Bodens kommun

**Kommunrevisionen** 2020-09-01

För kännedom
Fullmäktiges presidium
Partiernas gruppledare

Till
**Kommunstyrelsen**

# Revisionsgranskning – Uppföljning av 2018 års cybersäkerhetsgranskning inkl. granskning av informationssäkerheten

I egenskap av förtroendevalda revisorer i Bodens kommun har vi genomfört en uppföljande granskning avseende vår cybersäkerhetsgranskning från år 2018, samt en granskning av kommunens informationssäkerhetsarbete. I granskningen har vi biträtts av sakkunniga från PwC.

Utifrån genomförd granskning gör vi en **sammantagen revisionell bedömning** utifrån granskningens två områden enligt följande:

- Kommunstyrelsen har **inte vidtagit ändamålsenliga åtgärder** baserat på revisionens tidigare granskning och rekommendationer inom området. Den interna kontrollen bedöms i sammanhanget som **inte tillräcklig**.
- Kommunstyrelsen **delvis** bedriver **ett ändamålsenligt** arbete med informationssäkerhet. Den interna kontrollen avseende arbetet med informationssäkerhet bedöms som **delvis tillräcklig**.

Vår granskning visar bland annat att kommunstyrelsen ej beslutat om eller vidtagit några åtgärder, eller genomfört någon analys, utifrån dennes behandling av revisionens tidigare granskning inom cybersäkerhetsområdet.

Vi bedömer vidare att informationssäkerhetsarbetet inte bedrivs i enlighet med gällande styrning inom området då klassificering av system och information inte sker på ett systematiskt sätt. Vi ser även brister i uppföljningen av informationssäkerhetsarbetet.

För att utveckla granskningsområdet lämnas följande **rekommendationer**, att:

- Kommunstyrelsen säkerställer att identifierade brister åtgärdas, samt tillser att uppföljning, utvärdering/analys och rapportering genomförs till styrelsen i syfte att upprätthålla en tillräcklig intern kontroll inom IT-säkerhetsområdet.
- Kommunstyrelsen tillser att arbetet med informationssäkerhet bedrivs i enlighet med den styrning som finns inom området.
- Kommunstyrelsen tillser att uppföljningen av informationssäkerhetsarbetet bedrivs så att rimlig säkerhetsnivå uppnås.

Vi emotser kommunstyrelsens svar på vår granskning till senast 2020-12-15.

För revisorerna i Bodens kommun

Per-Ulf Sandström
Ordförande

Roland Dahlqvist
Revisor

**Bilaga:** Revisionsrapport ”Uppföljning av 2018 års cybersäkerhetsgranskning inkl. granskning av informationssäkerhet”, PwC september 2020


| Postadress | Telefon | E-post | Organisationsnummer |
|---|---|---|---|
| 961 86 Boden | 0921-620 00 vx. med direktval | kommunen@boden.se | 212000-2767 |

# Uppföljning av cybersäkerhetsgranskningen 2018

# inkl granskning av informationssäkerheten

**Bodens kommun**

September 2020

*Projektledare Erik Jansen*

*Projektmedarbetare Robert Bergman*

pwc

**Revisionsrapport**

# Innehållsförteckning

# Inledning

## Bakgrund

Revisionen genomförde under revisionsåret 2018 en granskning av intrångsskyddet inom Bodens kommun. Den sammanfattande bedömning var att kommunstyrelsen inte hade säkerställt att kommunens tekniska IT-säkerhet var tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå. Den interna kontrollen bedömdes därmed inte vara tillräcklig. Härutöver lämnades tre rekommendationer (se vidare information gällande dessa under granskningens första revisionsfråga).

En kritisk del av en organisations säkerhetssystem är även dess informationssystem. Utöver externa och interna intrångsattacker är samhällskritisk infrastruktur såsom informationssystem, organisationens styrning, ledning, uppföljning och kontroll av denna ett potentiellt riskområde. Ny teknik innebär nya möjligheter. Den nya tekniken medför även nya risker. Kommunikationen med omvärlden ökar i omfattning och systemen blir mer integrerade, såväl inom organisationen som med andra intressenter. Detta ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete avseende organisationens informationssystem.

Utifrån en bedömning av risk och väsentlighet har revisorerna beslutat att genomföra en uppföljning av den tidigare granskningen av kommunens cybersäkerhet. Vidare har revisionen beslutat att genomföra en granskning av kommunens arbete med informationssäkerhet.

## Syfte och revisionsfrågor

Syftet med granskningen är att bedöma om kommunstyrelsen vidtagit ändamålsenliga åtgärder samt haft en tillräcklig intern kontroll inom cybersäkerhetsområdet, baserat på revisionens tidigare granskning och rekommendationer. Vidare är syftet att bedöma om Bodens kommun har ett ändamålsenligt arbete med informationssäkerhet, samt ifall den interna kontrollen inom området är tillräcklig.

Uppföljning av tidigare cybersäkerhetsgranskning:

- Vilka åtgärder har, utifrån styrelsens behandling av revisionens tidigare granskning, beslutats om och vidtagits?
- I vilken utsträckning har beslutade åtgärder återrapporteras till kommunstyrelsen?
- Finns kvarstående åtgärdsbehov och i så fall vilka?

Informationssäkerhet

- Bedriver kommunstyrelsen ett ändamålsenligt arbete med att identifiera, prioritera och hantera hot mot kommunens IT/IS-säkerhet?
- Är det interna kontrollen i sammanhanget tillräcklig?

Bedömningen baseras på NIST-ramverkets fem perspektiv, se vidare under metod.

## Revisionskriterier

- Kommunallag kap 6 § 6
- Kommuninterna styrdokument som rör granskningsområdet
- Iakttagelser från tidigare granskning (2018)

## Avgränsning och metod

I tid avgränsas granskningen till att i huvudsak avse år 2020. Granskningen betonar kommunens övergripande cyber- och informationssäkerhetsmognad. I övrigt se syfte och revisionsfrågor samt även metod och genomförande.

*Metod avseende uppföljning av tidigare genomförd granskning:*

- Dokumentstudier av styrelsens behandling över revisionsrapporten, ev. fattade beslut och åtgärder med anledning av rapporten, samt övriga relevanta dokument och protokoll.
- Intervjuer med IT-chef samt företrädare från kommunens IT-kontor. Därutöver intervju med kommunstyrelsens ordförande, kommundirektör samt med oppositionsföreträdare i kommunstyrelsen.

*Metod avseende informationssäkerhetsgranskning:*

Metoden grundar sig på den vedertagna NIST Cyber security framework-modellen som tagits fram för att stärka informationssäkerheten i samhällskritisk infrastruktur. Granskningen sker genom att göra en nulägesanalys av organisationens förmågor inom fem perspektiv;

> ***Identifiera**, vilket innebär analyser av organisationens förmåga att identifiera det skyddsvärda, förmågan till riskanalys och riskhantering samt förmågan till styrning av informationssäkerheten.*
>
> ***Skydda**, vilket innebär värdering av organisationens förmåga till behörighetskontroller, utbildning av personal, skyddsmekanismer som brandväggar med mera.*
>
> ***Upptäcka**, vilket innebär en bedömning av organisationens förmåga att upptäcka eventuella avvikelser från normalbilden, övervaknings-processer, logghantering med mera.*
>
> ***Agera/Avbryta**, vilket handlar om organisationen förmåga till incidenthantering, kommunikationsplaner, avhjälpande åtgärder samt utveckling.*
>
> ***Återhämta**, vilket handlar om organisationens förmåga att så snart som möjligt efter en incident återgå till normaldrift samt förmågan till att göra analyser av det inträffade och förbättra/förändra rutiner.*

Inhämtning av information har skett genom följande steg:

1. Dokumentinsamling av styrande dokument relevanta för granskningsområdet.
2. Gruppintervju med ledande tjänstemän
3. Intervju med företrädare för kommunens IT-verksamhet.

Granskningen har även beaktat händelser och incidenter kopplat till kommunens cybersäkerhet under de senaste 12 månaderna.

De sammanställda granskningsiakttagelserna beskriver organisationens mognadsgrad inom ovan fem områden. Beskrivningen ligger till grund för bedömning av granskningens syfte och frågeställningar.

# Iakttagelser och bedömningar

## Uppföljning av 2018 års granskning

I nedan avsnitt redogörs för iakttagelser och bedömningar avseende uppföljning av tidigare cybersäkerhetsgranskning:

## Vilka åtgärder har, utifrån styrelsens behandling av revisionens tidigare granskning, beslutats om och vidtagits

*Iakttagelser*

Revisorerna i Bodens kommun behandlade på sin överläggning 2018-11-13 granskningen av kommunens intrångsskydd. Revisionens sammanfattande bedömning var att kommunstyrelsen inte säkerställt att kommunens tekniska IT-säkerhet var tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå. Den interna kontrollen bedömdes därmed inte vara tillräcklig.

I syfte att utveckla verksamheten rekommenderades kommunstyrelsen

- att säkerställa att åtgärder vidtas skyndsamt för att åtgärda sårbarheter samt öka IT-säkerheten och höja säkerhetsnivån.
- att säkerställa att utdaterade mjukvaror uppdateras samt utveckla utvärdering och inventering av mjukvaror då detta är bristande idag.
- att arbeta för ökad IT-mognad och säkerhetsmedvetande i organisationen.

Granskningsrapport och missiv överlämnades till kommunstyrelsen. Revisorerna begärde inte svar eller återrapportering från kommunstyrelsen i samband med överlämnandet.

Vår granskning visar att revisionsrapporten delgavs kommunstyrelsen på mötet 2018-12-10 under § 195 *Delegationsbeslut och delgivningar*. Kommunstyrelsen beslutade att lägga redovisningen av delegationsbeslut och delgivningar till handlingarna.

Vid intervjuerna inom ramen för denna granskning bekräftas att kommunstyrelsen ej fattat några beslut utifrån dennes behandling av revisionens granskning inom området. Däremot bekräftas att kommunchefen gav kommunens IT-kontor i uppdrag att vidta åtgärder utifrån de brister inom området som revisionsrapporten påvisade. Vid intervju bekräftas även att detta inte var resultatet av några politiska beslut inom området.

*Bedömning*

Vår granskning visar att kommunstyrelsen ej beslutat om några åtgärder utifrån dennes behandling av revisionens tidigare granskning. Vår bedömning är därmed att några åtgärder *inte* har beslutats om med anledning av styrelsens behandling av revisionens tidigare granskning.

Däremot noterar vi de åtgärder som kommunchefen lämnade i uppdrag till kommunens IT-kontor att åtgärda utifrån de i revisionsgranskningen påtalade bristerna. I sammanhanget finner vi det dock viktigt att poängtera att vidtagna åtgärder därmed inte är ett resultat av en politisk analys eller något politiskt övervägande avseende beslut om omfattning och prioritering.

## I vilken utsträckning har beslutade åtgärder återrapporteras till kommunstyrelsen?

*Iakttagelser*

Som framgår av revisionsfrågan ovan fattade kommunstyrelsen ej några beslut med anledning av dennes behandling av revisionens rapport.

Vår granskning visar följande:

- att KSau, vid sitt sammanträde 2019-09-16 under § 107, erhöll information gällande kommunens IT-säkerhet av verksamhetsutvecklare/projektledare inom området.
- den information som arbetsutskottet erhöll främst gällde aktuell hotbild samt åtgärder som vidtagits för att kunna upptäcka angrepp, skydda mot angrepp utifrån samt skydda mot angrepp från insidan.
- KSau erhöll ovan informationspunkt i ärendet. Utskottet rapporterade inte informationen vidare till kommunstyrelsen.

Kommunstyrelsen erhöll härutöver vid sitt sammanträde 2020-06-08 § 111 information utifrån en sammanställning av de åtgärder som förvaltningsorganisationen vidtagit efter uppdrag av kommunchefen med anledning av revisorernas granskning av kommunens IT-säkerhet. Kommunstyrelsen fattade inte på sammanträdet 2020-06-08 något beslut om åtgärder utifrån den verksamhetsinformation som styrelsen erhöll inom området.

*Bedömning*

Då kommunstyrelsen ej fattat några beslut utifrån revisionens rapport kan vår granskning ej heller styrka att någon återrapportering skett till kommunstyrelsen utifrån några sådana beslut inom området. Kommunstyrelsen har dock erhållit viss information relaterat till IT-säkerhetsområdet vid sitt sammanträde 2020-06-08 § 111.

Vår granskning visar att KSau erhöll viss verksamhetsinformation kopplat till IT-säkerhet 2019-09-16, men denna information rapporterades inte vidare till kommunstyrelsen.

Vid kommunstyrelsens sammanträde 2020-06-08 erhöll kommunstyrelsen en verksamhetsrapport inom IT-området. Återrapporteringen föranledde ej kommunstyrelsen att fatta några vidare beslut inom området.

## Finns kvarstående åtgärdsbehov och i så fall vilka?

*Iakttagelser*

Vår granskning visar att kommunens IT-kontor gjort en sammanställning av hur man på tjänstemannanivå omhändertagit de rekommendationer som lämnades i revisionens granskning. Vi noterar att det finns kvarstående områden där det pågår ett förbättringsarbete för att ytterligare stärka skyddet av Bodens kommuns informationstillgångar.

Denna sammanställning delges till viss del kommunstyrelsen vid sammanträdet 2020-06-08. Som framgår ovan i denna rapport fattade kommunstyrelsen ej några beslut med anledning av IT-kontorets sammanställning och information till styrelsen.

Härutöver framkommer vissa kvarstående åtgärdsbehov avseende informations-säkerhet, vilka redogörs för närmare under avsnittet informationssäkerhet/skydda på sidan 12 i denna rapport.

*Bedömning*
Vår bedömning är att det finns kvarstående identifierade åtgärdsbehov inom IT-säkerhetsområdet, vilka även informerats om till kommunstyrelsen. I sammanhanget noterar vi att kommunstyrelsen ej beslutat om vidare åtgärder inom området med anledning av den information som styrelsen erhöll på sitt sammanträde 2020-06-08 §111.

## Informationssäkerhet
I nedan avsnitt redogörs för iakttagelser och bedömningar avseende granskning av kommunens informationssäkerhetsarbete.

## Formella utgångspunkter
I syfte att uppnå en hög informationssäkerhet i samhället har lagar inom området stiftats. NIS-direktivet eller *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster* liksom GDPR, är exempel på lagar som organisationer behöver beakta i sitt arbete med informationssäkerhet. Lagstiftningen ställer krav på informationssäkerhet och incidentrapportering för organisationer som hanterar personuppgifter.

NIST-ramverket är en metod för att utvärdera en organisations nuvarande cybersäkerhetsförmåga, dvs säkerställa att information hanteras korrekt, hindra otillbörlig åtkomst av information samt motverka avbrott i IT-miljön, inom fem olika områden/funktioner, *identifiera, skydda, upptäcka, agera och återställa*. NIST cybersäkerhetsramverket omfattar en riskbaserad sammanställning av riktlinjer som syftar till att hjälpa organisationer att identifiera, genomföra och förbättra säkerhets-praxis och skapa ett gemensamt språk för intern och extern kommunikation av säkerhetsproblem. Ramverket introducerar inga nya standarder, snarare integrerar det redan etablerade standarder och praxis. Utvärderingen av organisationens mekanismer möjliggör för verksamheten att bestämma dess nuvarande cybersäkerhetsförmåga, sätta mål och etablera en plan för åtgärder och upprätthållandet av cybersäkerhetsprogram.

I följande avsnitt kommer vi att på ett övergripande sätt redogöra för hur Bodens kommun arbetar med informationssäkerhet utifrån NIST-ramverkets fem områden.

## Kommunstyrelsens arbete och interna kontroll avseende kommunens IT/IS-säkerhet
Följande avsnitt redogör för iakttagelser och bedömningar avseende följande revisionsfrågor:

- Bedriver kommunstyrelsen ett ändamålsenligt arbete med att identifiera, prioritera och hantera hot mot kommunens IT/IS-säkerhet?
- Är det interna kontrollen i sammanhanget tillräcklig?

*Iakttagelser*

***Identifiera**, innebär analys av organisationens förmåga att identifiera det som är skyddsvärt i organisationen, organisationens förmåga till riskanalys och riskhantering samt förmågan till styrning av informationssäkerheten.*

Den övergripande styrningen av kommunens informationssäkerhet finns i form av följande dokument:

- Informationssäkerhetspolicy (KF 2019-04-08) - Beskriver bl.a. principer för kommunens informationssäkerhetsarbete, målsättningar, definition av informationssäkerhet, organisation och ansvar samt hur policyn ska följas upp.
- Strategi för trygghet och säkerhet 2020-2023 (KF 2019-10-17). Strategin innehåller ett särskilt avsnitt som rör informationssäkerhet. I både strategin och i ovan nämnda policy framgår att förvaltningarna ska aktivt, inom ramen för informationssäkerhets-arbetet, bl.a. utse säkerhetshandläggare och genomföra informationsklassificering av information som förvaltningen hanterar och som har ett värde att skydda.

Utöver dessa övergripande styrdokument har regler och rutiner tagits fram på verksamhetsnivå som rör användning av IT och hantering av information.

Granskning av kommunens strategiska plan 2020-2022 visar att ett gemensamt kontrollområde för styrelsens och nämndernas interna kontroll är att kontrollera efterlevnaden av informationssäkerheten. Av dokumentet framgår att detta kontrollmoment kan innebära att styrelsen/nämnderna följer upp hur regler och rutiner för informationssäkerhet efterlevs. Rapportering ska ske till kommunstyrelsen i samband med delårsrapport per augusti och i årsredovisning. Även föregående års strategiska plan har haft informationssäkerhet som ett gemensamt kontrollområde. Då rapportering avseende 2020 ännu inte ägt rum vid granskningstillfället har vi istället granskat rapporteringen avseende 2019.

Vår granskning visar att rapportering av nämndernas internkontrollarbete har rapporterats till kommunstyrelsen i samband med delårsrapport per augusti 2019 och årsredovisning för år 2019. Kontrollområdet *informationssäkerhet* har i varierad utsträckning hanterats av nämnderna. De flesta nämnder redovisar att de har genomfört utbildningsinsatser bland medarbetare, men att vissa fortsatta åtgärder kvarstår. Inom socialnämndens verksamheter har klassning av information skett.

Av intervju med kommunens informationssäkerhetssamordnare framgår att det endast är inom socialförvaltningen och inom tekniska förvaltningen (VA-avdelningen) som handläggare för informationssäkerhetsfrågor i enlighet med informationssäkerhets-policyn har utsetts. Detta innebär att det saknas utpekade resurser i form av personal för att driva ett fungerande informationssäkerhetsarbete inom verksamheterna, exempelvis för att utföra riskbedömningar eller säkerställa efterlevnad av styrande dokument. Detta uppges även ha inverkan på förankring av styrande dokument i verksamheterna.

Vidare framgår det av intervju att det saknas utpekade resurser i form av handläggare för att jobba systematiskt med riskhantering och riskanalys. Material i form av rutiner

och mallar för riskanalys finns att tillgå. Riskanalys utifrån NIS-direktivet[1] har skett inom socialförvaltningen och VA-verksamheten. Motsvarande analyser har dock inte skett inom övriga verksamheter.

Granskningen visar att rutiner för incidentrapportering har upprättats. Däremot framgår det av intervju att bristen på resurser påverkar hur implementering av dessa rutiner sker. Härutöver även hur verksamheterna efterlever dessa rutiner och riktlinjer.

Vår granskning visar vidare att det saknas en uppföljning över hur upprättade dokument, i form av policys, riktlinjer och rutiner, efterlevs. Av intervju med informationssäkerhets-samordnare framgår att det inte finns något systematiskt arbete att följa upp och säkerställa att policys, rutiner och riktlinjer efterlevs.

Utrustning som ska kopplas upp mot kommunens nät beskriver IT-enheten sig ha god kontroll över vid våra intervjuer. För att en enhet ska kunna kopplas upp mot nätet krävs godkännande från IT-enheten. Av intervjuer med företrädare för IT-enheten framgår att IT-enheten äger kommunens IT-utrustning och interndebiterar förvaltningarna för den utrustning som förvaltningarna använder. På så sätt har IT-enheten möjlighet att utöva kontroll över vilken utrustning som finns inom kommunen. Undantaget i dagsläget är mobil utrustning, exempelvis telefoner, där IT-enheten i dagsläget inte har programvaror för att hantera denna utrustning.

När det gäller system och program inom kommunens IT-system skall dessa enligt rutin installeras via IT-enheten. Möjlighet finns dock för enskilda inom kommunen att installera system och program på egen hand utan IT-enhetens vetskap. Vår granskning visar att ingen inventering inom kommunens samlade IT-system sker för att se vilka program som finns installerade inom kommunens IT-system. Därav saknas även en lägesbild över det samlade tillståndet gällande system och program inom Bodens kommun IT-system.

**Skydda**, *vilket innebär värdering av organisationens förmåga till behörighetskontroller, utbildning av personal, skyddsmekanismer som brandväggar med mera.*

Kommunstyrelsens arbetsutskott har under 2019 erhållit redovisning av IT-enhetens åtgärder för att förbättra skyddet av kommunens IT-infrastruktur. Som framgår i tidigare avsnitt i denna rapport baseras redovisningen dock inte på något politiskt beslut gällande åtgärder inom området. Av intervju med företrädare för IT-avdelningen har ett förbättringsarbete pågått sedan revisionens granskning 2018.

Av intervjuer med företrädare för IT-enheten framgår att behörigheter och åtkomst styrs via personalsystemet, vilket innebär att närmaste chef ska säkerställa och godkänna att underställd har tillräcklig åtkomst till information. Vid ändrad eller avslutad anställning sker ändring i personalsystemet och därmed också i behörigheterna. Förfarandet finns beskrivet i dokumentet *Anvisning för åtkomst och behörighet.*

Av intervju med kommunens informationssäkerhetssamordnare framgår att kommunens arbete med behörighetstilldelning och behörighetskontroll är ett utvecklingsområde. Det saknas bl.a. en gemensam syn på vilka behörigheter vissa användarroller ska ha. Det

[1] Reglerar krav på samhällsviktiga funktioners rapportering av informationssäkerhetsincidenter.

finns heller ingen standard i kommunen för hur identitets- och behörighetshantering ska ske. Däremot finns regler för lösenordsstandard inom kommunen. Dessa regler framgår av dokumentet *Informationssäkerhet - Regler för användare (2019-10-31).* Anvisningen beskriver även hur lösenord ska hanteras.

Granskning visar att de styrande dokumenten även reglerar att användare som är anställda eller jobbar på uppdrag av Bodens kommun är skyldiga att följa regler för informationssäkerhet. Detta kan exempelvis innebära att aldrig lämna ut inloggningsuppgifter till annan person, att anmäla förlust av IT-utrustning omgående eller att inte ansluta icke-godkänd IT-utrustning eller system till kommunens nätverk.

I syfte att hantera information på ett säkert och korrekt sätt behöver informationsägare göra en konsekvensbedömning av den information som verksamheten hanterar. Detta kallas för informationssäkerhetsklassning. I dokumentet *Informationssäkerhet - Regler för användare* finns en beskrivning av kommunens modell för klassning av information. Det finns vidare beskrivet regler för hur olika typer av information ska skyddas/hanteras samt hur skyddsnivå ska bestämmas.

Av intervju med säkerhetssamordnare framgår att klassning av information inte sker inom verksamheterna på ett systematiskt sätt. Detta uppges beror till stora delar på att det saknas resurser inom förvaltningarna för att driva detta arbete. En förutsättning för IT-enheten att kunna skydda information är att verksamheterna har klassat och värderat den information som finns lagrad. Enligt företrädare för IT-enheten har klassning av information inte skett i tillräcklig omfattning för att IT-enheten ska kunna ha en fullgod bild och kunna skapa ett tillräcklig omfattande skydd.

[redacted]

***Upptäcka**, handlar om att bedöma organisationens förmåga att upptäcka eventuella avvikelser från normalbilden, övervakningsprocesser, logghantering med mera.*

Som nämnts i tidigare avsnitt har IT-enheten till politisk nivå rapporterat vidtagna åtgärder för att öka förmågan att upptäcka intrång, utförda externt såväl som internt. Det har dock identifierats att det finns behov att införa system för att upptäcka och reagera på attacker mot kommunens IT.  Av intervju framgår att kravställning (inför upphandling) för ett sådant system har påbörjats.

Bodens kommun har en extern leverantör som sköter driften av kommunens IT. Av intervju med IT-enheten framgår att det är leverantören som i första hand kommer att upptäcka om något sker. Vid en händelse upprättas en incidentrapport tillsammans med kommunens leverantör där det bl.a. framgår möjliga åtgärder för att förhindra en eskalering av incidenten.

[redacted]

[redacted]

***Agera/Avbryta**, omfattar organisationen förmåga till incidenthantering, avhjälpande åtgärder samt utveckling av organisationens förmågor genom lärdomar av organisationens agerande vid en incident.*

På verksamhetsnivå har en rutin för incidenthantering upprättats, *Rutin för eskalering av incidenter i IT-miljön (upprättad 2020-02-26).* Syftet med rutinen är att beskriva hur informationssäkerhetsincidenter i IT-miljön ska hanteras och samordnas i kommunen. Av rutinen framgår även målsättningen "att säkerställa ett konsekvent och verkningsfullt tillvägagångssätt för hantering av eskalerade incidenter inklusive incidenter som behöver samordning". Vi kan konstatera att rutinen reglerar målgrupp, ansvariga för dokumentet, definitioner av informationssäkerhetsincidenter, rollbeskrivningar samt processen för att hantera en incident. Rutinen innehåller även en beskrivning av hur eskalering av IT-incidenter ska hanteras.

Av intervju med informationssäkerhetssamordnare framgår att rutinen upprättades som ett led i att en incident inträffade inom kommunen vilken påvisade att tydliga rutiner för hantering av incidenter saknades. Rutinen har ännu inte testats och utvärderats.

En viktig del i att upprätthålla en god IT- och informationssäkerhet är att utvärdera incidenter och identifiera vad som kan förbättras. Enligt informationssäkerhets-samordnaren har detta skett i samband med att kommunen drabbades av en incident varpå en åtgärdsplan har upprättats. Det framgår dock av rutin för incidenthantering att en rapport ska upprättas när en incident har lösts där bl.a. genomförda åtgärder, framgångsfaktorer och framtida åtgärder ska framgå.

Av intervjuer och dokumentstudier framgår att när en incident eller avvikelse har inträffat meddelar leverantören IT-enheten att detta har upptäckts. Utifrån dokumenterad rutin vidtas åtgärder. Dessa åtgärder baseras bl.a. på den information som finns avseende vilka system som har klassificerats. Exempelvis vid ett större avbrott i kommunens IT finns rutiner för vilka system som ska prioriteras vid en uppstart.

Utifrån våra intervjuer framgår att såväl personella resurser samt kompetens inom området är utvecklingsområden avseende området systemförvaltning. Vissa systemförvaltare har andra uppgifter och när IT-enheten behöver genomföra en åtgärd med stöd av dessa systemförvaltare kan problem uppstå. Ett exempel på en situation där IT-enheten behöver stöd och hjälp från systemförvaltarna är vid en återläsning av back-up där IT-enheten inte själva kan avgöra om all information har lästs tillbaka i sin helhet.

***Återhämta**, kartlägger organisationens förmåga att så snart som möjligt efter en incident återgå till normaldrift samt förmågan till att göra analyser av det inträffade och förbättra/förändra rutiner.*

Inom IT-enheten och hos kommunens leverantör av IT drift finns rutiner och anvisningar gällande hur teknisk återställning av organisationen system ska ske vid, samt efter, en

incident. Vår granskning visar att det finns viss förmåga att göra analyser inom IT-enheten utifrån genomförda åtgärder och ageranden.

I kommunens strategi för trygghet och säkerhet framgår att vid kriser ska kommunens organisation, så långt det är möjligt, vara densamma som i ett normalläge. Vår granskning har inte kunnat styrka att det finns dokumenterat hur återgång till normalt läge ska ske efter att en incident har eskalerats. Det vill säga, vi har inte kunnat styrka någon åtgärdsplan med analys över vilka system som är prioriterade att återta i drift efter att en incident är avhjälpt samt systemet återställt. Strategin innehåller inte heller någon instruktion eller krav på att verksamheterna ska analysera hur incidenten har hanterats och vilka åtgärder som är nödvändiga att vidta.

I rutin för eskalering av incidenter i IT-miljön finns beskrivet hur en upptäckt incident ska hanteras efter att den avhjälpts samt återgång till normalt läge skett. Det framgår bland annat av rutinen att incidentrapport ska upprättas där beskrivning av incident, vidtagna åtgärder, framgångsfaktorer och framtida åtgärder ska framgå. Av intervju med informationssäkerhetssamordnare framgår att det är svårt att säga om rutinen efterlevs då det inte har inträffat någon incident som medfört att rutinen tillämpats. Av intervju framgår även att det finns brister i kommunikationen mellan samordnaren och verksamheterna, exempelvis okunskap i vad som ska rapporteras, vilket kan innebära att incidenter kan ha inträffat utan samordnarens vetskap.

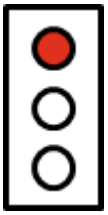
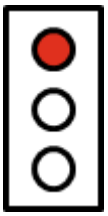
*Bedömning*

Vår bedömning är att kommunstyrelsen delvis bedriver ett ändamålsenligt arbete avseende hot mot kommunens IT-/informationssäkerhet. Bedömningen baseras på att vissa åtgärder återstår att vidta utifrån 2018 års granskning. Vidare framgår att verksamheternas arbete med att identifiera hot är ett utvecklingsområde då detta inte bedrivs i enlighet med den styrning som finns inom granskat område. Klassificering av system och information sker inte på ett systematiskt sätt vilket medför att ett heltäckande underlag för att vidta nödvändiga åtgärder och därmed skapa ett adekvat skydd saknas.

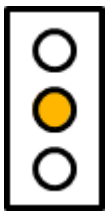
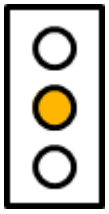
Vår bedömning är att den interna kontrollen delvis är tillräcklig i sammanhanget. Bedömningen baseras på att kommunstyrelsen har upprättat styrning över kommunens arbete med Informationssäkerhet och IT-säkerhet. Vår granskning kan däremot inte verifiera att kommunstyrelsen har säkerställt att organisationen för att driva arbetet med informationssäkerhet och IT-säkerhet är tillräcklig. Vår granskning ser även brister i uppföljningen av hur kommunens verksamheter bedriver informationssäkerhetsarbetet så att rimlig säkerhetsnivå uppnås.

# Avslutning

**Område: Uppföljning av 2018 års granskning**

| Revisionsfråga | Kommentar | |
|---|---|---|
| Vilka åtgärder har, utifrån styrelsens behandling av revisionens tidigare granskning, beslutats om och vidtagits? | Vår granskning visar att kommunstyrelsen **ej** beslutat om eller vidtagit några åtgärder utifrån dennes behandling av revisionens tidigare granskning. |  |
| I vilken utsträckning har beslutade åtgärder återrapporteras till kommunstyrelsen? | Då kommunstyrelsen ej fattat några beslut utifrån revisionens rapport kan vår granskning ej heller styrka att någon återrapportering skett till kommunstyrelsen utifrån några sådana beslut inom området.<br><br>Kommunstyrelsen har dock erhållit viss information relaterat till IT-säkerhetsområdet vid sitt sammanträde 2020-06-08 § 111. |  |
| Finns kvarstående åtgärdsbehov och i så fall vilka? | Vår bedömning är att det finns kvarstående identifierade åtgärdsbehov inom IT-säkerhetsområdet, vilka även informerats till kommunstyrelsen.<br><br>Kommunstyrelsen har dock ej beslutat om åtgärder inom området med anledning av den information som styrelsen erhöll på sitt sammanträde 2020-06-08 §111. |  |

## Område: Informationssäkerhet

| Revisionsfråga | Kommentar | |
|---|---|---|
| Bedriver kommunstyrelsen ett ändamålsenligt arbete med att identifiera, prioritera och hantera hot mot kommunens IT/IS-säkerhet? | **Delvis**<br>Bedömningen baseras på att åtgärder återstår att vidta utifrån 2018 års granskning samt att verksamheten inte bedrivs i enlighet med den styrning som finns inom granskat område. Klassificering av system och information sker inte på ett systematiskt sätt vilket medför att ett heltäckande underlag för att vidta nödvändiga åtgärder och därmed skapa ett adekvat skydd saknas. |  |
| Är den interna kontrollen i sammanhanget avseende IT/IS-säkerhet tillräcklig? | **Delvis**<br>Bedömningen baseras på att kommunstyrelsen har upprättat styrning över kommunens arbete med Informationssäkerhet och IT-säkerhet, samtidigt som vi inte kan verifiera att kommunstyrelsen har säkerställt att organisationen för att driva arbetet med informationssäkerhet och IT-säkerhet är tillräcklig. Vår granskning ser även brister i uppföljningen av informations-säkerhetsarbetet så att rimlig säkerhetsnivå uppnås. |  |

Efter genomförd granskning görs en sammantagen revisionell bedömning utifrån granskningens två områden enligt följande:

- Kommunstyrelsen har inte vidtagit ändamålsenliga åtgärder baserat på revisionens tidigare granskning och rekommendationer inom området. Den interna kontrollen bedöms i sammanhanget som delvis tillräcklig.
- Kommunstyrelsen delvis bedriver ett ändamålsenligt arbete med informationssäkerhet. Den interna kontrollen avseende arbetet med informationssäkerhet bedöms som delvis tillräcklig.

För att utveckla granskningsområdena bör följande rekommendationer prioriteras:

- Kommunstyrelsen säkerställer att identifierade brister åtgärdas. Vidare att kommunstyrelsen tillser att uppföljning, utvärdering/analys och rapportering genomförs till styrelsen i syfte att upprätthålla en tillräcklig intern kontroll inom IT-säkerhetsområdet.
- Kommunstyrelsen tillser att arbetet med informationssäkerhet bedrivs i enlighet med den styrning som finns inom området.
- Kommunstyrelsen tillser att uppföljningen av informationssäkerhetsarbetet bedrivs så att rimlig säkerhetsnivå uppnås.

September 2020

*Hans Forsström*
*Certifierad kommunal revisor*
*Uppdragsledare*

*Erik Jansen*
*Projektledare*