Uppföljning av tidigare granskningar

Solna Stads förtroendevalda revisorer

Mars 2022

Nicolas Berglund
Nur Nauti

pwc

Revisionsrapport

Innehållsförteckning

1.	**Inledning**	**2**
1.1.	Granskningsbakgrund	2
1.2.	Syfte och revisionsfråga	2
1.3.	Revisionskriterier	2
1.4.	Avgränsning	2
1.5.	Metod	2
2.	**Resultat**	**3**
2.1.	IT-säkerhet	3
2.2.	Krisberedskap	3

1. Inledning

1.1. Granskningsbakgrund

Av kommunallagen och god revisionssed följer att revisorerna årligen skall granska styrelser, nämnder och fasta fullmäktigeberedningar.

Revisionsprocessen kan delas in i följande delar: planering, genomförande, rapportering och uppföljning. Den sista delen av revisionsprocessen är viktig för att säkerställa att genomförd revision får önskad effekt, dvs. att lämnade rekommendationer beaktas och åtgärdas av berörda styrelser och nämnder.

Utifrån sin risk- och väsentlighetsanalys inför 2021 har Solna Stads revisorer valt att genomföra en uppföljning av tidigare granskningar avseende *IT-säkerhet* och *Krisberedskap*.

1.2. Syfte och revisionsfråga

Granskningen syftar till att besvara följande revisionsfrågor:

Uppföljningen syftar till att följa upp tidigare granskningar med avseende på nedanstående frågeställningar?

- Vad har åtgärdats av revisionens påpekanden?
- Vad kvarstår att åtgärda?
- Finns behov av att träffa ansvarig nämnd/förvaltning?

Följande granskningar har valts ut för att följas upp under 2021 inom ramen för denna granskning:

- IT-säkerhet och intrångsskydd (2018)
- Krisberedskap (2018)

1.2.1. Kontrollmål

De kontrollmål som legat till grund för uppföljningarna framgår av bifogade rapporter, se bilaga 1 och 2.

1.3. Revisionskriterier

Revisionskriterier är utarbetade för de ursprungliga granskningarna som är föremål för uppföljning, se ovan.

1.4. Avgränsning

Uppföljning sker av de rekommendationer som lämnades i samband med tidigare granskningar.

1.5. Metod

Intervjuer med ansvariga befattningshavare, insamling av relevant dokumentation i form av beslutsunderlag, riktlinjer, rutinbeskrivningar etc. I förekommande fall, stickprovsmässig kontroll av underlag och rutiner för att säkerställa att tidigare identifierade brister åtgärdats.

2. Resultat

Nedan redovisas en sammanfattning av resultatet för genomförda uppföljningar.

2.1. IT-säkerhet

Efter genomförd granskning är PwCs samlade bedömning att Solna Stad överlag har bra rutiner och arbetssätt på plats gällande IT- och informationssäkerhet men att vissa delar har förbättringspotential. PwC ser att positiv utveckling skett hos Solna Stad de senaste åren då de akuta säkerhetsbrister som identifierats av PwC 2018 idag bedöms vara åtgärdade. PwC kan utöver detta se att Solna Stad arbetar systematiskt med IT- och informationssäkerhet utifrån ett framtaget ledningssystem för informationssäkerhet (LIS) enligt ISO 27001.

PwC har dock noterat ett antal områden som behöver förbättras för att uppnå en än högre nivå av säkerhet av stadens informationstillgångar. Detta berör bl.a. hur viss styrdokumentation är utformad där det idag t.ex. saknas formella interna kontrollramverk för att genomföra uppföljning samt hanteringsrutiner kopplat till informationsklassning.

PwC noterade även ett par förbättringsområden i förhållande till stadens riskhantering. Då Kommunstyrelsen är informationsägare och därmed även riskägare är det Kommunstyrelsen som måste delegera och även säkerställa att riskanalyser genomförs systematiskt och att risker åtgärdas. Idag finns det inte tillräcklig kontroll och uppföljning av att risker identifieras i verksamhetsspecifika system.

Vidare har PwC identifierat rekommendationer kopplat till incidenthantering och anlitande av externa leverantörer. I bifogad rapport framgår mer detaljerat information utifrån uppföljningen, se bilaga 1.

2.2. Krisberedskap

Utifrån genomförd granskning är vår samlade bedömning att Kommunstyrelsen i allt väsentligt åtgärdat de rekommendationer som lämnades utifrån tidigare granskning. Staden har arbetat aktivt med krisledningsarbetet och utvecklat metoder och riktlinjer för att bli effektivare. Bedömningen grundas bl a på nedanstående.

Tydliga kontaktvägar har formaliserats i syfte att kunna eskalera händelser till den centrala krisledningen. Staden har arbetat fram ett tydligt larmkort samt tagit fram rutiner och riktlinjer för arbetet när krisledningsgruppen samlas.

Krisledningsnämnden är involverad i arbetet med RSA[1].

Vi bedömer att de helägda kommunala bolagen har inkluderats i det gemensamma strukturerna för krisberedskapsarbetet inom staden. Vi har dock inom ramen för uppföljningen inte tagit del av dokumentation eller information kring hur motsvarade inkludering genomförs mot delägda Norrenergi och Stiftelsen Signalisten/Solnabostäder.

Staden har uppdaterat relevant dokumentation sedan granskningen som genomfördes 2018. Staden följer riktlinjer och föreskrifter från relevanta myndigheter, det genomförs löpande uppdateringar om ändringar i föreskrifter eller lagar sker. Det finns fastställda rutiner för erfarenhetsåterföring efter övning, utbildning och skarpa händelser. Staden har upprättat dokumentation *Handbok för krishantering i Solna* med riktlinjer och rutiner för hur utvärderingar och erfarenhetsåterföring ska genomföras. I bilaga 2 redovisas genomförd uppföljning mer detaljerat.

[1] Risk- och sårbarhetsanalys

2.3. Sammanfattande bedömning

Sammanfattningsvis bedöms tidigare lämnade rekommendationer inom ovanstående områden i allt väsentligt vara åtgärdade. Det finns därför i dagsläget inget behov av att träffa Kommunstyrelsen särskilt i detta avseende.

2022-03-24

Anders Hägg

Henrik Fagerlind