Granskning av informationssäkerhet

Gällivare kommun

December 2021

Bo Rehnberg, certifierad kommunal revisor

Hugo Horstmann, revisionskonsult

pwc

Revisionsrapport

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Gällivare kommun genomfört en granskning inom området informationssäkerhet. Syftet med granskningen är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll. Revisionsobjekt i granskningen är kommunstyrelsen.

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

Utifrån genomförd granskning görs en sammantagen revisionell bedömning att kommunstyrelsen *inte* säkerställt att arbetet med informationssäkerhet bedrivs på ett ändamålsenligt sätt. Den interna kontrollen inom granskade områden bedöms vara *otillräcklig*.

Underlag för revisionell bedömning redovisas i avsnitt 2.1-2.5.

För att utveckla granskningsområdet lämnas följande rekommendationer:

- Att kommunstyrelsen prioriterar kommunens arbete med informationssäkerhet och vidtar åtgärder för att utveckla ett systematisk arbetssätt inom organisationen.
- Att kommunstyrelsen ser till att fullmäktiges styrdokument för informationssäkerhet aktualiseras och blir kända inom organisationen (politisk nivå respektive verksamhetsnivå). Vidare bör prövas om det på verksamhetsnivå ska utfärdas kompletterande styrdokument/vägledningar för arbetet med informationssäkerhet.
- Att kommunstyrelsen säkerställer att respektive facknämnd klargör hur ansvar/roller för informationssäkerhet fördelas i förvaltningsorganisationen.
- Att kommunstyrelsen utvecklar sin uppsikt inom området. Detta kan exempelvis ske genom att föra in området i årshjul/uppsiktsplan som plan för intern kontroll 2022.

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.

Information är värdefull och behöver många gånger skyddas. 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 2021 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att finns en god informationssäkerhet inom kommunen och har därför gett PwC ett uppdrag att granska området.

1.2 Syfte och revisionsfrågor

Revisorernas uppdrag regleras i kommunallagen kapitel 12. Syfte med granskningen är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker 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. Finns ett ledningssystem för informationssäkerhet implementerat?
4. Bedriver verksamhetsorganisationen ett aktivt arbete med informationssäkerhet? Fokus på aktiviteter/åtgärder, rapportering samt säkerhetskultur.
5. Följer kommunstyrelsen upp och utvärderar kommunens arbete med informationssäkerhet i tillräcklig grad?

Revisionsfråga 2, 4 och 5 utgör underlag för att bedöma om arbetet med informationssäkerhet bedrivs på ett ändamålsenligt sätt. Övriga revisionsfrågor används för att bedöma om den interna kontrollen inom granskningsområdet är tillräcklig.

1.3 Revisionskriterier

Följande revisionskriterier används i granskningen:

- Kommunallagen 6:1, 6:6, 6:13
- Kommuninterna styrdokument relevanta för granskningen.

1.4 Avgränsning

I tid avgränsas granskningen till år 2021. Revisionsobjekt i granskningen är kommunstyrelsen. Övrig avgränsning, se avsnitt “Syfte och revisionsfrågor”.

1.5 Metod

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

- Informationssäkerhetsstrategi
- Handlingsprogram för informationssäkerhet
- Informationssäkerhetsinstruktioner för användare.
- Säkerhetspolicy
- Reglemente för kommunstyrelsen
- Kommunstyrelsens protokoll för perioden 2020-11-01 -- 2021-10-31

Intervjuer har genomförts med företrädare för kommunstyrelsen, säkerhetschef, IT-chef, IT-samordnare på IT-enheten samt företrädare för systemägare inom socialförvaltning respektive förvaltning barn och ungdom. 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 Tobias Bjöörn, certifierad kommunal revisor, PwC enligt PwC:s rutiner för kvalitetssäkring.

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 detta arbete är att tydliggöra ansvar och roller inom en organisation.

Kommunrevisionen har 2014 genomfört en granskning av inom områdena IT respektive informationssäkerhet. I granskningen konstaterades att fanns ett behov att kommunicera hur ansvar och roller fördelas inom verksamhetsorganisationen.

Kommunfullmäktige har i olika styrande dokument angett hur ansvar och roller fördelas inom organisationen. I styrdokumenten anges följande:

- Kommunstyrelsen bär ett övergripande ansvar för kommunens informationssäkerhet. Nämnderna ansvarar för informationssäkerhetsarbetet inom respektive förvaltning.
- På verksamhetsnivå vilar ansvaret för arbetet med informationssäkerhet i första hand på *systemägare* och *systemförvaltare*. Systemägaren ansvarar för att analysera systemsäkerheten. Systemförvaltaren, som utses av systemägaren, ska initiera och genomföra analyser av systemsäkerhet. Systemägaren ska tillika vara verksamhetsansvarig.
- Befattningarna *systemadministratör*, *IT-chef* samt *säkerhetschef* har också ansvar och uppdrag inom området informationssäkerhet.
- Därutöver vilar vissa uppdrag även på *IT-enheten* och *IT-gruppen*.

I styrdokumenten ställs krav på att samtliga förekommande IT-system och systemägare ska vara förtecknade. Granskningen visar att det för närvarande saknas en aktuell och heltäckande sammanställning. Ett arbete har påbörjats inom IT-enheten för att upprätta en sådan förteckning. Enligt uppgift ska detta vara slutfört innan årsskiftet 21/22. En brist med kommunens styrdokument är att dessa inte reglerar vilket kommunalt organ som bär ansvar för att ajourhålla förteckning över IT-system.

De intervjuade upplever att ansvarsfördelning som anges i dokumenten i stort vara rimlig. Beskriven ansvarsfördelning uppges även ha legitimitet inom organisationen.

Av styrdokumenten framgår att det löpande arbetet med informationssäkerhet i första hand ska utföras av systemägare och systemförvaltare. Granskningen noterar skillnader i vilken grad dessa uppdrag decentraliserat inom olika förvaltningar.

I granskningen framkommer att det finns ett behov av att vidareutveckla, precisera samt aktualisera hur ansvar, roller och uppdrag fördelas inom verksamhetsorganisationen.

Det finns en samsyn bland de intervjuade att det saknas en fungerande rutin att informera/förankra hos berörda organ om hur ansvar och uppdrag fördelas inom kommunorganisationen.

Bedömning

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

- I styrdokument klargörs i huvudsak hur ansvar och roller för området fördelas inom organisationen. Beskriven ansvarsfördelning upplevs vara rimlig.
- En stor brist är att berörda organ i låg utsträckning har kunskap om gällande ansvarsfördelning. Ansvarsfördelningen har inte förankras inom verksamheten. Motsvarande iakttagelse noterades även i 2014 års revision.

För att utveckla området föreslås att kommunstyrelsen, i sin samordnande roll, ser till att respektive facknämnd klargör hur ansvar och roller för informationssäkerhet fördelas inom förvaltningsorganisationen. Styrelsen bör även pröva om styrdokumenten behöver aktualiseras när det gäller roll- och ansvarsfördelning.

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. Som stöd för arbete med informationssäkerhet har MSB utfärdat vägledningar och metodstöd som kan användas av exempelvis kommuner och regioner. 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. Säkerhetspolicy (beslutad av fullmäktige 2016)
2. Informationssäkerhetsstrategi (beslutad av fullmäktige 2013)
3. Handlingsprogram för informationssäkerhet (beslutad av fullmäktige 2013)
4. Informationssäkerhetsinstruktion för användare (beslutad av fullmäktige 2013)

Av sammanställningen framgår att dokumenten är från tidigare mandatperioder (2011-2014, 2015-2018). I kommunstyrelsens uppdrag ingår att handlägga de ärenden som ska beslutas av kommunfullmäktige. I styrelsens uppdrag ingår även att se till att fullmäktiges beslut och riktlinjer verkställs av organisationen.

Förekommande styrdokument innehåller framför allt följande delar:

- Vision och mål

- Organisation och ansvar
- Generella krav, regler och rutiner
- Revidering och uppföljning
- Förteckning över förekommande styrdokument

Företrädare för verksamheten upplever att styrdokumenten reglerar väsentliga områden.

En brist är att styrdokumenten i flera avseenden är inaktuella. Ett annat problem är att dokumenten i princip är okända i organisationen (politisk nivå respektive verksamhetsnivå). Flertalet av de intervjuade är relativt nya i sina uppdrag. Dessa upplever att det saknas rutin i fråga om att informera om förekommande styrdokument.

Arbetet med informationssäkerhet fullgörs i första hand av systemägare och systemförvaltare. En brist med kommunens styrdokument är att de i låg grad beskriver hur dessa organ i praktiken ska arbeta med exempelvis analys av systemsäkerhet.

Av undersökningar utförda av medlemsorganisationen Sveriges Kommuner och Regioner (2019) och MSB (2015) 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 interna styrdokument som ger vägledning hur organisationen ska arbeta med informationssäkerhet. Styrdokumenten är relativt heltäckande.
- Förekommande styrdokument är inte i alla delar aktuella. Aktualiteten kan ifrågasättas då merparten av dokumenten är från 2013. En annan brist är att de i låg grad kända inom organisationen. Styrdokumenten har inte implementerats på ett tillfredsställande sätt.

För framtiden föreslås att kommunstyrelsen, i sin samordnande roll, prioriterar att fullmäktiges styrdokument för informationssäkerhet aktualiseras och blir kända inom organisationen (politisk nivå respektive verksamhetsnivå). Vidare bör prövas om det på verksamhetsnivå ska utfärdas kompletterande styrdokument/vägledningar för arbetet med informationssäkerhet.

2.3 Ledningssystem

Revisionsfråga 3: Finns ett ledningssystem för informationssäkerhet implementerat?

Iakttagelser

Ett ledningssystem ger styrning hur en organisation ska bedriva ett systematisk arbete inom ett specifikt område, till exempel kvalitet, miljö, arbetsmiljö eller informations-säkerhet. Ledningssystemet fungerar som ett stöd för medarbetarna i deras dagliga arbete men även som ett verktyg för ledningen att säkerställa att verksamheten bedrivs på avsett sätt.

I revisionens granskning 2014 noterades att det inom kommunen initierats ett arbete för att på sikt skapa ett ledningssystem för informationssäkerhet (LIS). Vår granskning visar att Gällivare år 2021 alltjämt saknar en ledningssystem inom området.

Av MSB:s undersökning från 2015 framgår att få kommuner (knappt 20 procent) har ett ledningssystem för informationssäkerhet.

Bedömning

Vår bedömning är att det *saknas* ett ledningssystem för informationssäkerhet.
Bedömningen baseras på följande:

- Kommunen har inte verkställt 2014 års planer att tillskapa en särskilt ledningssystem för informationssäkerhet.
- Följaktligen har det inte skett implementering av ett sådant system i verksamheten.

För att utveckla verksamheten föreslås att kommunstyrelsen prövar om kommunen ska inrätta ett särskilt ledningssystem. Systemet kan skapa förutsättningar för den samlade verksamheten att bedriva ett systematiskt informationssäkerhetsarbete.

2.4 Systematiskt arbetssätt

Revisionsfråga 4: Bedriver verksamhetsorganisationen ett aktivt arbete med informationssäkerhet? Fokus på aktiviteter/åtgärder, rapportering samt säkerhetskultur.

Iakttagelser

Under senare år har *Myndigheten för samhällsskydd och beredskap* (MSB) betonat vikten av att svenska myndigheter och organisationer bedriver ett systematiskt arbete med informationssäkerhet. Myndigheten har tagit fram vägledningar och stöd för hur organisationer ska arbeta inom området. Ett systematiskt arbetssätt kännetecknas vanligtvis av följande moment:

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

Ett systematiskt arbetssätt främjas om det finns en säkerhetskultur i organisationen. Säkerhetskultur är de gemensamma attityder, värderingar och uppfattningar som chefer och anställda har till frågor som rör säkerhet. En god säkerhetskultur kännetecknas av att ledningen prioriterar och hanterar säkerhetsfrågor på alla nivåer av verksamheten och att de är en del av kulturen.

Av föregående avsnitt framgår att fullmäktige fastställt styrdokument som beskriver hur kommunens organisation ska arbeta med informationssäkerhet. Bland annat ställs krav på att organisationen fortlöpande arbetar med riskanalyser, mål, aktivitetsplaner, uppföljning och utvärdering.

Granskningen omfattar bland annat den verksamhet som bedrivs inom socialnämndens och barn- och utbildningsnämndens ansvarsområden. Vid intervjuer med företrädare för dessa verksamheter framkommer att de genomför vissa aktiviteter för att utveckla

informationssäkerheten. Vi kan inte se att detta arbete sker på det sätt som beskrivs i kommunens styrdokument.

Vår sammantagna bild är att det inom kommunens verksamheter inte bedrivs ett systematiskt arbete med informationssäkerhet. Vi noterar följande:

- Det sker ingen dokumenterad riskanalys av säkerhet i förekommande IT-system.
- Kommunövergripande mål har inte brutits ned till årsmål för respektive förvaltning/verksamhet.
- Det saknas handlings-/aktivitetsplaner för att utveckla informationssäkerhetsarbetet.
- Det sker ingen samlad uppföljning och utvärdering av genomförda insatser. Detta gäller såväl på förvaltningsnivå som på kommunövergripande nivå.

Enligt företrädare för verksamheterna finns ett flertal förklaringar till att verksamheten inte bedriver ett systematisk arbete inom området. Bland annat framhålls att ledningen inte tydligt uttryckt att detta arbete ska prioriteras inom organisationen. Andra faktorer som anges är avsaknad av tid, ekonomiska resurser och tillräcklig kompetens.

MSB tillhandahåller ett verktyg där organisationer genom självskattning kan pröva om dess arbete med informationssäkerhet sker på ett systematiskt sätt. Kommunen har under 2021 genomfört en självskattning samt inrapporterat resultatet till MSB. Rapporten visar att kommunen inte bedriver ett systematiskt arbete med informationssäkerhet.

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 finns inte handlingsplaner för att nå ledningens mål för informationssäkerhet. Företrädare för verksamheten upplever att Gällivare kommun har en låg mognadsgrad när det gäller dess arbete med informationssäkerhet.

Bedömning

Vi gör bedömningen att verksamhetsorganisationen *inte* bedriver ett aktivt arbete med informationssäkerhet. Bedömningen baseras på följande:

- Det saknas ett systematiskt arbetssätt när det gäller riskanalyser, aktivitetsplaner, uppföljning, utvärdering och rapportering.
- Arbetet med informationssäkerhet sker inte i enlighet med MSB:s vägledningar och fullmäktiges styrdokument.
- Kommunens egen självskattning och rapportering till MSB visar att kommunen inte bedriver ett systematiskt arbete med informationssäkerhet.
- Granskningen indikerar att det saknas en tillfredsställande säkerhetskultur inom organisationen.

Vi rekommenderar kommunstyrelsen att prioritera kommunens arbete med informationssäkerhet. Styrelsen bör även pröva vilka åtgärder som måste vidtas för att åstadkomma ett systematiskt arbetssätt inom organisationen (kommunstyrelse, nämnder och förvaltningar).

2.5 Kommunstyrelsens kontroll

Revisionsfråga 5: Följer kommunstyrelsen upp och utvärderar kommunens 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 avsnitt 2.2 återfinns en förteckning över kommuninterna styrdokument. I dokumenten, som beslutats av kommunfullmäktige, anges hur kommunstyrelsen ska utöva styrning och kontroll inom området. Här beskrivs formerna för återrapportering från verksamhet till kommunstyrelsen. Bland annat ska kommunstyrelsen årligen delges en skriftlig rapport för området informationssäkerhet. Rapporten ska bland annat innehålla uppföljning/utvärdering av fullmäktiges målsättningar inom området.

Vår granskning visar att kommunstyrelsen under innevarande mandatperiod varken begärt eller fått återkommande rapportering hur organisationen arbetar med informationssäkerhet. Återrapportering saknas för såväl den egna förvaltningen som för kommunens samlade verksamhet. Styrelsen har inte heller följt upp i vilken grad verksamheten når de övergripande mål som fullmäktige fastställt för informationssäkerhet.

Vår granskning visar att återrapportering till kommunstyrelsen inte sker enligt kommunfullmäktiges direktiv.

Till följd av att kommunstyrelsen inte fullgjort sin uppsikt inom området, har styrelsen följaktligen inte heller lämnat rapport till fullmäktige hur organisationen arbetar med informationssäkerhet. Enligt kommunstyrelsens reglemente ska den återkommande rapportera hur den samlade verksamheten utvecklas mot bakgrund av fastställda mål.

Bedömning

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

- Kommunstyrelsen har inte säkerställt att det sker en återkommande uppföljning och återrapportering inom området.
- Uppföljning och utvärdering sker inte i enlighet med direktiv som utfärdats av kommunfullmäktige.

För framtiden föreslås att kommunstyrelsen utvecklar sin uppsikt inom området. Detta kan exempelvis ske genom att föra in området i såväl årshjul/uppsiktsplan som plan för intern kontroll 2022.

3. Avslutning

3.1 Sammanfattande revisionell bedömning

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

Utifrån genomförd granskning görs en sammantagen revisionell bedömning att kommunstyrelsen *inte* säkerställt att arbetet med informationssäkerhet bedrivs på ett ändamålsenligt sätt. Den interna kontrollen inom granskade områden bedöms vara *otillräcklig*.

3.2 Rekommendationer

För att utveckla området bör följande rekommendationer prioriteras:

- Att kommunstyrelsen prioriterar kommunens arbete med informationssäkerhet och vidtar åtgärder för att utveckla ett systematisk arbetssätt inom organisationen.
- Att kommunstyrelsen ser till att fullmäktiges styrdokument för informationssäkerhet aktualiseras och blir kända inom organisationen (politisk nivå respektive verksamhetsnivå). Vidare bör prövas om det på verksamhetsnivå ska utfärdas kompletterande styrdokument/vägledningar för arbetet med informationssäkerhet.
- Att kommunstyrelsen säkerställer att respektive facknämnd klargör hur ansvar/roller för informationssäkerhet fördelas i förvaltningsorganisationen.
- Att kommunstyrelsen utvecklar sin uppsikt inom området. Exempelvis genom att föra in området i såväl årshjul/uppsiktsplan som plan för intern kontroll 2022.

2021-12-17

Erik Jansen

Uppdragsledare

Bo Rehnberg

Projektledare

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av revisorerna i Gällivare kommun enligt de villkor och under de förutsättningar som framgår av projektplan från 2021-03-23. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.