

Uppföljande granskning

Botkyrka kommun

April 2023

Jörn Wahlroth

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Botkyrka kommun genomfört en uppföljande granskning av under år 2020 genomförda granskningar; Granskning av tillsynsverksamheten (miljö- och hälsoskyddsnämnden), Granskning av fastighetsunderhåll (teknik- och fastighetsnämnden) och Granskning av intrångsskydd och IT-säkerhet (vård- och omsorgsnämnden, socialnämnden, samt utbildningsnämnden).

Uppföljningen har syftat till att följa upp tidigare granskningar med avseende på nedanstående revisionsfrågorna:

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

Vår samlade revisionella bedömning är att miljö- och hälsoskyddsnämnden, teknik- och fastighetsnämnden, vård- och omsorgsnämnden, socialnämnden, samt utbildningsnämnden delvis vidtagit tillräckliga åtgärder utifrån revisionsrapporternas rekommendationer. De allra flesta rekommendationerna är bedömda som pågående.

Vi vill från den uppföljande granskningen särskilt lyfta fram vikten av att teknik- och fastighetsnämnden tillser att ett ändamålsenligt fastighetssystem kommer på plats. Detta utgör en viktig grund för ett adekvat arbete med fastighetsunderhåll, samt att fullt ut kunna realisera rekommendationerna i övrigt. Vi gör bedömningen att det finns behov av att träffa teknik- och fastighetsnämnden under år 2023 för att stämma av hur arbetet fortskrider med att realisera rekommendationerna.

Vidare vill vi från granskningen av intrångsskydd och IT-säkerhet särskilt lyfta fram rekommendationen om att utbilda systemförvaltarna och att upprätta guide för att ställa krav mot leverantören avseende kontroll att avtalade rutiner uppfylls som exempelvis backup, restore, spårbarhet och intrångstest. För denna rekommendation hänvisas av förvaltningarna till behov av ett centralt stöd och vi gör bedömningen att det finns behov av att träffa kommunens centrala IT-funktion för att följa upp hur arbetet på central nivå sker med denna fråga, samt i övrigt hur funktionen arbetar med att ge stöd inom området intrångsskydd och IT-säkerhet till kommunens förvaltningar.

Innehållsförteckning

Innehållsförteckning

Sammanfattning	1
Inledning	3
Bakgrund.....	3
Syfte och revisionsfrågor.....	3
Revisionskriterier.....	3
Avgränsning	3
Metod.....	3
Granskningsresultat	5
Granskning av tillsynsverksamheten	5
Iakttagelser	5
Bedömning.....	7
Granskning av underhåll avseende fastigheter och anläggningar.....	7
Iakttagelser	7
Bedömning.....	11
Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - <i>Vård- och omsorgsnämnden</i>	11
Iakttagelser	11
Bedömning.....	14
Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - <i>Socialnämnden</i>	14
Iakttagelser	14
Bedömning.....	18
Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - <i>Utbildningsnämnden</i>	18
Iakttagelser	18
Bedömning.....	22
Samlad bedömning	22

Inledning

Bakgrund

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

Syfte och revisionsfrågor

Uppföljningen syftar till att följa upp tidigare granskningar med avseende på nedanstående revisionsfrågor:

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

Följande granskningar har valts ut för att följas upp under 2022 inom ramen för denna granskning:

- Granskning av tillsynsverksamheten (2020)
- Granskning av fastighetsunderhåll (2020)
- Granskning av intrångsskydd och IT-säkerhet (2020)

Revisionskriterier

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

Kontrollmål och revisionskriterier är utarbetade för de ursprungliga granskningarna som är föremål för uppföljning.

Avgränsning

Avgränsning görs till tidigare genomförda granskningar enligt ovanstående.

Metod

För respektive revisionsgranskning har revisorernas skrivelse, granskat organs yttrande över rapporten och sammanträdesprotokoll från när rapporten behandlades inhämtats. Vidare har inhämtats skriftliga beskrivningar från berörda förvaltningar gällande vilka förändringar som genomförts sedan respektive granskning genomfördes. De skriftliga underlagen från förvaltningarna har kompletterats med samtal/intervjuer.

Resultatet av uppföljningen av respektive granskning redovisas med status enligt följande:

- Rött = Rekommendationen har inte åtgärdats sedan tidigare granskning, vilket medför att relaterad risk och rekommendation kvarstår.

- Gult = Aktiviteter och åtgärder finns planerade eller är under genomförande, dock kvarstår risken då åtgärderna ännu inte är på plats.
- Grönt = Åtgärder och aktiviteter för att begränsa risken har implementerats och underlag har granskats, vilket säkerställer operativ effektivitet i kontrollen.

Granskningsresultat

Granskning av tillsynsverksamheten

lakttagelser

Sammanfattande bedömning vid 2020 års granskning

Utifrån genomförd granskning är vår revisionella bedömning att miljö- och hälsoskyddsnämnden inte helt bedriver tillsynsverksamheten på ett ändamålsenligt och effektivt sätt.

Av revisorernas missiv framgår att rapporten översändes till miljö- och hälsoskyddsnämnden för besvarande. Vi kan inte se att något svar på rapporten har behandlats av nämnden.

Uppföljande granskning

Rekommendation och nämndens svar	Status vid uppföljning
<i>Rekommendation till nämnden:</i> - att nämnden säkerställer att basbehovet av tillsyn framgår tydligt av tillsynsplanerna alternativt verksamhetsplanen. Basbehovet är summan av styrd tillsyn och händelsestyrd tillsyn, som nämnden alltid måste ha resurser för att kunna utföra. Detta behov flyttas över direkt från behovsutredningen till tillsynsplanen. <i>Nämndens svar:</i> Det saknas svar från nämnden.	<i>Vad har åtgärdats?</i> Nuvarande behovsutredning har tagits fram för perioden 2021-2023. Av behovsutredningen framgår nämndens behov av styrd tillsyn, behovsprioriterad tillsyn, händelsestyrd tillsyn och skattefinansierad tillsyn för perioden, jämte förvaltningens tillgängliga resurser. Verksamhets- och tillsynsplanen upprättas utifrån behovsutredningen. <i>Vad kvarstår att åtgärda?</i> I behovsutredningen har tydliggjorts tillgängliga resurser. Förvaltningen menar att detta utgör en tillräcklig koppling mellan behovsutredningen och tillsynsplanerna. Vi anser dock att det utifrån rekommendationen finns utrymme för att tydliggöra kopplingen mellan behovsutredningen och hur tillsynsplanen möter behoven. 

<i>Rekommendation till nämnden:</i> - att nämnden säkerställer att tillsynsplanerna omfattar samma tidsperiod som behovsutredningen, det vill säga tre år, men är detaljerad och specificerad för ett år i taget. All planerad återkommande tillsyn som nämnden bestämde i behovsutredningen ska synas i tillsynsplanen. <i>Nämndens svar:</i> Det saknas svar från nämnden.	<i>Vad har åtgärdats?</i> Nämndens verksamhets- och tillsynsplan gäller för ett år i taget och det finns koppling till nu gällande behovsutredning. Behovsutredningen grundar sig i resursbehovet utifrån kommande tre års tillsyn. Någon treårig tillsynsplan utifrån behovsutredningen har ej tagit fram. Förvaltningen delar inte uppfattningen om behov av en treårig tillsynsplan. I behovsutredningen har en bedömning gjorts av tillgängliga resurser över treårsperioden i förhållande till det behov av tillsyn som lyfts fram. <i>Vad kvarstår att åtgärda?</i> Någon treårig tillsynsplan tillämpas ej. Förvaltningen delar inte uppfattningen avseende behovet att ta fram en sådan. I behovsutredningen har dock tillgängliga resurser lyfts fram gentemot vart och ett av åren. 
<i>Rekommendation till nämnden:</i> - att nämnden beslutar om verksamhetsplanen, eftersom det är nämnden som ska avsätta resurser för den tillsyn som ska ske. <i>Nämndens svar:</i> Det saknas svar från nämnden.	<i>Vad har åtgärdats?</i> Nämnden beslutar årligen om verksamhets- och tillsynsplan och tar även beslut om en omprioritering behöver göras. <i>Vad kvarstår att åtgärda?</i> Bedömningen är att inget kvarstår att åtgärda. 
<i>Rekommendation till nämnden:</i> - att nämnden säkerställer att den återrapportering som erhålls inkluderar även resultatet av den oplanerade tillsynen samt verksamhetsplanen.	<i>Vad har åtgärdats?</i> I samband med tertiäl 1, 2 och 3 till nämnden sker uppföljning utifrån verksamhets- och tillsynsplan med genomförd tillsyn.

<i>Nämndens svar:</i> Det saknas svar från nämnden.	<i>Vad kvarstår att åtgärda?</i> Bedömningen är att inget kvarstår att åtgärda. 
<i>Rekommendation till nämnden:</i> - att nämnden säkerställer att den erhåller återrapportering gällande överklagade ärenden samt utfall i nästa instans. Detta i syfte att kunna arbeta riktat för att säkerställa rättssäkerhet i myndighetsutövningen. <i>Nämndens svar:</i> Det saknas svar från nämnden.	<i>Vad har åtgärdats?</i> Samtliga överinstansers avgöranden delges nämnden vid varje sammanträde. Separat redovisning görs av överinstansernas ärenden som är principiella och de som nämnden är intresserad av att få redovisade. <i>Vad kvarstår att åtgärda?</i> Bedömningen är att inget kvarstår att åtgärda. 

Bedömning

Vår bedömning är att revisionsrapportens rekommendationer delvis är hanterade. Nämnden fattar årligen beslut om verksamhets- och tillsynsplan. Återkopplingen till nämnden avseende genomförd tillsyn och överinstanser avgöranden har stärkts. Rekommendationen att transparensen kan förbättras mellan resursplanen och verksamhets- och tillsynsplan kvarstår.

Utifrån den uppföljande granskningens resultat gör vi bedömningen att det inte finns behov av att träffa ansvarig nämnd/förvaltning.

Granskning av underhåll avseende fastigheter och anläggningar

Iakttagelser

Sammanfattande bedömning vid 2020 års granskning

Efter genomförd granskning är vår bedömning att teknik- och fastighetsnämndens styrning och kontroll avseende underhåll av kommunens fastigheter och anläggningar ej är tillräcklig eller ändamålsenlig ur ekonomisk och verksamhetsmässig synvinkel.

Revisorerna betonade i missivet att de ser allvarligt på de brister som redovisas i rapporten. Utifrån uppsiktsplikten inhämtade revisorerna även svar från kommunstyrelsen. Kommunstyrelsen och nämnden lämnade ett samordnat svar till revisorerna.

Redan föregående år genomfördes en uppföljning av denna granskning. Bedömningen var då att revisionsrapporten delvis hade resulterat i åtgärder, men att det fanns ett fortsatt behov av att åtgärder vidtas gällande strategiska styrdokument och rutiner.

Uppföljande granskning

Rekommendation och nämndens svar	Status vid uppföljning
<i>Rekommendation till nämnden:</i> För att säkerställa tillräcklig styrning och kontroll avseende fastigheter bör styrdokument såsom fastighetsstrategi och underhållsstrategi arbetas fram. <i>KS och nämndens svar:</i> <i>Kommunstyrelsen och teknik- och fastighetsnämnden stödjer denna rekommendation. Teknik- och fastighetsförvaltningen kommer i samband med omorganisation under 2021 se över vilka styrdokument som behöver uppdateras eller tas fram och där är fastighetsstrategi och underhållsstrategi viktiga dokument där arbete kommer påbörjas under 2021. Såväl fastighetsstrategi som underhållsstrategi bör utgå från kommunens framtida lokalbehov, varför de långsiktiga lokalbehovsplanerna från verksamhetsförvaltningarna är väsentliga underlag.</i>	<i>Vad har åtgärdats?</i> En första generell fastighetsstrategi påbörjades i samarbete med kommunledningsförvaltningen och samhällsbyggnadsförvaltningen under år 2021 och lyftes till kommunledningsgruppen. Ett omtag har nyligen skett med vidareutveckling av fastighetsstrategin i samarbete med kommunstyrelseförvaltningen (tidigare KLF) och samhällsbyggnadsförvaltningen. Avseende underhållsstrategi har en översiktlig inventering av byggnadsbeståndets skick skett under 2020-2021. Denna resulterade i omfattande behov av åtgärder, där en stor andel av fastigheterna har byggnadsdelar och installationer som sedan lång tid tillbaka passerat sin tekniska livslängd. <i>Vad kvarstår att åtgärda?</i> Arbetet med fastighetsstrategin pågår och beräknas vara klar under 2023. Det saknas ännu en underhållsstrategi. Denna påverkas av de ekonomiska förutsättningarna kopplat till behovet. 
<i>Rekommendation till nämnden:</i> För att säkerställa korrekt uppföljning och analys av underhållskostnader rekommenderar vi att även	<i>Vad har åtgärdats?</i> Kommunstyrelseförvaltningen har inför 2023 beslutat om en timpenning till grund för bokföring i investerings- och reinvesteringsprojekt. En mall för rapportering har tagits

personalkostnader bokförs på objektsnivå. <i>KS och nämndens svar:</i> <i>En arbetsgrupp med ledning av investeringscontroller på kommunledningsförvaltningen har påbörjat ett arbete med att ta fram rutiner och ett enhetligt arbetssätt för aktivering av egen arbetad tid i kommunens samtliga investeringsprojekt enligt gällande redovisningsregler. I detta arbete kommer även reinvesteringar och övriga investeringsprojekt som avser underhåll att ingå. I och med att omfördelningar kommer att behöva ske mellan investerings- och driftbudget är tidplan för implementering anpassad efter processen för Mål och budget. Arbete kommer att ske under 2021 och i början av 2022 för att presenteras i samband med förutsättningarna till Mål och budget 2023. Teknik- och fastighetsförvaltningen följer framtagandet av dessa rutiner och deltar vid behov för att tillskapa effektiva tidsredovisningsrutiner.</i>	fram och teknik- och fastighetsförvaltningens projektcontroller. <i>Vad kvarstår att åtgärda?</i> Rutinen har ännu ej tillämpats (mars 2023). Tillämpning av rutinen kommer att ske inom kort. 
<i>Rekommendation till nämnden:</i> I samband med den pågående statusbesiktningen av fastigheternas tillstånd och skick är det viktigt att utreda vid vilken tidpunkt åtgärder måste vidtas och därmed få kontroll över vilka kostnader fastighetsorganisationen kommer att få över tid och för att kunna fatta strategiska beslut om fastighetsbeståndet. <i>KS och nämndens svar:</i> <i>I fastighetsbeståndets statusbesiktning som påbörjats i viss utsträckning hos teknik- och fastighetsförvaltningen kommer framtida åtgärdsbehov att bedömas.</i>	<i>Vad har åtgärdats?</i> Det finns en omfattande Excellfil över samtliga fastigheters identifierade och ackumulerade underhållsbehov. Samtliga fastigheter är graderade enligt trafikljusmodell. Röda fastigheter behöver åtgärd inom 1-3 år, gula fastigheter inom 3-5 år, gröna fastigheter inom 5-10 år, alternativt längre. Samtliga fastigheters åtgärdsbehov har kostnadsbedömts utifrån Repab:s nyckeltal för fastighetsunderhåll. <i>Vad kvarstår att åtgärda?</i> Vid föregående års uppföljande granskning angavs att ett nytt fastighetssystem som bland annat stöd för underhållsåtgärder förväntades vara i drift till maj 2022.

<i>Under 2021 kommer ett nytt fastighetssystem att handlas upp och implementeras inför verksamhetsåret 2022, i det systemet ska möjligheter skapas för att kunna planera, följa upp och få bättre kontroll på kommande underhållsåtgärder.</i>	Ett fastighetssystem är ännu inte i drift för detta ändamål, vilket ligger till grund för bedömningen "gult". (Se även under nedanstående). 
<i>Rekommendation till nämnden:</i> Säkerställ att det finns ändamåls- enliga rutiner för hur drift- och underhållsinformation ska dokumenteras och följas upp. <i>KS och nämndens svar:</i> <i>Teknik- och fastighetsförvaltningen kommer i samband med upphandling av nytt fastighetssystem se över rutiner och dokumentation för drift- och under-hållsinformation. Arbetet kommer att påbörjas när det nya fastighetssystemet är implementerat vilket enligt plan sker under senare delen av under 2021.</i>	<i>Vad har åtgärdats?</i> Ett omfattande arbete har genomförts för att identifiera fastigheternas status med dess olika komponenter. All besiktningspliktig utrustning har identifierats och rullande besiktningschema upprättats. Rutiner för arbetet är framtagna och arbetet bedrivs systematiskt. Dock saknas fortfarande ett ändamålsenligt systemstöd i form av fastighetssystem. Information återfinns i Excell-dokument. Upphandlingen och implementering av nytt fastighetssystem har pågått under år 2021 och 2022. Arbetet med systemet avbröts i ett sent skede då leverantören inte kunde uppfylla nödvändiga säkerhetskrav. En ny upphandlingsprocess har nu påbörjats. <i>Vad kvarstår att åtgärda?</i> Det kvarstår att upphandla ett ändamålsenligt systemstöd i form av fastighetssystem. Detta ligger till grund för bedömningen "gult". Ett Excellbaserat underlag är sårbart och ger en sämre intern kontroll. 
<i>Rekommendation till nämnden:</i> Ta fram nyckeltal för styrning och uppföljningen av underhållsarbetet. <i>KS och nämndens svar:</i>	<i>Vad har åtgärdats?</i> En omfattande inventering av fastigheternas ytor har skett. Flertalet, dock ännu inte samtliga, byggnader är nu uppmätta och ytuppgifterna är därefter justerade. Detta

Kommunstyrelsen och teknik- och fastighetsnämnden stödjer denna rekommendation. Även detta kommer teknik- och fastighetsförvaltningen påbörja under 2021 delvis i samband med ny organisation men framförallt efter upphandling och implementering av nytt fastighetssystem som ska möjliggöra en god framtida nyckeltalsuppföljning.	arbete utgör en grund för att kunna arbeta med nyckeltal. Jämförelse med branschnyckeltal och Repab/Momentums rekommendationer för drift och underhåll av fastigheter pågår. <i>Vad kvarstår att åtgärda?</i> Fortsatt inventering sker av kvarvarande fastigheter som återstår att ytinventera. Jämförelse med andra kommuners nyckeltal för internhyror/drift- och underhållskostnader kommer att ske under 2023. 
--	--

Bedömning

Vår bedömning är att revisionsrapportens rekommendationer delvis är hanterade. Arbetet har med inventering av fastighetsbeståndet och dess status har kommit längre än vid föregående uppföljande granskning. Samtidigt är ett systemstöd i form av fastighetssystem nödvändigt för att fullt ut realisera rekommendationerna. Ett arbetssätt med denna typ av data i Excell är sårbart vad avser att kunna dokumentera grunddata och behov av åtgärder, samt att följa upp åtgärder, vilket ger en svagare intern kontroll inom området.

Utifrån den uppföljande granskningens resultat gör vi bedömningen att det finns behov av att träffa ansvarig nämnd under år 2023 för att stämma av hur arbetet fortskrider med att realisera rekommendationerna.

Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - Vård- och omsorgsnämnden

Iakttagelser

Sammanfattande bedömning vid 2020 års granskning

Granskningen avsåg att bedöma om vård- och omsorgsnämnden, socialnämnden och utbildningsnämnden säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst för tre utvalda IT-system; Socialnämndens system Procapita, Utbildningsnämndens system Vklass och Vård- och omsorgsnämndens system Phoniro Care.

Efter genomförd granskning var bedömningen att det ej var säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risken för obehörig åtkomst.

I rapport och missiv riktades samtliga rekommendationer till tre nämnder med begäran om svar från respektive nämnd.

Uppföljande granskning

Rekommendation och nämndens svar	Status vid uppföljning
<i>Rekommendation till nämnden:</i> -att kommunens nämnder upprättar ett styrdokument för hur dokument löpande ska revideras och versionshanteras. Det rekommenderas även att de nämnder som saknar styrdokument för informationshantering, upprättar dessa för befintliga system. <i>Nämndens svar:</i> <i>Revisionen visar att detta inte uppfylls gällande Phoniro Care. Förvaltningen har påbörjat arbetet med att se över den styrdokumentation som finns om Phoniro Care och för att säkerställa att dokumentationen gällande rutiner och processer är uppdaterade och löpande revideras kommer ett kontrollmoment läggas till i internkontrollplanen.</i>	<i>Vad har åtgärdats?</i> Det uppges att till följd av pandemin har inte arbetet med att ta fram en informationshanteringsplan kunnat prioriteras fullt ut. Det har dock tagits fram en skriftlig rutin för Phoniro Care som är under implementering. Av rutinen framgår processen kring ansvar, behörighet och utbildning. Rutinen ska följas upp regelbundet och uppdateras vid förändring. <i>Vad kvarstår att åtgärda?</i> Det saknas ännu ett styrdokument för informationshantering, samt för hur dokument fortlöpande ska revideras och versionshanteras. Framtagen rutin för hantering av systemet kommer att implementeras i berörda verksamheter under våren 2023. Av svaret framgick att rutiner och processer inom området skulle omfattas av nämndens internkontrollplan. Så har inte varit fallet. 
<i>Rekommendation till nämnden:</i> - att man säkerställer att kommunens varje användare har genomgått utbildning i systemet och det görs löpande åtminstone 1 gång om året.	<i>Vad har åtgärdats?</i> För att säkerställa att alla berörda användare har kunskap i systemet framgår i framtagna rutin att närmaste chef ansvarar för att följa upp att medarbetare använder systemet på

Nämndens svar: Revisionen visade att detta var delvis uppfyllt för Phoniro Care men att det inte finns rutiner för uppföljning. Användare får inte behörighet till systemet utan genomgången utbildning. Förvaltningen har påbörjat arbetet med att fram rutiner för uppföljning.	ett korrekt sätt. I och med att medarbetare inte får tillgång till systemet utan genomgången utbildning bedöms inget behov av årlig utbildning om inget annat framgår vid chefens uppföljning. I dessa fall erbjuds utbildning på nytt enligt rutinen. Vad kvarstår att åtgärda? Bedömningen är att inget kvarstår att åtgärda. 
Rekommendation till nämnden: - att Botkyrka utbildar systemförvaltarna och upprättar en guide för hur de rutinmässigt kan ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som t.ex. backup, restore, spårbarhet och intrångstester. Nämndens svar: Revisionen visar att det finns bra rutiner hos leverantören men det finns en kompetensbrist på förvaltningen och hos systemförvaltare över vilka krav som behöver ställas mot leverantören. Det pågår ett förändringsarbete inom kommunen för att övergå till leverantörsstyrning som innebär att IT-enheten, där den tekniska kompetensen finns, får ansvar i att stötta förvaltningarna i att ställa krav på leverantörerna. Rutiner kommer tas fram tillsammans med IT-enheten för att säkerställa att intrång- och säkerhetstester genomförs regelbundet. Implementering av det nya arbetssättet mellan förvaltningarna och IT-enheten kommer ske under hösten 2020.	Vad har åtgärdats? Den återkoppling som förvaltningen fått från central IT-funktion (Digital utveckling) gällande arbetet med leverantörsstyrning är att ett arbete påbörjats med att ta fram en strategi och principer kopplat till styrningsfrågan. Än så länge saknas en samverkansmodell, ramverk och roller, men målet är att ha leverantörsstyrning på plats under 2023 för att kunna hantera frågor kring backup, restore, spårbarhet och intrångstester. Vad kvarstår att åtgärda? Som framgår av ovanstående är åtgärder utifrån rekommendationen för närvarande ett pågående arbete. 

<i>Rekommendation till nämnden:</i> -att förvaltningen dokumenterar beroendet mellan systemet och stödsystemen, för att uppmärksamma eventuella sårbarheter i behörighetshanteringen, så att en säker behörighetskontroll kan säkerställas. <i>Nämndens svar:</i> <i>Revisionen visar att förvaltningen saknar dokumenterade rutiner för behörighetskontroll. Det finns en hel del rutiner på förvaltningen kring behörighetskontroll och det pågår ett arbete med att ta fram en riktlinje för behörigheter som beräknas vara klar 2020-12-01. Förvaltningen kommer även ta fram rutiner för uppföljning av behörighetskontroll.</i>	<i>Vad har åtgärdats?</i> Det uppges att arbetet till följd av pandemin försenats, men en riktlinje för behörighet i system är nu framtagen och kommer under våren förankras inom förvaltningen. Det finns inget beroende mellan Phoniro Care och stödsystem som påverkar behörighetshanteringen. Det finns i praktiken ett arbetssätt för behörighetskontroll. <i>Vad kvarstår att åtgärda?</i> Det kvarstår att implementera framtagen riktlinje och att dokumentera den rutin som tillämpas. Det uppges att detta arbete kommer att slutföras under våren 2023 
---	--

Bedömning

Vår bedömning är att revisionsrapportens rekommendationer delvis är hanterade. För vissa dokument kvarstår att ta fram dessa, medan det för andra dokument kvarstår ett implementeringsarbete. Gällande arbetet med att rutinemässigt kunna ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som exempelvis backup, restore, spårbarhet och intrångstester, hänvisas av förvaltningen till ett kommungemensamt arbete på för kommunen central IT-nivå.

Utifrån den uppföljande granskningens resultat gör vi bedömningen att det inte finns behov av att träffa ansvarig nämnd/förvaltning. Däremot att träffa kommunens centrala IT-funktion för att följa upp hur arbetet på central nivå sker för att säkerställa kontroll och uppföljning av systemleverantörer, samt i övrigt hur funktionen arbetar med att ge stöd inom området intrångsskydd och IT-säkerhet till kommunens förvaltningar.

Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - Socialnämnden

Iakttagelser

Sammanfattande bedömning vid 2020 års granskning

Granskningen avsåg att bedöma om vård- och omsorgsnämnden, socialnämnden och utbildningsnämnden säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risker för obehörig åtkomst för tre utvalda IT-system; Socialnämndens system Procapita, Utbildningsnämndens system Vklass och Vård- och omsorgsnämndens system Phoniro Care.

Efter genomförd granskning var bedömningen att det ej var säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risken för obehörig åtkomst.

I rapport och missiv riktades samtliga rekommendationer till tre nämnder med begäran om svar från respektive nämnd.

Uppföljande granskning

Rekommendation och nämndens svar	Status vid uppföljning
<i>Rekommendation till nämnden:</i> -att kommunens nämnder upprättar ett styrdokument för hur dokument löpande ska revideras och versionshanteras. Det rekommenderas även att de nämnder som saknar styrdokument för informationshantering, upprättar dessa för befintliga system. <i>Nämndens svar:</i> <i>Revisionen visar att detta är delvis uppfyllt gällande Procapita. Socialförvaltningen har en informationshanteringsplan som beskriver hur information övergripande ska hanteras i alla olika system som finns inom förvaltningen. Det finns också en mängd styrdokument och enhetsanpassade guider som täcker in större delen av hanteringen/handläggningen i Procapita. Det som saknats tidigare är att visa att dokumentation uppdateras kontinuerligt och versionshanteras. Alla ändringar i dokument och riktlinjer har nu börjat versionhanteras för att leva upp till rekommendationen. För att säkerställa att dokumentationen</i>	<i>Vad har åtgärdats?</i> En ny och uppdaterad informationshanteringsplan togs fram augusti 2022. Den är mer tydlig och mer omfattande än tidigare. Alla styrdokument och riktlinjer versionshanteras men det saknas fortfarande ett övergripande styrdokument som beskriver detta. <i>Vad kvarstår att åtgärda?</i> Ett övergripande styrdokument kommer inom kort att tas fram vad avser hur dokument löpande ska revideras och versionshanteras. Av svaret framgick att rutiner och processer inom området skulle omfattas av nämndens internkontrollplan. Så har inte varit fallet. 

<i>gällande rutiner och processer är uppdaterade och löpande revideras enligt god praxis föreslås det läggas som kontrollmoment i internkontrollplanen att se över och uppdatera all dokumentation gällande informationshantering i Procapita.</i>	
<i>Rekommendation till nämnden:</i> - att man säkerställer att kommunens varje användare har genomgått utbildning i systemet och det görs löpande åtminstone 1 gång om året. <i>Nämndens svar:</i> <i>Revisionen visade att detta var delvis uppfyllt för Procapita men att det saknades kontroll över att nya handläggare tagit del av den utbildning och information som finns gällande informationssäkerhet. Åtgärd för detta är redan genomförd i och med det sedan sommaren är etablerad rutin att skicka en digital nanoutbildning till alla nya medarbetare som de måste genomföra innan de får tillgång och kan arbeta i Procapita. Utbildningen tar bland annat upp en del säkerhetsrelaterade element, som regler för inloggning och sekretess. Systemförvaltare kontrollerar sedan tekniskt att medarbetaren har genomgått utbildningen, och hur lång tid det tog, innan behörigheten slås på. Ett samarbete mellan systemförvaltare av Procapita och förvaltningens dataskyddsombud har påbörjats för att med stöd av ett årshjul följa upp att alla användare har tillräcklig information för att på ett säkert sätt arbeta i systemet.</i>	<i>Vad har åtgärdats?</i> Alla nya medarbetare genomgår en obligatorisk digital utbildning som tar upp bland annat informationssäkerhet och regler för sekretess och loggning. Utbildningen är en förutsättning för tillgång till systemet. (Sammanfaller med nämndens tidigare svar om redan genomförd åtgärd). Det finns en plan att ta fram ytterligare en obligatorisk Nanoutbildning riktad till alla medarbetare inom förvaltningen en gång per år. Den ska inte specifikt handla om systemet Procapita utan ta upp generell informations-säkerhet. Planen är att utbildningen ska bli klar till sommaren. <i>Vad kvarstår att åtgärda?</i> Bedömningen är att inget kvarstår att åtgärda. Att utveckla det årshjul som beskrivs i nämndens svar har dock inte realiserats. 
<i>Rekommendation till nämnden:</i> - att Botkyrka utbildar systemförvaltarna och upprättar en guide för hur de rutinmässigt kan ställa krav mot leverantören för att kontrollera att	<i>Vad har åtgärdats?</i> Den nya modellen för leverantörsstyrning som var planerad utgick från ett större stöd från i kommunen centrala IT-enhet. Sedan nämndens svar har inte något ytterligare stöd

avtalade rutiner uppfylls som t.ex. backup, restore, spårbarhet och intrångstester. <i>Nämndens svar:</i> <i>Revisionen visar att det finns bra rutiner hos leverantören Tieto men det finns en kompetensbrist hos förvaltningen/systemförvaltare över vilka krav som behöver ställas mot leverantören. Under våren 2020 beslutade Strategisk grupp organisationsutveckling (SGO) om en ny modell för leverantörsstyrning som utgår ifrån att IT-enheten kommer ta större ansvar i kontakten med leverantörerna och har ansvar för att framöver stödja förvaltningarna i detta arbete. Tidigare låg allt ansvar på de enskilda förvaltningarna som de facto inte besitter den tekniska kompetensen som krävs för att kunna ställa rätta krav på leverantören. Bedömningen är att det förändrade arbetssättet där IT-enheten tar större ansvar kommer leda till en kompetenshöjning hos systemförvaltarna och att adekvata krav kommer ställas på leverantören. Rutiner kommer tas fram tillsammans med IT-enheten för att säkerställa att intrång- och säkerhetstester genomförs regelbundet. Implementering av det nya arbetssättet mellan förvaltningarna och IT-enheten kommer ske under hösten 2020.</i>	förevarit till förvaltningens systemförvaltare från den centrala IT-enheten än vad som tidigare förelåg. Det pågår på den för kommunen centrala nivån ett arbete med hur arbetet med informationsförvaltning ska ske på ett mer strukturerat sätt, samt att samordna detta med frågor kring systemförvaltning samt informationssäkerhet. På den centrala nivån har även i ny organisation arbetats fram med nya roller inom kommunstyrelseförvaltningen, där förvaltningarna framöver ska erhålla stöd, bl a vad avser framöver bättre kunna kontrollera leverantörerna av system. I samband med systemupphandling under år 2022 har dock stöd erhållits i samband med arbetet med KLASSA systemet. <i>Vad kvarstår att åtgärda?</i> Det har kommunicerats att förvaltningarna kommer få ett centralt stöd i frågorna, men inte närmare hur eller när i tiden detta ska ske. Inom förvaltningen kommer tjänsteperson att genomgå särskild utbildning inom området under våren 2023 för att stärka förvaltningens egna kompetens, bl a i relation till systemleverantören. 
<i>Rekommendation till nämnden:</i> PwC rekommenderar att förvaltningen dokumenterar beroendet mellan systemet och stödsystemen, för att uppmärksamma eventuella sårbarheter i behörighetshanteringen,	<i>Vad har åtgärdats?</i> Det uppges att det inte finns något tekniskt beroende mellan stödsystemen och Procapita, utan manuell hantering av användare.

så att en säker behörighetskontroll kan säkerställas. <i>Nämndens svar:</i> Det framgår i revisionen att det finns bra rutiner för att se till att ingen obehörig har tillgång till information i Procapita som den inte har rätt till. Till exempel finns samarbete med Lönekontoret som varje månad skickar listor på de som avslutat sin anställning och dokumentation som visar alla anställdas roller och behörigheter. En planerad åtgärd är att sammanställa de rutiner som finns till ett och samma dokument så att det blir tydligare. Det finns också behov att dokumentera och implementera rutin för hur det går till när en anställd byter enhet, och behöver få ny behörighet, eftersom detta ofta missas att anmälas från närmaste chef till systemförvaltare. Åtgärderna är planerade att vara genomförda till den sista november 2020.	Förändringar har skett sedan granskningen. Det skickas inte längre listor från lönekontoret, utan förvaltningen tar själva månatligen ut dessa. Dessa listor ligger till grund för att i vid förändringar i anställningsförhållande ta bort behörighet. För nya behörigheter finns särskilt framtaget beställningsformulär. Rutiner har tagits fram som huvudsakligen ligger i linje med nämndens svar. <i>Vad kvarstår att åtgärda?</i> Bedömningen är att inget kvarstår att åtgärda. 
--	---

Bedömning

Vår bedömning är att revisionsrapportens rekommendationer delvis är hanterade. Styrande dokument och rutiner är till stora delar på plats. Gällande arbetet med att rutinmässigt kunna ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som exempelvis backup, restore, spårbarhet och intrångstester, hänvisas av förvaltningen till ett kommungemensamt arbete på central IT-nivå.

Utifrån den uppföljande granskningens resultat gör vi bedömningen att det inte finns behov av att träffa ansvarig nämnd/förvaltning. Däremot att träffa kommunens centrala IT-funktion för att följa upp hur arbetet på central nivå sker för att säkerställa kontroll och uppföljning av systemleverantörer, samt i övrigt hur funktionen arbetar med att ge stöd inom området intrångsskydd och IT-säkerhet till kommunens förvaltningar.

Granskning av intrångsskydd och IT-säkerhet i verksamhetssystem - Utbildningsnämnden

Iakttagelser

Sammanfattande bedömning vid 2020 års granskning

Granskningen avsåg att bedöma om vård- och omsorgsnämnden, socialnämnden och utbildningsnämnden säkerställt att informationshanteringen håller en tillräcklig och

tillfredsställande nivå för att reducera risker för obehörig åtkomst för tre utvalda IT-system; Socialnämndens system Procapita, Utbildningsnämndens system Vklass och Vård- och omsorgsnämndens system Phoniro Care.

Efter genomförd granskning var bedömningen att det ej var säkerställt att informationshanteringen håller en tillräcklig och tillfredsställande nivå för att reducera risken för obehörig åtkomst.

I rapport och missiv riktades samtliga rekommendationer till tre nämnder med begäran om svar från respektive nämnd.

Uppföljande granskning

Rekommendation och nämndens svar	Status vid uppföljning
<i>Rekommendation till nämnden:</i> -att kommunens nämnder upprättar ett styrdokument för hur dokument löpande ska revideras och versionshanteras. Det rekommenderas även att de nämnder som saknar styrdokument för informationshantering, upprättar dessa för befintliga system. <i>Nämndens svar:</i> <i>Utbildningsförvaltningen håller på med upprättandet av en ny informationshanteringsplan som beräknas vara färdigställd under hösten 2020.</i> <i>Informationshanteringsplanen omfattar bland annat vem som är ansvarig för olika typer av information samt hur denna ska hanteras. Nu gällande dokumenthanteringsplan är inte fullt uppdaterad och innehåller vissa brister. Utbildningsnämnden gör bedömningen att den nya informationshanteringsplanen som ersätter dokumenthanteringsplanen kommer att motsvara revisorernas rekommendation.</i> <i>Utöver informationshanteringsplanen har utbildningsförvaltningen genomfört en ny klassning av</i>	<i>Vad har åtgärdats?</i> Förvaltningen har tagit fram en informationshanteringsplan. Planen är dock inte antagen i nämnd på grund av att kommunstyrelseförvaltningen inte är klara med de kommungemensamma riktlinjerna. Den preliminära tidplanen är att KSF ska behandla ärendet under våren 2023. När riktlinjerna blir antagna kan informationssäkerhetsplanen antas i utbildningsnämnden. <i>Vad kvarstår att åtgärda?</i> Se ovanstående. 

systemet med hjälp av självskattningsverktyget KLASSA och kommer revidera handlingsplanen utefter den nya bedömningen. Förvaltningen kommer varje år att revidera handlingsplanen för att säkerställa att befintliga system bibehåller den säkerhet som krävs. Handlingsplanen kommer att implementeras fullt ut i det nya upphandlade systemet.	
<i>Rekommendation till nämnden:</i> - att man säkerställer att kommunens varje användare har genomgått utbildning i systemet och det görs löpande åtminstone 1 gång om året. <i>Nämndens svar:</i> Utbildningsförvaltningen anordnar årligen utbildningar för alla anställda som använder Vklass. Utbildningen innehåller för närvarande inte perspektivet informationssäkerhet och upplägget för utbildningen kommer därför att revideras. Från och med nu kommer utbildningen att omfatta informationssäkerhet. Förvaltningen kommer även att ta fram en webbaserad utbildning för befintlig personal i utbildningsförvaltningen. Utbildningen kommer att finnas tillgänglig nästa läsår. På så sätt kan förvaltningen säkerställa att alla som arbetar i Vklass och kommunens övriga system har fått nödvändig utbildning kring IT-säkerhet. Med anledning av att Botkyrka kommuns inloggning används i många system, bland annat Vklass, önskar utbildningsnämnden att informationssäkerhetsutbildningar på sikt anordnas centralt av kommunledningsförvaltningen då konton är kommungemensamt.	<i>Vad har åtgärdats?</i> Utbildningsförvaltningen uppger att kommunens anställda erbjuds utbildning regelbundet en ggr per år, samt skraddarsyr utbildning efter behov och förfrågan. Utbildningen är dock inte obligatorisk. Det som lyfts fram i utbildningen är användarorienterad information och saknar allmän information om informationssäkerhet. Förvaltningen lyfter fram att de anser att ansvaret för informationssäkerhetsperspektivet ligger på KSF eftersom det är ett kommunövergripande behov. <i>Vad kvarstår att åtgärda?</i> Det saknas en utbildning motsvarande den som framgår av rekommendation och nämndens svar. 
<i>Rekommendation till nämnden:</i>	<i>Vad har åtgärdats?</i>

- att Botkyrka utbildar systemförvaltarna och upprättar en guide för hur de rutinmässigt kan ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som t.ex. backup, restore, spårbarhet och intrångstester. <i>Nämndens svar:</i> <i>Utbildningsförvaltningen har regelbundna samverkansmöten med leverantören där informationssäkerhet kommer att vara en stående punkt på dagordningen. Utbildningsförvaltningen har också tagit hjälp av kommunens informationssäkerhetsansvarig för att förbättra rutiner och höja kunskapen om informationssäkerhet inom utbildningsförvaltningen.</i> <i>Kompleta riktlinjer och processer avseende rutiner för till exempel backup, restore, spårbarhet och intrångstester kommer att upprättas för den nya lärplattformen. Detta är en viktig del i kravställningen inför kommande upphandling.</i>	Upphandling har helt nyligen genomförts, där kommunens gemensamma grund för att arbeta med KLASSA har tillämpats. Bedömningen är att det inom förvaltningen saknas krav för att möta rekommendationen vad avser kontroll av leverantör. I detta avseende hänvisas till en för kommunen central samverkan. <i>Vad kvarstår att åtgärda?</i> Ett arbete sker på central nivå för att kunna möta rekommendationen och utgöra ett stöd i hela organisationen. 
<i>Rekommendation till nämnden:</i> PwC rekommenderar att förvaltningen dokumenterar beroendet mellan systemet och stödsystemen, för att uppmärksamma eventuella sårbarheter i behörighetshanteringen, så att en säker behörighetskontroll kan säkerställas. <i>Nämndens svar:</i> <i>Utbildningsförvaltningen har gjort en dokumentation för behörighetshantering i Vklass och det kan konstateras att systemet har vissa brister. Idag finns det endast ett fåtal behörighetsroller vilket ger begränsade möjligheter till behörighetsstyrning. Inför kommande</i>	<i>Vad har åtgärdats?</i> En generell lista över förvaltningens verksamhetssystem och dess olika beroenden har uppförts varav Vklass är en komponent. Målet är att kartlägga flöden av data och synliggöra säkerhetsbrister. Projektet går ut på att kartlägga systemberoenden. För behörigheter finns rutiner som styrs av delegation och system. <i>Vad kvarstår att åtgärda?</i> Se ovanstående.

upphandling är behörighetsstyrningen en viktig del i kravställningen som förvaltningen får ut med hjälp av självskattningsverktyget KLASSA. Nya rutiner och processer kommer att dokumenteras kring behörighetskontroller i det nya systemet.



Bedömning

Vår bedömning är att revisionsrapportens rekommendationer delvis är hanterade. Styrande dokument och rutiner är delvis på plats, men det saknas fortfarande en obligatorisk utbildning i informationssäkerhet för tillgång till systemet. Gällande arbetet med att rutinmässigt kunna ställa krav mot leverantören för att kontrollera att avtalade rutiner uppfylls som exempelvis backup, restore, spårbarhet och intrångstester, hänvisas från förvaltningen till ett kommungemensamt arbete på central IT-nivå.

Utifrån den uppföljande granskningens resultat gör vi bedömningen att det inte finns behov av att träffa ansvarig nämnd/förvaltning. Däremot att träffa kommunens centrala IT-funktion för att följa upp hur arbetet på central nivå sker för att säkerställa kontroll och uppföljning av systemleverantörer, samt i övrigt hur funktionen arbetar med att ge stöd inom området intrångsskydd och IT-säkerhet till kommunens förvaltningar.

Samlad bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Botkyrka kommun genomfört uppföljande granskning på av under år 2020 genomförda granskningar; Granskning av tillsynsverksamheten (miljö- och hälsoskyddsnämnden), Granskning av fastighetsunderhåll (teknik- och fastighetsnämnden) och Granskning av intrångsskydd och IT-säkerhet (vård- och omsorgsnämnden, socialnämnden, samt utbildningsnämnden).

Uppföljningen har syftat till att följa upp tidigare granskningar med avseende på nedanstående revisionsfrågorna:

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

Vår samlade revisionella bedömning är att miljö- och hälsoskyddsnämnden, teknik- och fastighetsnämnden, vård- och omsorgsnämnden, socialnämnden, samt utbildningsnämnden delvis vidtagit tillräckliga åtgärder utifrån revisionsrapporternas rekommendationer. De allra flesta rekommendationerna är bedömda som pågående.

Vi vill från den uppföljande granskningen särskilt lyfta fram vikten av att teknik- och fastighetsnämnden tillser att ett ändamålsenligt fastighetssystem kommer på plats. Detta utgör en viktig grund för ett adekvat arbete med fastighetsunderhåll, samt att fullt ut kunna realisera rekommendationerna i övrigt. Vi gör bedömningen att det finns behov av att träffa teknik- och fastighetsnämnden under år 2023 för att stämma av hur arbetet fortskrider med att realisera rekommendationerna.

Vidare vill vi från granskningen av intrångsskydd och IT-säkerhet särskilt lyfta fram rekommendationen om att utbilda systemförvaltarna och att upprätta guide för att ställa krav mot leverantören avseende kontroll att avtalade rutiner uppfylls som exempelvis backup, restore, spårbarhet och intrångstest. För denna rekommendation hänvisas av förvaltningarna till behov av ett centralt stöd och vi gör bedömningen att det finns behov av att träffa kommunens centrala IT-funktion för att följa upp hur arbetet på central nivå sker med denna fråga, samt i övrigt hur funktionen arbetar med att ge stöd inom området intrångsskydd och IT-säkerhet till kommunens förvaltningar.

2022-04-11

Rebecka Hansson

Jörn Wahlroth

Uppdragsledare

Projektledare

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