Storuman AB

November 2022

Bo Rehnberg, certifierad kommunal revisor

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Storumans kommun samt lekmannarevisorer i kommunägda bolag genomfört en granskning hur kommunens samlade verksamhet arbetar med informationssäkerhet. Revisionsobjekt i granskningen är kommunstyrelse, nämnder och kommunägda aktiebolag.

Granskningen har inriktats mot följande områden:
- Organisation, ansvar och roller
- Styrdokument
- Systematiskt arbetssätt
- Kommunstyrelsens kontroll

Utifrån genomförd granskning görs en sammantagen revisionell bedömning att koncernens arbete med informationssäkerhet *inte* bedrivs med tillräcklig intern kontroll.

Underlag för revisionell bedömning redovisas i avsnitt 2.1-2.4.

För att utveckla granskningsområdet lämnas följande rekommendationer:

- Att kommunstyrelsen prövar vilket eventuellt ansvar som ska vila på facknämnderna när det gäller området informationssäkerhet. Om nämnderna tilldelas ett ansvar bör detta i så fall dokumenteras i reglemente samt i informationssäkerhetspolicy.

- Att kommunstyrelsen tar fram en koncernövergripande styrdokument som beskriver hur kommun och dess bolag ska arbeta med informationssäkerhet. Fokus bör riktas på följande delar:
    - Organisation och ansvar för arbetet med informationssäkerhet.
    - Ge vägledning hur hur det systematiska arbetet ska bedrivas.
    - Formerna för hur bolagsstyrelser/nämnder ska följa upp området men även lämna rapport till kommunstyrelsen.

- Att kommunstyrelsen för in området “Informationssäkerhet” i sin årliga uppföljningsplan.

Innehållsförteckning

1. Inledning

1.1 Bakgrund

Kommuner och regioner har ett av det svenska samhällets mest komplexa uppdrag. Detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. Förtroendet för en organisation tar lång tid att bygga upp, men kan snabbt raseras av en enskild säkerhetsincident. Med dagens snabba digitalisering blir informationssäkerhet allt viktigare. Klassning av informationstillgångar är viktigt för att säkerställa att den mest skyddsvärda informationen verkligen får det skydd som krävs.

Det övergripande syftet med informationssäkerhet är att säkerställa att information för medarbetare, medborgare och andra intressenter hanteras med utgångspunkt i tillgänglighet, riktighet och konfidentialitet. Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering. Vilket i sin tur skapar förtroende både inom och utanför organisationen.

Revisorerna har i sin riskanalys för 2022 bedömt att det finns en risk att kommunkoncernen inte har säkerställt att finns en god informationssäkerhet och har därför gett PwC ett uppdrag att granska området.

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

1.2 Syfte och revisionsfrågor

Revisorernas uppdrag regleras i kommunallagen kapitel 12 och aktiebolagslagen kapitel 10. Syfte med granskningen är att bedöma om koncernens arbete med informationssäkerhet bedrivs med tillräcklig intern kontroll. Följande revisionsfrågor ska besvaras i granskningen:

1. Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning? Fokus på följande områden: aktualitet, heltäckande samt förankring i kommunorganisationen.
2. Finns styrande riktlinjer för informationssäkerhet och är dessa implementerade i verksamheten?
3. Bedriver verksamhetsorganisationen ett aktivt arbete med informationssäkerhet? Fokus på aktiviteter/åtgärder och rapportering.
4. Följer kommunstyrelsen upp och utvärderar koncernens arbete med informationssäkerhet i tillräcklig grad?

1.3 Revisionskriterier

Följande revisionskriterier används i granskningen:

- Kommunallagen 6:1, 6:6, 6:13
- Aktiebolagslagen 8:4
- Styrdokument inom kommunen och dess bolag som är relevanta för granskningen.

1.4 Avgränsning

I tid avgränsas granskningen i första hand till år 2022. Övrig avgränsning, se avsnitt “Syfte och revisionsfrågor”.

1.5 Metod

Analys av för granskningen relevant dokumentation. Följande kommuninterna dokument har granskats:

- Informationssäkerhetspolicy Storumans kommun (2007)
- Säkerhetsinstruktion: Förvaltning, Storumans kommun (2009)
- Säkerhetsinstruktion: Användare, Storumans kommun (2009)
- Verksamhetsplaner: KS och nämnder 2022
- Ägardirektiv för moder- och dotterbolag
- Reglemente för kommunstyrelse och nämnder
- Kommunstyrelsens protokoll för perioden 2021-08-01 -- 2022-07-31

Intervjuer har genomförts med koncernchef, stabschef, säkerhetssamordnare samt VD:ar i kommunens dotterbolag. 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).

2. Granskningsresultat

2.1 Organisation, ansvar och roller

Revisionsfråga 1: Finns en organisation för informationssäkerhet med tydlig roll- och ansvarsfördelning? Fokus på följande områden: aktualitet, heltäckande samt förankring i kommunorganisationen.

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. En otydlig ansvarsfördelning riskerar försvåra möjligheten att utkräva ansvar av organisationen.

Kommunstyrelse, nämnder och bolagsstyrelser

Av reglemente för kommunstyrelse och nämnder (Kommunfullmäktige 2018-11-20) framgår att kommunstyrelsen har ett övergripande ansvar för kommunens säkerhetsfrågor. I styrelsens uppgifter ingår att ta hand om kommunens IT-system. Kommunens styrdokument reglerar inte vilket eventuellt ansvar som vilar på nämnderna när det gäller informationssäkerhet.

Information är värdefull och behöver skyddas efter behov. Kommunen har i ägarrollen inte utövat någon formell styrning hur kommunägda bolag ska arbeta med informationssäkerhet. Bolagsstyrelsens ansvar för förvaltningen av dess angelägenheter regleras i aktiebolagslagen.

Verksamhetsorganisationen inom kommun respektive bolag

I kommunens styrdokument beskrivs hur arbetet med informationssäkerhet ska organiseras inom kommunens förvaltningar. Följande befattningar och organ har uppdrag att fullgöra inom området:

- Kommunledningsgruppen
- Informationssäkerhetssamordnare
- IT-chef och IT-beredningsgrupp
- Systemägare
- Samtliga chefer
- Medarbetare

Granskningen visar att den verksamhetsorganisation som beskrivs i styrdokumenten i flera avseenden är inaktuell. En brist är att dokumenten inte beaktar att kommunen sedan några år tillbaka valt att överlåta driften av kommunens IT-system till kommunalförbundet Lystkom.

Kommunstyrelsen har under 2021 sett ett behov att stärka kommunens organisation inom området säkerhet och beredskap. Inom kommunstyrelseförvaltningens kanslienhet

har det bildats en stödfunktion som bland annat ska arbeta med informationssäkerhet. Företrädare för kanslienheten framhåller att den verksamhetsorganisation som beskrivs i 2007 års informationssäkerhetspolicy varken är aktuell eller fullt ut ändamålsenlig.

Inom bolagen regleras ansvar och roller i första hand genom styrelsens arbetsordning och VD-instruktion. VD ansvarar enligt aktiebolagslagen för den löpande förvaltningen av bolagets angelägenheter. Granskade bolag har i flertalet fall inte preciserat hur organisation, ansvar och roller fördelas inom området informationssäkerhet. I flygplatsbolaget regleras ansvaret inom verksamhetsorganisationen delvis genom dess drifthandbok.

Bedömning

Vår bedömning är att organisation för informationssäkerhet endast *delvis* är tydlig. Bedömningen baseras på följande:

- Kommunstyrelsens och bolagsstyrelsernas ansvar är i huvudsak tydligt. En brist är att kommuninterna styrdokument ej klargjort nämndernas eventuella ansvar inom området.
- Ansvaret på verksamhetsnivå är i flera avseenden otydligt.
- Den organisation som beskrivs i kommunens styrdokument från 2007-2009 är inte aktuell, heltäckande eller förankrad inom nuvarande organisation.

För att utveckla området föreslås att kommunstyrelsen prövar vilket eventuellt ansvar som ska vila på facknämnderna när det gäller området informationssäkerhet. Om nämnderna tilldelas ett ansvar bör detta i så fall dokumenteras i reglemente samt i informationssäkerhetspolicy.

Kommunstyrelsen rekommenderas även att fastställa en organisation som omfattar hela koncernens verksamhet, det vill säga även den verksamhet som bedrivs i bolagsform.

2.2 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 styrdokument har noterats i denna granskning:

1. Informationssäkerhetspolicy (Kommunfullmäktige 2007-10-16)
2. Säkerhetsinstruktion: Förvaltning (Kommunledningsgruppen 2009-03-16)

3. Säkerhetsinstruktion: Användare (Kommunledningsgruppen 2009-03-16)

Informationssäkerhetspolicyn (styrdokument 1) innehåller följande avsnitt:
- Mål på kort och lång sikt
- Organisation och ansvar
- Vilka styrdokument som ska upprättas
- Generella krav
- Revidering och uppföljning

Företrädare för verksamheten upplever att policyn från 2007 innehåller vissa av de delar ett styrdokument ska innehålla, men att dokumentet i flera avseenden är inaktuellt. För närvarande pågår en revidering av kommunens informationssäkerhetspolicy. Revideringen utförs av kommunstyrelseförvaltningens kanslienhet.

Granskning av styrdokumenten 2-3, som beslutats på verksamhetsnivå, visar att dessa framför allt innehåller följande delar:
- Organisation och ansvar
- Regler och rutiner: förvaltning
- Regler och rutiner: användare
- Rapportering av säkerhetshändelser och svagheter.

Vetskapen om att kommunens styrdokument inte har ajourhållits under senare år har även medfört att inga särskilda insatser har genomförts på verksamhetsnivå för att implementera dokumenten.

Granskningen visar att de kommunägda bolagen i flertalet fall saknar egna styrdokument som som ger vägledning hur dessa ska arbeta med informationssäkerhet. Viss styrning ges i flygplatsbolagets drifthandbok. I intervjuer framkommer att det är önskvärt att kommunövergripande styrdokument inom området även innefattar bolagen.

Av undersökningar utförda av medlemsorganisationen Sveriges Kommuner och Regioner respektive MSB framgår att styrningen genom styrdokument och regelverk generellt är bristfällig inom kommuner och regioner. Exempelvis saknade merparten av Sveriges kommuner 2019 en informationssäkerhetspolicy.

Bedömning

Vi gör bedömningen att styrningen genom styrdokument endast *delvis* är tillräcklig. Bedömningen baseras på följande:
- Det finns förvisso äldre styrdokument inom kommunen, men att dessa dokument i flera avseenden är inaktuella.
- Förekommande riktlinjer har inte implementerats i verksamheten.

För framtiden föreslås att kommunstyrelsen tar fram en koncernövergripande styrdokument som beskriver hur kommun och dess bolag ska arbeta med informationssäkerhet.

2.3 Systematiskt arbetssätt

Revisionsfråga 3: Bedriver verksamhetsorganisationen 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

Granskningen visar att det arbetssätt som beskrivs i kommunens informationssäkerhetspolicy från 2007 i huvudsak motsvarar vad som anges i MSB:s vägledning (se ovan). Vissa avvikelser har dock noterats i fråga om metoder och arbetssätt. Av policyn framgår att arbetet med informationssäkerhet ska integreras med kommunens ordinarie verksamhet. Mål, aktiviteter och uppföljning ska inarbetas i förvaltningarnas årliga verksamhetsplaner.

Under 2021 har kommunen initierat en inventering och förteckning av förekommande IT-system i verksamhet som bedrivs i förvaltningsform. I förteckning, som administreras av kommunalförbundet Lystkom, anges vem i organisationen som är system-/informationsägare för respektive system. Vår granskning indikerar att det inte genomförts någon säkerhetsanalys av dessa IT-system under det senaste året. Enligt policy 2007 vilar på systemägare att fastställa och ajourhålla sådana analyser.

Granskningen kan inte se att området informationssäkerhet har inarbetats i kommunstyrelsens och nämndernas verksamhetsplaner för 2022. I så motto har policydokumentet inte efterlevts av verksamheten. Företrädare för kommunstyrelseförvaltningens kanslienhet överväger att åtgärder för informationssäkerhet framgent istället ska dokumenteras i särskilda handlingsplaner.

Vi noterar att kommunen vidtagit vissa åtgärder för att utveckla sitt arbete med informationssäkerhet. Under året ska det genomföras riktade utbildningsinsatser till förvaltningschefer, VD:ar i kommunägda bolag samt medarbetare inom kommunen. Utbildningsinsatserna ses som en förutsättning för att organisationen på sikt ska kunna bedriva ett systematiskt arbete inom området.

I övrigt registreras att kommunen, men även vissa bolag, har genomfört en översyn av befintliga dokumenthanteringsplaner. I dessa planer regleras hur dokument ska gallras och bevaras inom organisationen.

När det gäller bolagen noteras att flygplatsbolaget i närtid har utfört en säkerhetsskyddsanalys samt tillhörande utbildning. Insatserna innefattar i viss grad området informationssäkerhet. Övriga bolag har svårt att verifiera att dessa bedrivit

något systematiskt arbete under år 2022. I sammanhanget noteras att området informationssäkerhet inte är en fast punkt på dagordning varken i koncernledningsgrupp eller i gemensam VD-grupp för bolagen.

Företrädare för kommunstyrelseförvaltningens kanslienhet har för avsikt att genomföra återkommande uppföljning och utvärdering inom området informationssäkerhet. Någon uppföljning och utvärdering har dock ännu inte utförts av enheten vid granskningstillfället.

Av undersökningar utförda av SKR (2019) och MSB (2015) framgår att 9 av 10 kommuner har en låg mognadsgrad i sitt informationssäkerhetsarbete. Bland annat noteras att i flertalet kommuner saknas handlingsplaner för att nå ledningens mål för informationssäkerhet.

Bedömning

Vi gör bedömningen att det inom verksamheten påbörjats insatser för att utveckla koncernens arbete med informationssäkerhet. Arbetat bedöms ännu *inte* ske på ett tillräckligt systematiskt sätt. Bedömningen baseras på följande:

- Riskbedömning, handlingsplan, uppföljning samt utvärdering utförs inte på ett återkommande sätt inom kommun och dess aktiebolag.

Vi rekommenderar att i övergripande styrdokument för informationssäkerhet regleras vilka delar som ska ingå i koncernens arbete med informationssäkerhet.

2.4 Kommunstyrelsens kontroll

Revisionsfråga 4: Följer kommunstyrelsen upp och utvärderar koncernens arbete med informationssäkerhet i tillräcklig grad?

Iakttagelser

I kommunstyrelsens uppdrag ingår att leda, samordna samt utöva uppsikt över kommunens samlade verksamhet. Uppsikten ska bland annat innefatta området informationssäkerhet.

I informationssäkerhetspolicy (KF 2007) framhålls att uppföljning och rapportering är en viktig del i arbetet med informationssäkerhet. Uppföljningen ska enligt policyn fokusera på följande delar:

- Att fastställda mål uppnås
- Att beslutade åtgärder är genomförda
- Att regler följs
- Att styrdokument och riskanalyser vid behov revideras.

Granskningen visar att kommunstyrelsen inte preciserat hur den ska utöva uppsikt inom området. Vi noterar att området informationssäkerhet inte finns med i den uppföljningsplan som årligen beslutas av styrelsen (KS 2022-02-01).

Av protokollsgranskning framgår att kommunstyrelsen under granskningsperioden inte fått någon återrapportering hur kommunen och dess aktiebolag arbetar med informationssäkerhet.

Företrädare för kommunens kanslienhet ser ett behov att utveckla uppföljning och återrapportering till kommunstyrelsen inom granskningsområdet.

Bedömning

Vår bedömning är att kommunstyrelsen *inte* i tillräcklig grad följer upp och utvärderar koncernens arbete med informationssäkerhet. Bedömningen baserar på följande:

- Kommunstyrelsen kan inte belägga att den under granskningsperioden utövat någon uppsikt inom området.
- Fullmäktiges anvisningar avseende uppföljning och rapportering har inte efterlevts av kommunorganisationen.

För framtiden föreslås att koncernens styrdokument reglerar dels vilken utsträckning bolagsstyrelse och nämnder ska utöva uppföljning och kontroll inom området informationssäkerhet, dels hur nämnder/bolag ska lämna eventuell rapportering till kommunstyrelsen.

Kommunstyrelsen rekommenderas även att föra in området “informationssäkerhet” i sin årliga uppföljningsplan.

3. Avslutning

3.1 Sammanfattande revisionell bedömning

Område	Bedömning	
Organisation, ansvar och roller	**Delvis uppfyllt**	Gul
Styrdokument	**Delvis uppfyllt**	Gul
Systematiskt arbetssätt	**Nej, ej uppfyllt**	Röd
Kommunstyrelsens kontroll	**Nej, ej uppfyllt**	Röd

Utifrån genomförd granskning görs en sammantagen revisionell bedömning att koncernens arbete med informationssäkerhet *inte* bedrivs med tillräcklig intern kontroll.

3.2 Rekommendationer

För att utveckla arbetet med informationssäkerhet bör följande rekommendationer prioriteras:

- Att kommunstyrelsen prövar vilket eventuellt ansvar som ska vila på facknämnderna när det gäller området informationssäkerhet. Om nämnderna tilldelas ett ansvar bör detta i så fall dokumenteras i reglemente samt i informationssäkerhetspolicy.
- Att kommunstyrelsen tar fram en koncernövergripande styrdokument som beskriver hur kommun och dess bolag ska arbeta med informationssäkerhet. Fokus bör riktas på följande delar:
    - Organisation och ansvar för arbetet med informationssäkerhet.
    - Ge vägledning hur hur det systematiska arbetet ska bedrivas.
    - Formerna för hur bolagsstyrelser/nämnder ska följa upp området men även lämna rapport till kommunstyrelsen.
- Att kommunstyrelsen för in området “Informationssäkerhet” i sin årliga uppföljningsplan.

2022-11-09

Bo Rehnberg

Uppdragsledare
